

# ***CERT.LV sadarbība ar valsts un pašvaldību institūcijām***



**Seminārs “Esi drošs – 2”, Rīga, 2013.gada 3.decembris  
Egils Stūrmanis, CERT.LV**

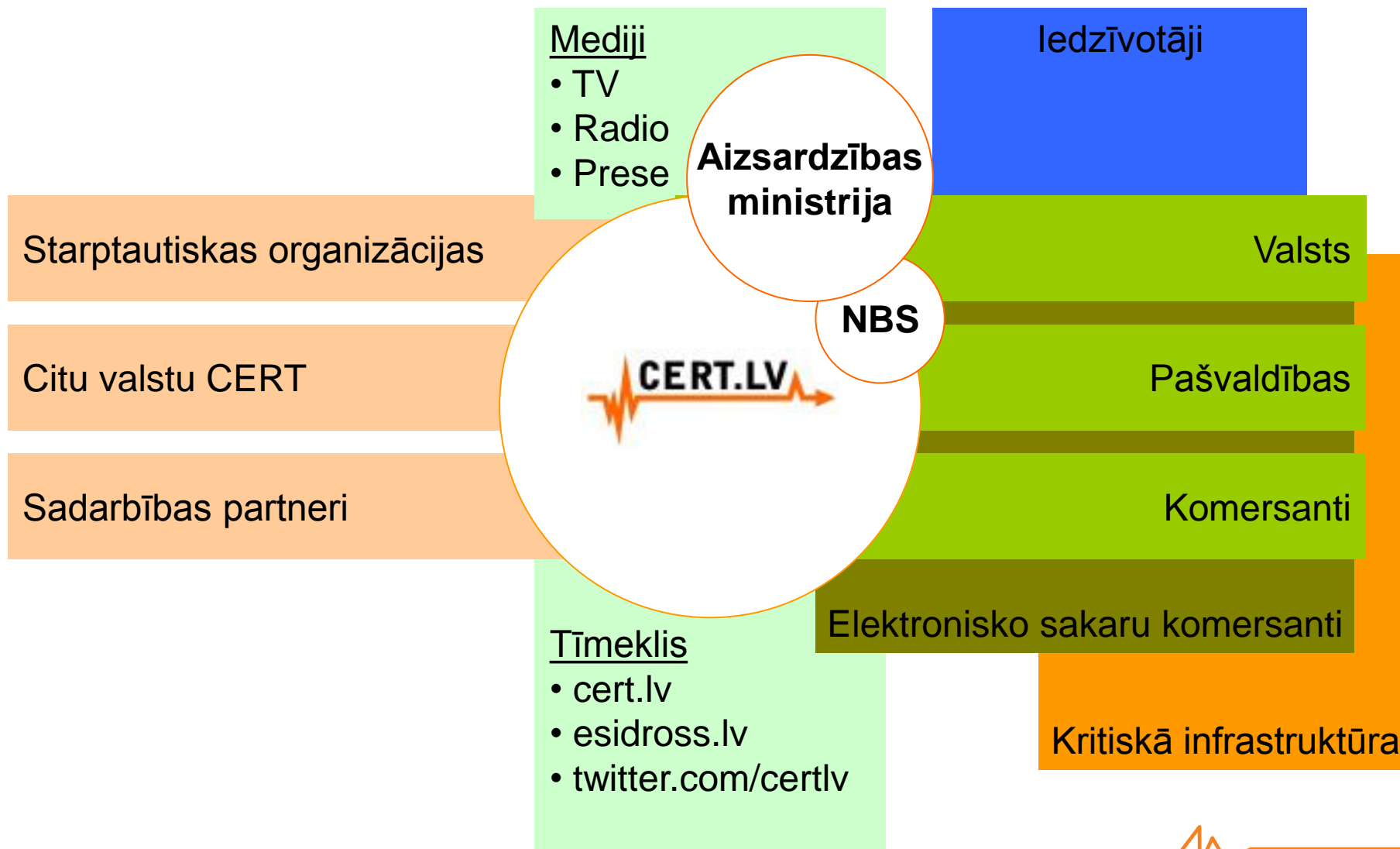
## Saturs

- Informācijas tehnoloģiju drošības likums un saistītie MK noteikumi
- Sadarbības partneri
- Sadarbības principi
- Kopsavilkums

## IT drošības likums un saistītie MK noteikumi

- IT drošības likums – 8.pants
  - Institūcijas vadītājs nosaka atbildīgo personu par IT drošības pārvaldību un par to informē CERT.LV
  - Atbildīgā persona
    - organizē IT drošības pārvaldību,
    - ne retāk kā reizi gadā veic IT drošības pārbaudes,
    - vismaz reizi gadā apmeklē CERT.LV rīkotos seminārus
    - ne retāk kā reizi gadā veic darbinieku apmācību
- MK not. Nr.100 – attiecas uz kritisko infrastruktūru
- MK not. Nr. 327 - attiecas ESK darbību

# Sadarbības partneri



## Informācijas apmaiņa (1)

### Notikumu saraksts katru dienu no sensoriem

- Automātiski datubāzē – pamatā izmanto ESK (ISP)
- Automātiski csv formāta fails uz e-pastu (testa režīmā)
- Incidentu ziņojumi manuāli apstrādāti uz e-pastu

