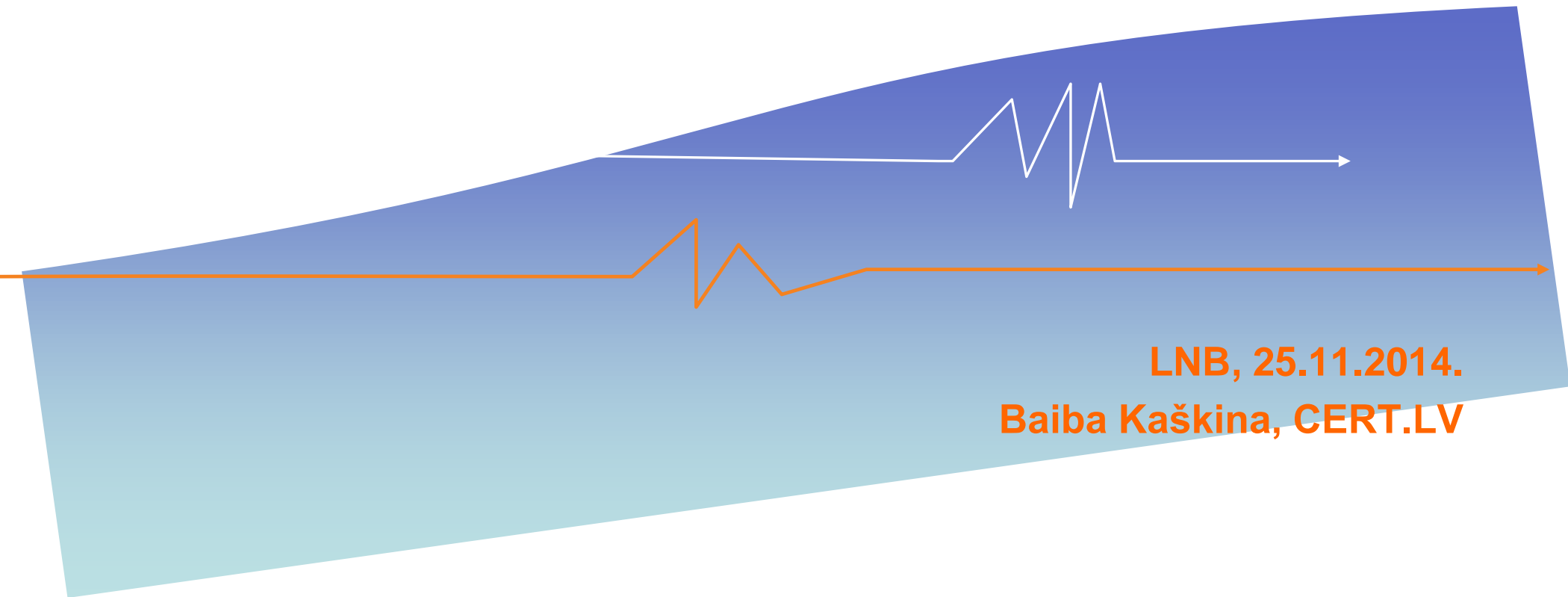


IT drošība Latvijā un bibliotēkas



LNB, 25.11.2014.

Baiba Kaškina, CERT.LV

Saturs

- Tiesiskais regulējums Latvijā
- Par CERT.LV
- Pienākumi valsts un pašvaldību institūcijām
- Informācija par inficētajām IP adresēm
- CERT.LV piedāvā



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** (pieņemts 2010.gadā).
- Latvijas Informācijas tehnoloģiju drošības stratēģija (pieņemta 2014.gadā)

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

Mērķis

Uzlabet 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

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



CERT.LV

Par CERT.LV



CERT.LV

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija
- Misija: “Veicināt IT drošību Latvijā”
- Virzība: “IT drošības kompetences centrs”

