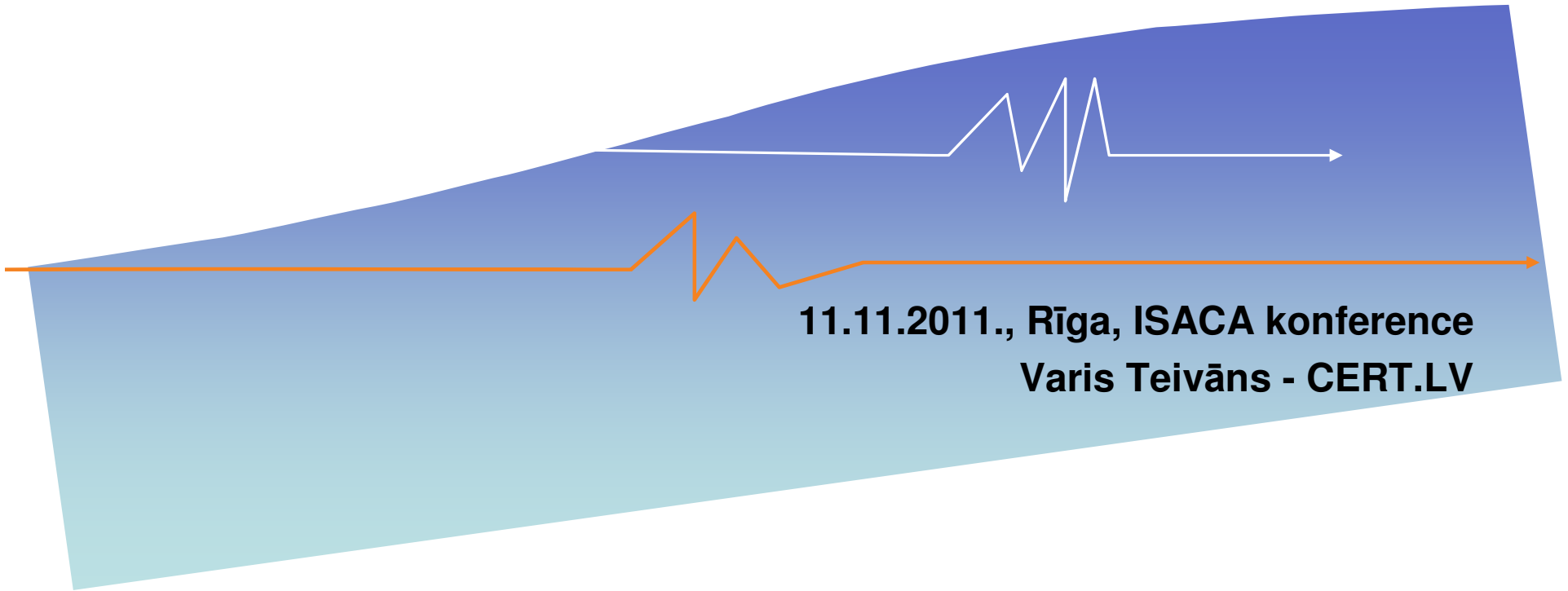
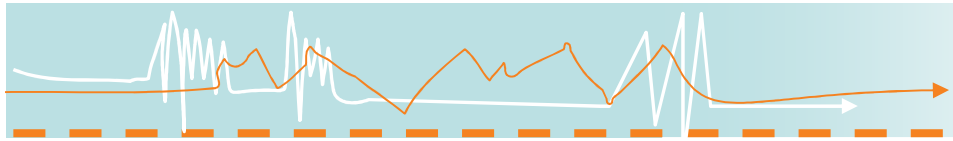
CERT.LV pieredze darbā ar drošības incidentiem un IT drošības mācību organizēšanu



11.11.2011., Rīga, ISACA konference

Varis Teivāns - CERT.LV



CERT.LV

Īsi par CERT.LV

IT drošības likums

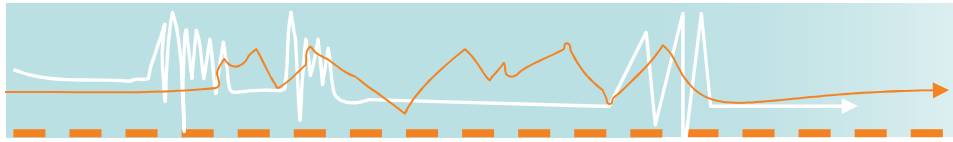
- Pieņemts Saeimā 2010.gada 28.oktobrī
- Stājas spēkā 2011.gada 1.februārī
- Nosaka CERT.LV izveides kārtību
- Paredz MK noteikumu izstrādi par
  - Kritiskās infrastruktūras drošības pasākumu plānošanu (spēkā no 2011.gada 1.februāra)
  - Elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanu (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



CERT.LV

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?

