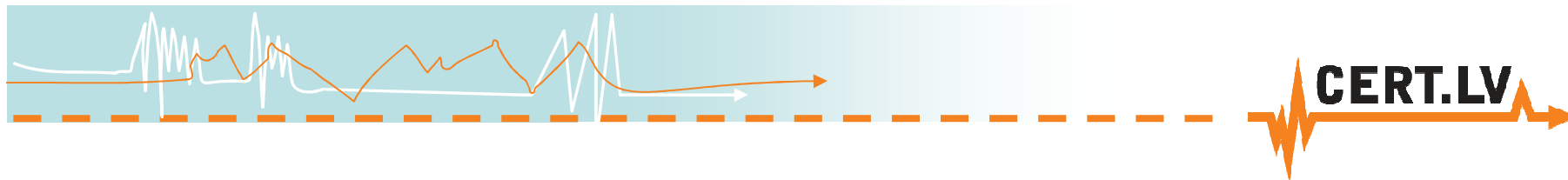




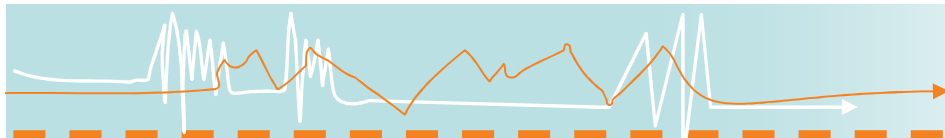
***CERT.LV***  
***pieredze darbā ar drošības incidentiem***  
***un IT drošības mācību organizēšanu***

**11.11.2011., Rīga, ISACA konference**  
**Varis Teivāns - CERT.LV**



# Īsi par CERT.LV

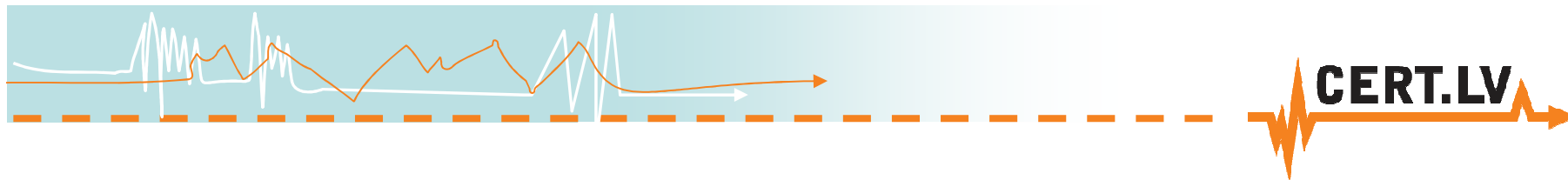




# IT drošības likums

- Pieņemts Saeimā 2010.gada 28.oktobrī
- Stājas spēkā 2011.gada 1.februārī
- Nosaka CERT.LV izveides kārtību
- Paredz MK noteikumu izstrādi 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

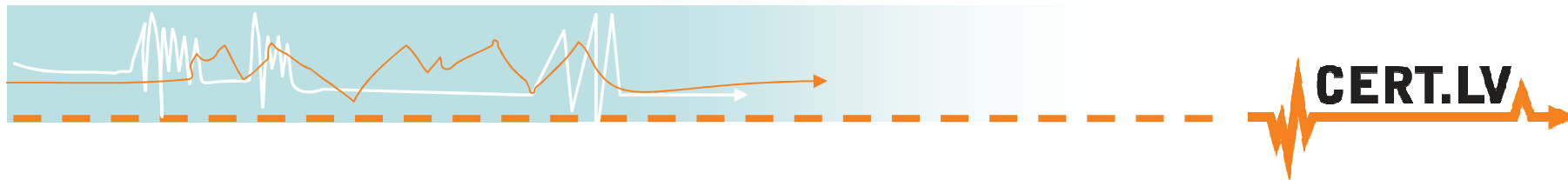




# CERT.LV

- Darbojas saskaņā ar “Informācijas tehnoloģiju drošības likumu” kopš 1.februāra
- Darbības uzdevumi un tiesības tiek deleģētas Latvijas Universitātes aģentūrai “Latvijas Universitātes Matemātikas un informātikas institūts”
- Finansēta no valsts budžeta (87 991 LVL)
- 2011.gadā - 10 darbinieki, ~5 slodzes

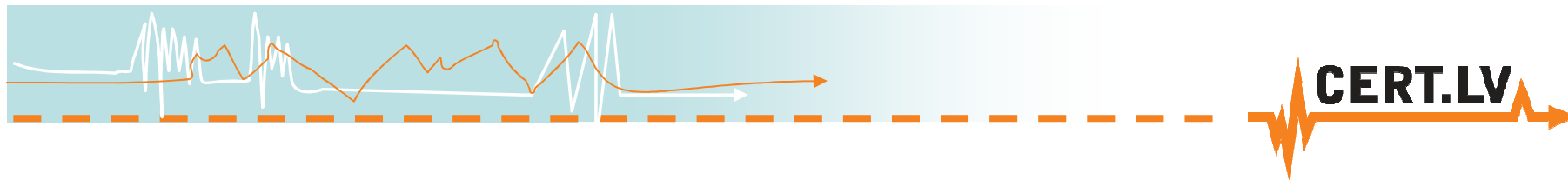




## CERT.LV

- Apvienots CERT NIC.LV + DDIRV
- Veic IT drošības incidentu apstrādi no 2006.gada
- Ir pilntiesīgi *FIRST* dalībnieki no 2009.gada
- Ir *Trusted Introducer* akreditēta vienība no 2007.gada



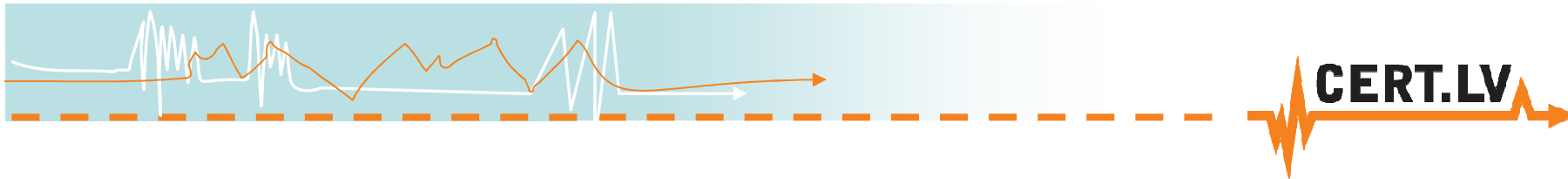


# Pieredze darbā ar IT drošības incidentiem



## IT drošības incidenti

- Apkopota informācija par inficētajām IP adresēm
- Īpaša pieeja valsts un pašvaldību iestāžu inficētajām IP adresēm
- Dažādi informācijas avoti
- Tikai daļa no informācijas kļūst par incidentu ziņojumiem
- Sadarbība ar IPS



## Situācija Latvijā – 31.10.2011.

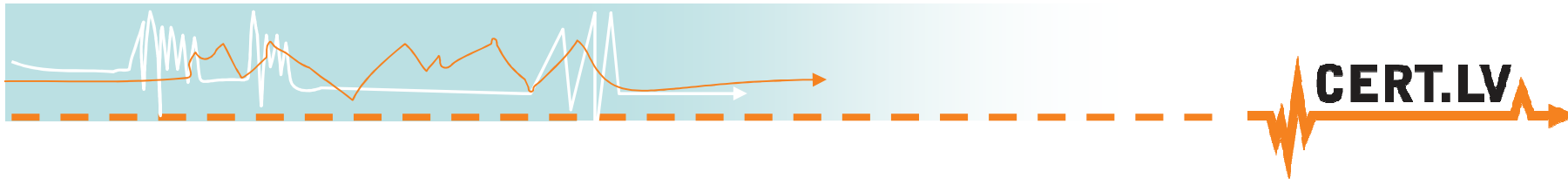
3240 inficēti datori  
(2011.g. martā bija 4582)

Kā skaidrojams samazinājums?