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 galvenie uzdevumi

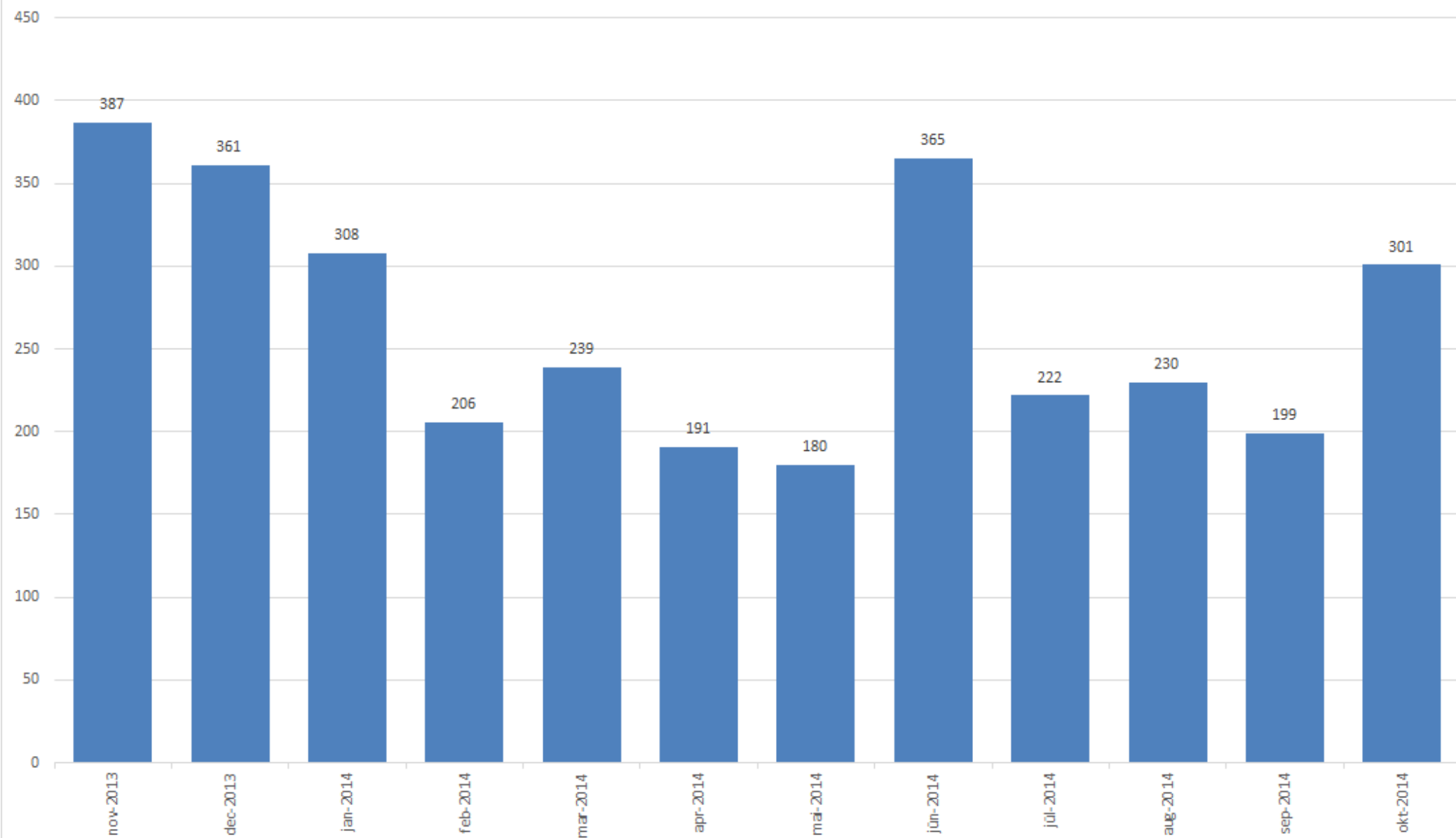
1. – tehniskie uzdevumi

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



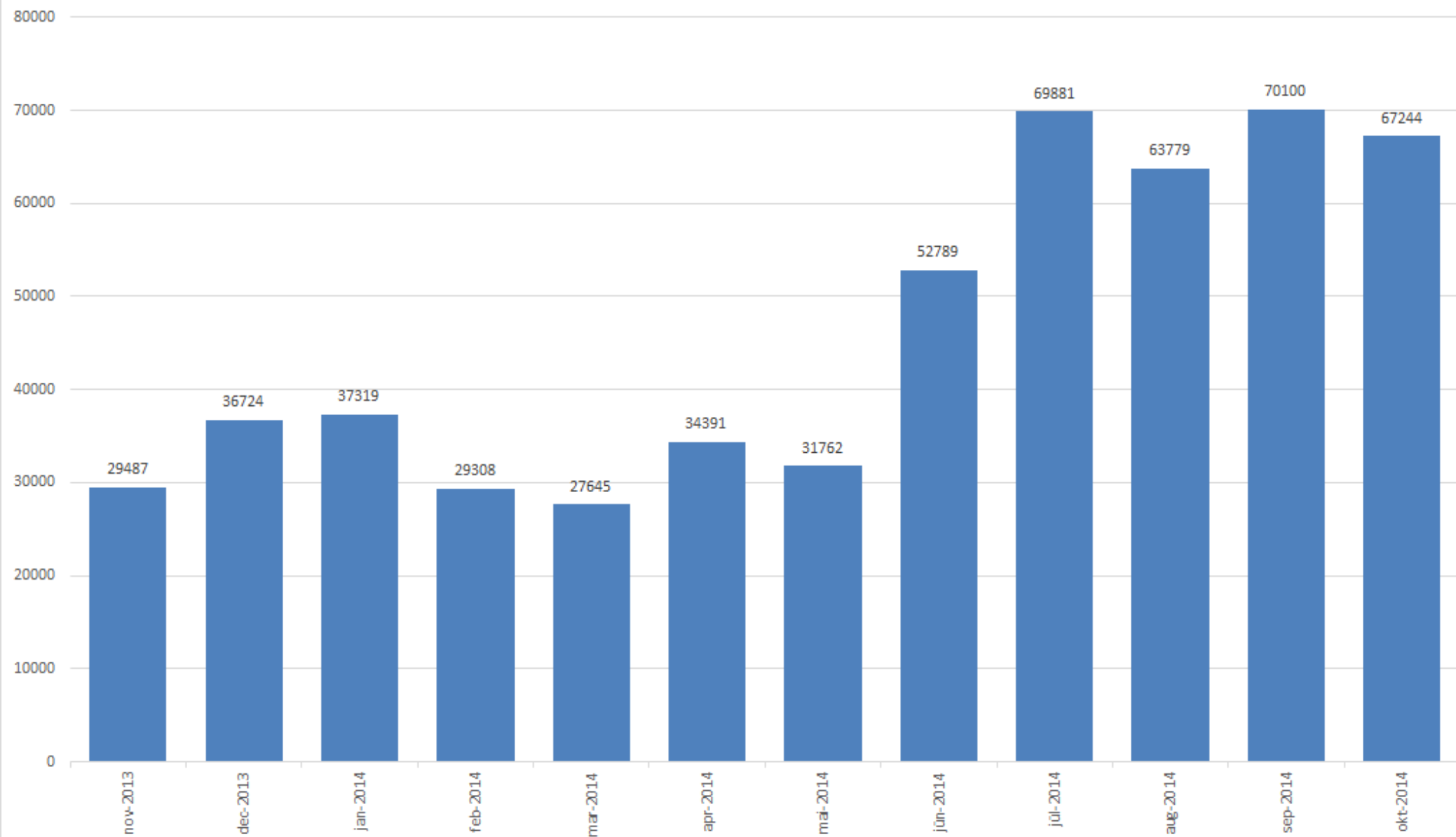
Incidentu sadalījums pa mēnešiem

■ Augstas prioritātes incidenti



Incidentu sadalījums pa mēnešiem

■ Zemas prioritātes incidenti





Atlikušais laiks: 47:57:29



IP: [REDACTED]

Valsts: LV Latvia
Rajons: Rīga
Pilsēta: Rīga
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 tiek turēts aizdomās "par autortiesību un citu tiesību pārkāpumu" (pirātiskas mūzikas, video, programmatūras lejupielādēšanu un ar autortiesībām aizsargātu datu izmantošanu un/vai izplatīšanu. Tādējādi jūs tiek 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

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 mašīnā. Tu vari iegādāties PaySafeCard daudzos lielveikalos, pirmās nepieciešamības preču veikalos, degvielas uzpildes stacijās un kioskos (R-Kiosk).



