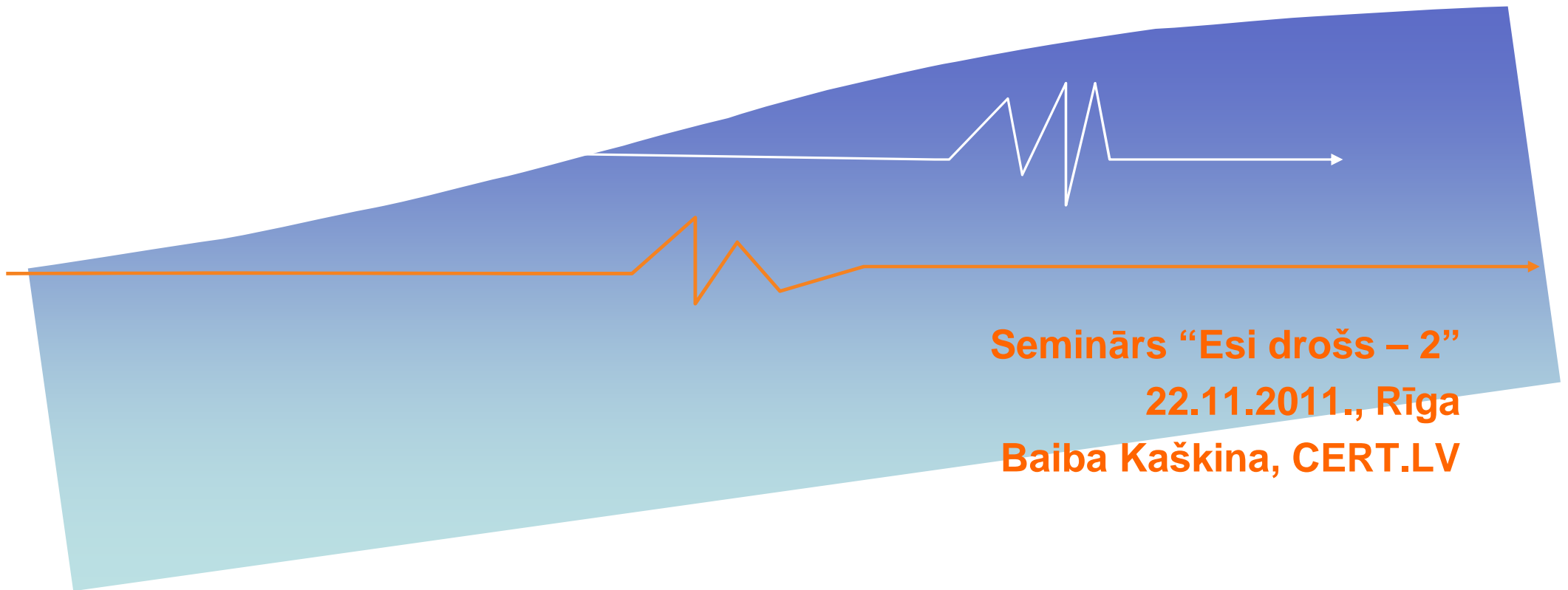


Seminārs “Esi drošs – 2”

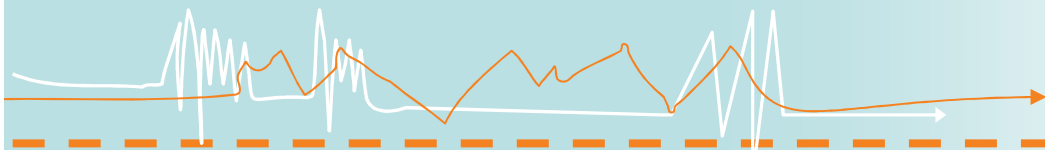
22.11.2011. - programma

1. „Informācijas tehnoloģiju drošības incidentu novēršanas institūcija - izaugsme 2011.gadā” - Baiba Kaškina, CERT.LV, 30 minūtes
 2. „Informācijas drošības izglītības programma” valsts un pašvaldību institūciju darbiniekiem” – Egils Stūrmanis, CERT.LV, 30 minūtes
 3. „Informācijas tehnoloģiju drošības noteikumu izstrādes pamatprincipi” - Mārtiņš Kaļķis, ISACA Latvijas nodaļa, izpildu viceprezidents, 30 minūtes
- Pārtraukums --
4. „Informācijas tehnoloģiju drošības juridiskie aspekti” - Pēteris Reinfelds, Valsts Policija, 30 minūtes
 5. „Apdraudējumi virtuālajā vidē - atspoguļojums medijos” - Juris Kaža, LETA.LV, NOZARE.LV, telekomunikāciju un IT nozares žurnālists, 30 minūtes

