IT Security system in Latvia - achievements, statistics and challenges

DSS Conference - 07.11.2013, Riga,

Baiba Kaškina, CERT.LV

Outline

- Legal environment
- CERT.LV overview
- Current situation overview
- CERT.LV awareness rising activities

Legal environment and policies

IT Security Law

- In force since 1 February 2011
- Sets CERT.LV tasks and responsibilities
- Defines responsibilities for:
  - Public sector
  - Internet Service Providers (ISPs)
  - Critical IT infrastructure owners

IT Security Law – Public sector

- In every institution – IT security officer responsible for:
  - IT security document creation
  - IT security audit execution
  - Annual employee education
  - Security incident reporting to CERT.LV
  - Participation in CERT.LV seminars

IT Security Law – ISPs

- All ISPs submit «Action plan for continuous operations»
- Report to CERT.LV on major incidents
- CERT.LV can request
  - IT Security incident information
  - IT Security audits
  - Disconnection of an end user for 24h

IT Security Law – CII

- Critical infrastructure list – state secret
- Report incidents to CERT.LV
- Establish IT Security documentation
- CERT.LV can do black-box penetration testing

National IT security strategy

- Improvement of legal regulations
- Increasing human and material-technical resources for state institutions
- Rising cooperation at a national scale
- Intensifying international cooperation
- Hardening of education, science and social responsibility