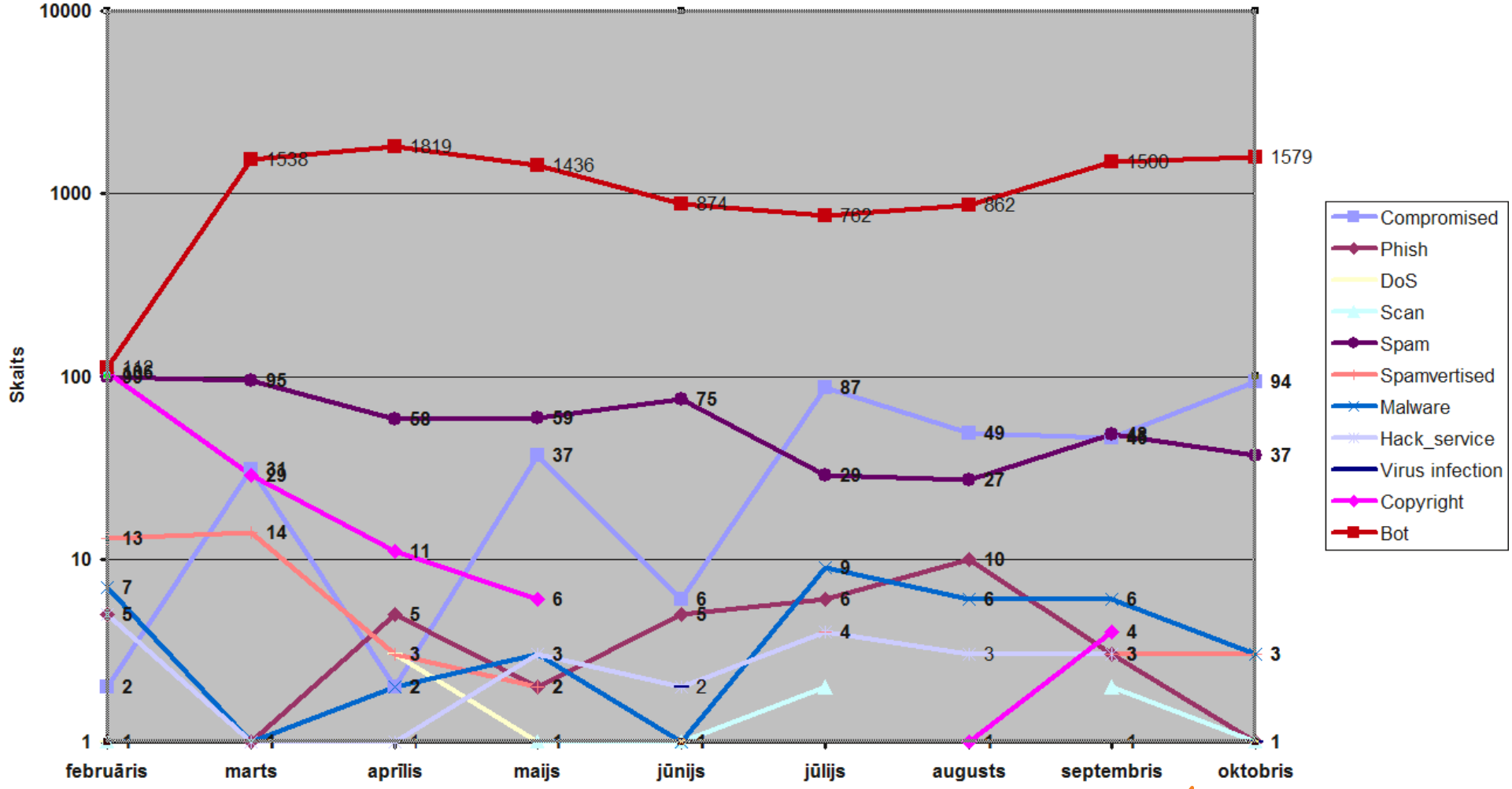
Kopējās tendences

- 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

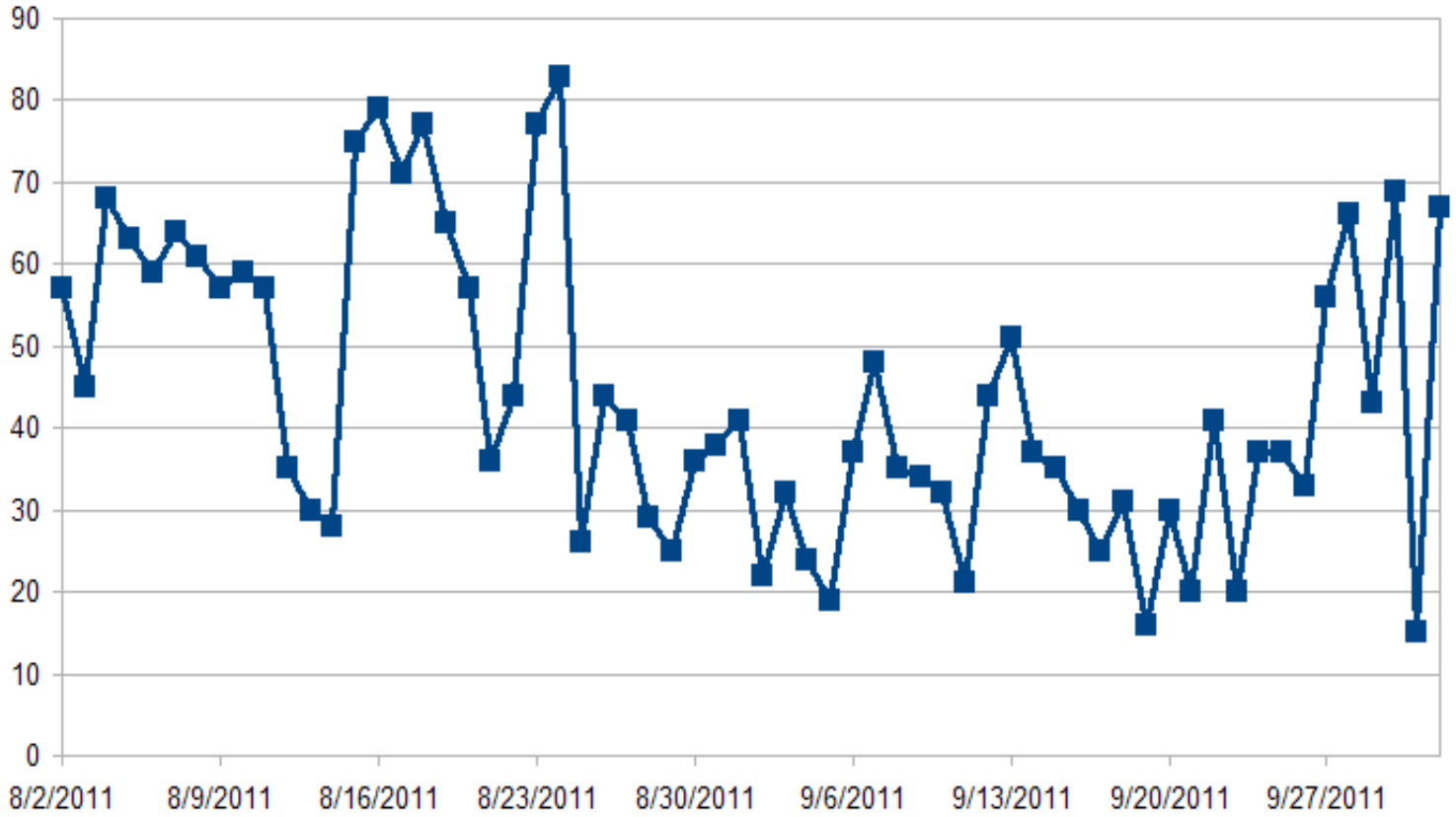
Incidentu risināšana

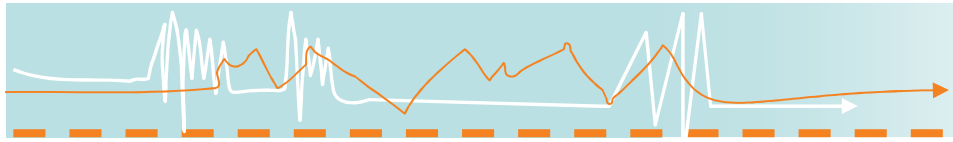
- Apstrādāti vairāk nekā 12000 incidenti

CERT.LV incidentu statistika – 9 mēneši



Inficēto valsts un pašvaldību iestāžu IP skaits





CERT.LV

Incidentu risināšana

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

Dati par inficētajām IP adresēm no CERT.LV

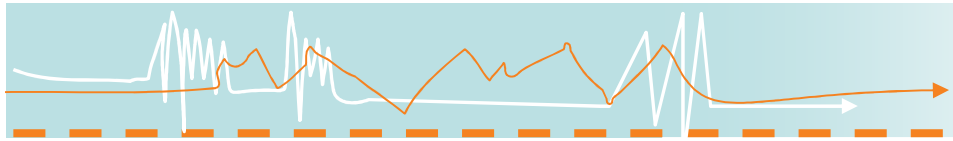
- Tiek veidots datu apmaiņas formāts ar IPS
- Notiek testi sadarbībā ar IPS