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija - izaugsme 2011.gadā



**Seminārs “Esi drošs – 2”
22.11.2011., Rīga
Baiba Kaškina, CERT.LV**



CERT.LV



IT drošības likums



IT drošības likums

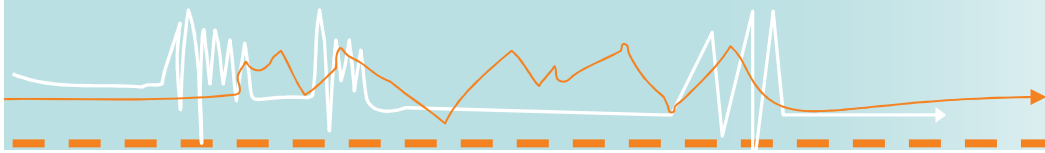
- Pieņemts Saeimā 2010.gada 28.oktobrī
- Stājās spēkā 2011.gada 1.februārī
- Nosaka CERT.LV izveides kārtību
- Paredz MK noteikumu izstrādi par
 - Kritiskās infrastruktūras drošības pasākumu plānošanu (no 2011.gada 1.februāra)
 - Elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanu un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam (no 2011.gada 1.maija)
- Nosaka Nacionālās informācijas tehnoloģiju drošības padomes izveidi

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

Atbildīgās personas noteiktas

- 381 iestādē
 - 195 valsts iestādes
 - 186 pašvaldību iestādes



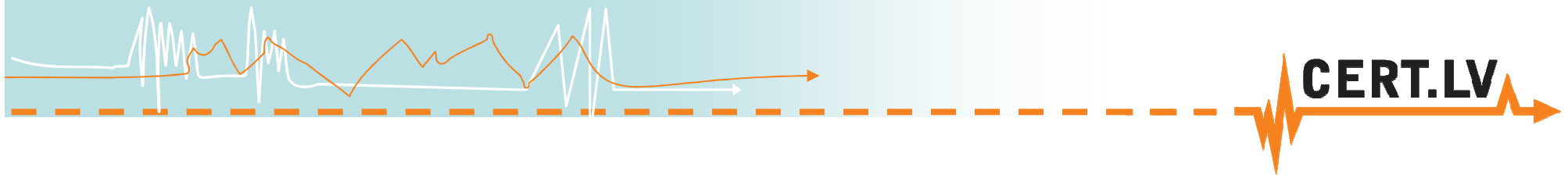
CERT.LV

CERT.LV



CERT.LV

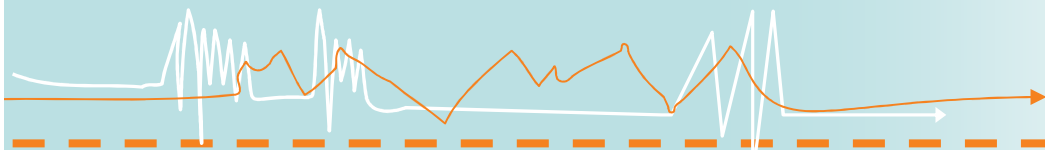
- Darbojas saskaņā ar “Informācijas tehnoloģiju drošības likumu”
- Darbības uzdevumi un tiesības tiek deleģētas Latvijas Universitātes aģentūrai “Latvijas Universitātes Matemātikas un informātikas institūts”
- Finansēta no valsts budžeta
- 2011.gadā - 10 darbinieki, 5 slodzes