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"

Pikšķerēšana

From: LATNET Webmail Serviss <famuk@latnet.lv>
Subject: **Jusu e-pasta driz beigsies**
To: undisclosed-recipients;

Cienijamais lietotāj

Jusu e-pasta driz beigsies

Lai izvairītos no jebkadiem partraukumiem, lūdzu noklikšķiniet uz saites zemāk, un uzlabot savu e-pastu

Klikšķiniet šeit <http://www.iepi.com.br/player/Scripts/mail.ls.lv.htm>, lai parietu

Sirsnīgi
Klientu Help Desk

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 sadarbības

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

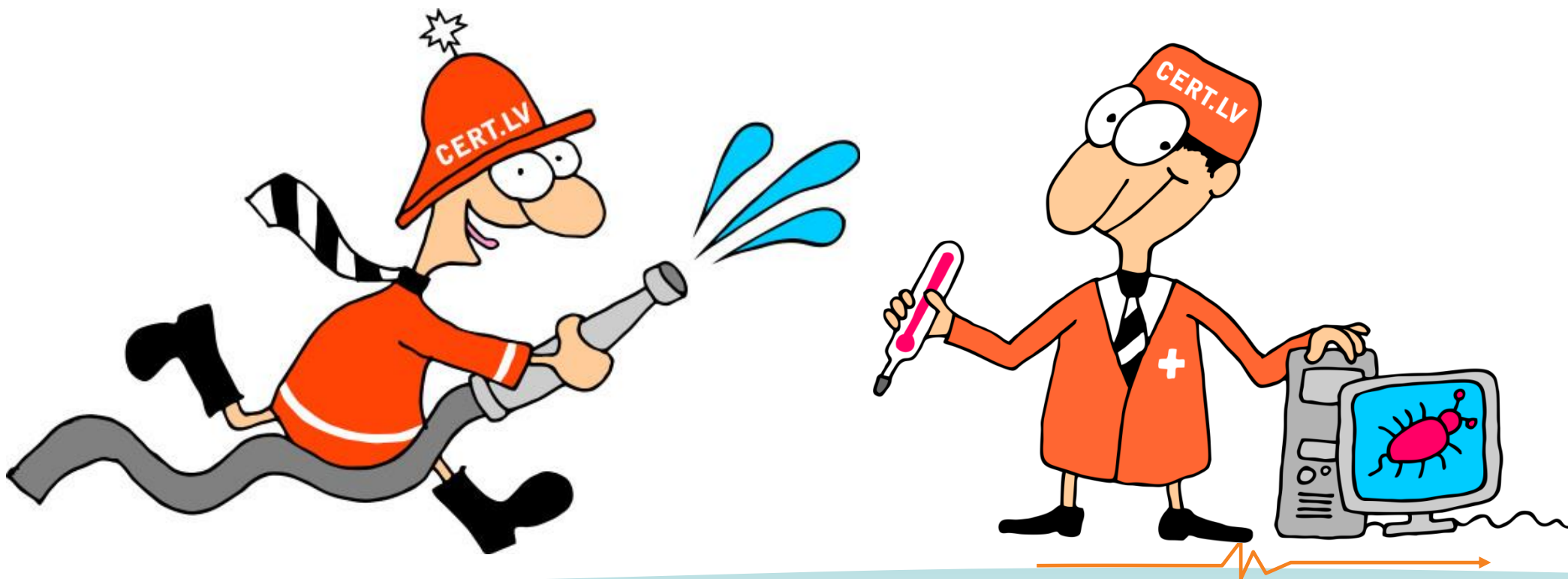
CERT.LV galvenie uzdevumi

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

CERT.LV

“Ģimenes ārsts” un “ugunsdzēsējs” e-vidē



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.

