How to engage everyone? - CERT.LV collaborations with ISPs, security professionals and ordinary people

Baiba Kaškina, CERT.LV
28.09.2012. - Ljubljana, Slovenia
Outline

• Collaboration with ISPs
• Establishment of Security Expert Group
• Why it is so difficult?
• Future plans
Collaboration with ISPs
IT Security law - ISPs

- All ISPs have to submit to CERT.LV “Action plan for continuous operations”
- Report to CERT.LV major incidents
- CERT.LV can request
  - IT Security documentation
  - IT Security audits
  - Disconnect of an end user
What we want?

• Good collaboration with ISPs
  • More than 400 ISPs in Latvia...
  • “Action plans” received from ~35 biggest
• Help to inform end users about infected computers
• Collaboration on more serious incidents
Some solutions

- Individual approach
- Examples for “Action plans”
- Establishment of “Responsible ISP” sign
- Mandate by the Law helps
Responsible ISP

- In collaboration with NetSafe centre
- 6 MoUs signed so far
- Public campaign in October 2012
What needs to be done?

- Collaboration on fight with criminal pornography
- Informing end users about infections
  - Some details for emails specified
- Content filters available when requested by user
Security Expert Group
LV CSIRT group – the history

• Established in 2007 – just before the events in Estonia

• Main goals
  • Contact details exchange
  • Information & experience exchange
LV CSIRT – main problems

- People were very inactive
- Too few meetings
- Luck of trust
  - Who is in this list?
Outside pressure

- Estonian example – Cyber Security League
- Interests of different Ministries in Latvia
- Interests of CERT.LV
Solution

• “Security Expert Group” – adjacent to CERT.LV
• Cyber Security League – under the Ministry of Defence
• People can participate in any of them or both
SEG (DEG)

- DEG = on fire
- New charter and code of ethics
- Monthly meetings
- Special rules on how to join
- ~25 members
Why it is so difficult?
CERT.LV incident statistics – low priority - Q2 – 43489 – TOP 10

Top10 infekcijas Q2 2012

- downadup 34545
- slenfbot 2808
- dnschanger 1776
- sinkhole 1704
- salty 778
- salty2 649
- conficker.c 472
- irc 139
- virut 118
- kelihos 105
Current situation

- 2500-3000 infected unique computers monthly
- > 400 ISPs
- Ordinary people care only if they lose money or something else valuable
ESI DROŠI!

Šī mājaslapa ir paredzēta labotām, ko rūpējas par savu datora drošību un savu drošību telpā.

Mājas lapu izstrādā informācijas tehnoloģiju drošības iniciatīvu nevēršanas institūta CERT/LV un tajā informācijas tehnoloģiju speciālistu ietekmē šīs grupas piedāvātām risinājumā, tāpat patiesajā līdzekļā izpildot, kas atrāpēja atbildīgu uz Jūsu jaunākajiem par Jūsu datora drošību un Jūsu drošību telpā.
New colleague - “Computerologist”

• Born in March @ E-skills week
• Last performance – 12 May, EU Garden-party
• Twitter account
Future plans
Future plans

- Next year – under the Ministry of Defence
- New PR person – awareness raising campaigns
- More activities for Computerologist
- Regional and thematic workshops
- Active engagement of all sectors
- Enhancement of technical skills
Thank you!!!

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