Dealing with the whole country:
creating a National CSIRT

Baiba Kaškina, CERT.LV
31.01.2012. Rome, Italy
Outline

• Short history & IT Security law
• First year results
• How to deal with the whole country
• Future plans
Short history & IT Security law
CERT.LV

- Operational since 1 February 2011
- Operates on the basis of IT Security Law
- Tasks delegated to Institute of Mathematics and Computer Science, University of Latvia
- Merged CERT NIC.LV + DDIRV
- State funded
- Year 2011 - 10 people, 5 FTE
CERT.LV

- Experience in security incident handling since 2006 (LATNET CERT, CERT NIC.LV)
- Full member of FIRST since 2009
- Accredited by Trusted Introducer since 2007
CERT.LV Constituency
IT Security law

• In force since 1 February 2011
• Implemented in 2011
• Sets CERT.LV tasks and responsibilities
• Sets responsibilities for:
  • Public sector
  • ISPs
  • Critical IT infrastructure owners
IT Security law – Public sector

• In every institution – responsible person for IT security, his/her tasks:
  • To establish IT security documents for institution
  • To organise IT security audits
  • To educate at least once per year all employees
  • To report CERT.LV security incidents
  • To participate in CERT.LV seminars
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
IT Security law - disconnect

- CERT.LV can request disconnect of an end user
- To up to 24 hours
- If threatens rights of other users, their IS or security of networks
- Reasoning needs to be provided
- Documentation in place, never implemented
IT Security law – Critical infrastructure

- List – State secret
- Report incidents to CERT.LV
- Establishes IT Security documentation
- CERT.LV can do pentesting
First year results
Monitoring of Latvian IT space and incident response
Situation in Latvia

- Overview of infected IPs in Latvia – on 31.12.2011. 3300 infections (bots)
- Different information sources
- Only part of infections become incidents in tracking system
- Cooperation with ISPs
Incident response

- Dealt with almost 15000 incidents
- More incidents reported by individuals
- More frequently report those who already have had a good collaboration experience with CERT.LV
CERT.LV incident statistics

![Bar chart showing incident statistics for various categories such as Compromised servers, Phishing, DoS, Scanning, SPAM related, Malware, Hacked services, Copyright, Botnets, and Defacement. The x-axis represents the incident count, while the y-axis represents the scale of incidents from 1 to 100,000.]
Awareness raising, education, exercise organization, recommendations
Information, recommendations

- Website, information on newest viruses and threats
- Articles, suggestions
- Examples for IT security principles and rules
- Portal www.esidross.lv (“be safe”)
- Twitter account “certlv”
Android – augošās popularitātes tumšās puses

Mūsdienu zinātnē atšķirības tik strauji, ka ne vien ir spējams un interesantās būt izveidot. Bet tā kā ir ļoti, kas...

AKTUĀLIE RAKSTI

Android – augošās popularitātes tumšās puses

Mūsdienu zinātnē atšķirības tik strauji, ka ne vien ir spējams un interesantās būt izveidot. Bet tā kā ir ļoti, kas...

Paroju pārvaldnieki

Mūsu dzīvē arī vairāki piesaista lomā un darbākām personas, kur ir jāattīstina, ta pašām dažādām sistēmām – e-pastām, interneta...

Jautājums roktīm

- Android – augošās popularitātes tumšās puses
- Paroju pārvaldnieki
- Kas ir SQL injekcijas?
- Kas ir XSS ierobežojumi?
- Tīmekļa vietnēs drošība un bīsa izplatītāja basts drošības apmācībās

Jautājumu atbildes

- Justin 12.11.2011 15:38:26: Man ir jāatbild, ka...
- Rinka 12.11.2011 15:42:34: Paroju pārvaldnieks...
- Kārļis 12.11.2011 15:43:21: Paroju pārvaldnieki...
- Janis 12.11.2011 15:44:12: Paroju pārvaldnieki...
- Ivars 12.11.2011 15:45:03: Paroju pārvaldnieki...
- Joni 12.11.2011 15:46:26: Paroju pārvaldnieki...
VIDEO: Kā justies droši elektroniskā vidē?
Jūties droši elektroniskā vidē from EsiDrošsLV on Vimeo. CERTLV piedāvā jums roskatītās Latvijas Universitātes informācijas sistēmu drošības pasniegājējas līdzības Mutācēs...
Events, presentations

- “Be safe -1” and “Be safe-2” seminars for state institutions
- IT Security exercises
  - Theoretical
  - Technical
- Seminar for Internet Service providers
- Targeted events
  - Legal issues
  - How to organize exercises
- Participation in World Wide Safer Internet day
Contacts

• Responsible persons for ~400 institutions
• Actions plans for ~30 ISP (out of ~400)
• > 500 people participated in CERT.LV events
How to deal with the whole country
We need automation

- Collaboration with ISPs
- Abuse Helper
- To separate incidents in two groups
  - Serious ones – processed by hand
  - Mass infections - processed automatically
Not all are equal 😊

• Which customers are more important?
• What should be processed by hand?
Incident processing – the goal

- Manual processing
  - All high priority institutions
  - All human submitted incident reports
  - Legacy – SigmaNet and Latnet incidents
- Automatic processing
  - All automated reports (via Abuse Helper)
  - Daily reports to ISPs
Future plans
Great changes

- 2.5 times more money from 1 March 2012
- Increase staff to 10 FTE
- New incident classification, more automation
- Ability to participate in more exercises, events, etc.
- Establishment of IT Security Guards
- More PR and awareness raising activities
Summary

• All parts of IT Security law are in place
• Established contacts with all parts of constituency
• People report more incidents
• Gaining political attention
• Need for incident response automation
• Growing responsibility
Thank you!!!

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