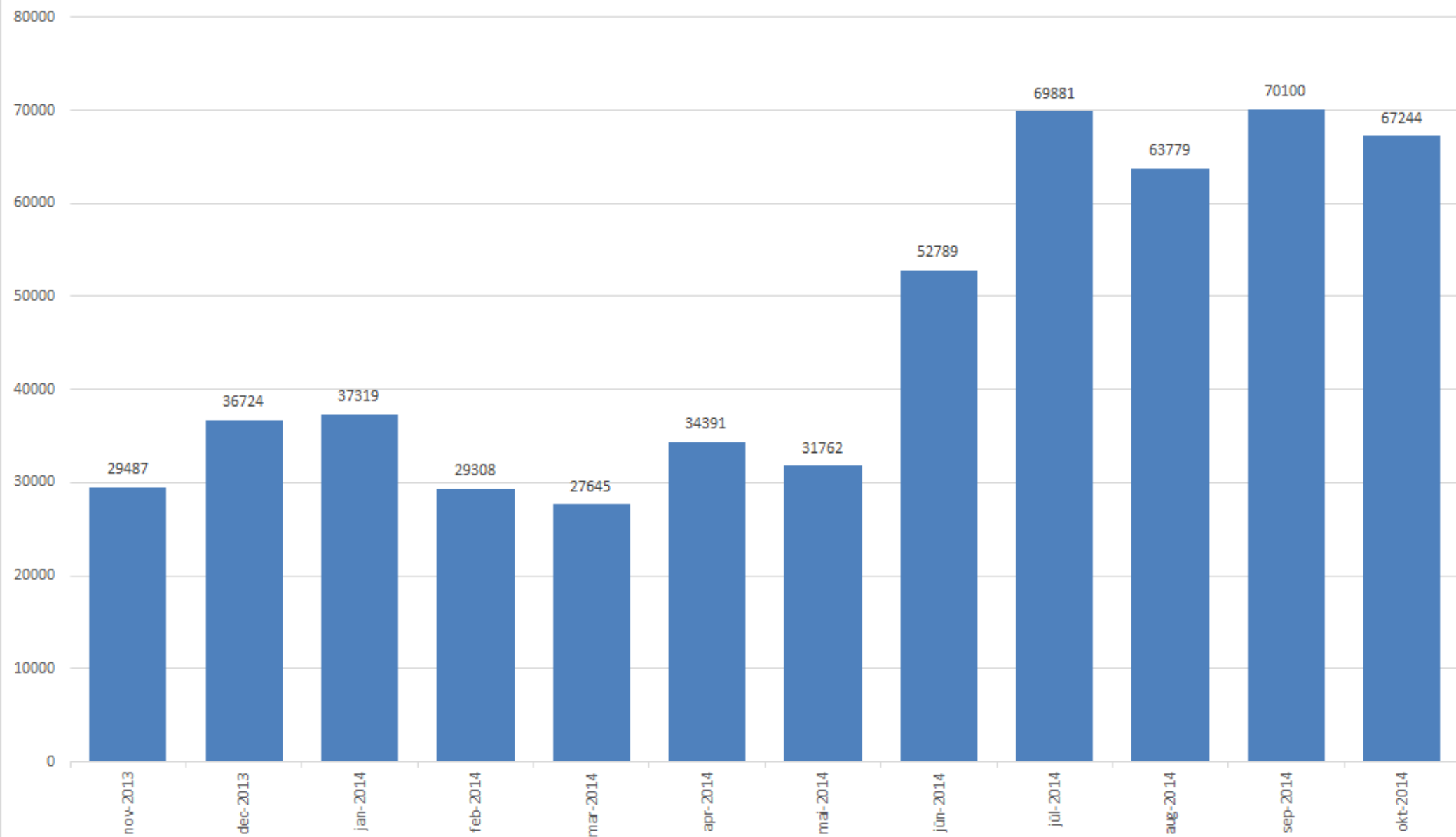
Ko CERT.LV nedara?