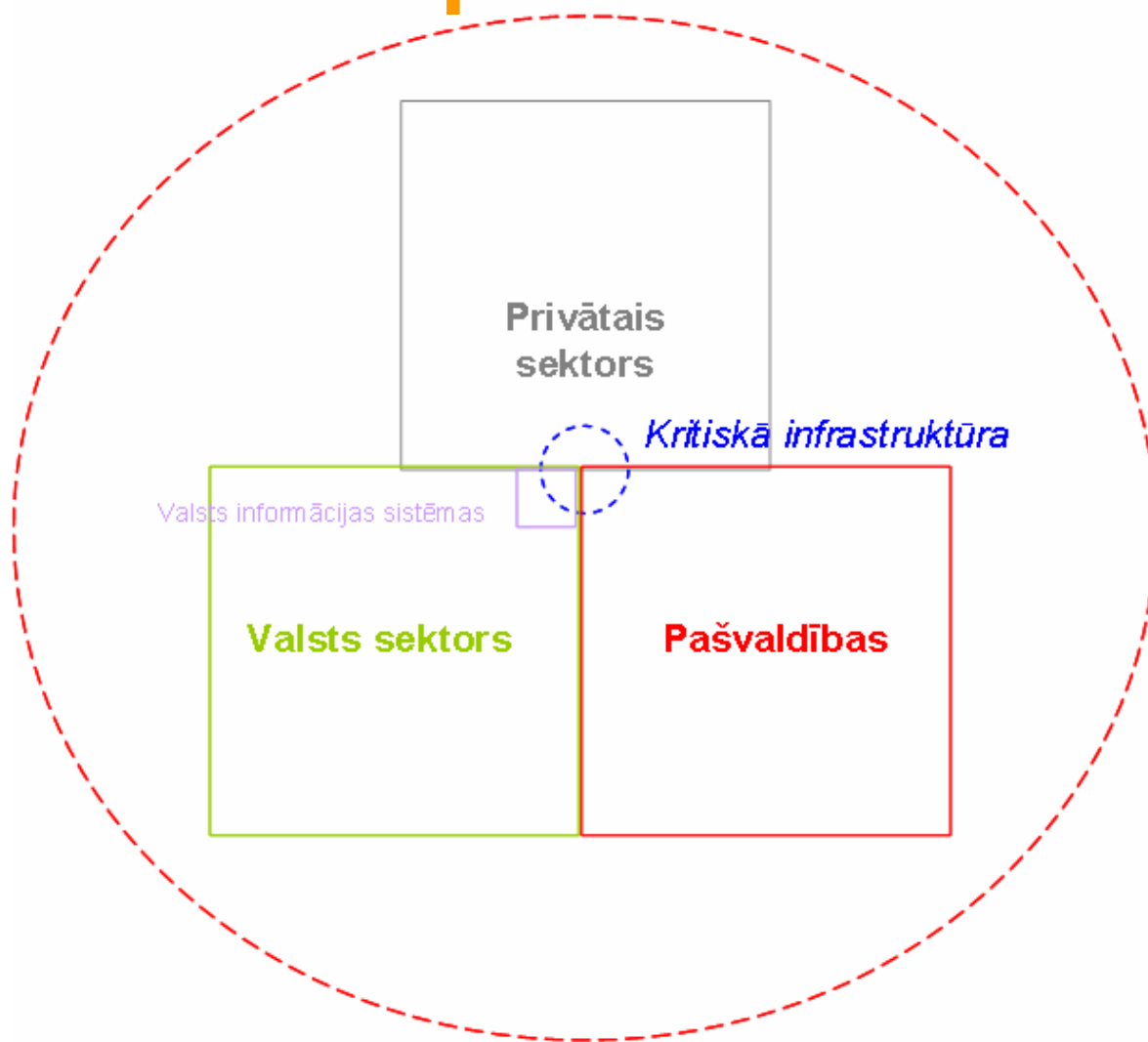
CERT.LV

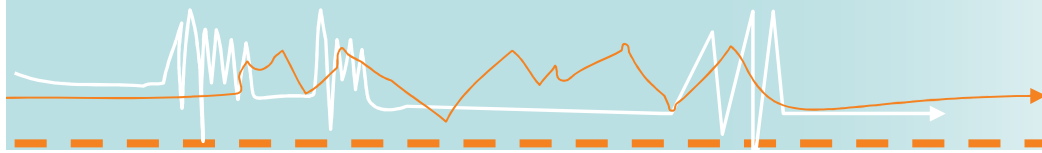
- Veic IT drošības incidentu apstrādi no 2006.gada
- Ir pilntiesīga *FIRST* dalībniece no 2009.gada
- Ir *Trusted Introducer* akreditēta vienība no 2007.gada





CERT.LV kopiena





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?