Nākotnes(?) tendences

Izmanto šādus “datorus” ->

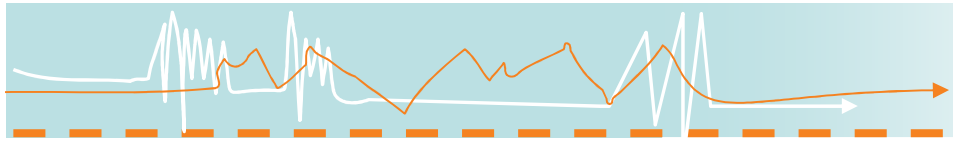
Nākotnes(?) tendences

Lai uzbruktu šādiem “datoriem”



CERT.LV

Tā ir šodiena!



CERT.LV

Sabiedrības izglītošana

Informācija, rekomendācijas

- Mājas lapā – jaunākie vīrusi un ievainojamības
- Raksti, ieteikumi
- Paraugi drošības noteikumiem
- Portāls www.esidross.lv
- Twitter konts certlv
- Sadarbība ar medijiem

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 (10)
- Darbā (10)
- Ieteikumu lāde (12)
- Mājās (10)
- Notikumi pasaulē (1)
- Pasākumi un notikumi (1)
- Publiskās vietās (11)

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 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				

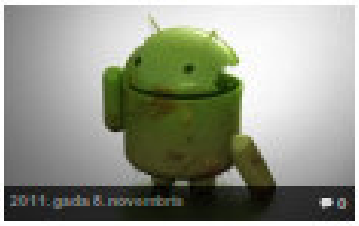
« Okt

Arhīvi

Android – augošās popularitātes tumšās puses

Mūsdienās zinātne attīstās tik strauji, ka ne visi ir spējīgi un ieinteresēti tai izsekot. Bet tā kā ir lietas, kas...

AKTUĀLIE RAKSTI



Android – augošās popularitātes tumšās puses

Mūsdienās zinātne attīstās tik strauji, ka ne visi ir spējīgi un ieinteresēti tai izsekot. Bet tā kā ir lietas, kas...

Paroļu pārvaldnieki

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

CERT.LV

NIC

Laipni lūdzam mājaslapā

ESI DROŠS!

Šī mājaslapa ir paredzēta ikvienam, kuru 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

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

Jaunākie komentāri

CERT.LV

esi drošs

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.

CERT.LV NIC

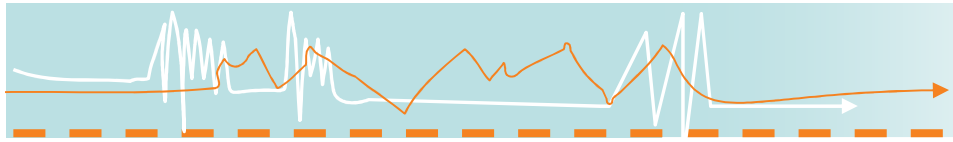
Laipni lūdzam mājaslapā

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



CERT.LV

Tehnisko IT drošības mācību organizēšanas pieredze

CERT.LV Tehniskās mācības

- Realizētas pateicoties cilvēku entuziasmam un pašaizliedzībai
- 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

