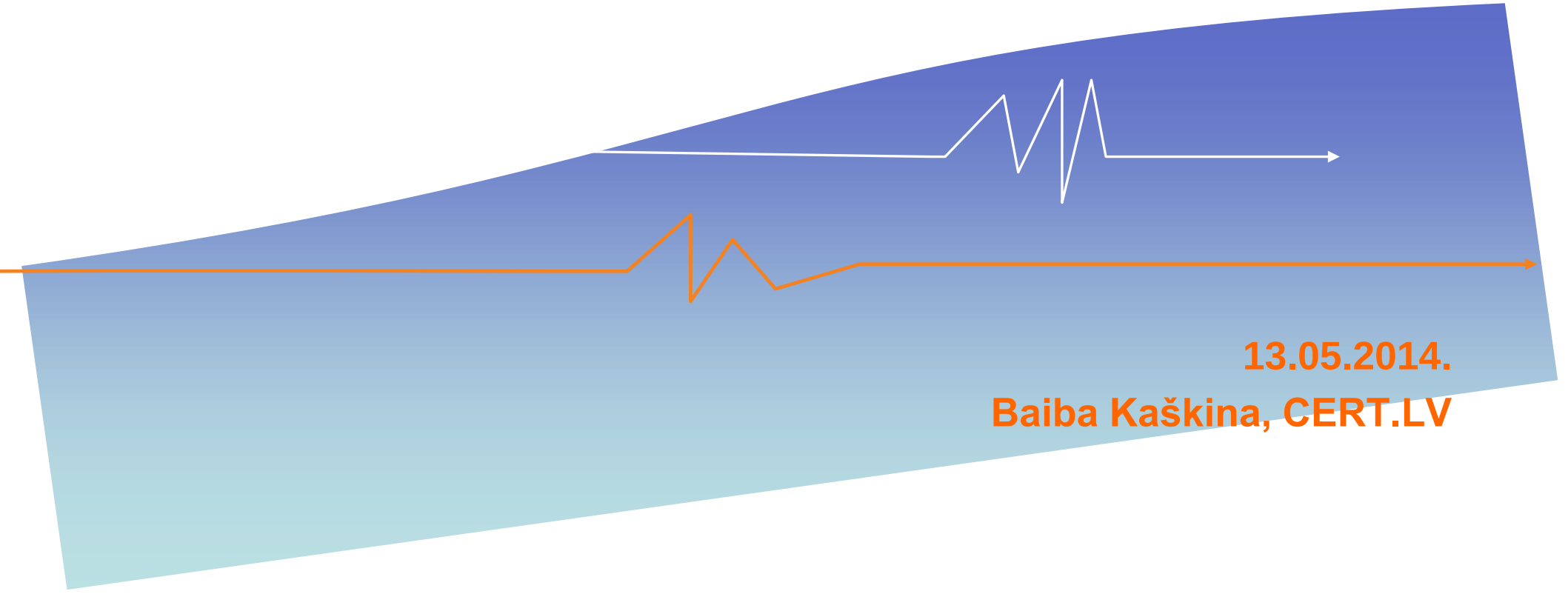
CERT.LV un IT drošība Latvijā



13.05.2014.

Baiba Kaškina, CERT.LV

Saturs

- Tiesiskais regulējums
- CERT.LV
  - Incidentu risināšana
  - Sadarbība
  - Sabiedrības izglītošana
- Pienākumi valsts un pašvaldību institūcijām
- Pienākumi elektronisko sakaru komersantiem
- Nākotne

Tiesiskais regulējums

Tiesiskais regulējums Latvijas Republikā

- Latvijas Republikas Satversmes 96.pants;
  - "Ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību."
- Likumi
  - Fizisko personu datu aizsardzības likums;
  - Valsts informācijas sistēmu likums;
  - Informācijas atklātības likums;
  - Informācijas sabiedrības pakalpojumu likums;
  - **Informācijas tehnoloģiju drošības likums.**

- Latvijas Informācijas tehnoloģiju drošības stratēģija.

IT drošības likums

- Pieņemts Saeimā 2010.gada 28.oktobrī
- Stājas spēkā 2011.gada 1.februārī
- Nosaka CERT.LV izveides kārtību
- Nosaka kārtību kā valsts un pašvaldību institūcijās jāorganizē IT drošības pārvaldība
- Pamatojoties uz likumu izstrādāti 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

CERT.LV

Mērķis

Uzlabot IT drošības līmeni Latvijā

Izveidota

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV

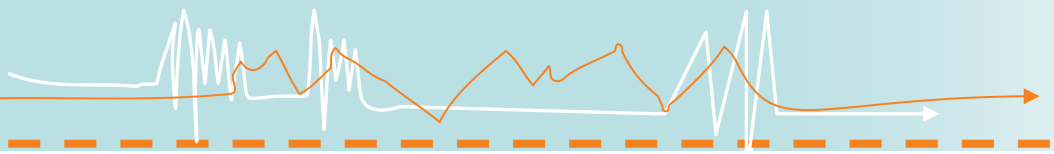
Nosaka galvenos

Pienākumus un tiesības:

- CERT.LV

Pienākumus:

- Valsts un pašvaldību institūcijām
- Elektronisko sakaru komersantiem



CERT.LV

Par CERT.LV

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

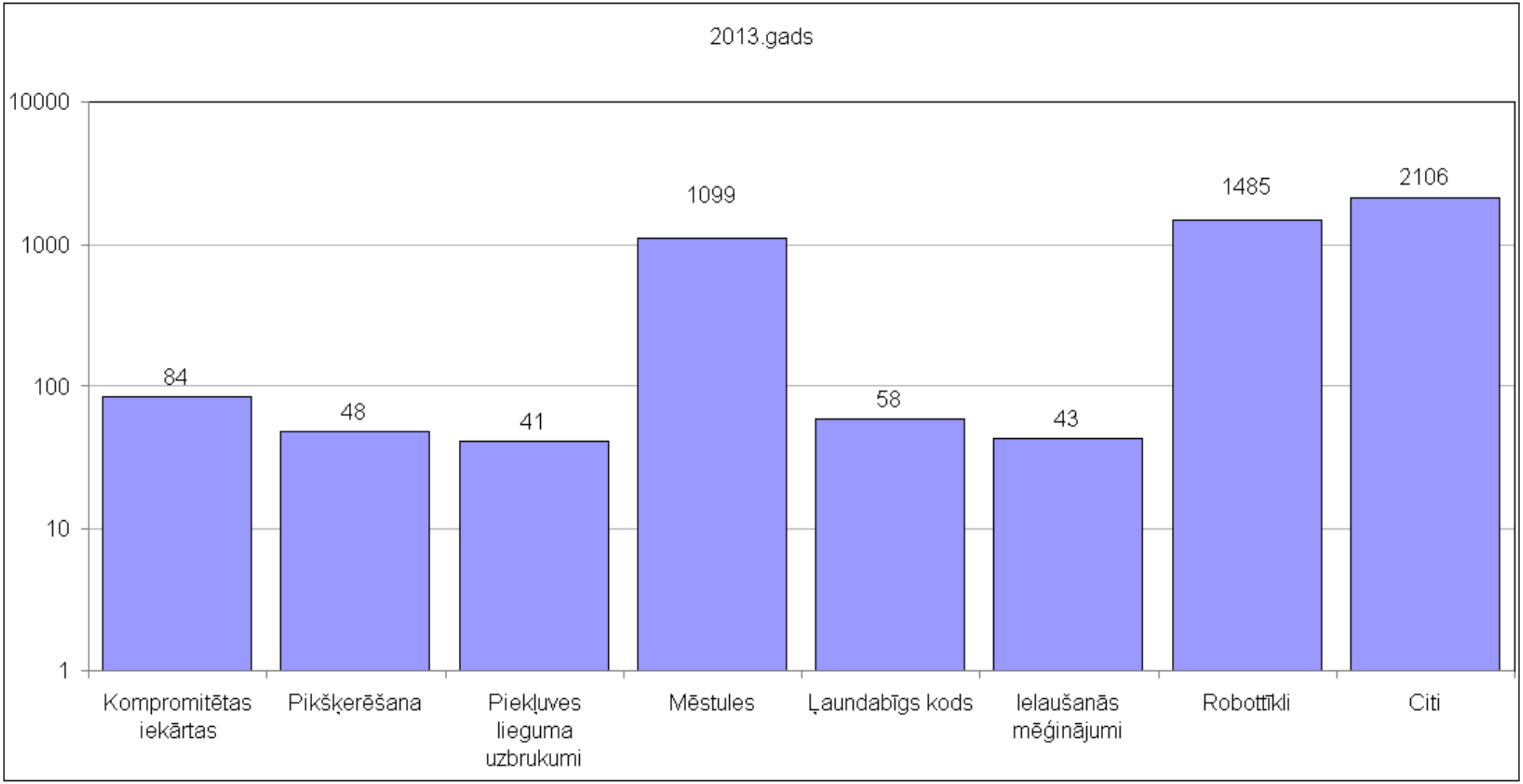
CERT.LV resursi

- Budžets 2014.gadā - 548 922 EUR
- 17 darbinieki, ~12PLE
- 3+5 gadu pieredze
- >600 kontaktpersonas dažādās organizācijās
- Laba sadarbība ar IPS

