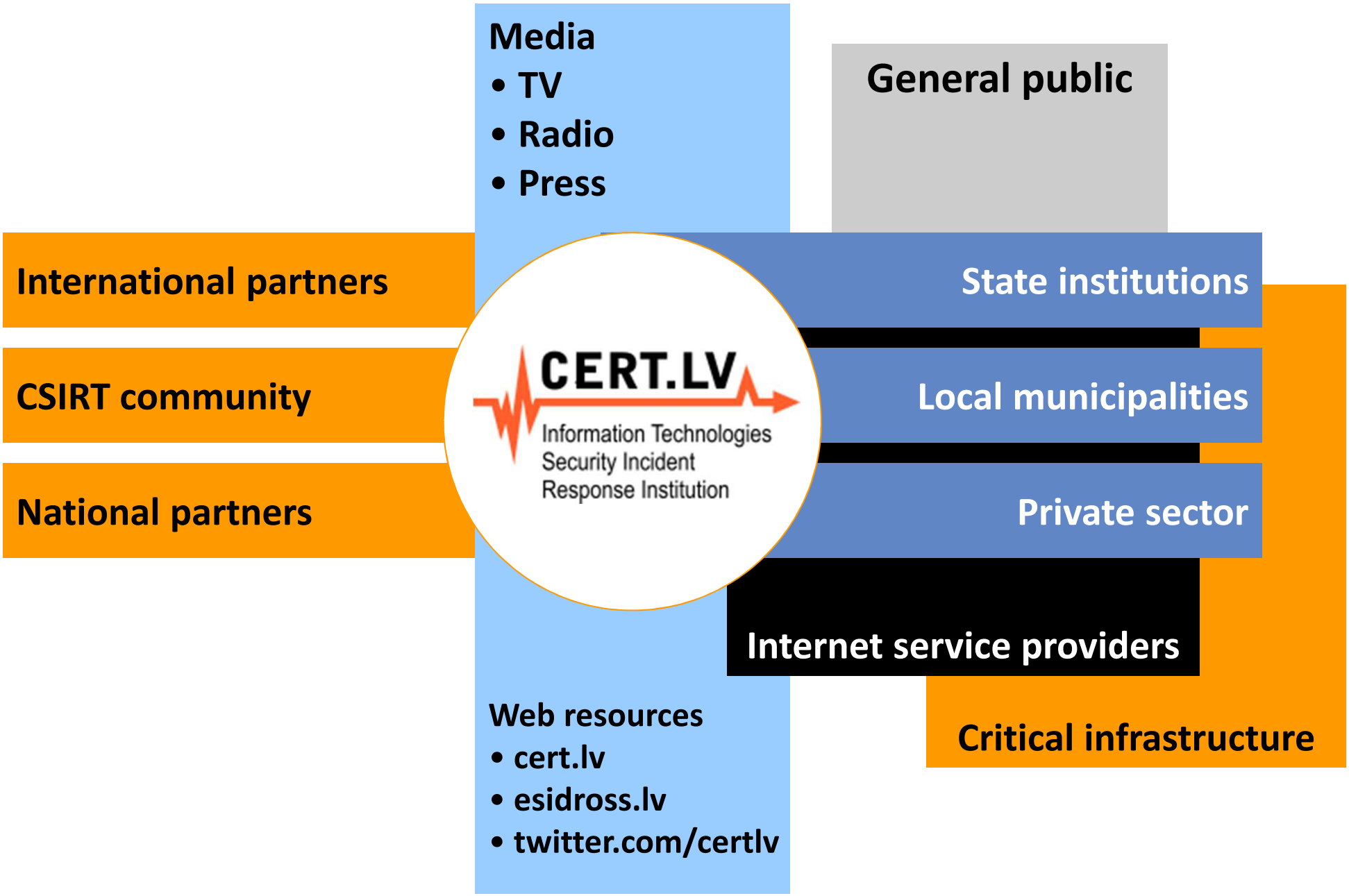
CERT.LV
Information Technologies
Security Incident
Response Institution

RDP in Latvia

Baiba Kaškina, CERT.LV

TF-CSIRT, Riga, 13.05.2016.