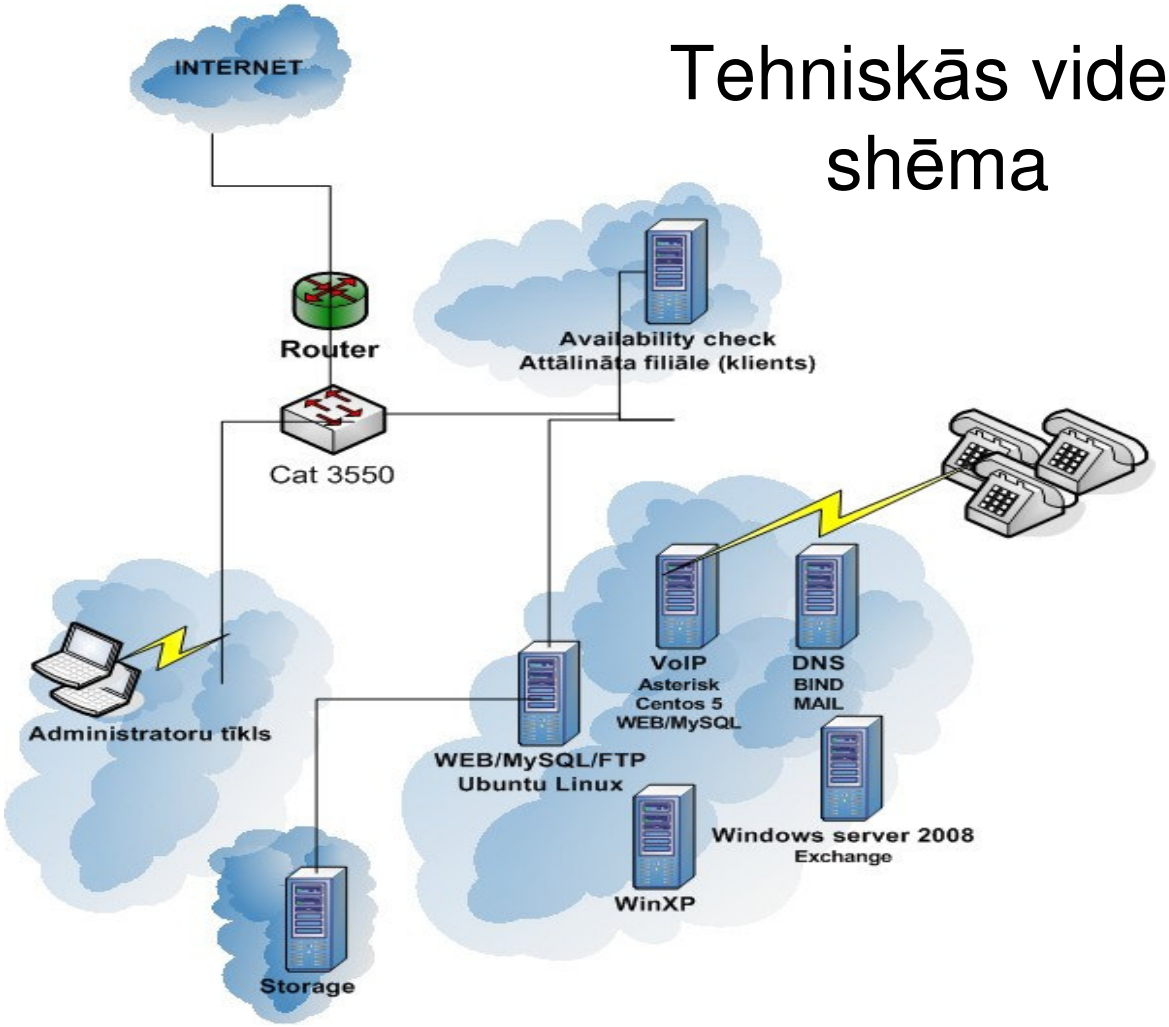
- Vides apraksts:

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

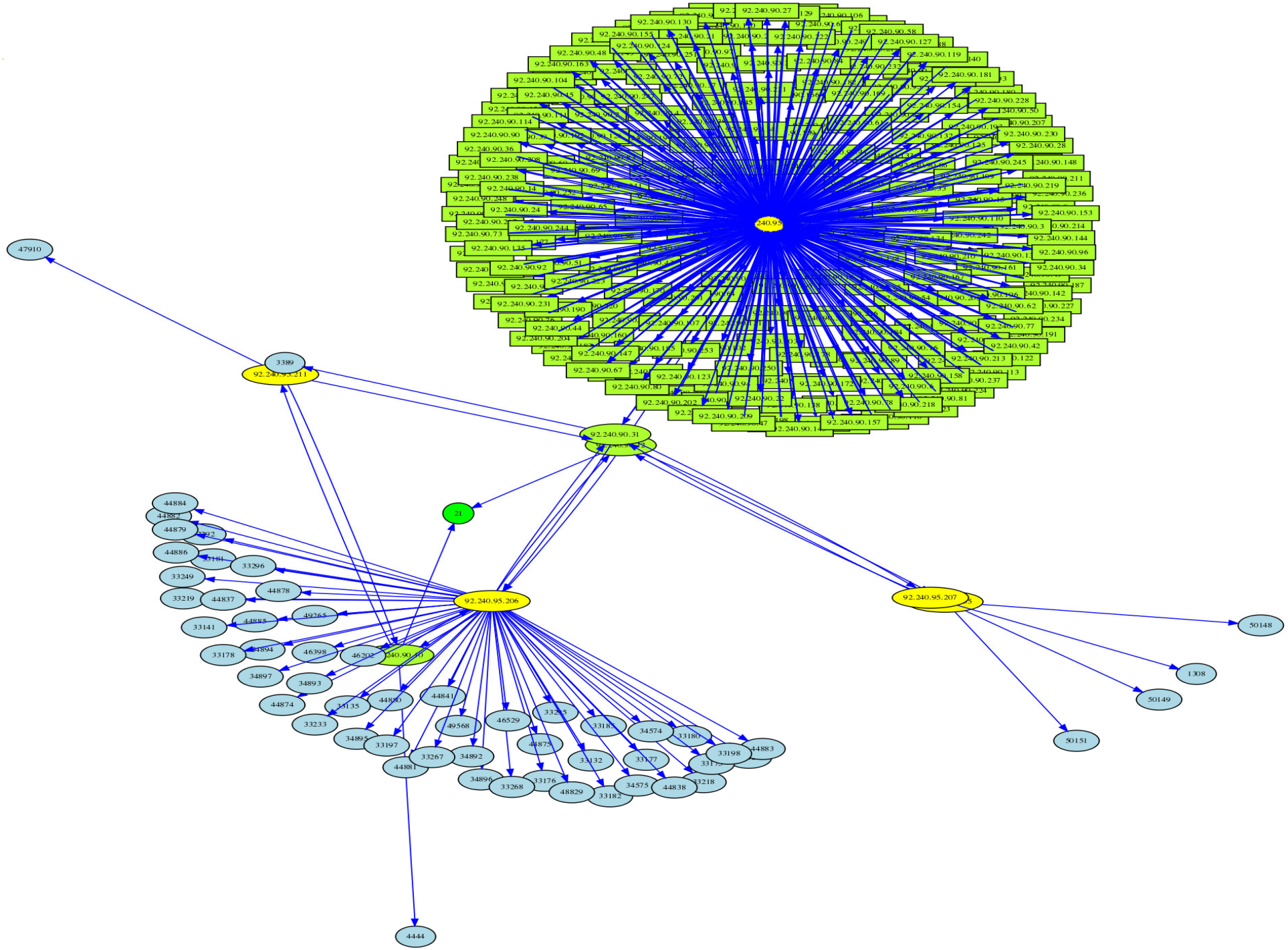
- Tehniskā vide ir nepieciešama daudz jaudīgāka
- 2 fiziski serveri kofigurācijā 2.6 GhZ quad core CPU un 500MB RAM uz katru virtuālo mašīnu (Linux) 1GB (WIN) ir nepietiekami
- 2 sarkanās komandas nav slikta ideja, bet ir jāpadomā par tādām lietām kā:
- Sarkanās komandas sāk bloķēt viena otru iegūstot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

