Seminārs Interneta pakalpojumu sniedzējiem 13.10.2011. - programma

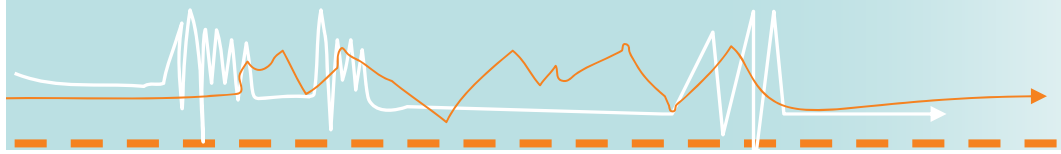
1. „Īsi par CERT.LV” - Baiba Kaškina, CERT.LV vadītāja, 20 minūtes
2. „IT drošības likuma un MK noteikumu prasības attiecībā uz IPS” - Baiba Kaškina, CERT.LV vadītāja, 45 minūtes
3. „Personas datu aizsardzības pārkāpuma paziņošana” - Mārtiņš Indāns, Datu valsts inspekcija, 15 minūtes
4. „Botnetu un datorvīrusu apkarošana sadarbībā ar CERT.LV” - Gints Mālkalnietis, CERT.LV tehniskais speciālists, 30 minūtes

“Botnetu un datorvīrusu apkarošana sadarbībā ar CERT.LV”