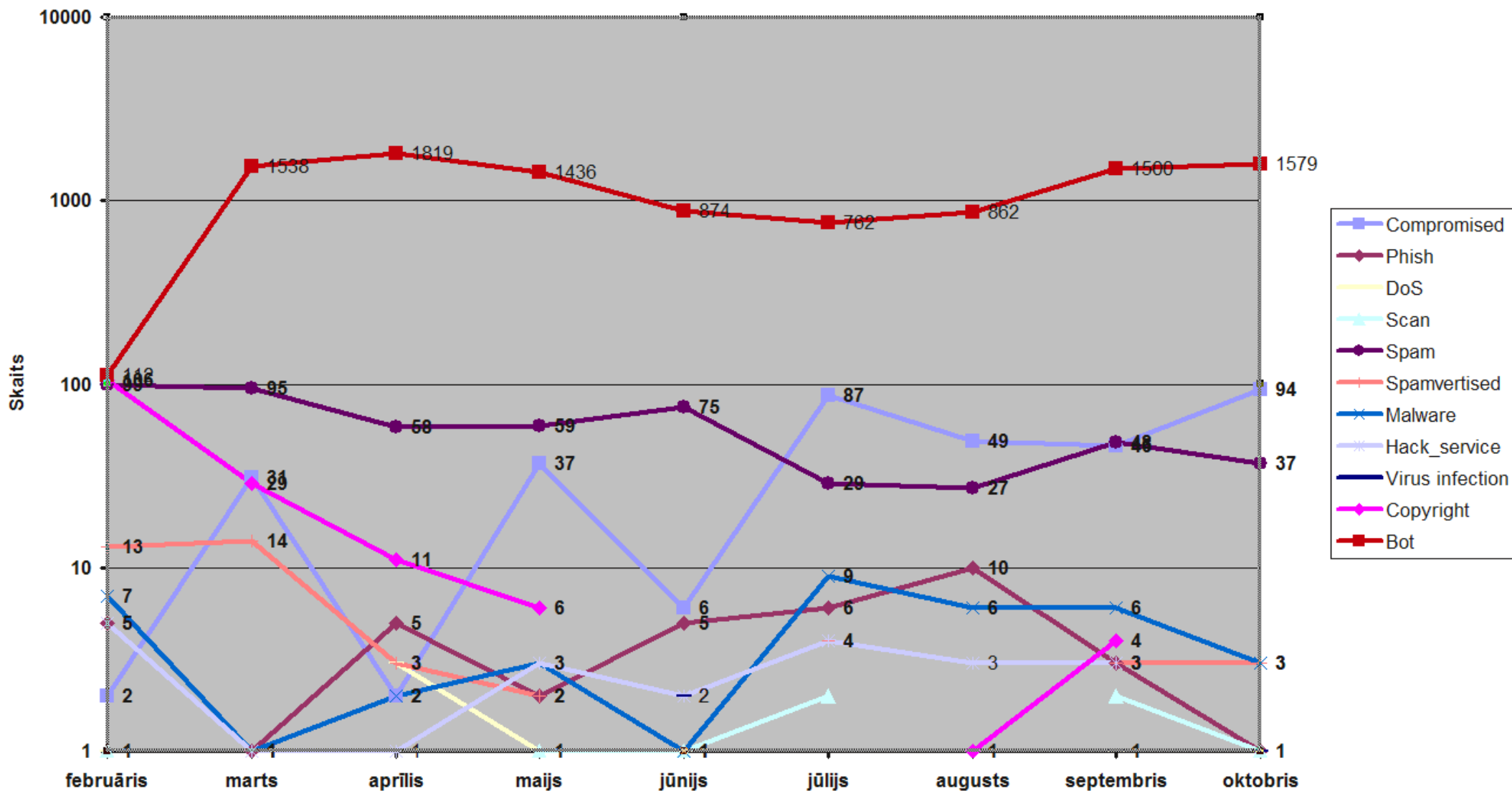
Kopējās tendences

- Cilvēki sāk biežāk ziņot CERT.LV 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