Rustock Botnet pārņemšana?



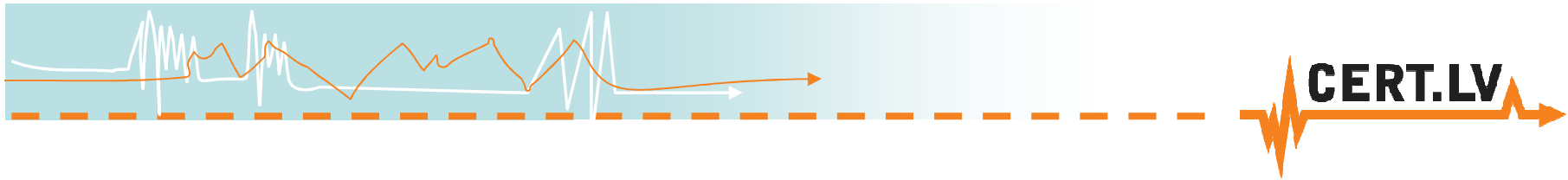




## Kopējās tendences

- Cilvēki sāk ziņot CERT.LV biežāk par incidentiem
- Biežāk ziņo tie, kam ir jau palīdzēts
- Palielinās pikšķerēšanas uzbrukumu daudzums un tie ir ar lielāku ticamību
- Pēc “Sagade” darbinieku aresta ir pamanāmas izmaiņas elektroniskās informācijas telpā