Media
• TV
• Radio
• Press
General public
International partners
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

What is Responsible Disclosure?

CERT.LV
Information Technologies Security Incident Response Institution

- **Responsible**
  - Coordinated disclosure
  - Rules of engagement & principle of doing the least possible harm just to provide POC
  - ISO/IEC 29147, ISO/IEC 30111
  - Intention
- **Full disclosure**
  - Good
  - Bad
  - Ugly

CERT.LV
Information Technologies
Security Incident
Response Institution

Responsible or Coordinated Disclosure Policy

- Issues
  - How to protect the researcher?
  - How to help the constituency?
  - How to manage the vulnerability?
- Some CSIRTs are heavily involved
- All CSIRTs can get involved – i.e. Heartbleed bug

RDP/CDP in Latvia – current status

CERT.LV
Information Technologies Security Incident Response Institution

- Policy implemented in 1 bank
- Multiple real cases, most of them have been coordinated via CERT.LV
    - eID software
    - Social network
    - E-banking
    - Riga city transportation system

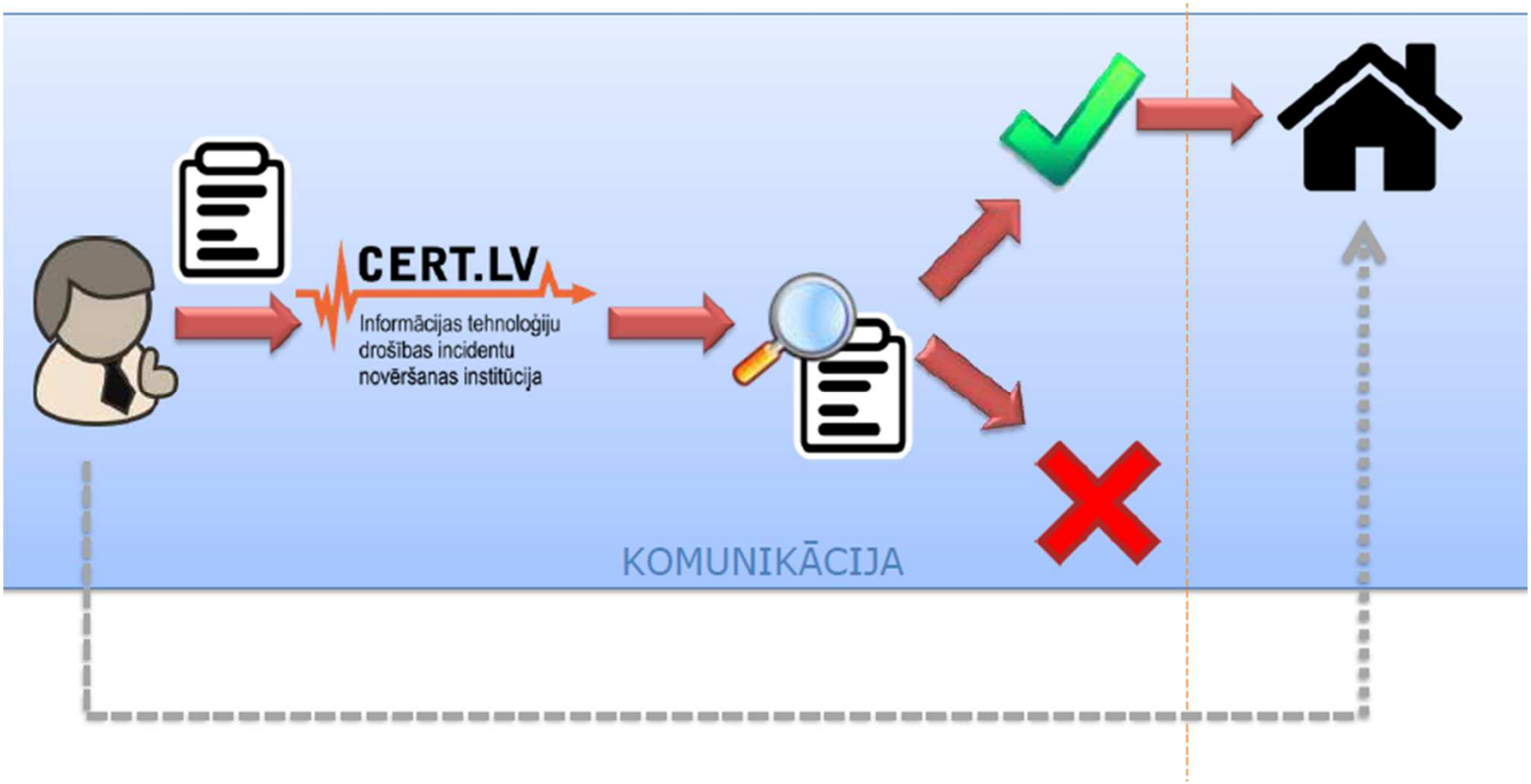
RDP/CDP in Latvia – we go for the law!

