CERT.LV
Information Technologies
Security Incident
Response Institution

CVD model in Latvia – attempts and failures

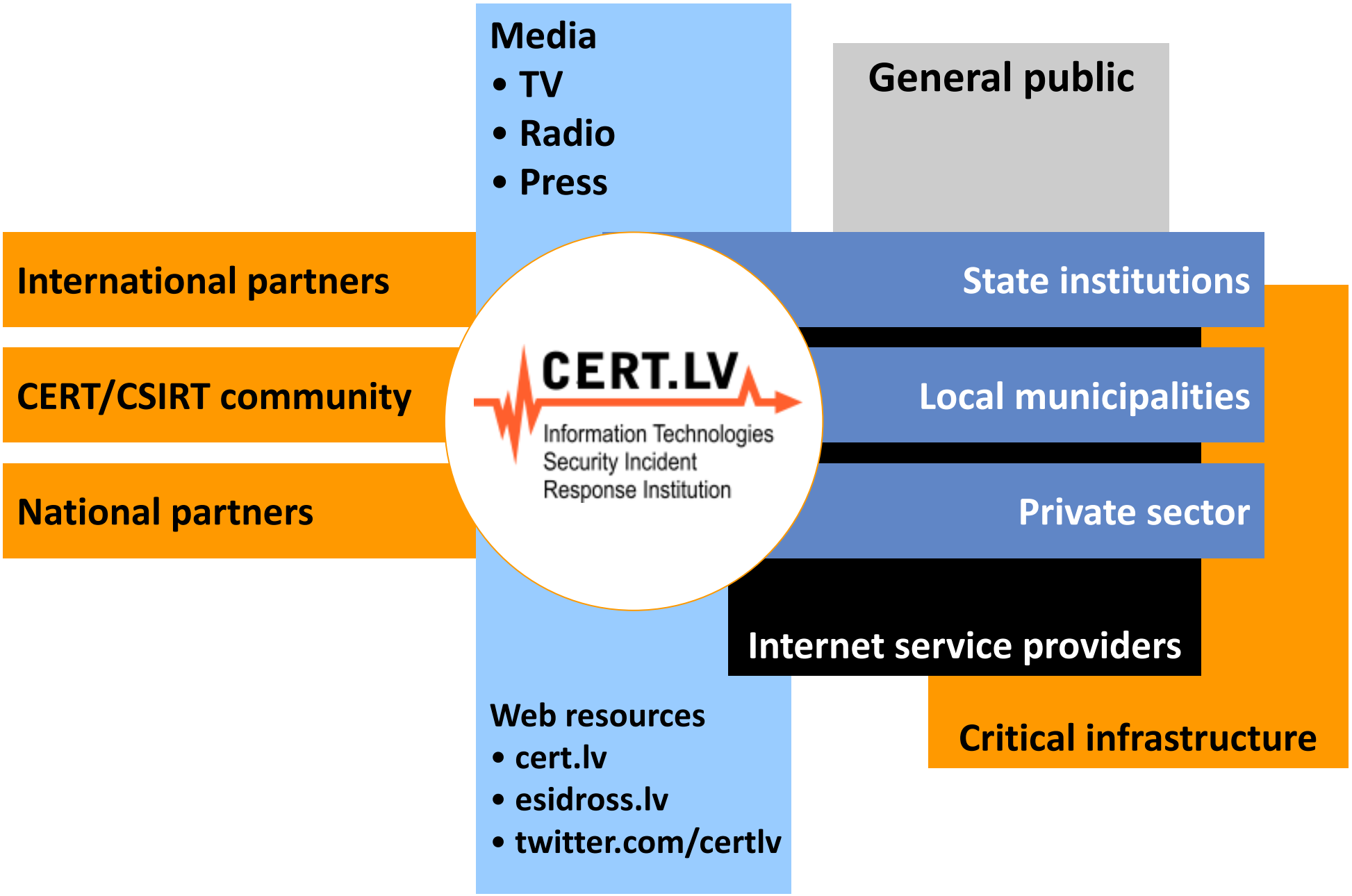
Baiba Kaškina, CERT.LV

Brussels, 29.11.2017.