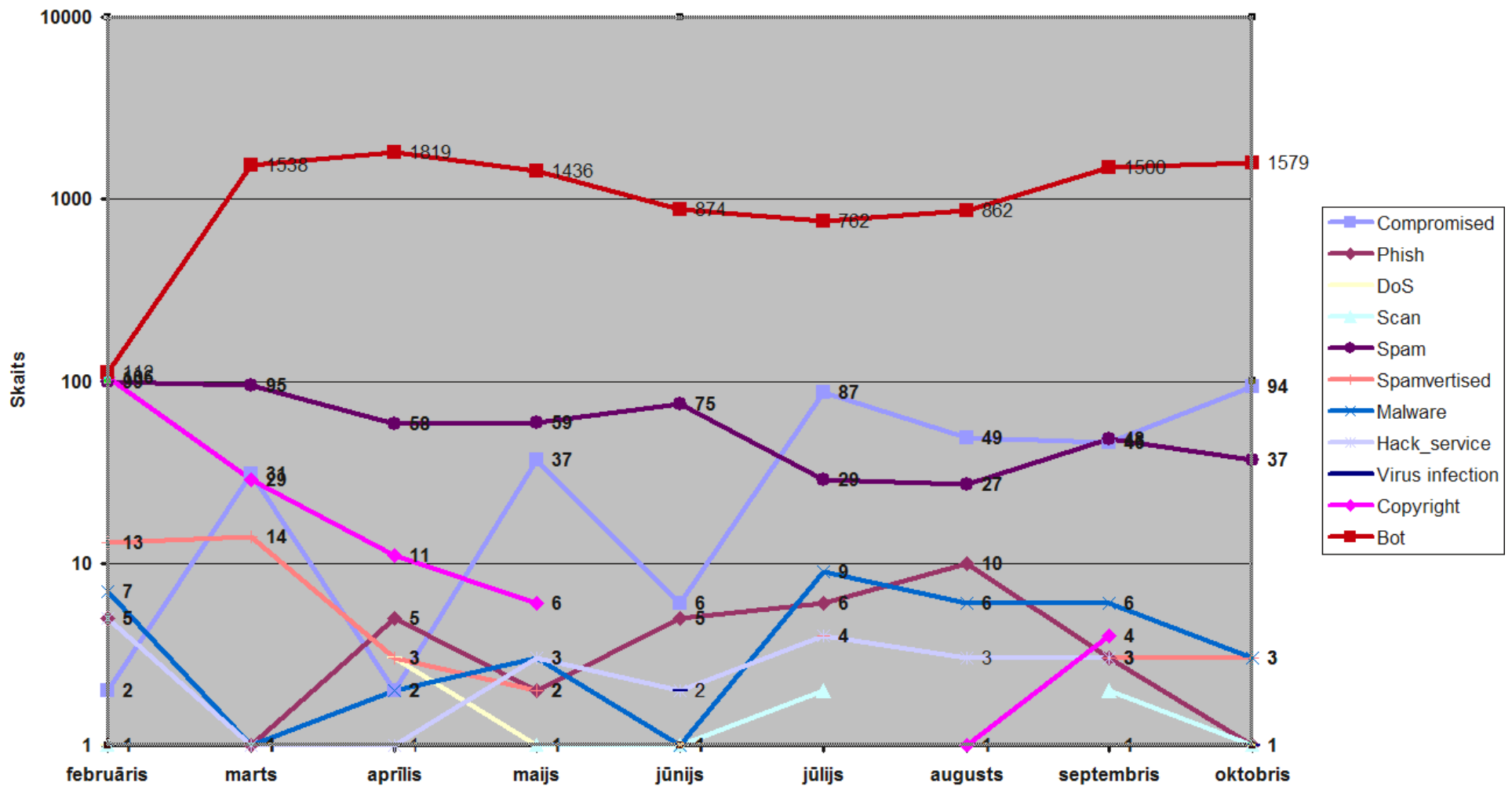


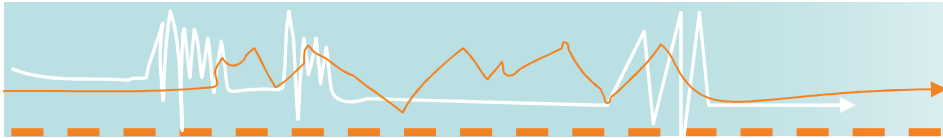
## Incidentu risināšana

- Apstrādāti vairāk nekā 12000 incidenti

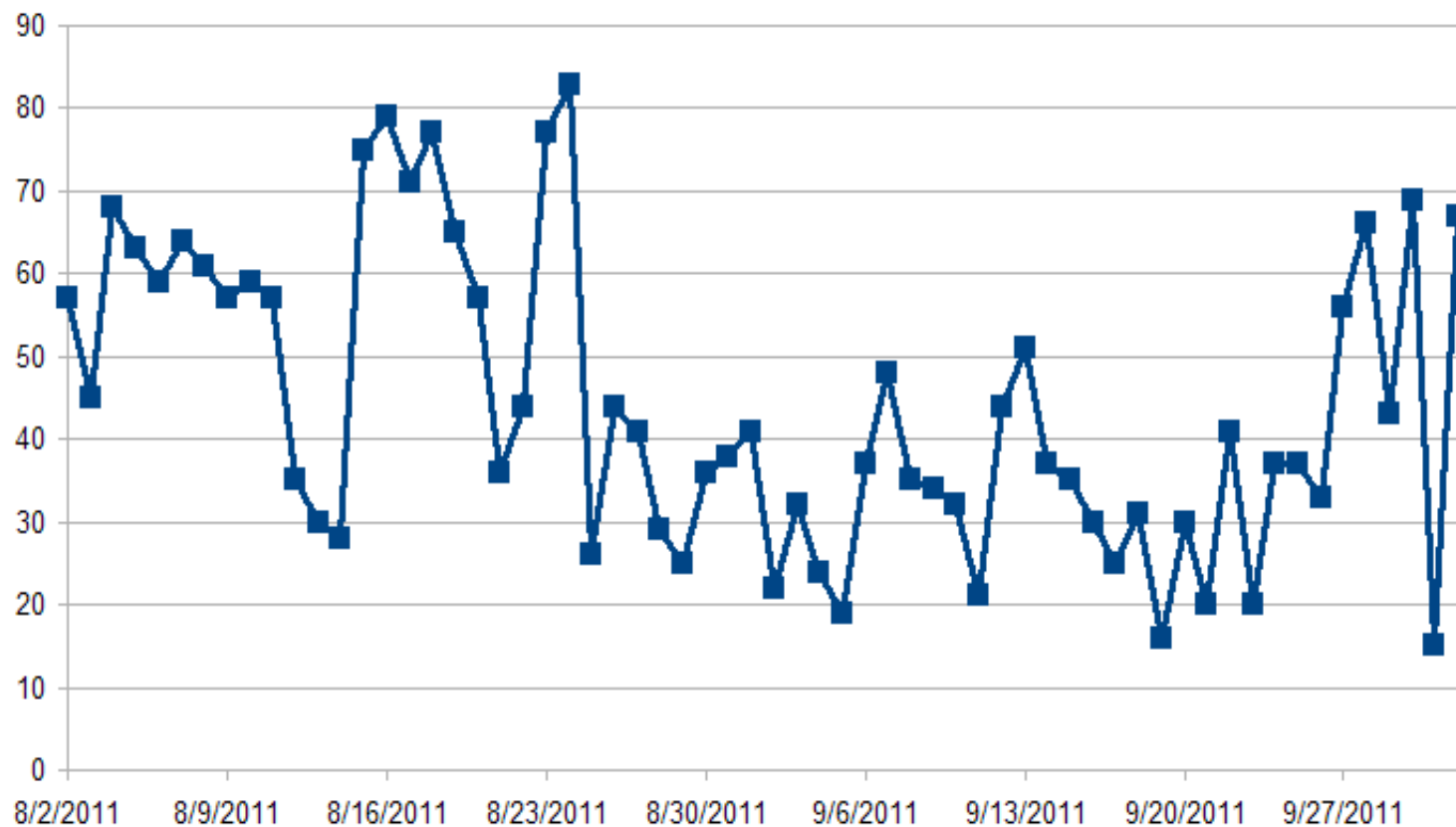


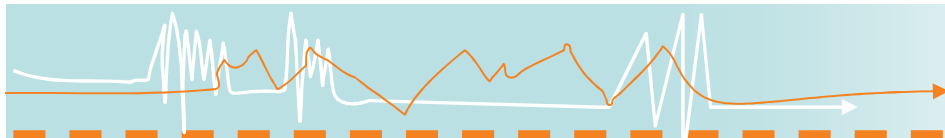
# CERT.LV incidentu statistika – 9 mēneši





## Inficēto valsts un pašvaldību iestāžu IP skaits

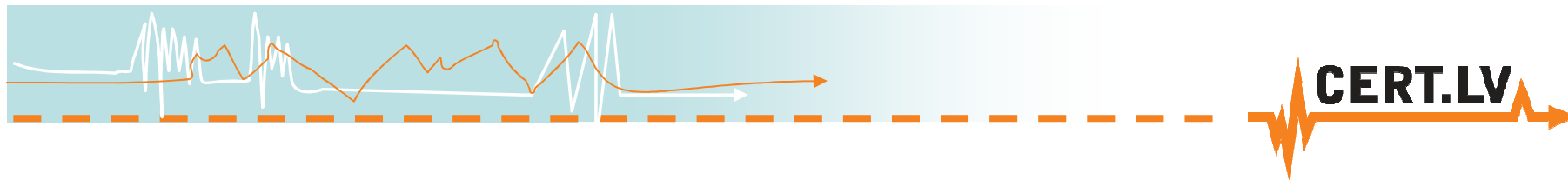




## Incidentu risināšana

- Lielākā daļa – botnet, spam
- Banku lapu pikšķerēšana
- Uzlauzti serveri
- Mājas lapu izķēmošana
- Botnet C&C
- Statistikas un uzbrukumu tendenču uzskaitē

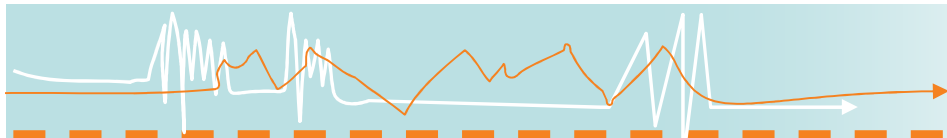




## Dati par inficētajām IP adresēm no CERT.LV

- Tiek veidots datu apmaiņas formāts ar IPS
- Notiek testi sadarbībā ar IPS



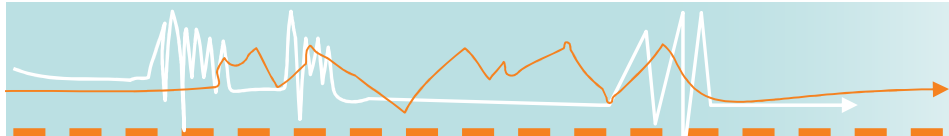


**CERT.LV**

## Nākotnes(?) tendencies

Izmanto šādus  
“datorus” ->





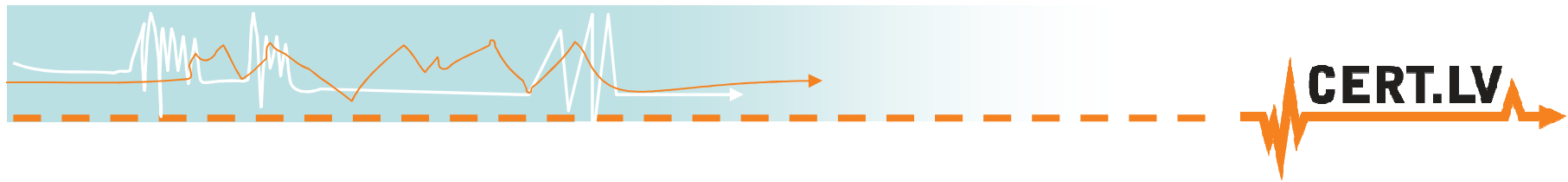
## Nākotnes(?) tendencies



Lai uzbruktu  
šādiem  
“datoriem”

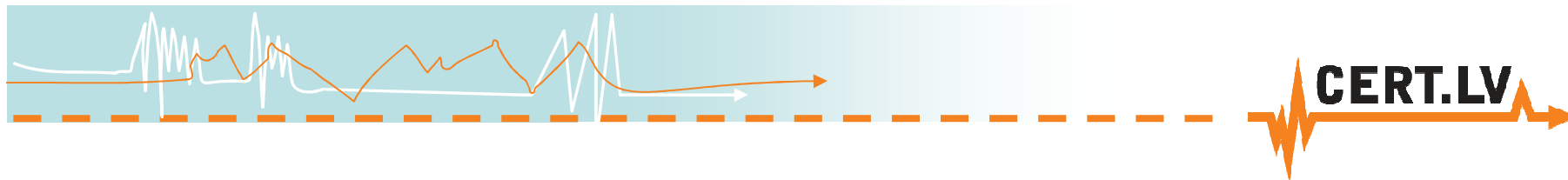






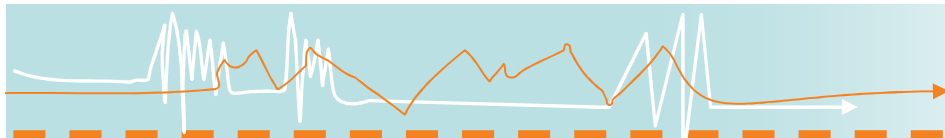
Tā ir šodiena!