CERT.LV overview

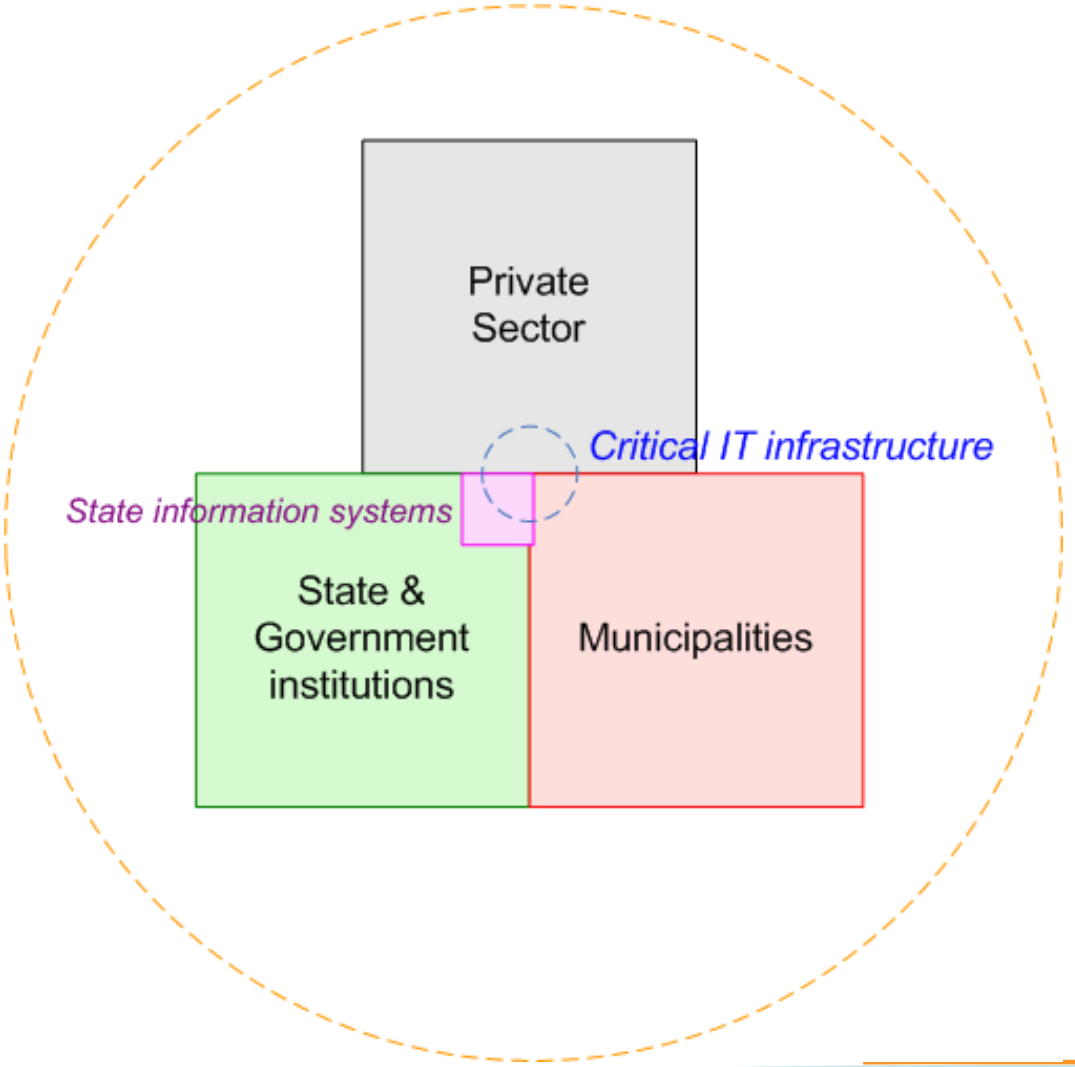
CERT.LV

- Information technology security incident response institution
- Mission: “Fostering IT security in Latvia”
- From 1 January 2013 - CERT.LV supervised by the Ministry of Defence

CERT.LV