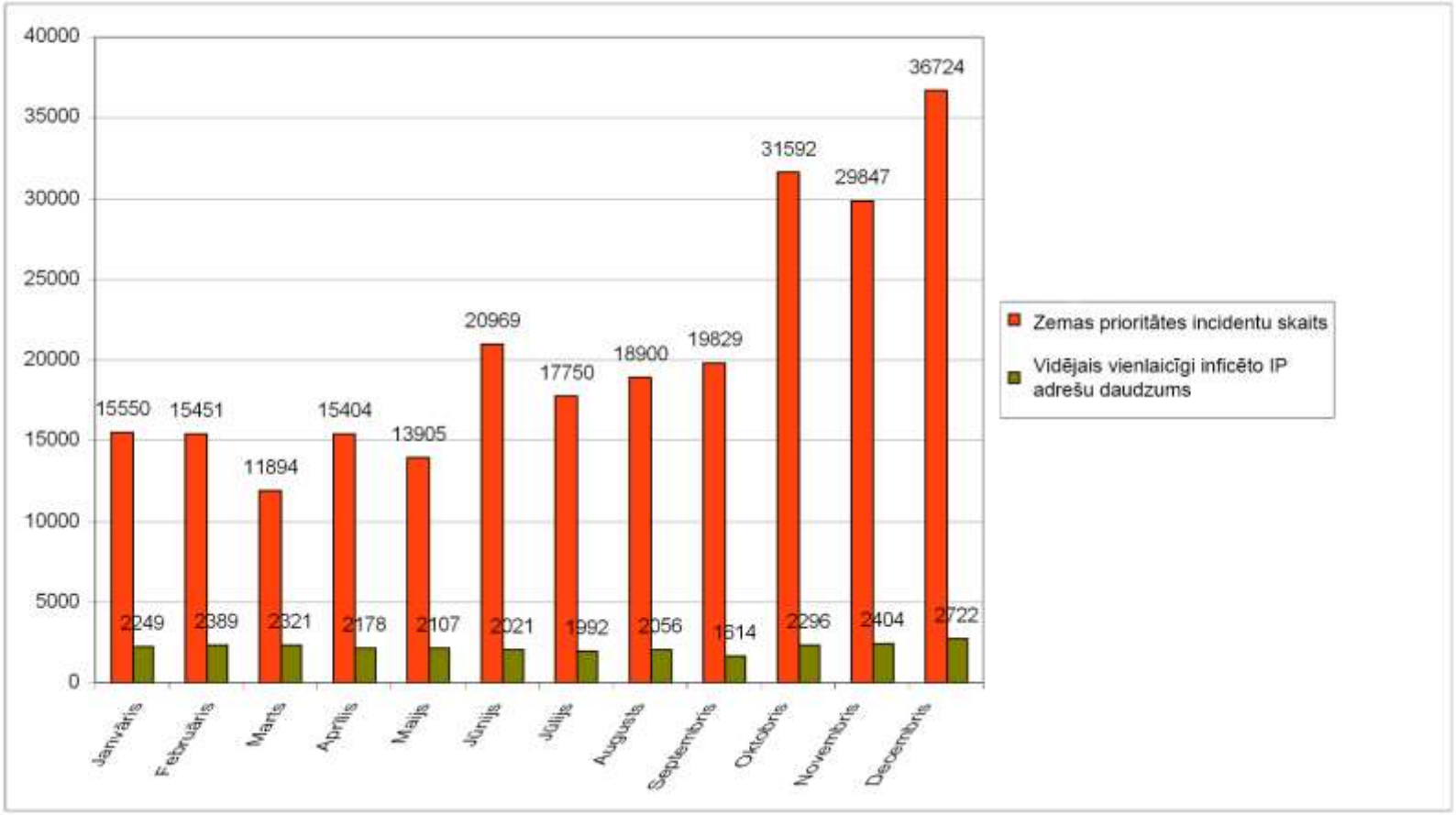
CERT.LV galvenie uzdevumi 1. – tehniskie uzdevumi

- Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu
- Sniegt atbalstu IT drošības incidenta novēršanā vai koordinēt to novēršanu