# Sabiedrības izglītošana





**CERT.LV**

## Informācija, rekomendācijas

- Mājas lapā – jaunākie vīrusi un ievainojamības
- Raksti, ieteikumi
- Paraugi drošības noteikumiem
- Portāls [www.esidross.lv](http://www.esidross.lv)
- Twitter konts certlv
- Sadarbība ar medijiem



#### Tēmas

- Ap un par drošību (10)
- Darbā (10)
- Ietiekumu tīkls (12)
- Māja (10)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (1)
- Publiskās vietās (11)

#### Saistīta tēma

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Saiksmes ministrija
- LV CSIRT iniciatīva
- Net-Safe Latvija Drošība Interneta centrā

#### Publīcību kalendārs

novembris 2011						
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				
« Okt						

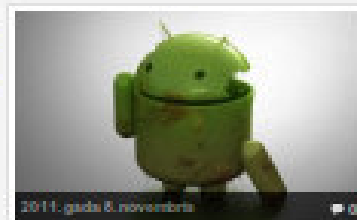
#### Arhīvs



### Android – augošās popularitātes tumšās puses

Mūsdienās zinātnie atklātās tik strauji, ka ne visi ir spējīgi un vērienisti tai izsekot. Bet tā kā ir tāss, kas...

#### AKTUĀLIE RAKSTI



2011. gada 8. novembris

#### Android – augošās popularitātes tumšās puses

Mūsdienās zinātnie atklātās tik strauji, ka ne visi ir spējīgi un vērienisti tai izsekot. Bet tā kā ir tāss, kas...



2011. gada 24. oktobris

#### Paroju pārvaldnieki

Mūsu ikdienā arvien pieaugoša loma ir dažādām parolēm un kodiem, kuri ir jāatceras, lai piekļūtu dažādām sistēmām – e-pastam, internetā...



Lasiet šodien mājlapā!

### ESI DROŠI!

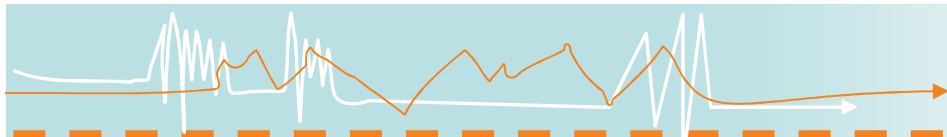
Šī mājlapa ir paredzēta lietotājiem, kuri rūpējas par savu datu drošību un savu drošību internetā.

Māja lapa uzrunā Informācijas tehnoloģiju drošības incidentu novēršanas institūciju (CERT.LV) un tālā informācijas tehnoloģiju speciālisti no LV-CSIRT iniciatīvas grupas sniedz padomus, dalās pieredzi, kā arī ir gatavi atbildēt uz Jūsu jautājumiem par Jūsu datu drošību un Jūsu drošību internetā.

#### Jasmināte raksti

- Android – augošās popularitātes tumšās puses
- Paroju pārvaldnieki
- Kas ir SQL injekcijas?
- Kas ir XSS uzbrukumi?
- Tīmekļa vietnes drošība un tās izplatītākie tās drošības apdraudējumi

#### Jasmināte komentāri



**CERT.LV**



*Mēs atbildam par savu drošību  
informācijas tehnoloģiju laikmetā*

Meklēt...



Mājās Darbā Publiskās vietās Ieteikumi Pasākumi Notikumi pasaulē Par drošību Raksti



#### Tēmas

- Ap un par drošību (5)
- Darbā (7)
- Ieteikumu lāde (9)
- Mājās (15)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (1)
- Publiskās vietās (7)

#### Saišu lenta

- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija – CERT.LV
- LR Satiksmes ministrija



#### VIDEO: Kā justies droši elektroniskā vidē?

Jūties droši elektroniskā vidē from EsiDrossLV on Vimeo. CERT.LV piedāvā jums noskatīties Latvijas Universitātes Informācijas sistēmu drošības pasniedzējas Ilzes Murānes...

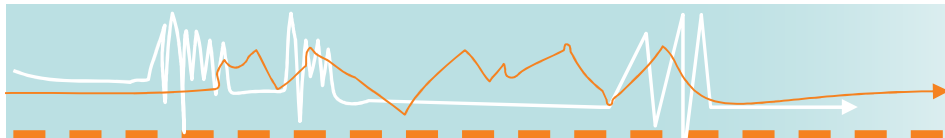
**Uzmanību!** Saskaņā ar CERT.LV datiem, Jūsu dators ar IP adresi [redacted] ir inficēts ar datorvīrusu! [Vairāk informācijas.](#)



Laipni lūdzam mājaslapā

#### ESI DROŠS!

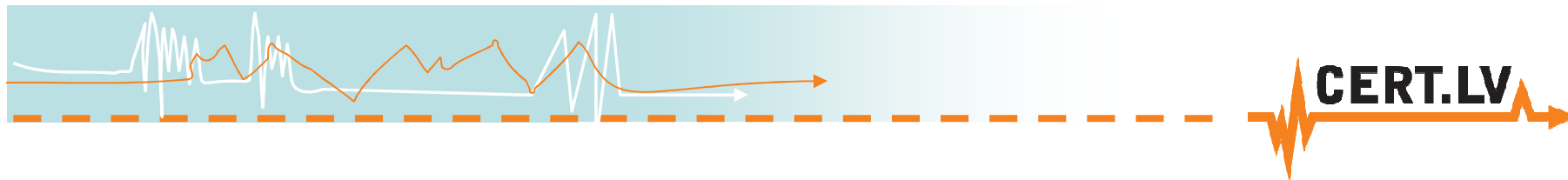
Šī mājaslapa ir paredzēta ikvienam, kurš rūpējas par sava datora drošību un savu drošību internetā.