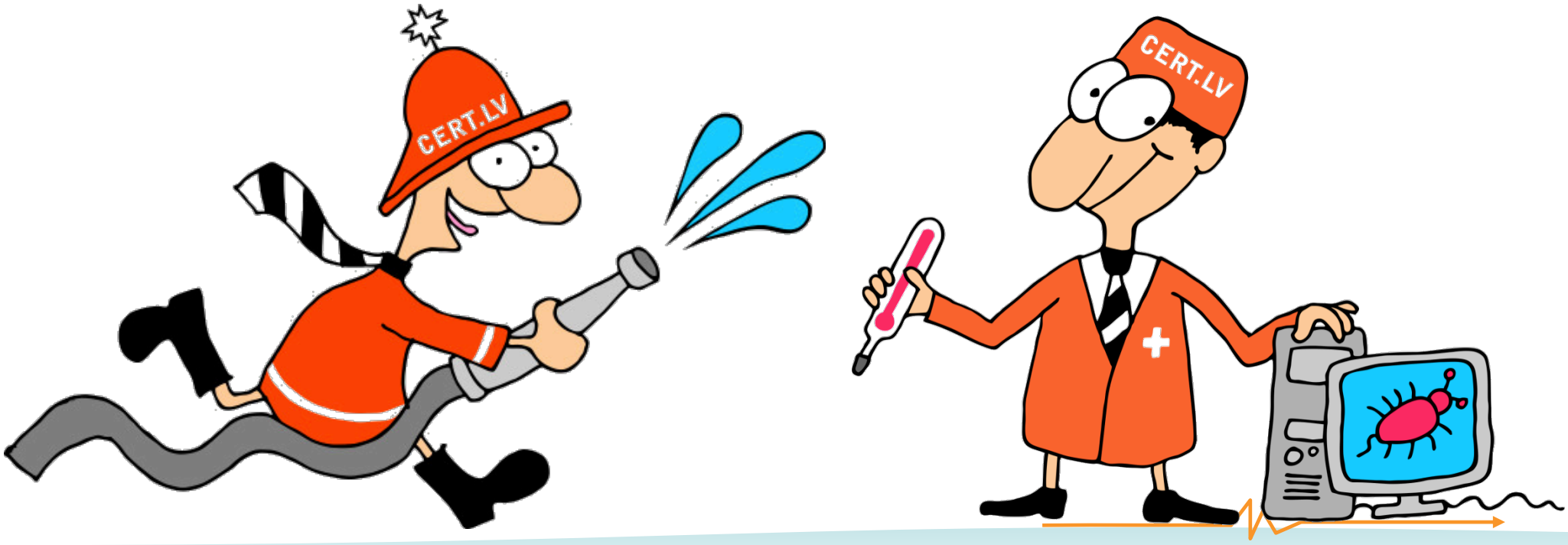
- Used to be CERT.NIC.LV est. 2006
- Operational since 1 February 2011
- Operates on basis of IT Security Law
- State funded
- All services are free of charge
- Tasks delegated to Institute of Mathematics and Computer Science, University of Latvia