Augstas prioritātes incidenti - 4964

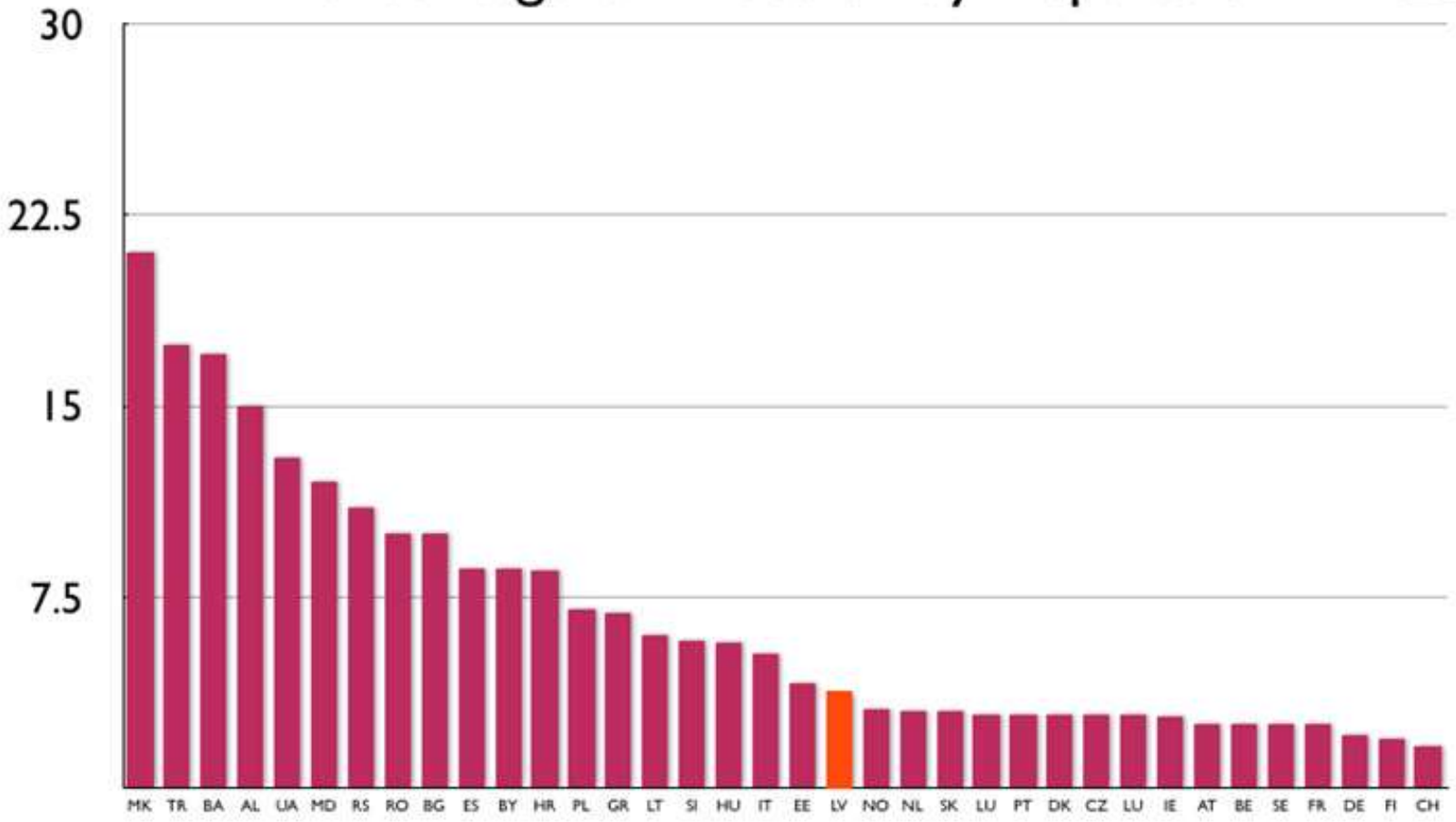


Zemas prioritātes incidenti 2013.gadā – 247 815



TEAM CYMRU

Percentage of Infection by Population



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 PaySafeCar

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

Banku vīruss

==========

Cau!

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

http://failiem.lv/u/goefclr

Juris

==========

VID vīruss

Re:Sudziba nodoklu dienestam

==========

Labdien! Informacija par sudzibu nosutita nodoklu dienestam, nosutu

Jums kopiju, skatit pielikuma. Ref id:xz27dns94m

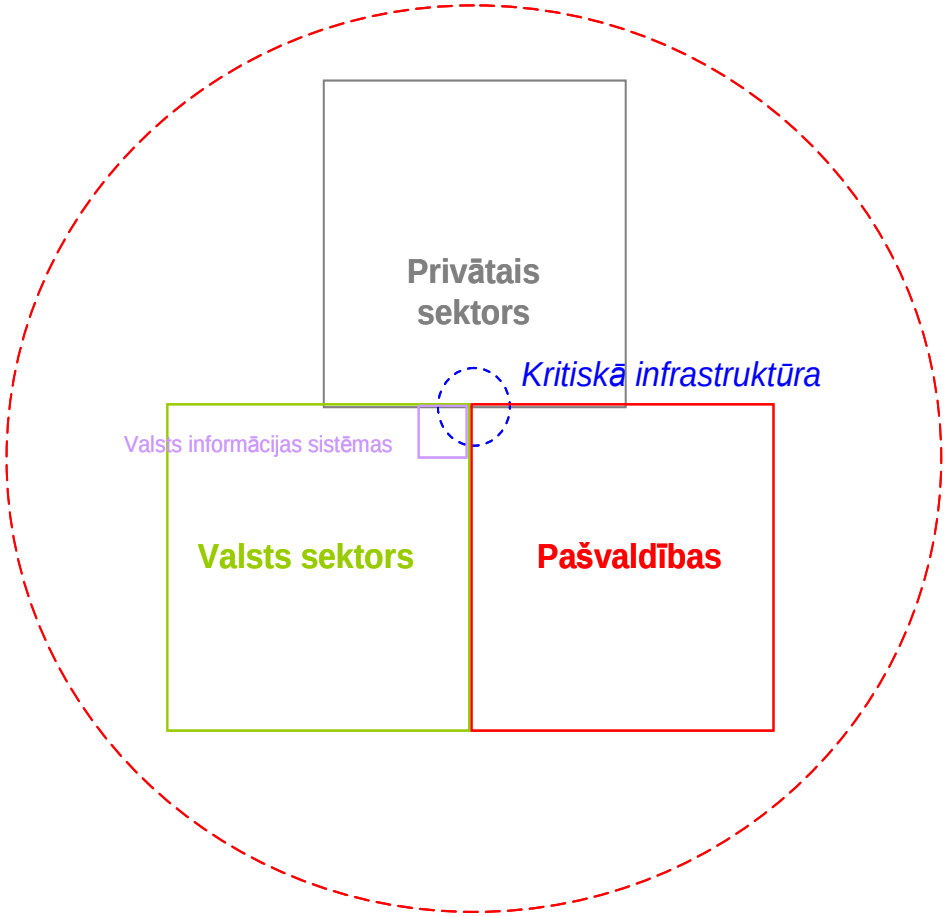
==========

Pielikumā: "nodokludienestam.doc.scr” vai "sudziba.doc.scr”