CERT.LV
Information Technologies Security Incident Response Institution

- Several countries have implemented policies – NL!
- Latvia – legal system where only the law is relevant in the court
- So – different approach – what can be done in the law?
  - Extensive consultations with lawyers
  - Discussion with white hackers' community

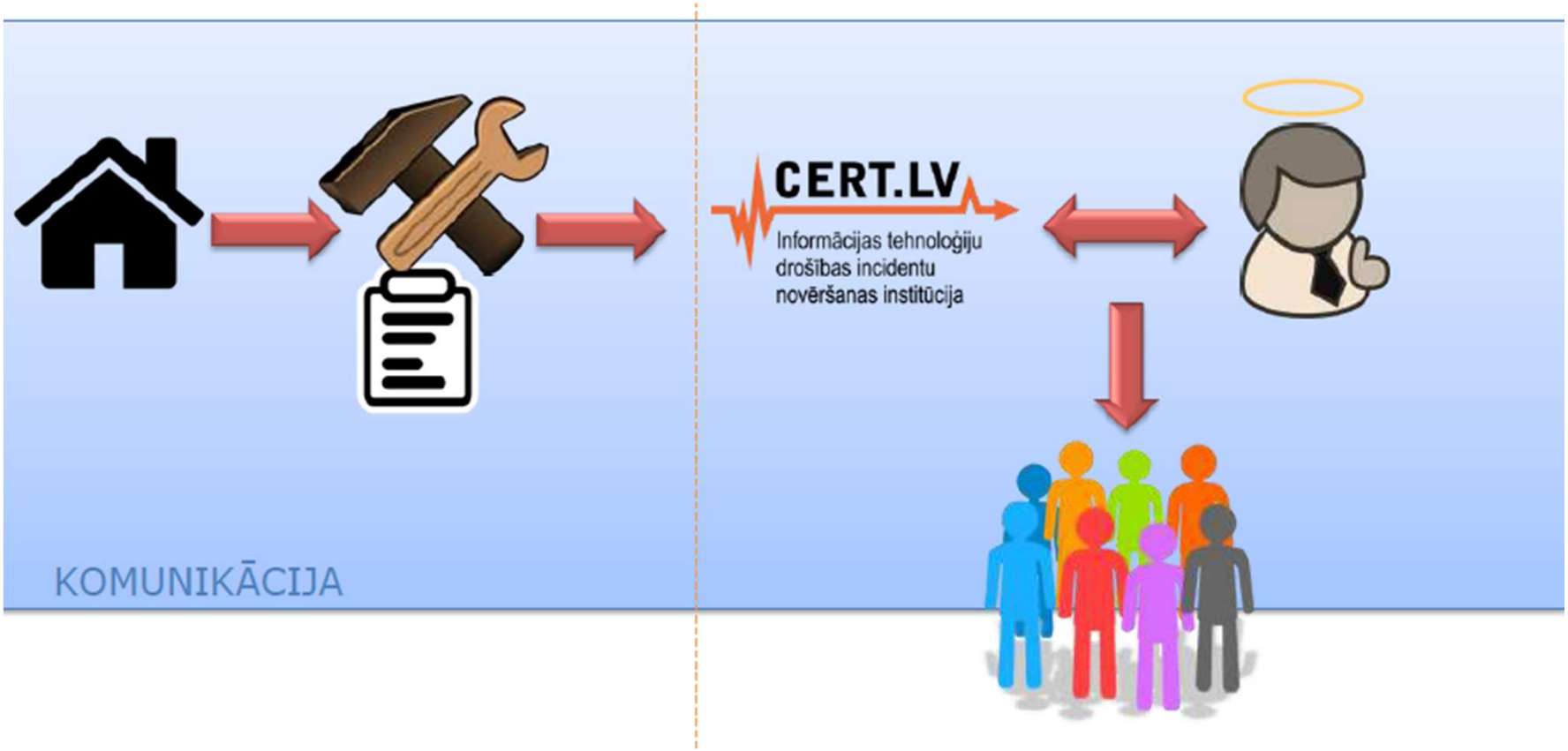
CERT.LV
Information Technologies
Security Incident
Response Institution