CERT.LV constituency



What is CERT.LV?

- “Family doctor” and “fire-fighter” in the virtual environment



CERT.LV main activity areas

- Incident response
- “Security through cooperation”
- Awareness raising

CERT.LV collaboration

- State and municipal institutions
- IT Critical infrastructure
- Private sector
  - ISPs
  - Financial institutions
- National Armed Forces
- International collaboration
  - NATO, EU, ENISA, CCD CoE
  - TF-CSIRT, FIRST

January 2012 – MoU with NATO

CERT.LV participation

- Cyber Defense Exercises:
  - CCD CoE «Locked Shields»
  - NATO «Cyber Coalition»
  - EU «Cyber Europe»

Responsible ISP

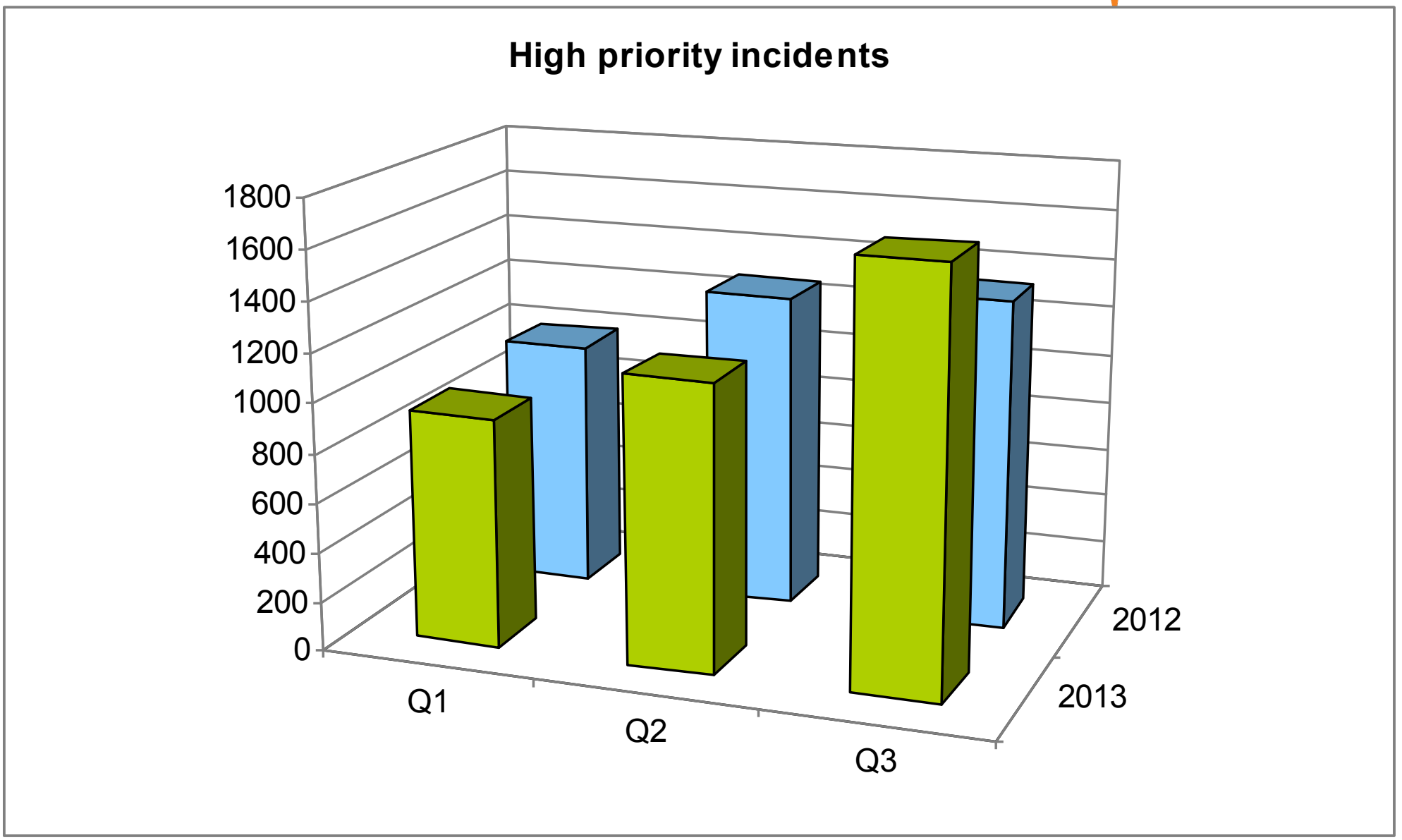
Symbol of quality, received by IPS that:

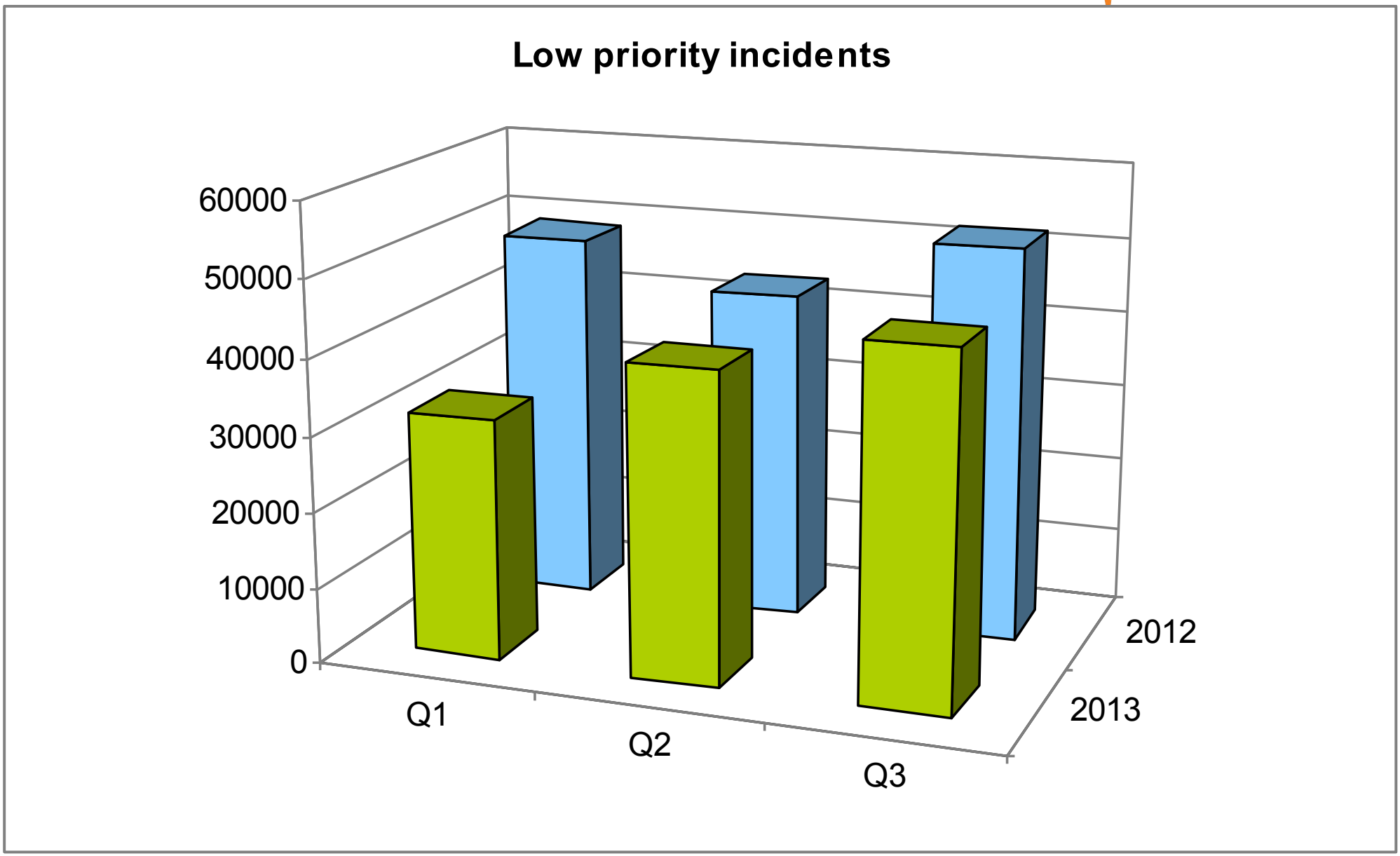
- Cooperates with CERT.LV and provides incident information to end users
- Cooperates with Net-Safe Latvia for illegal material takedown off the Internet
- Provides free Internet content filter setup upon customers request