CERT.LV Tehniskās mācības

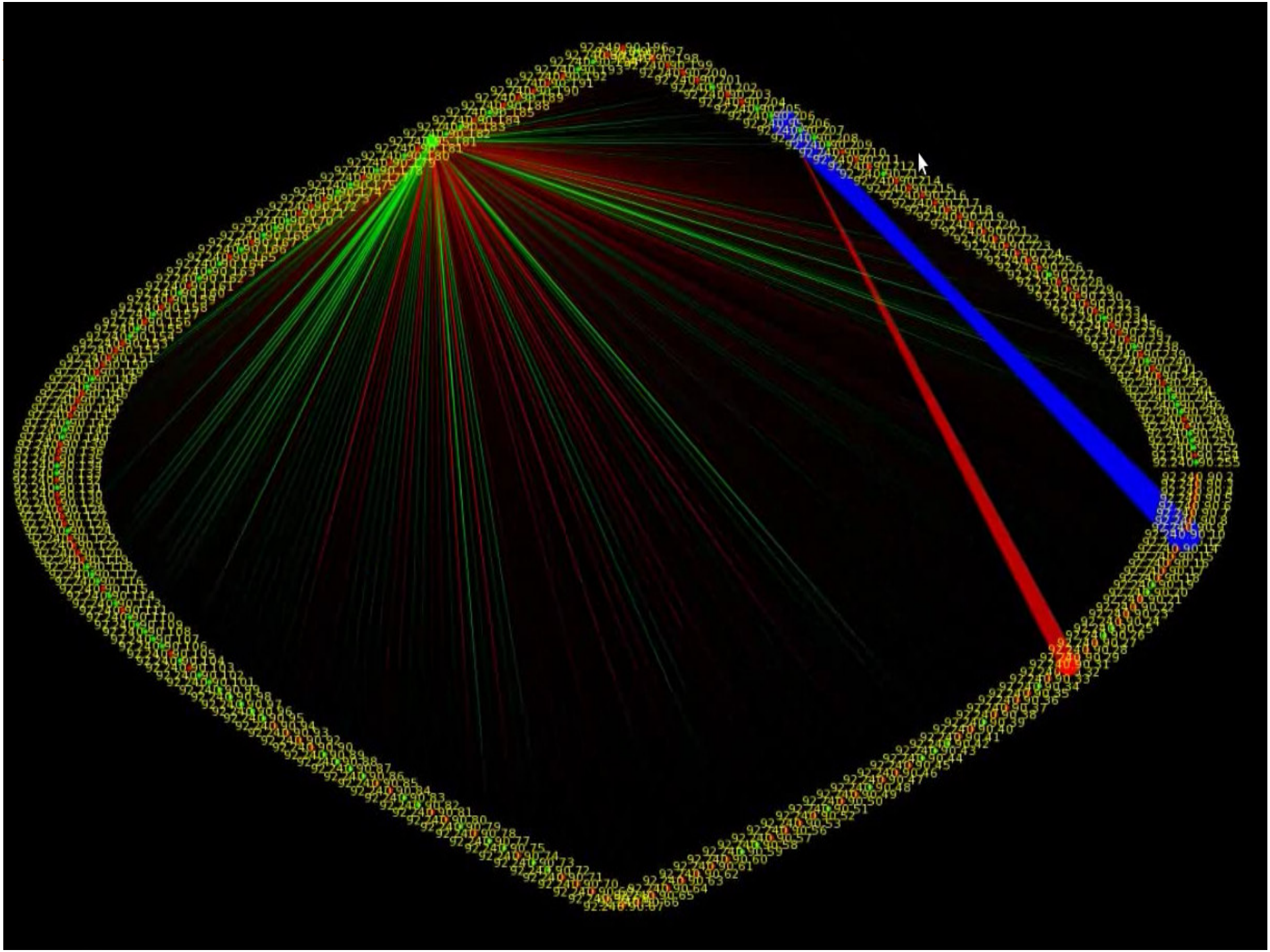
secinājumi

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

Uzbrukuma vizualizācija


47910
3389
92.240.93.211
92.240.90.31
21
92.240.95.206
92.240.95.207
50148
1308
50149
50151
4444
AfterGlow 1.6.2 - Property File: graph/sample.properties

Video demonstrācija



Sarkanās komandas pirmā viltīgā rīcība iegūstot kontroli pār sistēmu :)

#cd dnsadm

#ls -l

#ifconfig

#adduser certivo
Adding user `certivo' ...
Ading new group `certivo' (1001) ...
Adding new user `certivo' (1001) with group `certivo' …

#Iptables …. - DESTRUKTĪVI, bet var saprast iemeslus – ir konkurents

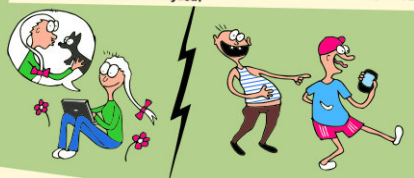
Citas aktivitātes

- 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 jebkuram citam cilvēkam, kas attēlots fotogrāfijā. Pēc tam, kad attēls ir „ielikts" internetā, to vairs nevar iznīcināt vai padarīt par nebijušu.

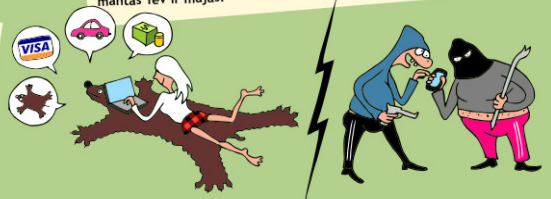


Lieto drošas paroles!

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

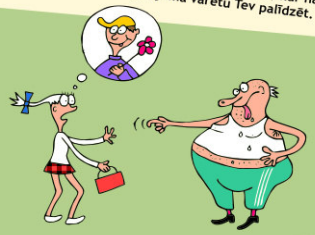
Neatklāj datus par sevi nepazīstamiem cilvēkiem!

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! Nepiekrīti tikties ar nepazīstamiem cilvēkiem nomaļās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.

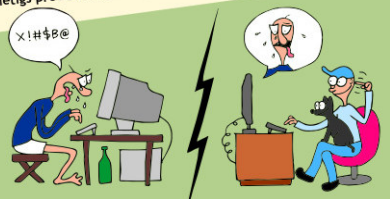


Darbības internetā nav anonīmas!

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

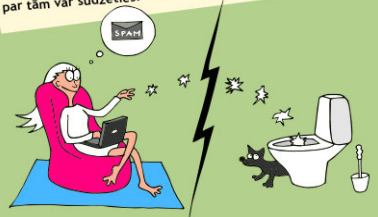
Neraksti aizskarošus komentārus!

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



Mēstules nav vēstules!

Ignorē mēstules, ko saņem 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.

Rūpējies par datora veselību!