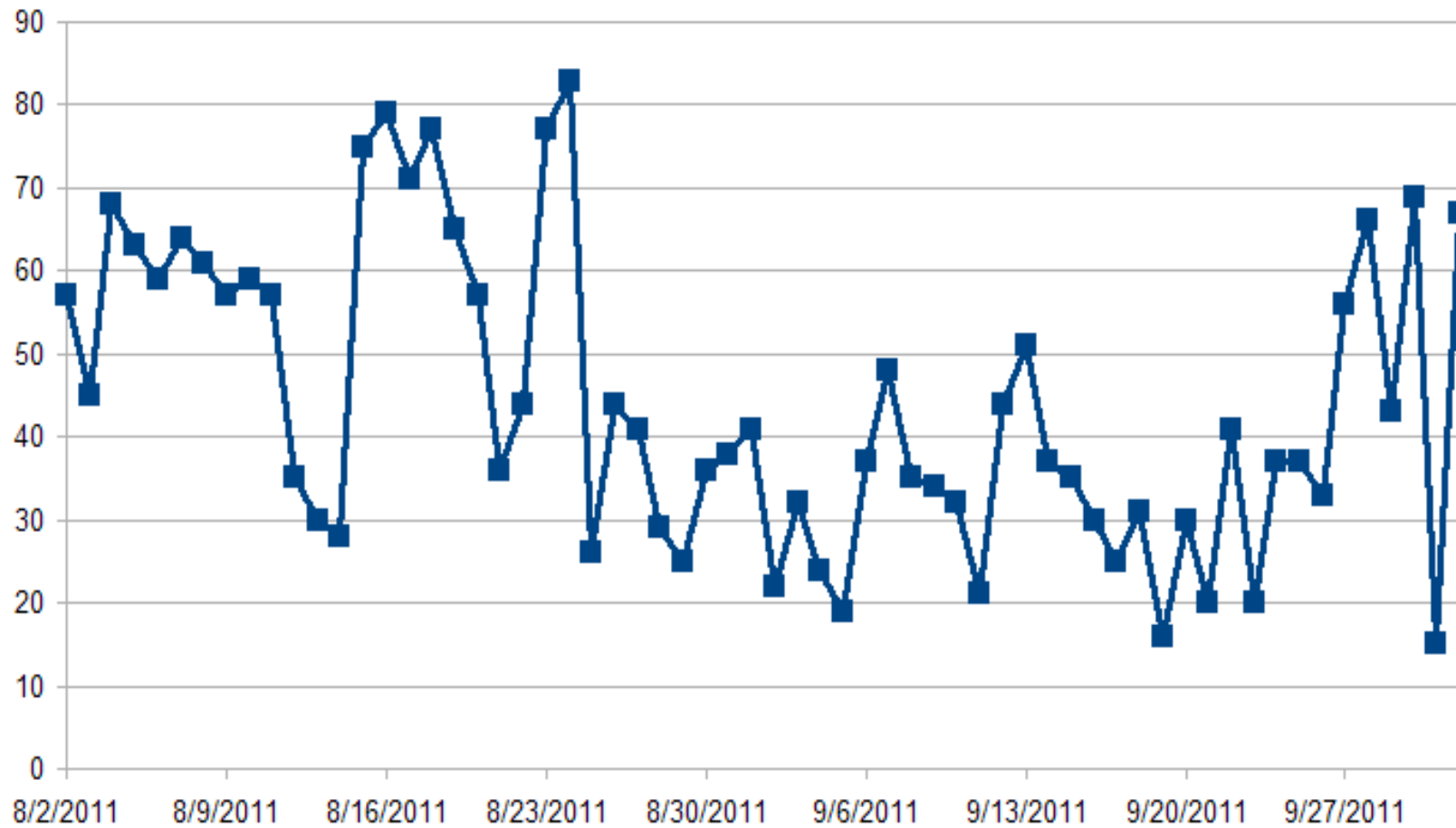
Incidentu risināšana

- Apstrādāti vairāk nekā 12000 incidenti

CERT.LV incidentu statistika – 9 mēneši



Inficēto valsts un pašvaldību iestāžu IP skaits



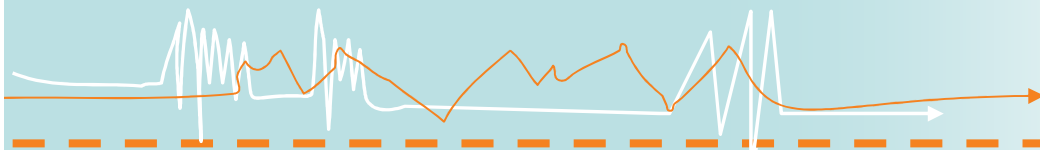
Incidentu risināšana

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

Nākotnes (?) tendences

Izmanto šādus
“datorus” ->



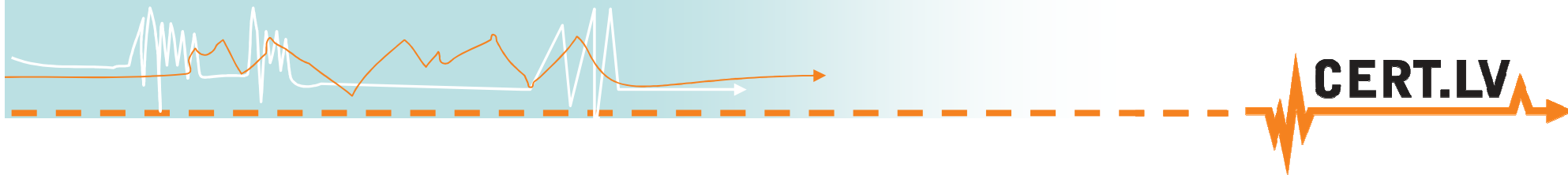


Nākotnes (?) tendences



Lai uzbruktu
šādiem
“datoriem”





Tā ir šodiena!



Sabiedrības izglītošana



Informācija, rekomendācijas

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

Dokumentu paraugi www.cert.lv

- Piemērs: IT drošības pārvaldības shēma
- Pašvaldību un valsts iestāžu IT drošības noteikumu vadlīnijas
- Ieteicamās prasības izmaiņu pārvaldībai
- Piemērs: Virtuālas iestādes apraksts
- Piemērs: Resursu klasifikācija, Risku analīze un pārvaldība



Temas

- Ap un par drošību (10)
- Darbs (10)
- Informācijas tīkla (32)
- Māja (10)
- Notikumi pasaulē (7)
- Pasākumi un notikumi (1)
- Publiskās vietās (11)

Darba tēmas

- Informācijas tehnoloģiju drošības incidentu novērtēšanas institūcija – CERT.LV
- LN Drošības ministrija
- LV CERT iniciatīva
- Net-Safe Latvia Drošības interneta centrs

Publisko vietņu 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				
» Dec						

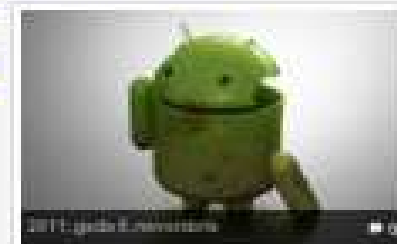
Arhīvs



Android – augošās popularitātes tumšās puses

Mūsdienu vairošās attiecības tā ātrajā, ka ne var tikt spējīgi un ietekmēti tā izveidot. Die tā kā ir tāpat, kas...

AKTUĀLIE RAKSTI



Android – augošās popularitātes tumšās puses

Mūsdienu vairošās attiecības tā ātrajā, ka ne var tikt spējīgi un ietekmēti tā izveidot. Die tā kā ir tāpat, kas...