## Pasākumi, prezentācijas

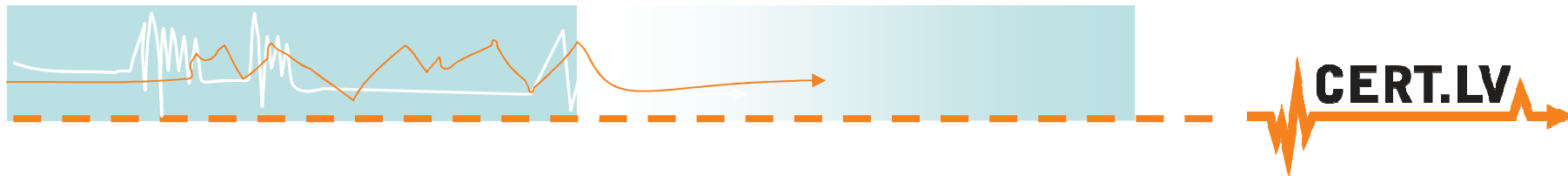
- “Esi drošs – 1” un “Esi drošs - 2” semināri valsts un pašvaldību iestāžu atbildīgajām personām
- Seminārs Interneta pakalpojumu sniedzējiem
- IT drošības mācības
  - Teorētiskās
  - Tehniskās
- Citi pasākumi
  - ENISA seminārs par IT drošības mācību organizēšanu
  - Sanāksme ar NATO CCDCOE par likumdošanas jautājumiem





# Tehnisko IT drošības mācību organizēšanas pieredze



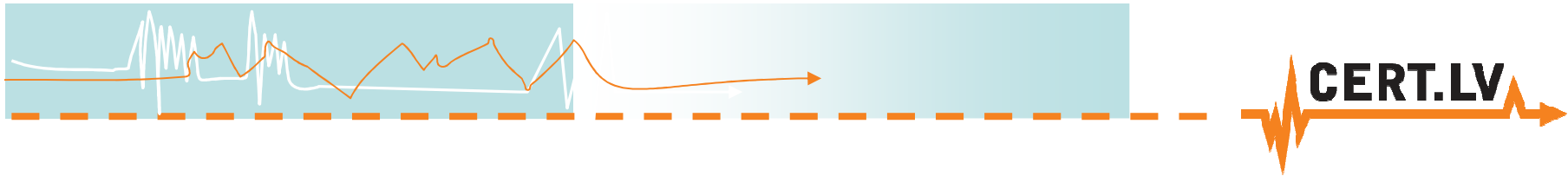


# CERT.LV Tehniskās mācības

- Realizētas pateicoties cilvēku entuziasmam un pašizliedzībai
- Vides apraksts:
  - 2 uzbrūkošās komandas (RED teams)
  - 3 komandas, kas aizstāv infrastruktūru (BLUE teams)
  - Katra komanda savā telpā
  - Blue Team: Jauns un strauji augošs programmatūras izstrādes uzņēmums "BlueTeamTechnologies"







# CERT.LV Tehniskās mācības

- Vides apraksts:

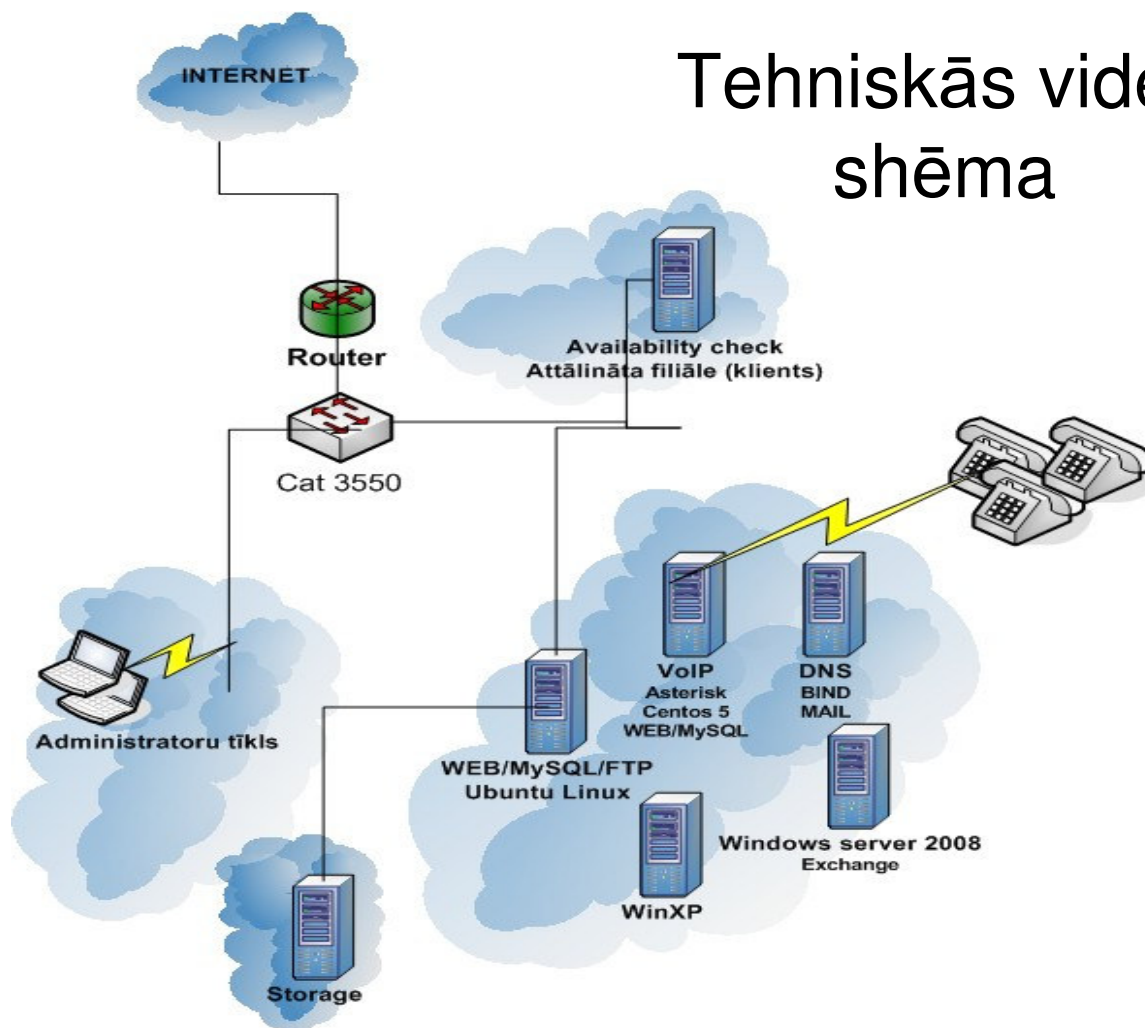
Router, switch, 4 Linux servers hosting WEB,  
FTP, DNS, DB, VoIP gateway, IP phones,  
1 windows 2008 server, 1 XP SP3

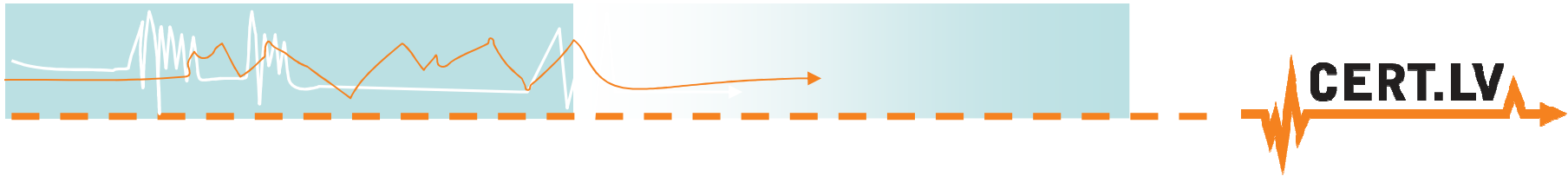
Jebkura iekārta, kas pieslēgta pie mācību vides



# CERT.LV Tehniskās mācības

## Tehniskās vides shēma





# CERT.LV Tehniskās mācības

- Katra komanda saņēma tikai īsu aprakstu un tehniskās vides shēmu dažas dienas pirms mācībām.
- Komandām bija iespēja ierasties dienu iepriekš.
- Spēles noteikumi ir zināmi gan Sarkanām, gan Zilām komandām
- Sarkanām komandām tiek atļauta piekļuve Zilo komandu infrastruktūrai 1 stundu pēc Zilo komandu darba sākuma
- Komunikācija – panākumu, novērojumu, pārkāpumu ziņošana