CERT.LV galvenie uzdevumi 2. – sadarbība

- Sniegt atbalstu valsts institūcijām valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likumpārkāpumu atklāšanā (izmeklēšanā) informācijas tehnoloģiju jomā
- Uzraudzīt, kā valsts un pašvaldību institūcijas un elektronisko sakaru komersanti izpilda likumā noteiktos pienākumus
- Sadarboties ar starptautiski atzītām IT drošības incidentu novēršanas institūcijām

CERT.LV kopiena



CERT.LV sadarbojas

- Valsts un pašvaldību iestādes
- IT Kritiskā infrastruktūra
- Privātais sektors
  - Elektronisko sakaru komersanti
  - Finanšu sektors
- Nevalstiskās organizācijas
- NBS, Kiberaizsardzības vienība

Starptautiskā sadarbība

- CERT komandas citās valstīs
  - TF-CSIRT (Trusted Introducer), FIRST
- NATO, CCDCoE
- ENISA, ENISA darba grupas
- Starptautiskās IT drošības mācības
  - Cyber Europe
  - Cyber Coalition
  - Locked Shields
- Baltijas sadarbība

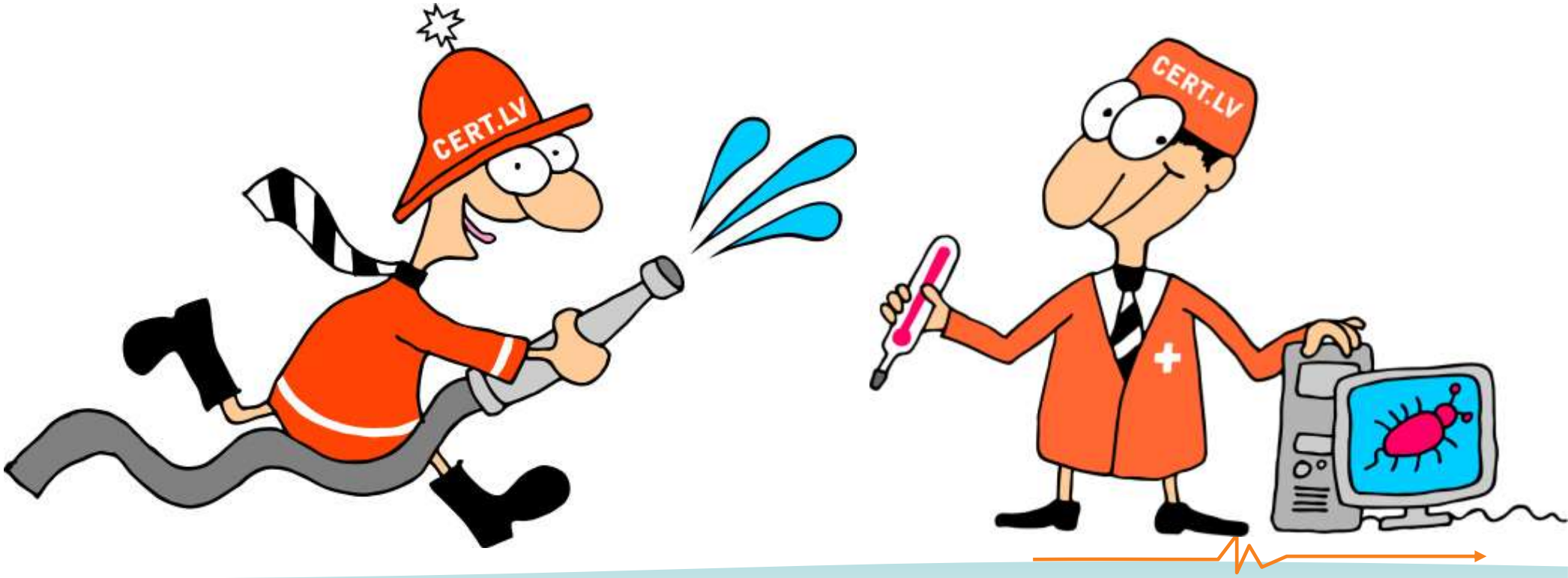
CERT.LV galvenie uzdevumi 3. – sabiedrības izglītošana

- Veikt pētniecisko darbu, organizēt izglītojošus pasākumus, apmācību un mācības informācijas tehnoloģiju drošības jomā
- Uzturēt sabiedrībai pieejamā veidā atbilstoši aktuālajiem apdraudējumiem izstrādātas rekomendācijas par aktuālo informācijas tehnoloģiju risku novēršanu

Sabiedrības izglītošana

- Tehniskie un teorētiskie semināri;
- Informācijas drošības izglītības programma, Realitāte-2014;
- IT drošības mācības;
- Plakāti pieaugušajiem un bērniem;
- Portāls Esidrošs – www.esidross.lv;
- Datorologs.

“Ģimenes ārsts” un “ugunsdzēsējs” e-vidē



CERT.LV piedāvā

- Palīdzību incidentu risināšanā
- Piemēru darbinieku apmācības programmai
- Piemērus IT drošības dokumentiem
- Informāciju par inficētām IP adresēm un incidentiem
- Reģionālos seminārus

Portāls www.esidross.lv

Vai esi Interneta profiņš?