Paroļu pārvaldnieki

Mūsu šodienā arvien pieaugošā loma ir stabilām parolēm un kodiem. Ievērojot šādas, ir iespējams izveidot drošākus un efektīvākus interneta...



Lapam šķērsojam mājlapam

ESI DROŠI!

Šī mājaslapa ir paredzēta šķērsošanai, kas ir nepieciešama par savu drošību un savu drošību interneta.

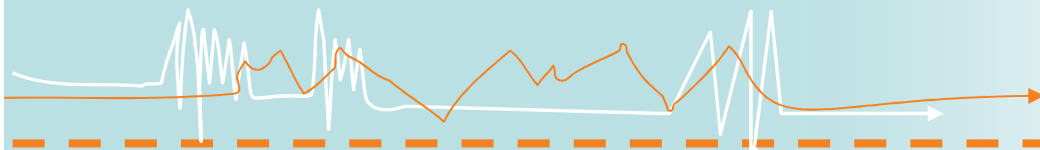
Māja lapu satur informāciju tehnoloģiju drošības incidentu novērtēšanas institūcija (CERT.LV) un tāpat informācija tehnoloģiju speciālisti no LV-CERT iniciatīvas grupas ir veidoti padarīti, daļu pārvaldi, kā arī ir gatavi atbildēt uz jūsu jautājumiem par jūsu drošību interneta un jūsu drošību interneta.

Jautājumu tēmas

- Android – augošās popularitātes tumšās puses
- Paroļu pārvaldnieki
- Kas ir SQL injektācijas?
- Kas ir XSS uzbrukumam?
- Tīmekļa vietnes drošība un tās izpildītājs tā drošības apdraudējumi

Jautājumu tēmas





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 – CERTLV
- LR Satiksmes ministrija

VIDEO: Kā justies droši elektroniskā vidē?

Jūties droši elektroniskā vidē from EsiDrošsLV on Vimeo. CERTLV piedāvā jums noskatīties Latvijas Universitātes Informācijas sistēmu drošības pasniedzējas Ilzes Murānes...

Uzmanību! Saskaņā ar CERTLV 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.



“Esi drošs” semināri

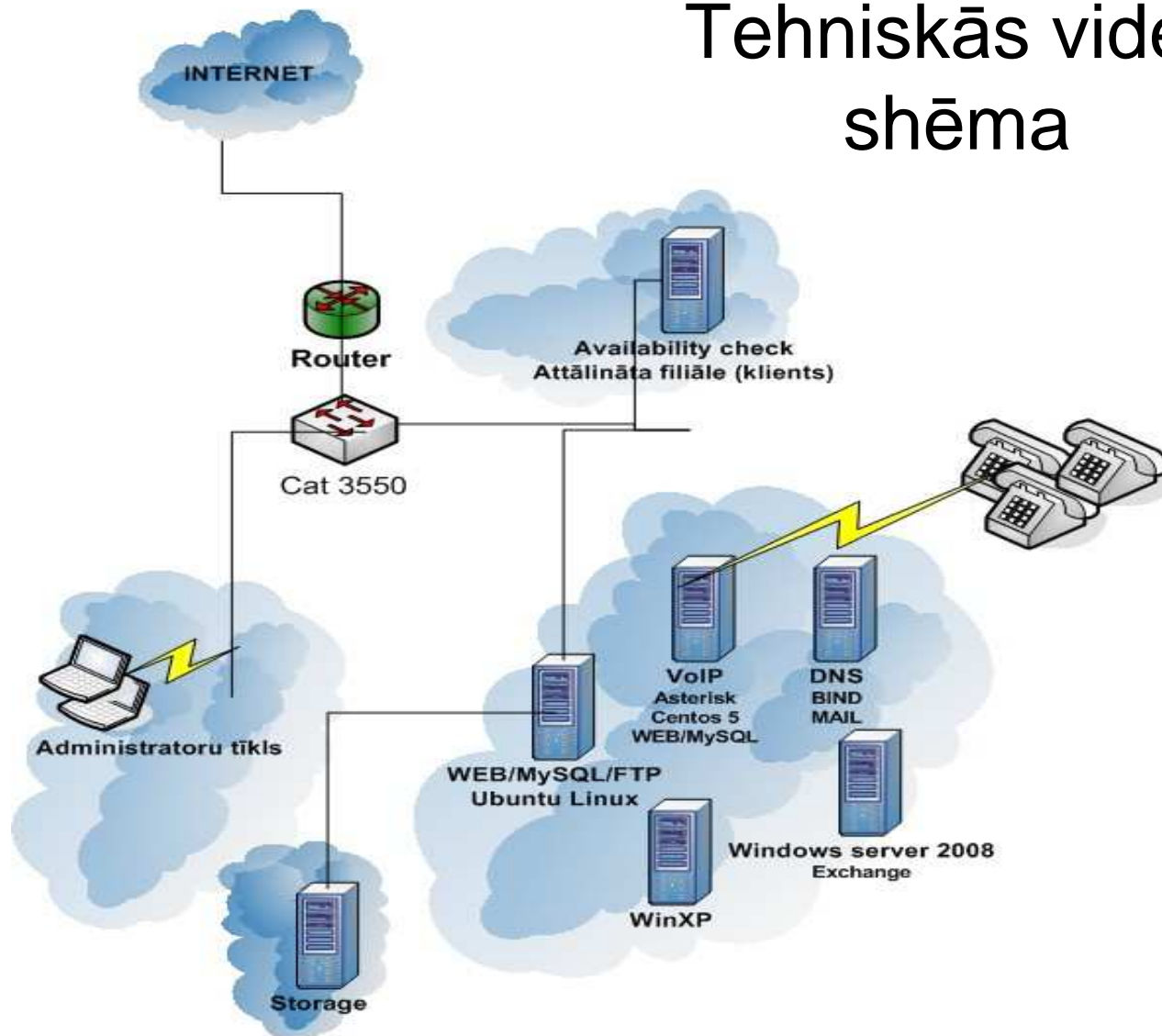
- “Esi drošs – 1” un “Esi drošs - 2” semināri valsts un pašvaldību iestāžu atbildīgajām personām
- “Esi drošs – 1” – Rīgā un Kuldīgā
- “Esi drošs – 2” – Rīgā
- Kādas tēmas nākotnē?
 - Sarežģītākas tēmas?
 - Atkārtot tēmas jaunpienācējiem?
 - Tehniskāki semināri?