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

Informācija par inficētajām IP adresēm

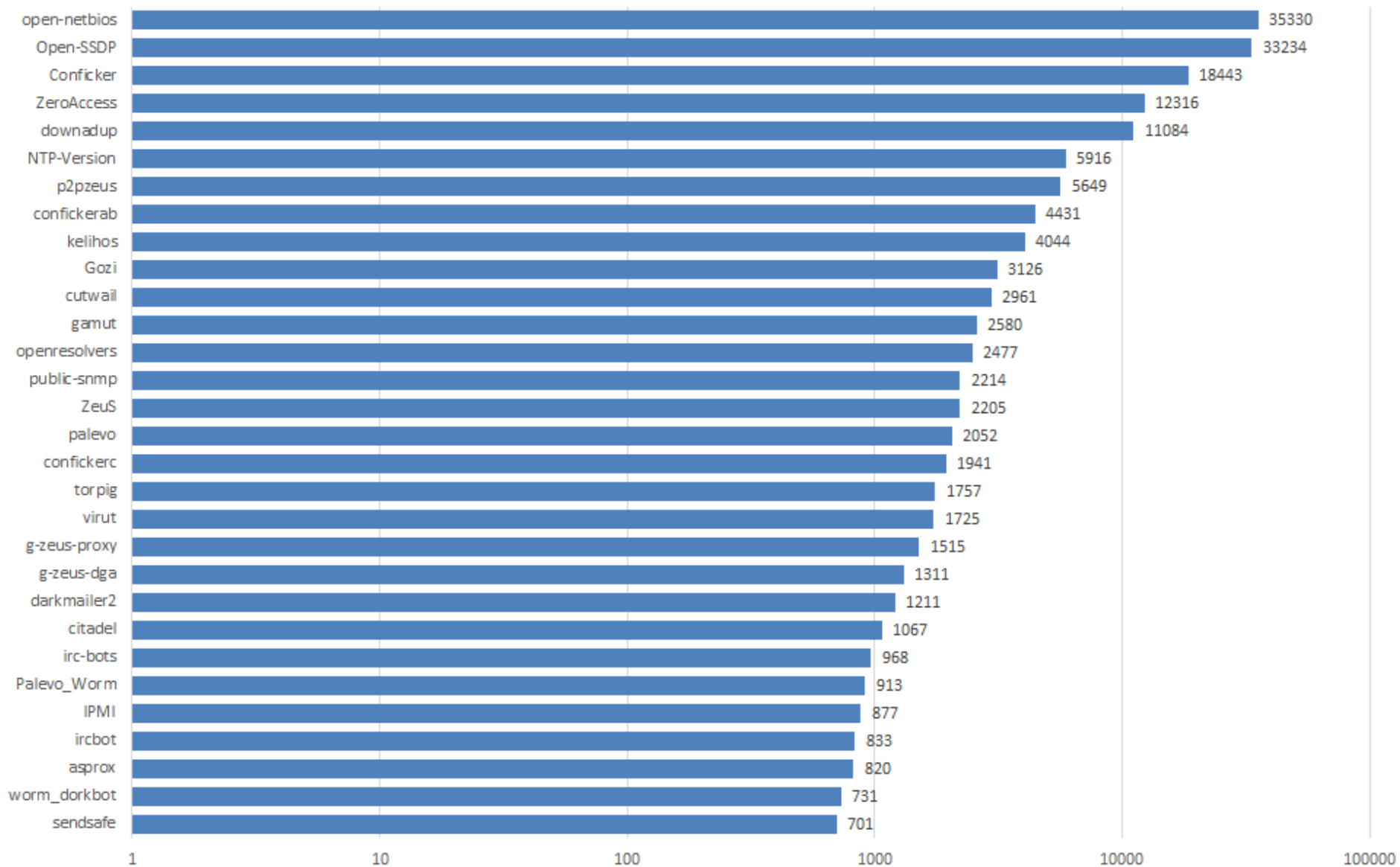
Incidentu sadalījums pa mēnešiem

■ Zemas prioritātes incidenti



2014.gada 3.ceturksnis

■ Izplatītāko apdraudējumu skaits



CERT.LV sūta informāciju par inficētām IP adresēm

- Valsts un pašvaldību iestādēm
- Interneta pakalpojumu sniedzējiem
 - Atbildīgs IPS
- Bibliotēkām
 - Uz kulturaskarte.lv norādīto e-pastu
- Citiem interesentiem par Latvijas IP adresu apgabalu

CERT.LV sūtītā informācija

; CERT.LV ziņojums
; Copyright 2013 CERT.LV. Lauku apraksts:
;
; time - laiks UTC formātā
; ip - avota IP adrese
; asn - avota autonomā sistēma (ja pieejama)
; infection - infekcijas nosaukums
; destination - mērķa IP adrese (ja pieejama)
; destination_port - mērķa ports (ja pieejams)
; destination_asn - mērķa autonomā sistēma (ja pieejama)
; url - saistītā tīmekļa vietne (ja pieejama)
; domain - saistītās tīmekļa vietnes domena nosaukums (ja pieejams)
; source - CERT.LV
; priority - prioritāte (1-zema, 2-vidēja, 3-augsta, 4-ļoti augsta)
; hash - kontrolsumma (izmantojama papildus informācijas iegūšanai
<https://www.esidross.lv/cert-lv-bridinajums/?hash/<hash>>)