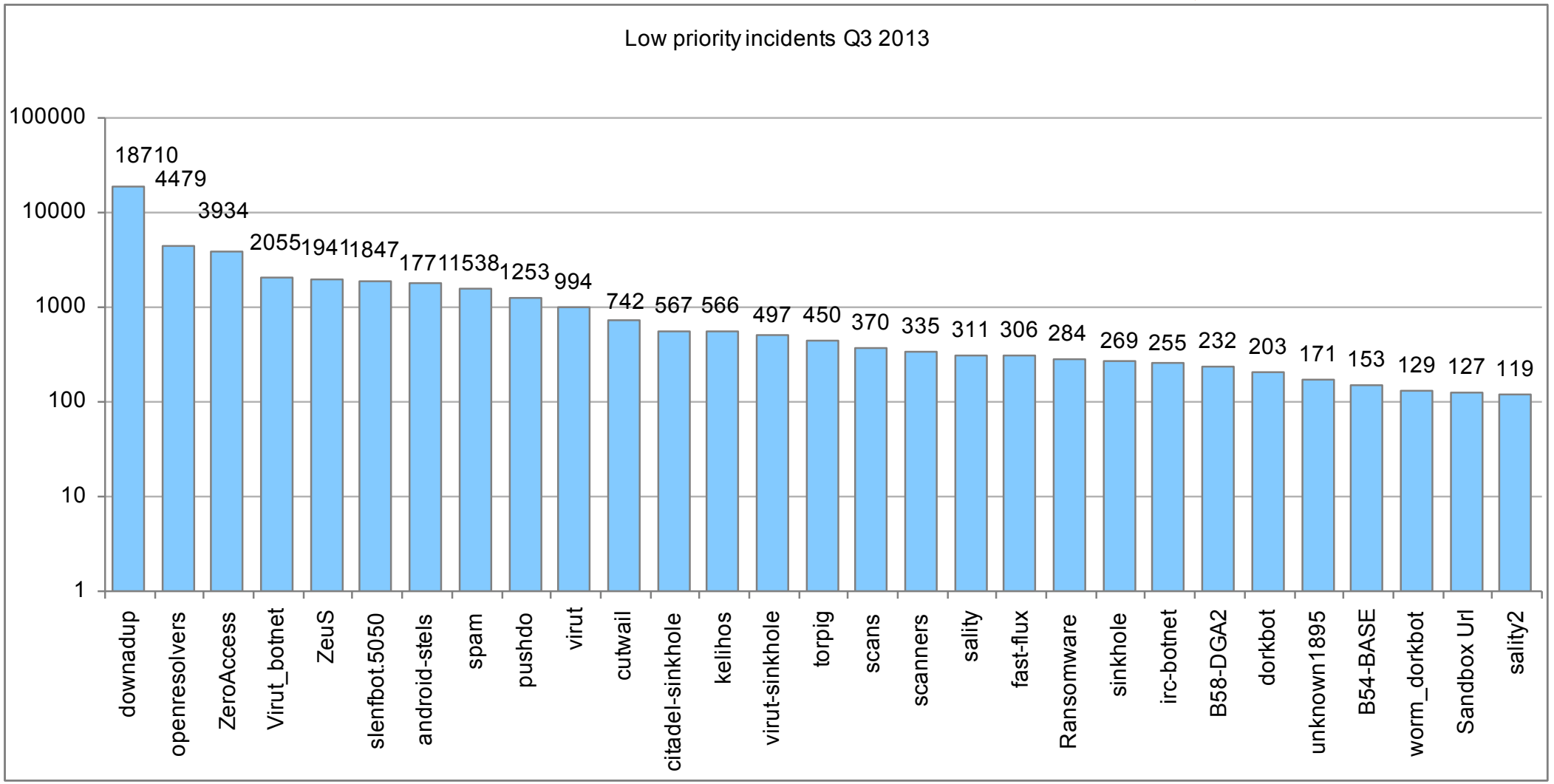
Current situation overview

Current situation

- Large amount of incident reports every day
- High and low priority incidents


High priority incidents
1800
1600
1400
1200
1000
800
600
400
200
0
Q1
Q2
Q3
2012
2013


Low priority incidents
60000
50000
40000
30000
20000
10000
0
Q1
Q2
Q3
2012
2013


Low priority incidents Q3 2013
100000
10000
1000
100
10
1
18710
4479
3934
2055
1941
1847
1771
1538
1253
994
742
567
566
497
450
370
335
311
306
284
269
255
232
203
171
153
129
127
119
downadup
openresolvers
ZeroAccess
Virut_botnet
ZeuS
slenfbot.5050
android-stels
spam
pushdo
virut
cutwail
citadel-sinkhole
kelihos
virut-sinkhole
torpig
scans
scanners
sality
fast-flux
Ransomware
sinkhole
irc-botnet
B58-DGA2
dorkbot
unknown1895
B54-BASE
worm_dorkbot
Sandbox Url
sality2

Current trends

- Botnet numbers are still very large
- Infections via browsers (Drive-by Exploits) – the most common vector
- Server hacking, phishing, DoS
- Malware distribution
- Attacks in socially sensitive moments

Atlikušais laiks: 47:57:29

paysafecard

IP: [redacted]

Valsts: **LV Latvia**
Rajons: **Riga**
Pilsēta: **Riga**
ISP: [redacted]
OperētājSistēma: **Windows 7 (64-bit)**
Lietotāja Vārds: [redacted]

UZMANĪBU! Jūsu dators ir bloķēts zemāk norādīto drošības apsvērumu dēļ.

Jūs esat apsūdzēts par aizliegtu pornogrāfisku datu (bērnu pornogrāfija/zoofilija/izvarošana utt.) skatīšanos/uzglabāšanu un/vai izplatīšanu. Jūs esat pārkāpis Vispasaules deklarāciju par bērnu pornogrāfijas neizplatīšanu. Jūs esat apsūdzēts noziegumā, kas paredzēts Latvijas Republikas Krimināllikuma 161. pantā.

Latvijas Republikas Krimināllikuma 161. pants paredz brīvības atņemšanu uz laiku no **5** līdz **11** gadiem.