# CERT.LV Tehniskās mācības

## secinājumi



- Tehniskā vide ir nepieciešama daudz jaudīgāka
- 2 fiziski serveri konfigurācijā 2.6 GhZ quad core CPU un 500MB RAM uz katru virtuālo mašīnu (Linux) 1GB (WIN) ir nepietiekami
- 2 sarkanās komandas nav slikta ideja, bet ir jāpadomā par tādām lietām kā:
  - Sarkanās komandas sāk bloķēt viena otru iegūstot kontroli zilajā vidē
  - Sarkanās komandas uzbrūk viena otrai



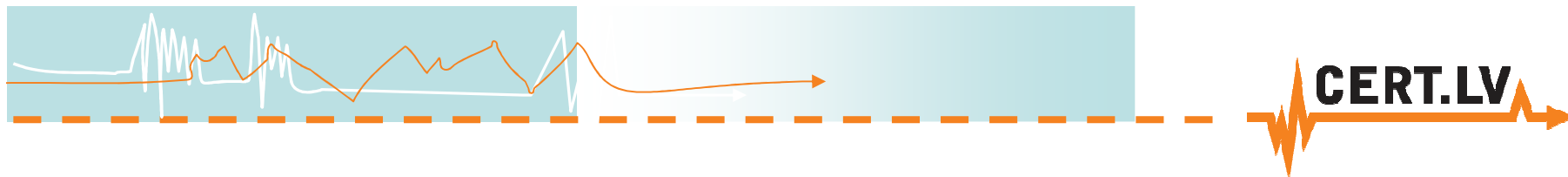


# CERT.LV Tehniskās mācības secinājumi



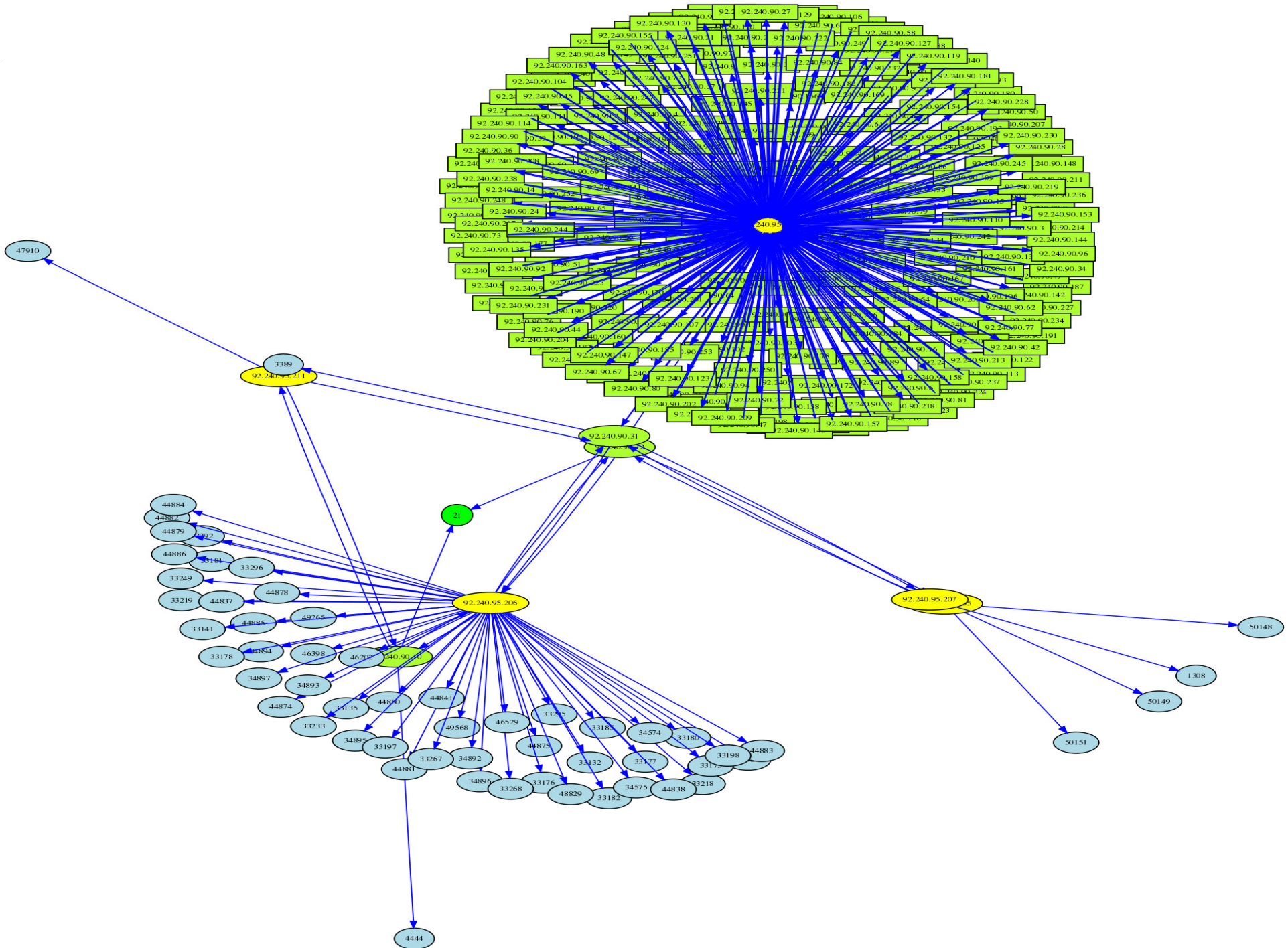
- Spēles noteikumu definīcija. Sarkanām komandām jāzin Zilo komandu spēles noteikumi
- Vērtēšanas sistēma
- Nebūtiski, bet iespējams nākotnē jāizvairās no nosaukuma “[Zilā komanda](#)”