Apdomā pirms publisko attēlus internetā!

Padomā, vai šie attēli neaizskar un nekaitē Tev, Taviem draugiem, klasesbiedriem, vecākiem vai jebkuram citam cilvēkam, kas attēlots fotogrāfijā. Pēc tam, kad attēls ir „ielikts" internetā, to vairs nevar iznīcināt vai padarīt par nebijušu.

Lieto drošas paroles!

Katram portālam izmanto citādāku paroli. Veido to pietiekami sarežģītu, lai to nevarētu uzminēt pat tie cilvēki, kas Tevi labi pazīst!

Neraksti aizskarošus komentārus!

Cilvēki, kas aizvaino citus, paši jūtas nelaimīgi. Taču, aizvainojot citus, neviens laimīgāks nekļūst. Nesāpini apkārtējos! Esi iecietīgs pret citu viedokli, dzīvesveidu, dzīves uzskatiem.

Nesarunā tikšanās ar tīklā satiktajiem paziņām!

Atceries, ka tīklā satiktie cilvēki ne vienmēr ir tie, par ko izliekas! Sargā sevi, lai neviens nevar nodarīt Tev pāri! Nepiekrīti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.

Neatklāj datus par sevi nepazīstamiem cilvēkiem!

Nebūt ne visi, ko Tu satiec virtuālajā vidē, ir tie, par ko uzdodas. Bieži vien ļaundari slēpj savu patieso seju, lai vieglāk piekļūtu Tev, Taviem radiem un draugiem. Jo vairāk Tu par sevi atklāsi, jo vieglāk viņi varēs nodarīt Tev pāri reālajā dzīvē. Neatklāj, kā Tevi sauc, kur Tu dzīvo, kas ir Tavi vecāki vai kādas mantas Tev ir mājās.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Vai esi Interneta profiņš?

- Par IT drošības incidentiem var ziņot CERT.LV - cert@cert.lv
- IT drošības izglītošanas portāls - www.esidross.lv
- CERT.LV mājas lapa - www.cert.lv

Mēstules nav vēstules!

Ignorē mēstules, ko saņem no nepazīstamiem cilvēkiem. Neatsaucies to „vilinošajiem" piedāvājumiem. Visbiežāk tie ir mēģinājumi izkrāpt Tavu naudu. Mēstules var izfiltrēt, un par tām var sūdzēties.

Neiepērcies internetā bez vecāku ziņas!

Nesniedz internetā savas vai vecāku kredītkartes datus, iepriekš neapspriežoties ar vecākiem. Atceries – izmantojot kredītkartes datus, var nozagt visu naudu, kas pieejama ar šo karti.

Darbības internetā nav anonīmas!

Tavas darbības internetā nav anonīmas! Vajadzības gadījumā tām var izsekot gan skolotāji, gan vecāki, gan likumu sargājošas iestādes.

Rūpējies par datora veselību!

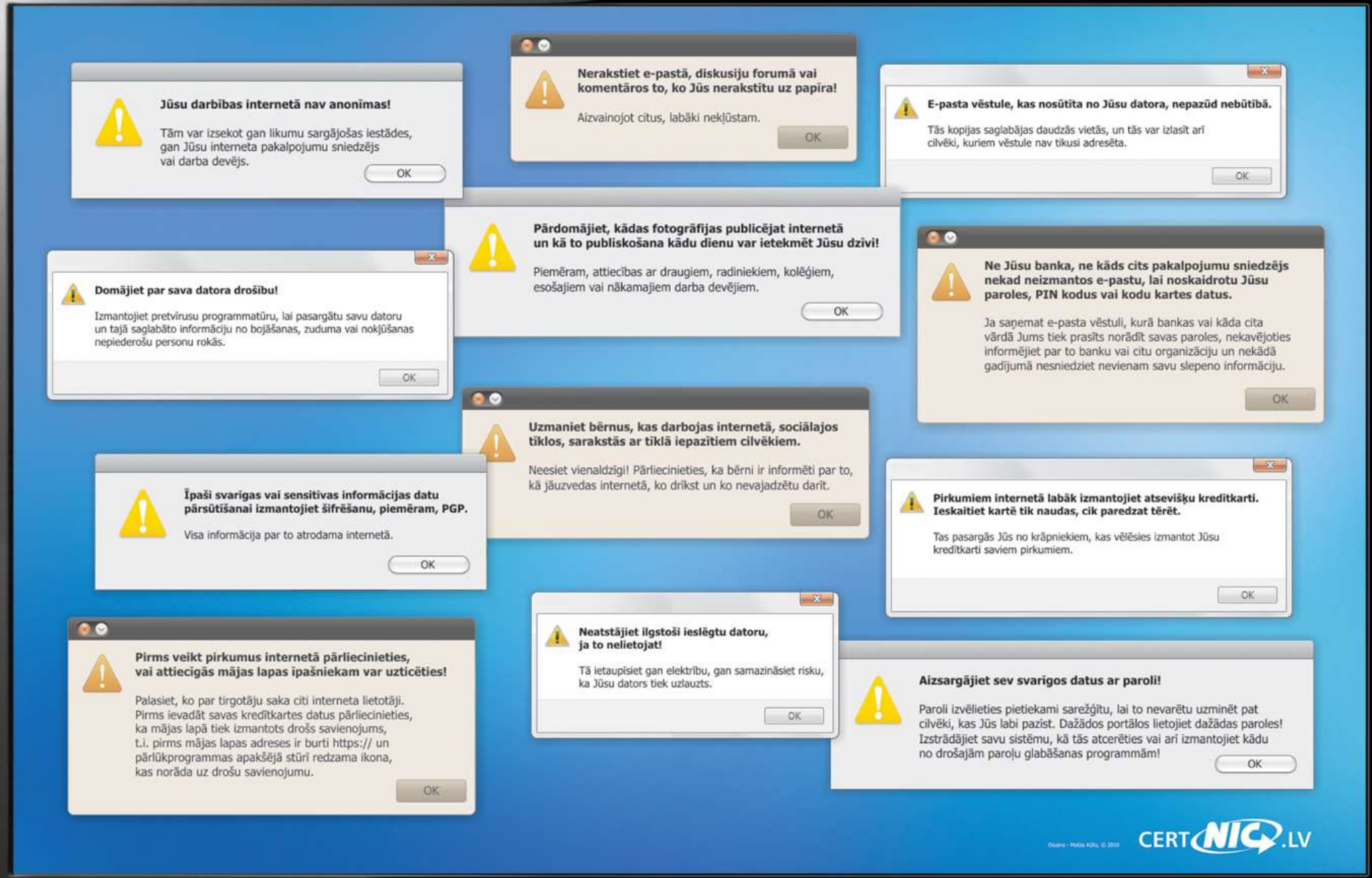
Neinstalē nezināmas izcelsmes programmas datorā, ko Tu lieto. Programma ļoti viegli var "izlikties" par spēli, bet patiesībā būt vīruss, kam Tu pats paver ceļu uz savu datoru.