Tēmas

- Ap un par drošību (80)
- Bezmaksas risinājumi (15)
- Darbā (27)
- datora drošība (6)
- Datorologs (2)
- Ieteikumu lāde (61)
- Mājās (39)
- Mobilā drošība (6)
- Notikumi pasaulē (4)
- pārbaude (1)
- Pasākumi un notikumi (11)
- Publikās vietās (23)
- Raksti (12)
- vīrusi (2)

Saišu lenta

- DEG – Drošības ekspertu grupa
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Aizsardzības ministrija
- LR Satiksmes ministrija
- Net-Safe Latvia Drošāka interneta centrs

CERT.LV brīdinājums

Jūsu IP adrese: 10.10.10.10 ir inficēta

Incidenta datums: 2014-11-20 19:11:42

Datorvīrusa nosaukums: Conficker

Labā prakse: Redzama datorvīrusa "downadup" zināms arī kā Conficker, Kido (<http://support.kaspersky.com/faq/?qid=208279973>) aktivitāte. Masveida datoru pārbaudei var izmantot turpat minēto KidoKiller komandrindas rīku.

Lai jūsu dators (vai datortīkls) būtu drošībā, iesakām atslēgt inficēto datoru no datortīkla (Internet) un vērsties pie datorspeciālista.

Lai iztīrītu datoru no datorvīrusa veiciet šādas darbības:

1. Jāveic pilna skanēšana ar atjauninātu Antivīrusu programmatūru; Iesakām izmantot kādu no šiem bezmaksas rīkiem: **BOTFREI, F-SECURE**
2. Ja nav iespējams pieslēgties, lai atjauninātu Antivīrusu programmatūru (vai jūsu Antivīrusu programmatūra neko neatrod), dators jāielādē un jāizārstē no citas vides - CD, DVD vai USB diska, to iepriekš sagatavojot uz cita, neinficēta datora. CD sagatavošanai iesakām izmantot, piemēram: **KASPERSKY RESCUEDISK F-SECURE RESCUE-CD**
3. Dažos gadījumos pēc infekcijas likvidēšanas, iespējams, ka kādi faili būs bojāti un tie būs jāatjauno no datora rezerves kopijas.

Lai turpmāk jūsu dators būtu labāt pasargāts, iesakām ņemt vērā šeit aprakstīto: **CERT.LV**



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

- Mobilo iekārtu drošība – padomi lietotājiem
- Virtuālā izmeklēšana, reāls

Inficētie datori ir jātīra!

- Likums liek rūpēties par IT drošību
- Inficētos datoros
 - Tiek zagta informācija (kredītkartes, identitātes)
 - Nelietderīgi tiek tērēti datora un tīkla resursi
 - Notiek uzbrukumi citiem datoriem, mēstuļu sūtīšana

CERT.LV piedāvā



CERT.LV piedāvā

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

Portāls www.esidrošs.lv



*Mēs atbildam par savu drošību
informācijas tehnoloģiju laikmetā*


[Mājās](#)
[Darbā](#)
[Publiskās vietās](#)
[Ieteikumi](#)
[Par drošību](#)
[Pasākumi](#)
[Notikumi pasaulē](#)


Uzmanību! Saskaņā ar CERT.LV datiem, Jūsu dators ar IP adresi **255.255.255.252** ir inficēts ar datorvīrusu! [Vairāk informācijas](#). ☒



*Mēs atbildam par savu drošību
informācijas tehnoloģiju laikmetā*

[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 lentā

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



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



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.

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 izcināt 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!



Nesarunā tikšanās ar tīklā satiktajiem paziņām!

Atceries, ka tīklā satiktie cilvēki ne vienmēr ir tie, par ko izliekas! Sargā sevi, lai nevienam nevar dotarīt cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.

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.



Neatklāj datus par sevi nepazīstamiem cilvēkiem!

Nebūt ne visi, ko Tu satic virtūālajā 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.



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 pamanījies 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

Paldies par uzmanību!

<http://www.cert.lv/>

cert@cert.lv

baiba.kaskina@cert.lv