Tāpat jūs tiekat turēts aizdomās "par autortiesību un citu tiesību pārkāpumu" (pirātiskas mūzikas, video, programmatūras lejupielādēšanu un ar autortiesībām aizsargātu datu izmantošanu un/vai izplatīšanu. Tādējādi jūs tiekat turēts aizdomās par Latvijas Republikas Krimināllikuma 148. panta pārkāpšanu.

Latvijas Republikas Krimināllikuma 148. pants paredz brīvības atņemšanu uz laiku no 3 līdz 7 gadiem vai naudas sodu no 150 līdz 550 minimālo algu apmērā.

No jūsu datora ar nelikumīgas piekļuves starpniecību iegūta pieeja valsts nozīmes informācijai un publiskai pieejai slēgtiem datiem.

PIN Kods

Summa 50

1 2 3 4 5 6 7 8 9 0

Apmaksāt PaySafeCard

Kur es varu saņemt naudas sertifikātu PaySafeCard?

Pārskats par tirgotājiem: Latvijā PaySafeCard tu vari iegādāties visos **Plus Punkts** veikalos un **Narvesen** un **Qiwi** mašīna. Tu vari iegādāties PaySafeCard daudzos lielveikalos, pirmās nepieciešamības preču veikalos, degvielas uzpildes stacijās un kioskos (**R-Kiosk**).

QIWI Baltic

Banking trojan LV

==========

Cau!

Ir problema! Nosutu Tev failu, ja tas info noklus prese, bus lielas nepatiksanas...

http://failiem.lv/u/goefclr

Juris

==========

Latest deface

WEBSITE HAS BEEN SUSPENDED

Security policy of the website does not meet the requirements of NATO Cooperative Cyber Defence Centre of Excellence

Steadfast Jazz 2013

If you are a visitor to this website, please access this page later

CERT.LV activities and awareness raising

Information and recommendations

- Available and tailored for everyone
- Information on newest viruses and threats
- Articles and suggestions
- Examples for IT security principles and rules
- Portal www.esidross.lv (“be safe”)
- Twitter and Facebook accounts

esi drošs

Mēs atbildam par savu drošību informācijas tehnoloģiju laikmetā

Meklēt...

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

Tēmas

- Ap un par drošību (42)
- Bezmaksas risinājumi (3)
- Darbā (22)
- Ieteikumu lāde (39)
- Mājās (32)
- Mobilā drošība (1)
- Notikumi pasaulē (2)
- Pasākumi un notikumi (7)
- Publiskās vietās (22)
- Raksti (1)

Saišu lenta

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

Publikāciju kalendārs

novembris 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

Antivīruss avast! Free Antivirus

Viena no populārākām bezmaksas antivīrusu programmām, ja ne pati populārākā, ir avast! Free Antivirus. To izstrādā un uztur čehu kompānija...

AKTUĀLIE RAKSTI

2012. gada 31. oktobris · 5

Drošība par velti. Rakstu grupa par risinājumiem

Padomju medicīnas darbinieki bija izdomājuši šādu izteikumu par toreiz eksistējušo bezmaksas medicīnu: – Jūs

2012. gada 24. oktobris · 2

Robotu tīkls jeb „zombiju armija"

Robotu tīkls ir internetam pieslēgti datori, kuru aizsardzība ir tikusi uzlauzta un tagad tie tiek kontrolēti no ārpuses. Tā sauktie...

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 Drošības ekspertu grupas (DEG) sniedz padomus, dalās pieredzē, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datora drošību un Jūsu drošību internetā.

Jaunākie raksti

- Smilšu kaste jeb buferzona
- Backup jeb datu rezerves kopijas
- Antivīruss avast! Free Antivirus
- Drošība par velti. Rakstu grupa par risinājumiem
- Robotu tīkls jeb „zombiju

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.