Ja Tu:

- saņem nepatīkamas, aizvainojošas vēstules internetā,
- esi saskāries ar nepatīkamiem materiāliem internetā,
- esi pamanījis aizdomīgas darbības internetā,
- esi satraukts par savu drošību internetā,

pastāsti par to saviem vecākiem vai kādam citam no pieaugušajiem, kam uzticies! Vari zvanīt Bērnu un jauniešu bezmaksas uzticības tālrunim 116111 vai rakstīt uz: zinojumi@drossinternets.lv vai abuse@cert.lv

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija


Jūsu darbības internetā nav anonīmas!
Tām var izsekot gan likumu sargājošas iestādes, gan Jūsu interneta pakalpojumu sniedzējs vai darba devējs.
OK
Nerakstiet e-pastā, diskusiju forumā vai komentāros to, ko Jūs nerakstītu uz papīra!
Aizvainojot citus, labāki nekļūstam.
OK
E-pasta vēstule, kas nosūtīta no Jūsu datora, nepazūd nebūtībā.
Tās kopijas saglabājas daudzās vietās, un tās var izlasīt arī cilvēki, kuriem vēstule nav tikusi adresēta.
OK
Pārdomājiet, kādas fotogrāfijas publicējat internetā un kā to publiskošana kādu dienu var ietekmēt Jūsu dzīvi!
Piemēram, attiecības ar draugiem, radiniekiem, kolēģiem, esošajiem vai nākamajiem darba devējiem.
OK
Domājiet par sava datora drošību!
Izmantojiet pretvīrusu programmatūru, lai pasargātu savu datoru un tajā saglabāto informāciju no bojāšanas, zuduma vai nokļūšanas nepiederošu personu rokās.
OK
Ne Jūsu banka, ne kāds cits pakalpojumu sniedzējs nekad neizmantos e-pastu, lai noskaidrotu Jūsu paroles, PIN kodus vai kodu kartes datus.
Ja saņemat e-pasta vēstuli, kurā bankas vai kāda cita vārdā Jums tiek prasīts norādīt savas paroles, nekavējoties informējiet par to banku vai citu organizāciju un nekādā gadījumā nesniedziet nevienam savu slepeno informāciju.
OK
Uzmaniet bērnus, kas darbojas internetā, sociālajos tīklos, sarakstās ar tīklā iepazītiem cilvēkiem.
Neesiet vienaldzīgi! Pārliecinieties, ka bērni ir informēti par to, kā jāuzvedas internetā, ko drīkst un ko nevajadzētu darīt.
OK
Īpaši svarīgas vai sensitīvas informācijas datu pārsūtīšanai izmantojiet šifrēšanu, piemēram, PGP.
Visa informācija par to atrodama internetā.
OK
Pirkumiem internetā labāk izmantojiet atsevišķu kredītkarti. Ieskaitiet kartē tik naudas, cik paredzat tērēt.
Tas pasargās Jūs no krāpniekiem, kas vēlēsies izmantot Jūsu kredītkarti saviem pirkumiem.
OK
Pirms veikt pirkumus internetā pārliecinieties, vai attiecīgās mājas lapas īpašniekam var uzticēties!
Palasiet, ko par tirgotāju saka citi interneta lietotāji. Pirms ievadāt savas kredītkartes datus pārliecinieties, ka mājas lapā tiek izmantots drošs savienojums, t.i. pirms mājas lapas adreses ir burti https:// un pārlūkprogrammas apakšējā stūrī redzama ikona, kas norāda uz drošu savienojumu.
OK
Neatstājiet ilgstoši ieslēgtu datoru, ja to nelietojat!
Tā ietaupīsiet gan elektrību, gan samazināsiet risku, ka Jūsu dators tiek uzlauzts.
OK
Aizsargājiet sev svarīgos datus ar paroli!
Paroli izvēlieties pietiekami sarežģītu, lai to nevarētu uzminēt pat cilvēki, kas Jūs labi pazīst. Dažādos portālos lietojiet dažādas paroles! Izstrādājiet savu sistēmu, kā tās atcerēties vai arī izmantojiet kādu no drošajām paroļu glabāšanas programmām!
OK
CERT NIC .LV
VIRTUĀLĀ REALITĀTE