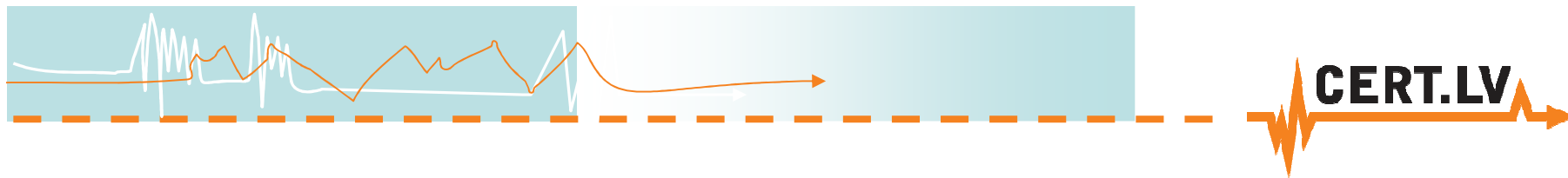




# Uzbrukuma vizualizācija



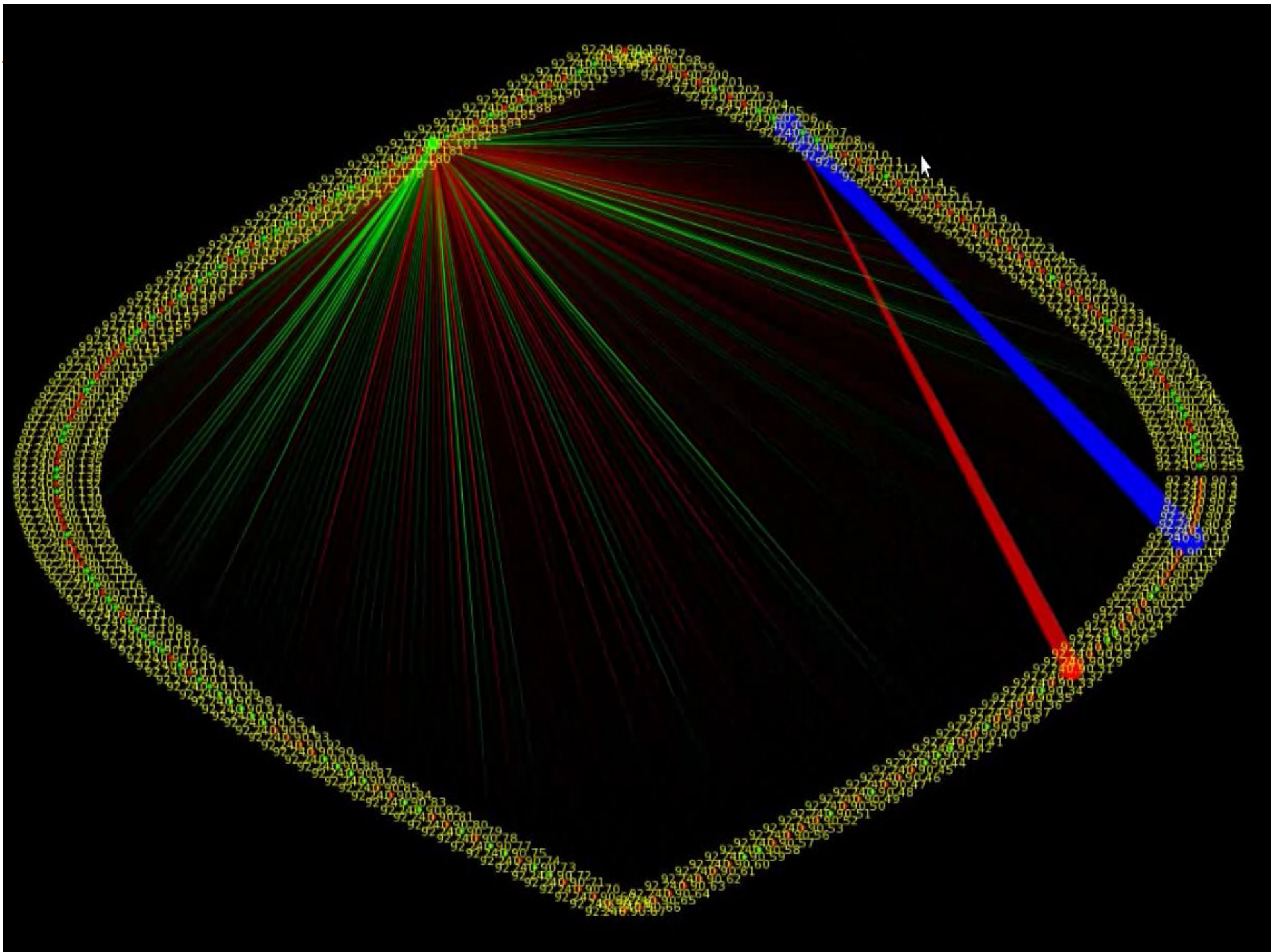


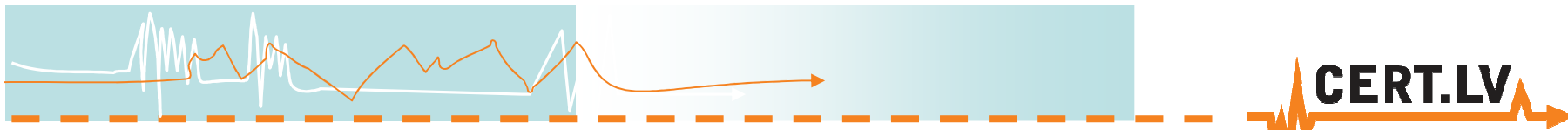


# Video demonstrācija









# Sarkanās komandas pirmā viltīgā rīcība iegūstot kontroli pār sistēmu :)

```
#cd dnsadm
```

```
#ls -l
```

```
#ifconfig
```

```
#adduser certivo
```

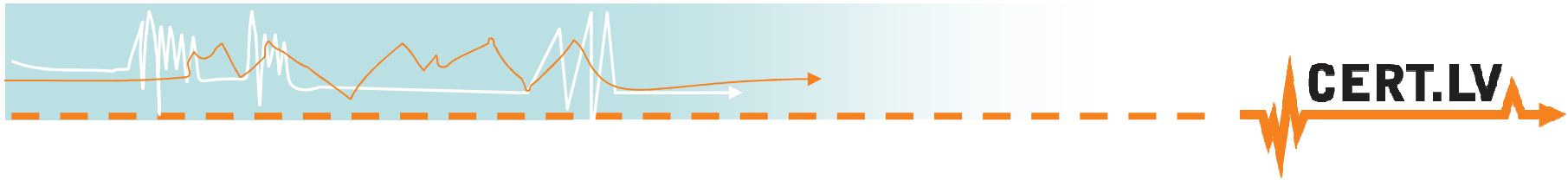
```
Adding user `certivo' ...
```

```
Adding new group `certivo' (1001) ...
```

```
Adding new user `certivo' (1001) with group `certivo' ...
```

```
#iptables .... - DESTRUKTĪVI, bet var saprast iemeslus – ir  
konkurents
```





## Citas aktivitātes

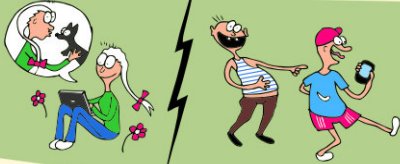
- Izglītojošie plakāti
- Sadarbība ar radio, TV, presi
- Akadēmiskā darbība



# Vai esi Interneta profiņš?

## Apdomā pirms publisko attēlus internetā!

Padomā, vai šie attēli neaizskar un nekaitē Tev, Taviem draugiem, klasesbiedriem, vecākiem vai jebkurai 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 savādāku paroli. Veido to pietiekami sarežģītu, lai to nevarētu uzminēt pat tie cilvēki, kas Tevi labi pazīst!



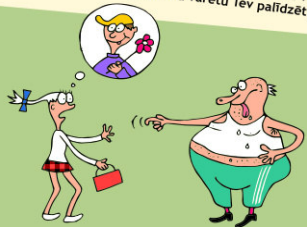
## Neatklāj datus par sevi nepazīstamiem cilvēkiem!

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.



## 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! Nepiekriti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviens, kas nepieciešamības gadījumā varētu Tev palīdzēt.



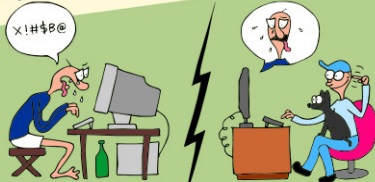
## Darbības internetā nav anonīmas!

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



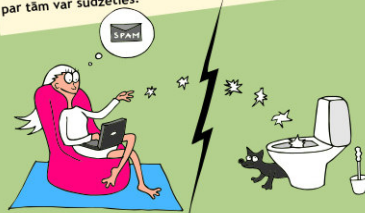
## Neraksti aizkarošus komentārus!