CERT.LV

CERT.LV
Information Technologies
Security Incident
Response Institution

- **Information Technology Security Incident Response Institution of the Republic of Latvia**
- **Operates on basis of IT Security Law**
- **State funded**
- **All services are free of charge**


Media
• TV
• Radio
• Press
General public
International partners
CERT/CSIRT community
National partners
CERT.LV
Information Technologies
Security Incident
Response Institution
State institutions
Local municipalities
Private sector
Internet service providers
Critical infrastructure
Web resources
• cert.lv
• esidross.lv
• twitter.com/certlv

CERT.LV
Information Technologies Security Incident Response Institution

CVD in Latvia – current status

- **Policy implemented in some organisations**
- **Many real cases, most of them have been coordinated via CERT.LV**
  - **eID software**
  - **Social network**
  - **E-banking**
  - **Riga city transportation system**
- **In 2017 – about 40 reports**

CERT.LV
Information Technologies Security Incident Response Institution

CVD – attempt to put it in the law

- **Experience from 2016**
- **Working group included lawyers and the hacker community**
- **Proposal for the law**
- **Failure**

CVD – attempt to put it in the law

- **Several countries have implemented policies**
- **Latvia – legal system where only the law is relevant in the court**
- **So – different approach – what can be done in the law?**

CERT.LV
Information Technologies
Security Incident
Response Institution

Parts of the CVD process

1. **Discovery**
2. **Reporting**
3. **Response**
4. **Disclosure**

- **Every process must have beginning and end**
- **Precise and strict rules**
- **Fair and effective implementation**

CERT.LV
Information Technologies Security Incident Response Institution

The idea

- **To define CVD process in the law. If a researcher has followed the process, then the liability is waved.**
- **CERT.LV (or MilCERT) as the main coordinating entity**
- **Applies to State institutions, local municipalities, CII**

CERT.LV
Information Technologies
Security Incident
Response Institution

The CVD process - 1

- Researcher
  - Logs his actions
  - Finds vulnerability
  - Informs CERT.LV (or MilCERT) within 5 days
- CERT
  - Verifies the vulnerability
  - Informs the researcher (true or false)
  - If true – informs the owner of the system

CERT.LV
Information Technologies
Security Incident
Response Institution

The CVD process - 2

- Owner of the system
  - Obliged to fix the vulnerability in 90-180 days
  - Informs CERT.LV
- CERT.LV
  - Verifies if fixed
  - Informs the researcher
- The researcher – can publish info about vulnerability

CERT.LV
Information Technologies
Security Incident
Response Institution

What is hard to specify in the law

- When does the vulnerability discovery process start?
  - Immediately after discovery or max 5 days prior submission of report
- Amount of information researched would be allowed to gather during this phase
  - Causing minimal possible damage ?
  - Gather only minimal amount of data required for discovery process
- Legitimacy of methods and instruments
- Publishing
  - If published before fixed – then liability is not waved
  - Freedom of speech?

CERT.LV
Information Technologies Security Incident Response Institution

Failure – why?

- **Process in general too complicated**
- **Objections from State Police**
  - **Sufficient and grounded risk analysis is not presented**
  - **May lead to unexpected and unpredicted consequences**
  - **Did not foresee creating a researchers register = no anonymous reporting**

CERT.LV
Information Technologies
Security Incident
Response Institution

Conclusions

- **It is not a defeat**
- **Government approved the idea of CVD process in the law**
- **Private sector is encouraged to have CVD policy**
- **CERT.LV acts as the trusted party de facto**
- **Next iteration – when?**

CERT.LV
Information Technologies
Security Incident
Response Institution

For the next iteration

- **CERT.LV – trusted party**
- **Better definition of proportional and disproportional activity**
- **Concerns about the anonymity of a researcher should be addressed**

Based on the scientific article by Uldis Ķinis

Paldies!
Thank you!

https://www.cert.lv

baiba.kaskina@cert.lv