Seminārs Interneta pakalpojumu sniedzējiem

13.10.2011., Rīga

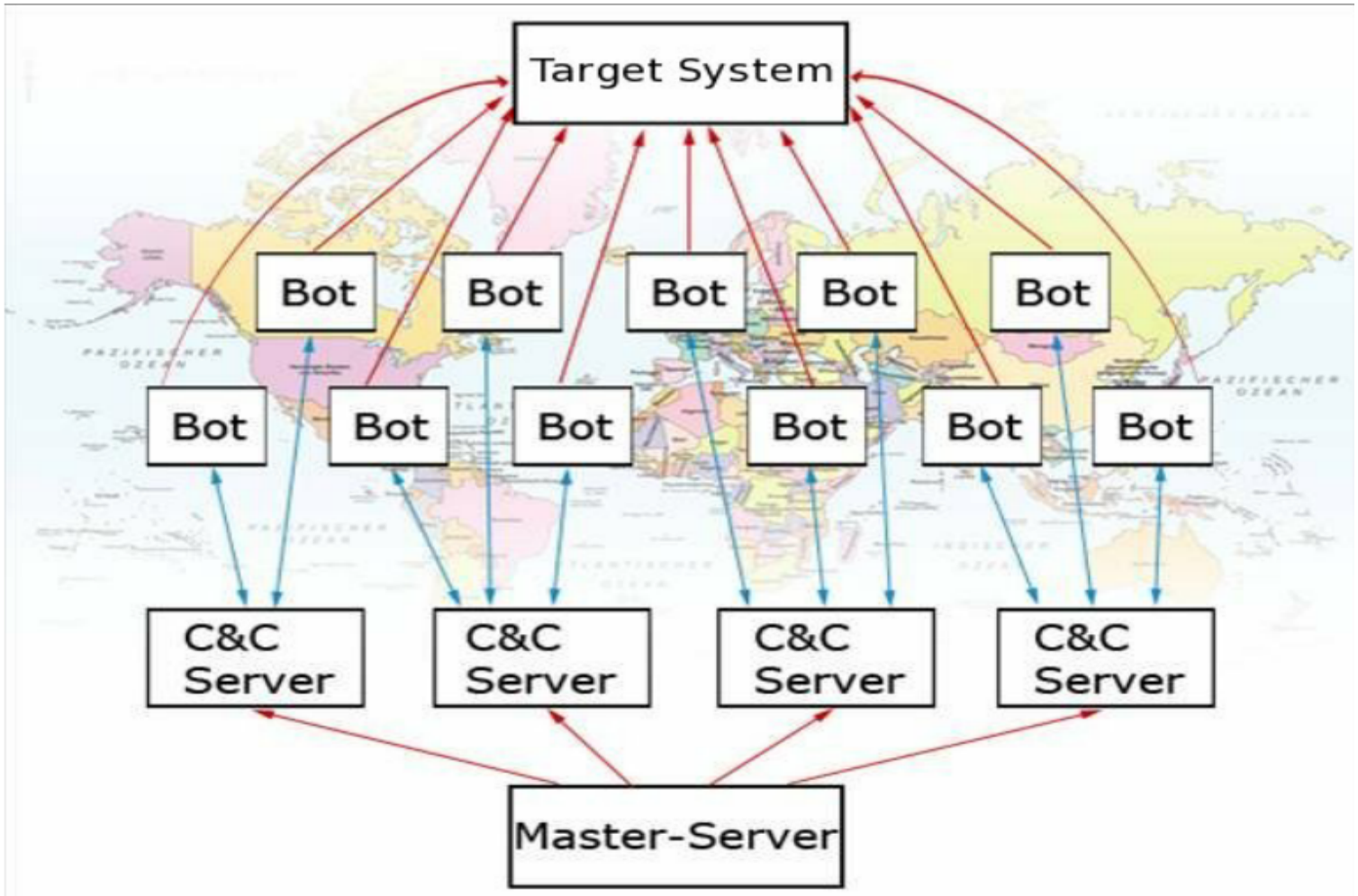
Gints Mālkalnietis, CERT.LV



CERT.LV

Botneti

Kas ir botnets?



Ietekme uz klientiem

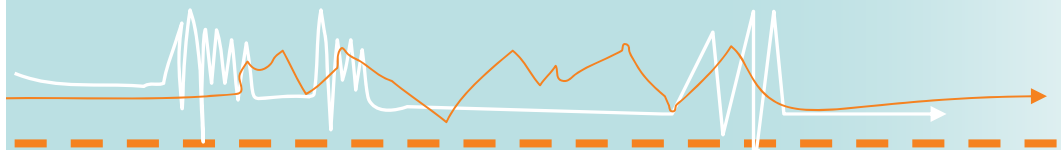
- Finansiāli zaudējumi
  - kredītkaršu datu zādzības
  - viltoti tiešsaites maksājumi
- Konfidenciālu dokumentu noplūde
- Datora darbības traucējumi

Ietekme uz IPS

- Sakaru kanālu pārslodze
- IPS tīkli nonāk melnajos sarakstos
  - klientiem traucē e-pastu apmaiņu
  - viss IPS tīkls var tikt bloķēts ugunsmūrī
- IPS pasliktinās reputācija

Apzināta datorvīrusu uzturēšana IPS tīklā!

- Problēmas ar tiesībsargājošām iestādēm
- IPS tīkli nonāk melnajos sarakstos
  - viss IPS tīkls var tikt bloķēts ugunsmūrī
- IPS pasliktinās reputācija
- Iespējams izsaukt DDoS u.c. uzbrukumus



CERT.LV

Infekcijas savā tīklā

Kā uzzināt, ka klienta dators ir inficēts?

- Iekšējās monitoringa sistēmas
- Ziņojumi no citiem klientiem
- Ziņojumi no specializētiem servisiem
- Ziņojumi no CERT.LV
- Tīkla darbības traucējumi

Ko iesākt ar inficētu klientu?

- Pārtraukt tā iespējamo kaitējumu citiem!
- Informēt klientu par problēmu
- Ieteikt risinājumu

Kā informēt klientu?

- Brīdinājums pa e-pastu
- Zvans klientam
- Pakalpojuma sniegšanas pārtraukšana vai ierobežošana
- Klienta automātiska novirzīšana uz brīdinošu lapu
    - Automātisks risinājums
    - Viegli savienot ar ienākošo ziņojumu apstrādi