RDP/CDP in Latvia



CERT.LV
Information Technologies
Security Incident
Response Institution

RDP/CDP in Latvia



Changes in 2 laws – in preparation

1. **Criminal law**
   - **Clause on professional risk**
   - **Risk accepted for greater good**
   - **Amendment needed to apply professional risk for clauses on cyber crime**

Changes in 2 laws – in preparation

CERT.LV
Information Technologies Security Incident Response Institution

2. IT Security law – currently:

- Establishes and defines CERT.LV
- Duties and rights in case of an incident
- Duties for state institutions, local authorities and CI
- Clauses on ISPs, personal data, IT Security counsel, etc.
- Since 2015 – <u>clause on vulnerabilities</u>

IT Security law – clause on vulnerabilities

CERT.LV
Information Technologies Security Incident Response Institution

- **Defines vulnerability**
- **Sets responsibilities for CERT.LV and state institutions, local authorities and CI in case a vulnerability is found**
  - **What to do if the institution finds it**
  - **What to do if CERT.LV finds (learns) about it**
- **Institutions are obliged to fix the problem within 90 days**

IT Security law – updated clause on vulnerabilities

CERT.LV
Information Technologies Security Incident Response Institution

- **Adds a clause on what to do if another person finds/learns about the vulnerability**
- **This clause should establish what is the responsible disclosure process and imply if person follows this process he/she more likely will not be prosecuted based on the Criminal law Professional risk point**

IT Security law – updated clause on vulnerabilities

- **In process!!!**
- **Some things are decided:**
  - **CERT.LV have to be informed (state, local authorities, CI)**
  - **CERT.LV will verify the vulnerability and do the coordination part**

IT Security law – updated clause on vulnerabilities

- **Problems (1):**
  - **How to define that vulnerability has to be found with minimal damage?**
    - **Impact to confidentiality, integrity and availability**
    - **Minimal set of data to proof the problem**
  - **How to put in the law the communication process? How granular?**
    - **«Thank you» when the report is received**
    - **«Yes/no» when the vulnerability is verified**
    - **90 days process from that day – updates?**
    - **CERT.LV can extend 90 days period?**

IT Security law – updated clause on vulnerabilities

CERT.LV
Information Technologies Security Incident Response Institution

- **Problems (2):**
  - **Publishing – what to say/not to say in the law about it?**
    - **Freedom of speech**
    - **If you publish before «the time» you can get prosecuted**
  - **Criminal law – which clauses are related to the professional risk exception?**
    - **What about usage of automated systems for attacking?**
    - **To prosecute 4 attributes of a criminal offence have to be present – including malicious, motivated intention**

RDP/CDP in Latvia – way forward

- **We'll get there! - changes in the IT Security law and Criminal law**
- **Explanation, educational work**
- **Additional duties for CERT.LV**

RDP/CDP – what's in it for CSIRTs?

CERT.LV
Information Technologies Security Incident Response Institution

- How much CSIRTs want / have to be involved?
- Are we the only coordinating body?
- Cooperation with the hackers' community
  - CVE numbers
- Help to the constituency
  - How to deal with the vulnerability
  - How to handle the PR part
  - How to explain to the management
  - …

Paldies!
Thank you!

https://www.cert.lv

baiba.kaskina@cert.lv