Ko CERT.LV nedara?

- Satura izvērtēšana
- Personas datu aizsardzība
- Valsts informācijas sistēmu jautājumi
- Noziegumu izmeklēšana
- Iestāžu, sistēmu auditi

Pienākumi valsts un pašvaldību institūcijām

Valsts un pašvaldību institūciju pienākumi

- Noteikt atbildīgo personu, kura īsteno IT drošības pārvaldību
- Organizēt institūcijas IT drošības pārvaldību
- Informēt CERT.LV incidenta gadījumā
- Ne retāk kā reizi gadā veikt IT drošības pārbaudi un atbilstoši tās rezultātiem organizēt atklāto trūkumu novēršanu
- Apmeklēt CERT.LV organizētu apmācību IT drošības jautājumos
- Veikt darbinieku instruktāžu IT drošības jautājumos

Pienākumi elektronisko sakaru komersantiem

Elektronisko sakaru komersantu pienākumi

- Nodrošināt maksimāli iespējamo pakalpojumu sniegšanas nepārtrauktību
- Iesniegt CERT.LV Rīcības plānus
- Informēt CERT.LV būtisku incidenta gadījumā
- Sniegt CERT.LV pieprasīto informāciju saistībā ar incidentiem
- Pēc CERT.LV pieprasījuma slēgt galalietotājam piekļuvi elektronisko sakaru tīklam

Atbildīgs interneta pakalpojumu sniedzējs

ATBILDĪGS INTERNETA PAKALPOJUMU SNIEDZĒJS ir kvalitātes zīme, kuru var saņemt Elektronisko sakaru pakalpojumu komersants, kurš:

- Sadarbojas ar CERT.LV un informē gala lietotājus par to, ka viņu datori ir inficēti ar kādu no datorvīrusiem un kļuvuši par robotu tīklu sastāvdaļu,
- Sadarbojas ar Net-Safe Latvia Drošāka interneta centru, lai nodrošinātu iespējami ātru nelegālā satura (bērnu pornogrāfijas) izņemšanu no publiskas aprites internetā,
- Pēc klientu pieprasījuma nodrošina bezmaksas interneta satura filtru uzstādīšanu atbilstoši Elektronisko sakaru likumam.

Nākotne

2014.gada darbības prioritātes

1. Uzlabot IT drošību valsts pārvaldē – apmācība, regulāra komunikācija, sensoru tīkla veidošana, apziņošana;
2. Kritiskās infrastruktūras aizsardzība – jāsakārto dokumentācija, ielaušanās mēģinājumu realizēšana;
3. Analītisko spēju palielināšana ļaunatūru pētniecībai un analīzei, pilnvērtīgāka elektroniskās informācijas telpā notiekošo darbību analizēšana un attēlošana;
4. Sabiedrības izglītošana un kopējā izglītības par IT drošības jautājumiem līmeņa celšana;
5. Starptautiskās sadarbības veicināšana un Latvijas prestiža celšana IT drošības jomā.

Agrās brīdināšanas sistēma

- Agrās brīdināšanas sistēmas sensoru izvietošana valsts iestādēs
- Laicīga bīstamu un mērķētu incidentu atklāšana un veiksmīgāka novēršana
- Vēsturiska informācija par to, kas noticis iestādē – iespēja atklāt mērķētu uzbrukumu pēdas

Citi 2014.gada darbi

- Līdzšinējo darbu turpināšana +
- Vairāk ielaušanās mēģinājumu realizēšanas
- Ļaunatūras pētniecība
- Sadarbība ar KI
- Ikgadējā konference 16.oktobrī

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
- Jāveicina akadēmiskie pētījumi IT drošības jomā
- Jāveicina un jāorganizē kvalitatīvas diskusijas par drošības jautājumiem

Nākotne (2)

- Latvijas Informācijas tehnoloģiju drošības stratēģijas Rīcības plāna realizācija
- Normatīvo aktu regulējuma izmaiņas
- IT izpratnes un kapacitātes paaugstināšana tiesībsargājošajās iestādēs

Paldies par uzmanību!

http://www.cert.lv/

cert@cert.lv

baiba.kaskina@cert.lv