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

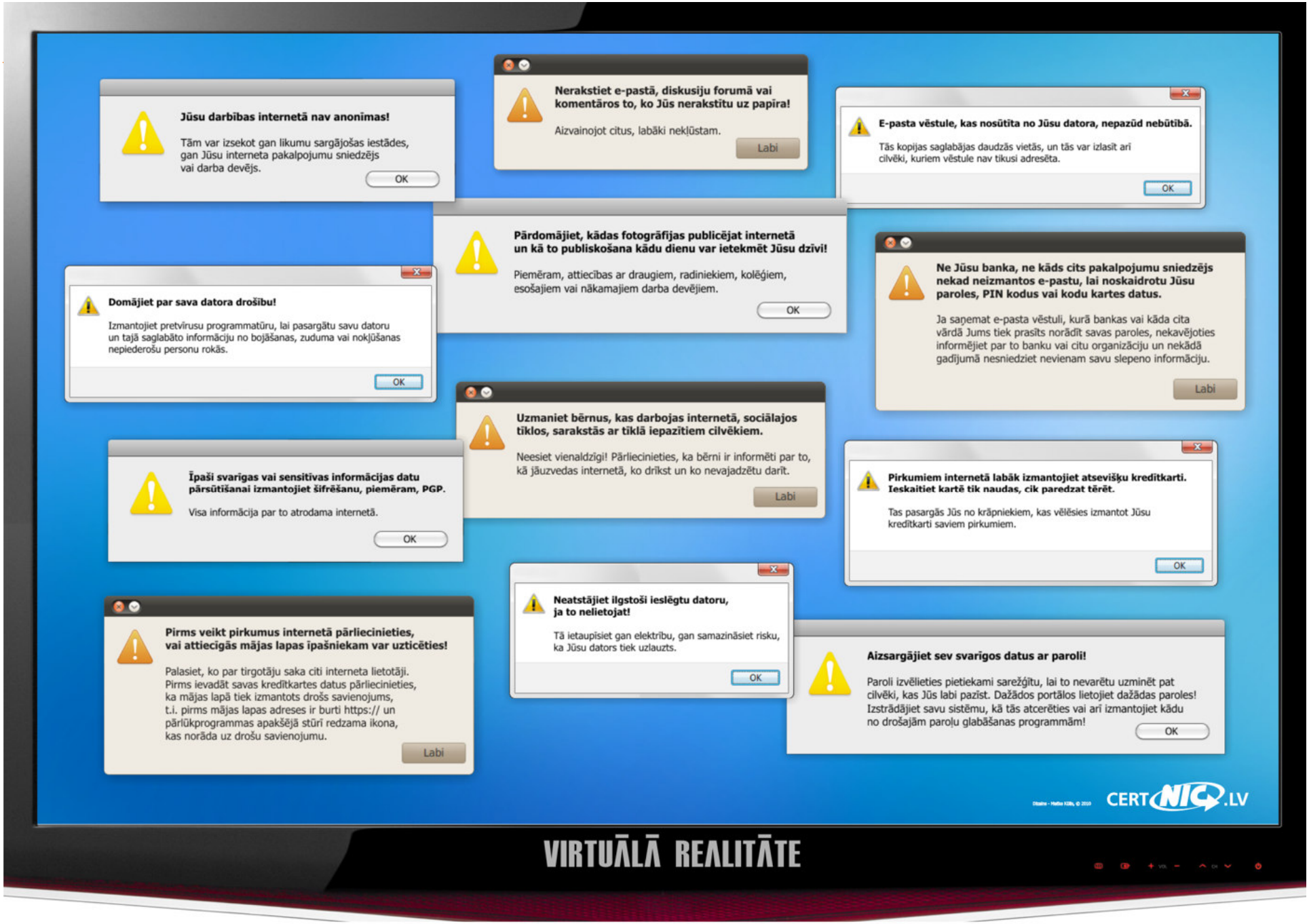
Ja Tu:

- 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@nic.lv

CERT.LV

CERT.LV



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

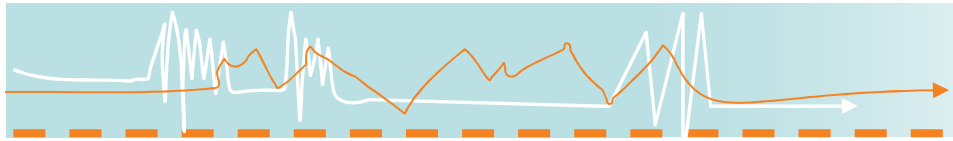
- Rīkot regulārus seminārus un mācības
- Sadarbība ar medijiem, presi – palielināt redzamību
- Aktivizēt LV-CSIRT grupu

Tuvākie pasākumi

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

Plāni:

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



CERT.LV

Paldies par uzmanību!

http://ww.cert.lv/
cert@cert.lv
varis.teivans@cert.lv