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"

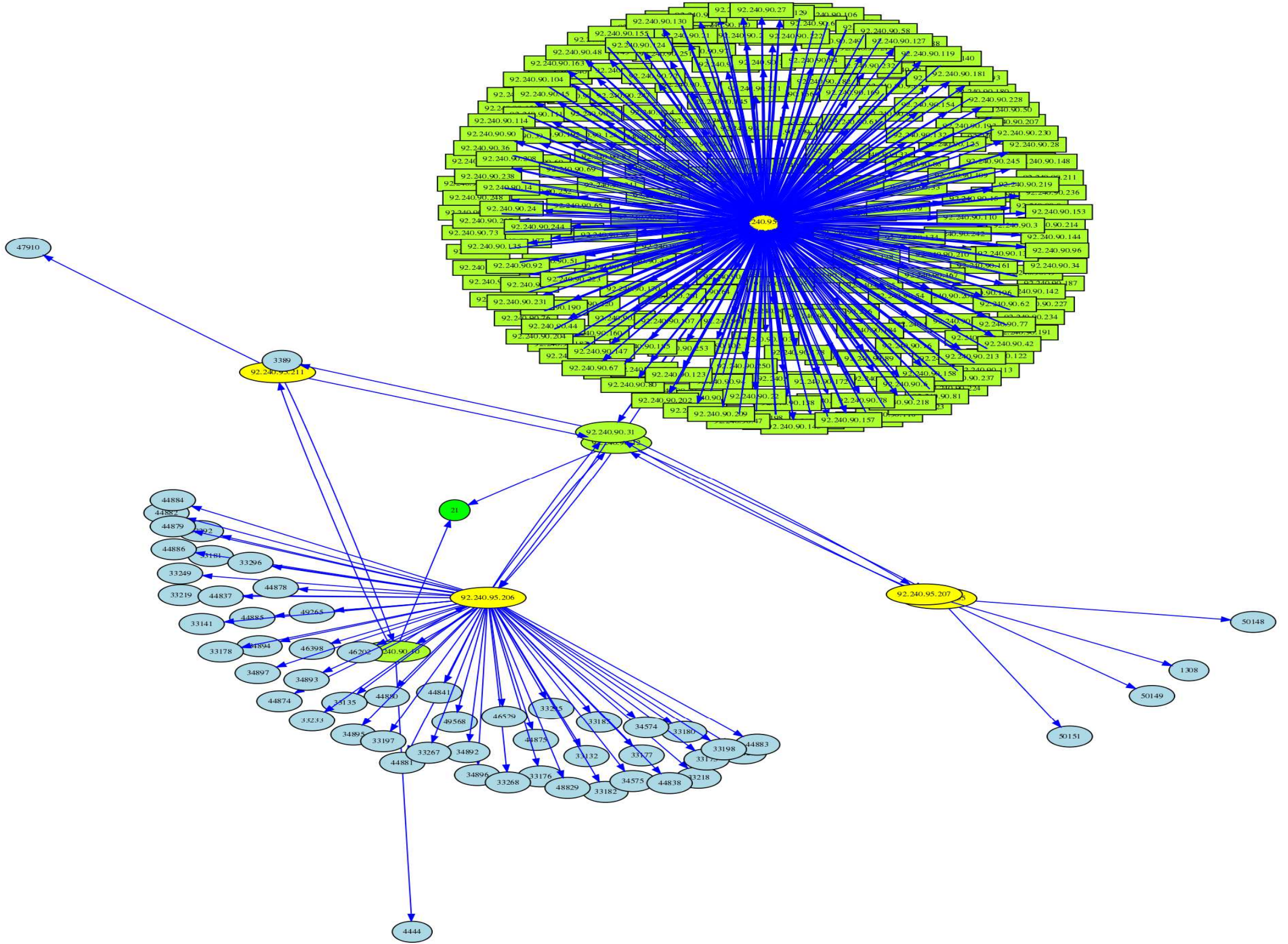
CERT.LV Tehniskās mācības

Tehniskās vides shēma



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 Sarkanajām, gan Zilajām komandām
- Sarkanām komandām tiek atļauta piekļuve Zilo komandu infrastruktūrai 1 stundu pēc Zilo komandu darba sākuma
- Komunikācija – panākumu, novērojumu, pārkāpumu ziņošana



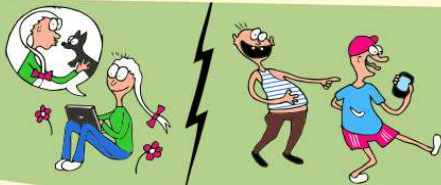
Citas aktivitātes

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

Vai esi Interneta profiņš?

Apdomā pirms publicē 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 draugiem un ģimenei. Jo vairāk Tu par sevi atklāsi, jo vieglāk viņi varēs nodarīt Tev pāri draugiem. 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 nomājās vietās, kur nav neviena, kas nepieciešamības gadījumā varētu Tev palīdzēt.



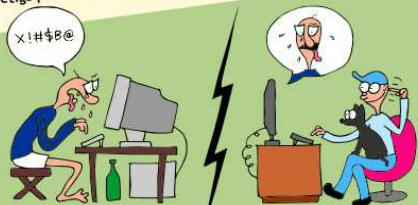
Darbības internetā nav anonīmas!

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



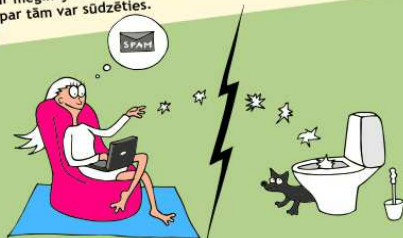
Neraksti aizskarošus komentārus!

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.



Neieņņemies 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, 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



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



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



Domājiet par sava datora drošību!

Izmantojiet pretvirusu 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.

Labi



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

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