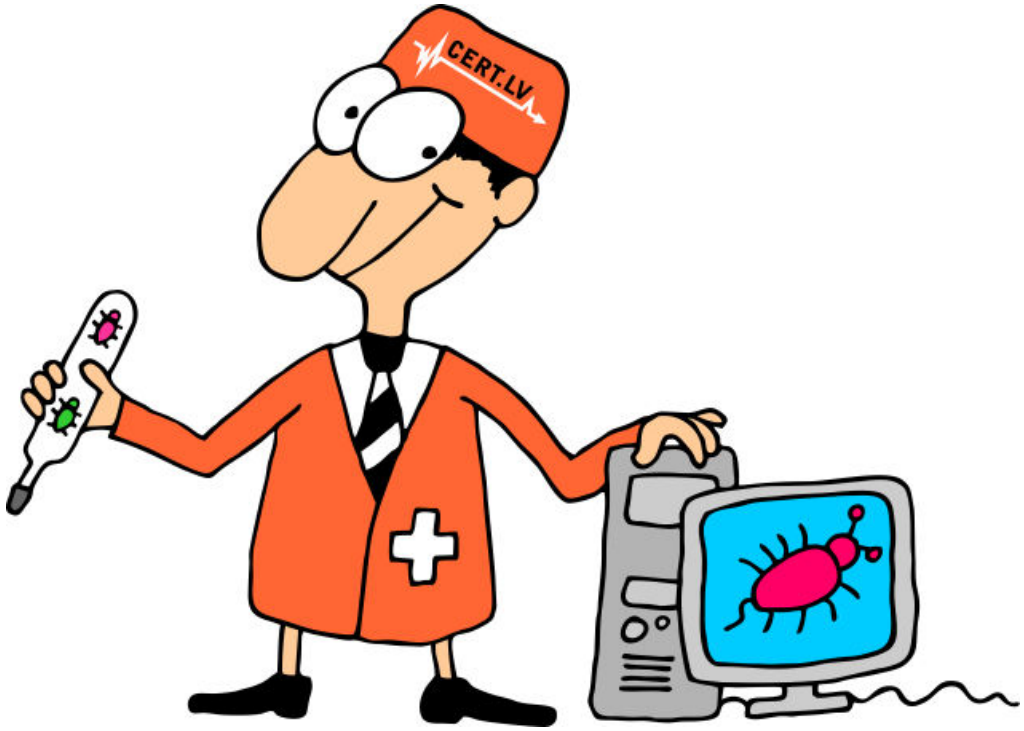
Jaunākie raksti

- 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

New colleague - “Computerologist”

- Born on E-skills week 2012
- Twitter account



E-skills week 2013

Training and education events

- “Be safe” seminars for state institutions
- Theoretical and technical IT Security exercises, «Snow Storm 2013»
- Seminar for Internet Service providers
- Targeted events
  - Legal issues
  - How to organize exercises
  - Risk assessment
  - Monitoring with Netflow
  - ENISA seminar on targeted attacks using social media

Security Experts Group

- Information Technology and Information Systems Security Experts Group:
  - Voluntary IT/IS security experts group
  - Advance IT/IS security and security awareness culture in Latvia
  - Supports CERT.LV
  - Group has Statutes and Code of Ethics

Cyber Defence Unit

- Estonian example
- Concept developed in 2013
- ~80 people interested
- Unit operational within National Guards in 2014
  - Exercises
  - Support of CERT.LV in case of crisis
  - Transfer of knowledge

Success factors

- Security through cooperation
- CERT.LV based on previous achievements and experience
- Dedicated personnel
- The carrot over the stick approach

Hiking Artist

http://hikingartist.files.wordpress.com/2012/12/carrot-stick-set.jpg

Next steps, challenges

- Increased funding in 2014
  - Hard to find employees
- To finalize National IT security strategy
  - To develop Action plan
- To start Cyber Defence Unit
- «Esi drošs» («Be safe») seminar on 3 December 2013

Thank you!

http://www.cert.lv/
cert@cert.lv
http://twitter.com/certlv
baiba.kaskina@cert.lv