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



## Mēstules nav vēstules!

Ignorē mēstules, ko saņem nepazīstamiem cilvēkiem. Neatsaucies to „villinošajiem” piedāvājumiem. Visbiežāk tie ir mēģinājumi izkrāpt Tavu naudu. Mēstules var izfiltrēt un par tām var sūdzēties.



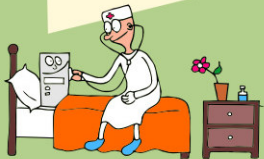
## Neiepērcies internetā bez vecāku ziņas!

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



## Rūpējies par datora veselību!

Neinstalē nezināmas izcelsmes programmas uz datora, ko Tu lieto. Programma ļoti viegli var izlikties par spēli, bet patiesībā būt vīrus, 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](mailto:zinojumi@drossinternets.lv) vai [abuse@nic.lv](mailto:abuse@nic.lv)

CERT.LV



**Jūsu darbības internetā nav anonimas!**

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.

Labi

**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

**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

**Pārdomājiet, kādas fotogrāfijas publicējat internetā un kā to publicēšana kādu dienu var ietekmēt Jūsu dzīvi!**

Piemēram, attiecības ar draugiem, radniekiem, kolēģiem, esošajiem vai nākamajiem darba devējiem.

OK

**Ne Jūsu banka, ne kāds cits pakalpojumu sniedzējs nekad neizmanto 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.

Labi

**Īpaši svarīgas vai sensitīvas informācijas datu pārsūtīšanai izmantojiet šifrēšanu, piemēram, PGP.**

Visa informācija par to atrodama internetā.

OK

**Uzmaniet bērnus, kas darbojas internetā, sociālajos tīklos, sarakstās ar tiklā iepazītiem cilvēkiem.**

Neesiet vienaldzīgi! Pārlicinieties, ka bērni ir informēti par to, kā jāuzvedas internetā, ko drīkst un ko nevajadzētu darīt.

Labi

**Pirkumiem internetā labāk izmantojiet atsevišķu kredītkarti. Ieskaitiet kartē tik naudas, cik paredzat tērēt.**

Tas pasargās Jūs no krāpniekiem, kas vēlēšies izmantot Jūsu kredītkarti saviem pirkumiem.

OK

**Pirms veikt pirkumus internetā pārlicinieties, vai attiecīgās mājas lapas īpašniekam var uzticēties!**

Palasiet, ko par tirgotāju saka citi interneta lietotāji. Pirms ievadīt savas kredītkartes datus pārlicinieties, 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.

Labi

**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 parolu glabāšanas programmām!

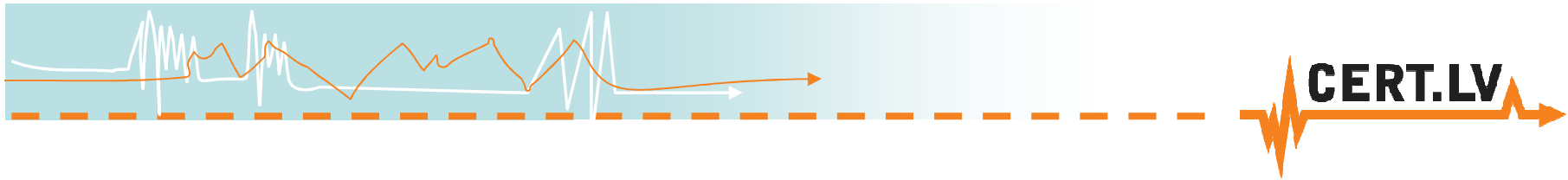
OK

Statins - Maģis 1234, © 2010

CERT **NIC** .LV

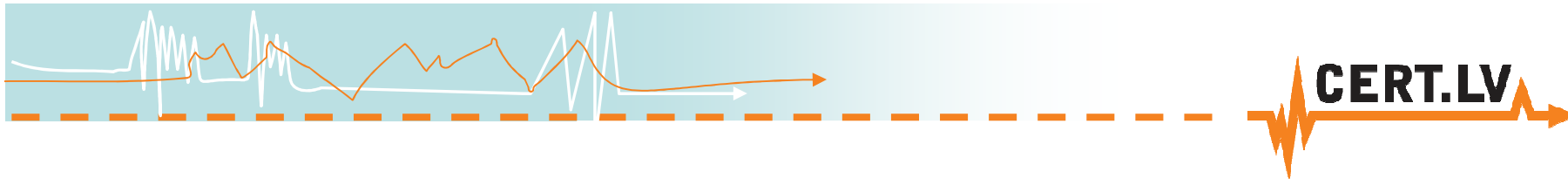
VIRTUĀLĀ REALITĀTE

VIRTUALA REALITATE



# Nākotnes plāni





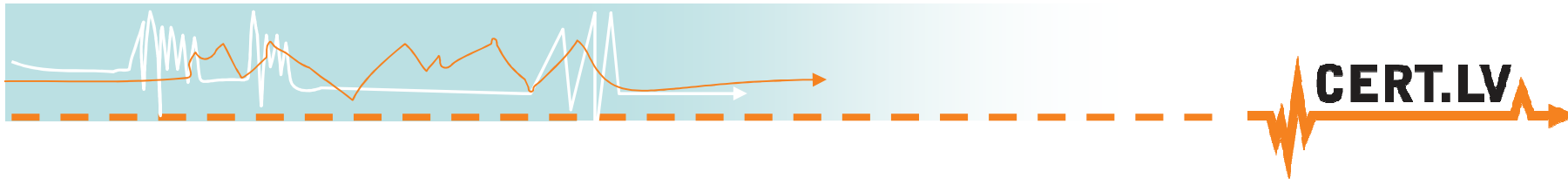
## CERT.LV nākotnes plāni

- Palielināt tehniskās iespējas
- Nostiprināt sadarbību ar valsts un pašvaldību institūcijām
- Uzlabot sadarbību ar Interneta pakalpojuma sniedzējiem

Uzturēt izglītošanās portālu [www.esidross.lv](http://www.esidross.lv)

- Rīkot regulārus seminārus un mācības
- Sadarbība ar medijiem, presi – palielināt redzamību
- Aktivizēt LV-CSIRT grupu





## Tuvākie pasākumi

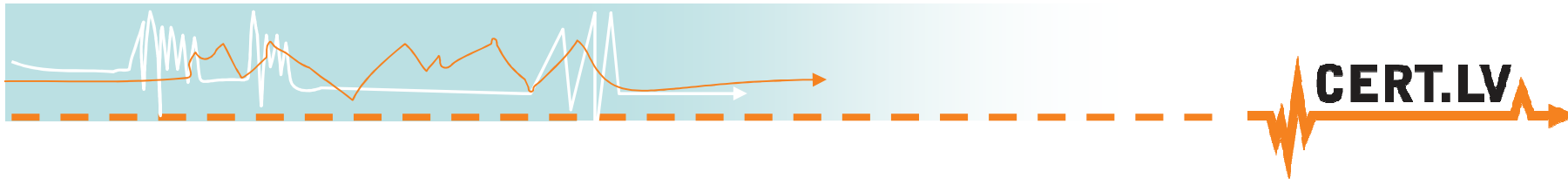
- 22.novembris – “Esi Drošs – 2” seminārs

### Plāni:

- 2. teorētiskās mācības
- LV-CSIRT grupas pasākums
- Netflow datu analīzes seminārs







# Paldies par uzmanību!

<http://ww.cert.lv/>  
[cert@cert.lv](mailto:cert@cert.lv)  
[varis.teivans@cert.lv](mailto:varis.teivans@cert.lv)