Labi



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 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!

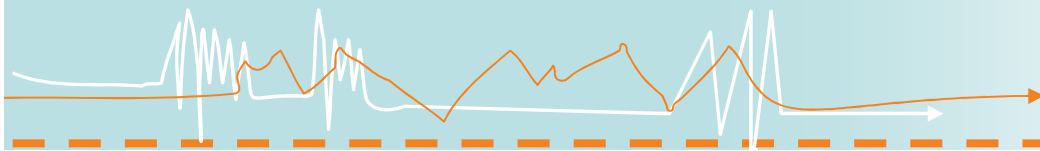
OK

Zinātnis - Helms Lībā, © 2009

CERT **NIC**.LV

VIRTUĀLĀ REALITĀTE

VIRTUALA REALITATE



CERT.LV

Nākotnes plāni



CERT.LV nākotnes plāni

- Palielināt tehniskās iespējas
- Nostiprināt sadarbību ar valsts un pašvaldību institūcijām
- Uzlabot sadarbību ar Interneta pakalpojuma sniedzējiem
- Uzturēt izglītošanas portālu www.esidross.lv
- Rīkot regulārus seminārus un mācības
- Sadarbība ar medijiem, presi – palielināt redzamību
- Sadarbība ar LV-CSIRT grupu

Tuvākie plāni

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

Paldies par uzmanību!

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

cert@cert.lv

baiba.kaskina@cert.lv



Seminārs “Esi drošs – 2”

22.11.2011. - programma

1. „Informācijas tehnoloģiju drošības incidentu novēršanas institūcija - izaugsme 2011.gadā” - Baiba Kaškina, CERT.LV, 30 minūtes
 2. „Informācijas drošības izglītības programma” valsts un pašvaldību institūciju darbiniekiem” – Egils Stūrmanis, CERT.LV, 30 minūtes
 3. „Informācijas tehnoloģiju drošības noteikumu izstrādes pamatprincipi” - Mārtiņš Kaļķis, ISACA Latvijas nodaļa, izpildu viceprezidents, 30 minūtes
- Pārtraukums --
4. „Informācijas tehnoloģiju drošības juridiskie aspekti” - Pēteris Reinfelds, Valsts Policija, 30 minūtes
 5. „Apdraudējumi virtuālajā vidē - atspoguļojums medijos” - Juris Kaža, LETA.LV, NOZARE.LV, telekomunikāciju un IT nozares žurnālists, 30 minūtes