### Ziņojumi uz e-pastu no incidentu *Tracking* sistēmas

- Incidentu ziņojumi manuāli apstrādāti un nosūtīti uz e-pastu

### Brīdinājumi e-pasti

- kalendārie
- uz notikumiem balstīti

### Dokumentu paraugi CERT.LV tīmekļa vietnē

- IDIP
- IT drošības noteikumu paraugs
- Rīcības plāna paraugs

## Informācijas apmaiņa (2)



CERT.LV darbinieka  
sūtīts ziņojums vai zvans

**AIRT**  
**Application for Incident Response Teams**  
CERT.LV

Please enter your username and password  
or authenticate using your SSL [certificate](#)

Username:   
Password:

Copyright (C) AIRT Project



CERT.LV robota  
sūtīts ziņojums ESK  
SQL formātā

**CERT.LV Klientu Reģistrs**

Lietotājvārds

Parole



Sadarbības partneru  
sensori

# Informācijas apmaiņa (3)



CERT.LV darbinieka  
sūtīts ziņojums vai zvans



CERT.LV robota  
sūtīts ziņojums ESK  
SQL formātā



CERT.LV robota  
sūtīts ziņojums  
csv formātā

Not logged in. RT for CERT.LV BEST PRACTICAL

### Login

4.0.17-75-g7e99f2a

Username:

Password:


Login

### CERT.LV Klientu Reģistrs

Lietotājvārds

Parole

Ierīnākt



Sadarbības partneru  
sensori



# CERT.LV ziņojums CSV formātā

```

; 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 domēna nosaukums (ja pieejams)
; source - CERT.LV
; priority - prioritāte (1-zema, 2-vidēja, 3-augsta, 4-loti augsta)
; hash - kontrolsumma (izmantojama papildus informācijas iegūšanai
https://www.esidross.lv/cert-lv-bridinajums/?hash/<hash> )

#Here is data
> 2013-11-26 15:05:48,213.1XX.127.228,0,cutwail,,25,,,CERT.LV,2,04179c059e261fad378dfb3c4571bed4
> 2013-11-27 11:54:41,213.175.126.33,12443,ZeuS,95.211.120.23,80,16265,,/,,CERT.LV,2,7dde355d0e2d97aaf62663aeddcbcad00
> 2013-11-12 04:38:14,213.175.126.3,12443,ZeuS,82.165.37.26,80,0,/drop1,,CERT.LV,2,95b233672a149947265684193536db59
> 2013-11-21 07:31:25,213.175.126.94,12443,downadup,38.102.150.27,80,0,,CERT.LV,2,07b4bba96536b1e3c5bbdfab4e6b0e66
> 2013-10-24 12:07:46,213.175.124.132,0,Ransomware,,,,,CERT.LV,1,d650c0d7e658cc36d13b85343acbbde7
  
```



## Ziņojuma formāta skaidrojums

- ; 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 domēna 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>> )

# Hash kontrolsummas izmantošana esidross.lv

The screenshot shows a Mozilla Firefox browser window displaying the CERT.LV website. The address bar shows the URL: <https://www.esidross.lv/cert-lv-bridinajums/?hash/07b4bba96536b1e3c5bbdfab4e6b0e66>. The website header features the 'esi drošs' logo and a search bar. The main navigation menu includes: Mājas, Darbā, Publikās vietās, Ieteikumi, Par drošību, Bezmaksas risinājumi, Pasākumi, and Notikumi pasaulē.

The main content area displays a security alert titled "CERT.LV brīdinājums". The alert text reads: "Jūsu IP adrese: 2[redacted]4 ir inficēta". Below this, it states: "Incidentā datums: 2013-11-21 09:31:25" and "Datorvīrusa nosaukums: downadup (Ko darīt)".

The "Ko darīt:" section provides instructions: "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."

Additional text includes: "Lai jūsu dators (vai datortīkls) būtu drošībā, iesakām atslēgt inficēto datoru no datortīkla (Internet) un vērsties pie datorspeciālista." and "Lai iztīrītu datoru no datorvīrusa veiciet šādas darbības:".

On the right side, there is a "CERT.LV NIC" logo and a message: "Laipni lūdzam mājaslapā" followed by the heading "ESI DROŠS!". The text below reads: "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..."

The bottom right corner of the browser window shows the IP address "85.254.193.4".

## Kas nepieciešams

- Iestādēm:
  - Atbildīgā persona (elektroniskais pasts)
  - IP adresu lauks
  - labā griba saņemto informāciju, apstrādāt to un sadarboties ar CERT.LV
- CERT.LV: izsūtīt e-pastu ar lūgumu
  - sniegt informāciju par savā atbildībā esošajiem resursiem (ja informācijas nav)
  - aktualizēt informāciju par savā atbildībā esošajiem resursiem (ja informācija ir)
    - aktualizācija paredzēta reizi gadā

## Kopsavilkums

- Ziņojumi CSV formātā no 2014.01.01 tiks izsūtīti visu iestāžu atbildīgajiem par IT drošību, kuru e-pasti un IP adresu laiku ir zināmi
- CERT.LV darbinieku apstrādātie ziņojumi no *Tracking* sistēmas tiks izsūtīti manuāli un parakstīti ar CERT GPG atslēgu
- Ziņojumu apstrādes un izsūtīšanas automatizācija
  - nekavējoši nosūta informāciju
  - nepieļauj kļūdas informācijas apmaiņā
  - portālā esidross.lv atbalsts/palīdzība katram ziņojuma notikumam 24x7
  - atslogo CERT.LV cilvēkresursus
  - strādā arī brīvdienās un svētku dienās

# Paldies par uzmanību!

<http://www.cert.lv>

[cert@cert.lv](mailto:cert@cert.lv)

[egils.sturmanis@cert.lv](mailto:egils.sturmanis@cert.lv)