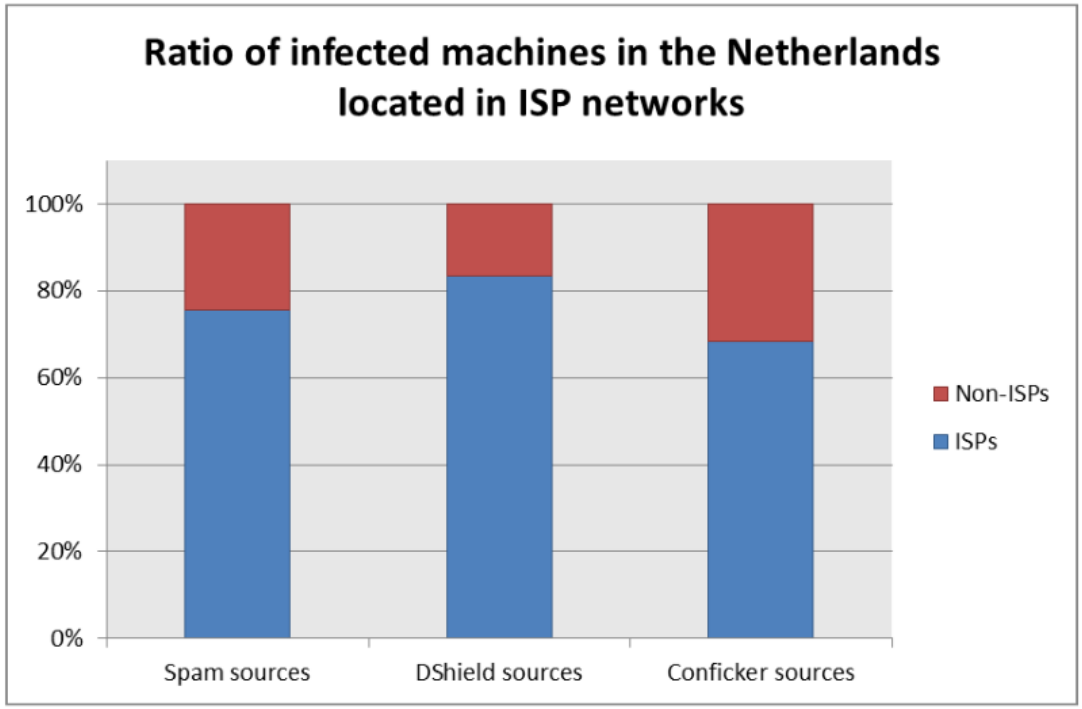
Brīdinošā lapa

- Informējošs paziņojums
- Ieteikumi klientiem patstāvīgai datora iztīrīšanai:
    - Saites uz bezmaksas programmām
    - Padomi drošai datora konfigurācijai
- Saites uz profesionāla datorservisa sniedzējiem.

Pieredze ārzemēs

Starptautiskā pieredze - Nīderlande

Anti-botnet Working Group = 12 IPS, vairāk nekā 90% tirgus daļa



Starptautiskā pieredze - Vācija

Anti-Botnet Beratungszentrum

- Pagaidām apvieno 11 IPS
- Atbalsta Vācijas Iekšlietu ministrija
- Piedāvā savu zvanu centru, kas palīdz klientiem iztīrīt datoru
- Uztur lapu ar padomiem klientiem www.botfrei.de

Starptautiskā pieredze - Austrālija

ACMA Australian Internet Security Initiative

- Darbojas no 2005.gada
- 106 IPS
- Iesaistītie IPS saņem ikdienas ziņojumus par savu IP apgabalu
- Izveidots ar Austrālijas valdības atbalstu

Ko darīt Latvijā?

Sadarbības iespējas

- Regulāra informācija par inficētajām IP adresēm
- Incidentu risināšanā – paraugi incidentu atrisināšanai
- CERT.LV un citi gatavo materiālus klientu izglītošanai - www.esidross.lv
- CERT sensori (*honeypot*) pie IPS

Informācijas apmaiņa ar IPS

Incidenti, kuri prasa nekavējošu rīcību (augsta prioritāte)

- Sadarbības formāts
  - E-pasts
  - Telefons
- Laika intervāls
  - Informācijas apmaiņa tikko incidents ir reģistrēts
- Informācijas apmaiņa *(feedback)*
  - Līdz incidenta atrisināšanai

Informācijas apmaiņa ar IPS

Incidenti, kuri neprasa tūlītēju rīcību (zema prioritāte)

- Sadarbības formāts
  - E-pasts
  - Pieeja incidentu datubāzei
- Laika intervāls
  - Incidentu datubāzi CERT.LV atjauno reizi dienā
- Informācijas apmaiņa (*feedback*)
  - Netiek gaidīts par katru nenozīmīgo incidentu, bet var tikt lūgts informēt par paveikto

Kā uzsākt sadarbību?

- Rakstīt cert@cert.lv
  - AS, IP adreses
  - Kontaktpersonas
- Sūtīt Rīcības plānu uz kontakti@cert.lv (vēlams līdz 01.11.2011.)
  - Atbildīgajām personām e-pasta liste
- LV-CSIRT inicatīvas grupa – www.csirt.lv

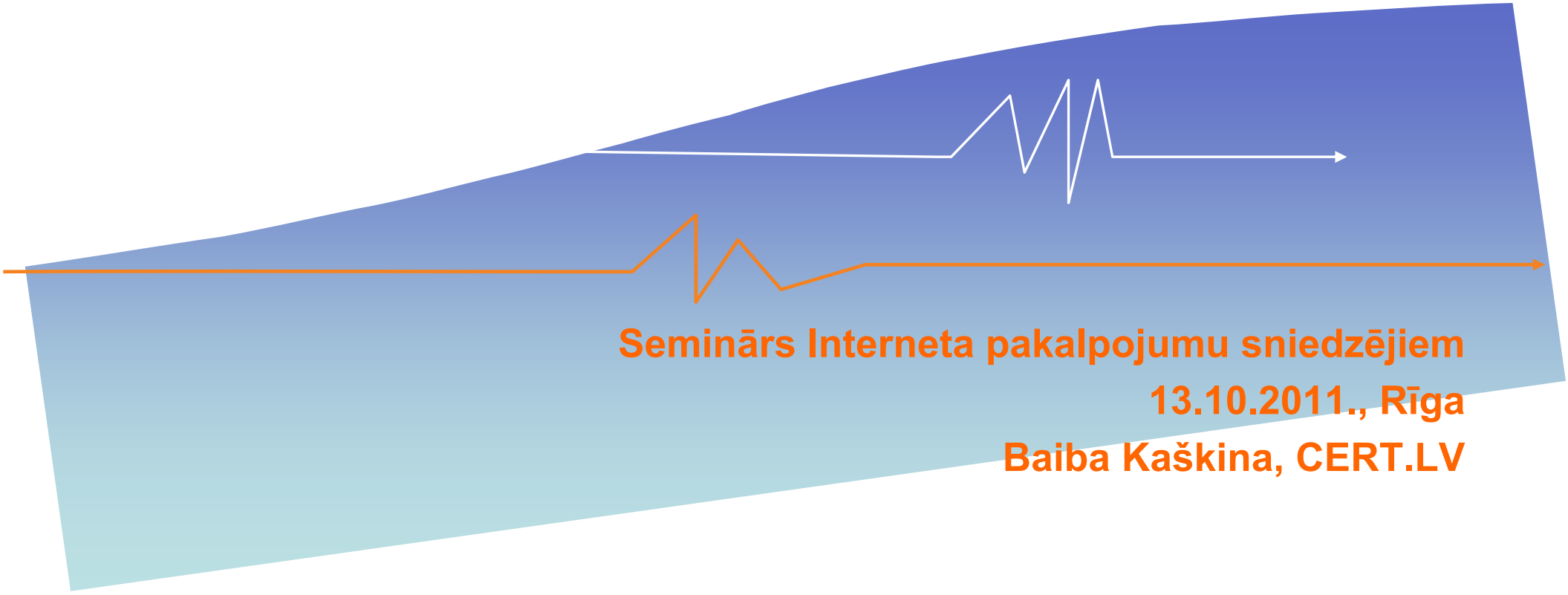
Jautājumi?

http://ww.cert.lv/

cert@cert.lv

gints@cert.lv

Noslēgums



Seminārs Interneta pakalpojumu sniedzējiem

13.10.2011., Rīga

Baiba Kaškina, CERT.LV

CERT.LV plāni

- Palielināt tehniskās iespējas
- Nostiprināt sadarbību ar valsts un pašvaldību institūcijām
- Ieviest sadarbības modeli ar Interneta pakalpojuma sniedzējiem
- Izveidot tīmekļa platformu zemas prioritātes incidentu pārvaldībai
- Uzturēt izglītošanas portālu www.esidross.lv
- Rīkot regulārus seminārus un mācības

Kopsavilkums

- Likums sakārto ar IT drošību saistīto vidi LV – tas definē visu iesaistīto pušu tiesības un pienākumus
- Stājušies spēkā MK noteikumi saistībā ar kritiskās infrastruktūras aizsardzību
- Stājušies spēkā MK noteikumi par elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanu
- Ar IT drošību saistītos jautājumus valsts līmenī koordinē Nacionālā informācijas tehnoloģiju drošības padome
- CERT.LV pilda IT drošības likumā noteiktos pienākumus un aicina visus IPS uz sadarbību

CERT.LV rudens pasākumi

- **13.oktobris** – seminārs Interneta pakalpojumu sniedzējiem
- **28.oktobris** – 1.tehniskās IT drošības mācības
- **22.novembris** – “Esi Drošs – 2” seminārs

Plāni:

- 2. teorētiskās mācības
- LV-CSIRT grupas pasākums

Paldies par uzmanību!

http://www.cert.lv/
cert@cert.lv
baiba.kaskina@cert.lv