

«Legal, technical and coordination challenges of the responsible disclosure process»

Panel discussion

Panelists

- **Nathalie Falot**, Senior Legal Consultant, Considerati
- **Ieva Ilves**, MoD
- **Varis Teivāns**, CERT.LV deputy manager
- **Kirils Solovjovs**, IT security researcher

What is Responsible Disclosure?

A security researcher finds a vulnerability, he/she can:

- **Do nothing**
- **Make it public (full disclosure)**
- **Sell it on the black market**
- **Tell the vendor / IS owner / CSIRT**

If the info is provided to the IS owner/vendor/CSIRT and not released publicly before it is fixed, it is responsible disclosure!

Problem space

Researcher is vulnerable

Legal responsibility for vendors
who do not fix bugs?

Security through obscurity is a
bad strategy

Educational challenges

What is the role of CSIRTs?

Owners have to have capacity
to react

Bug bounties

Naming and shaming should
not be one sided

Legal frameworks

What is the role of
governments?

Companies / institutions do not
want to pay for security

Legal challenges in Latvia

- **To establish RD in the law – IT Sec & Criminal**
- **To define:**
 - **The RD process**
 - **When liability is waved**

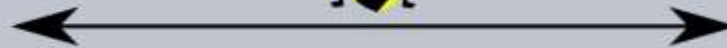
**Responsible vulnerability disclosure
process in accordance with version
08.09.2016. of law proposal No. VSS-448**




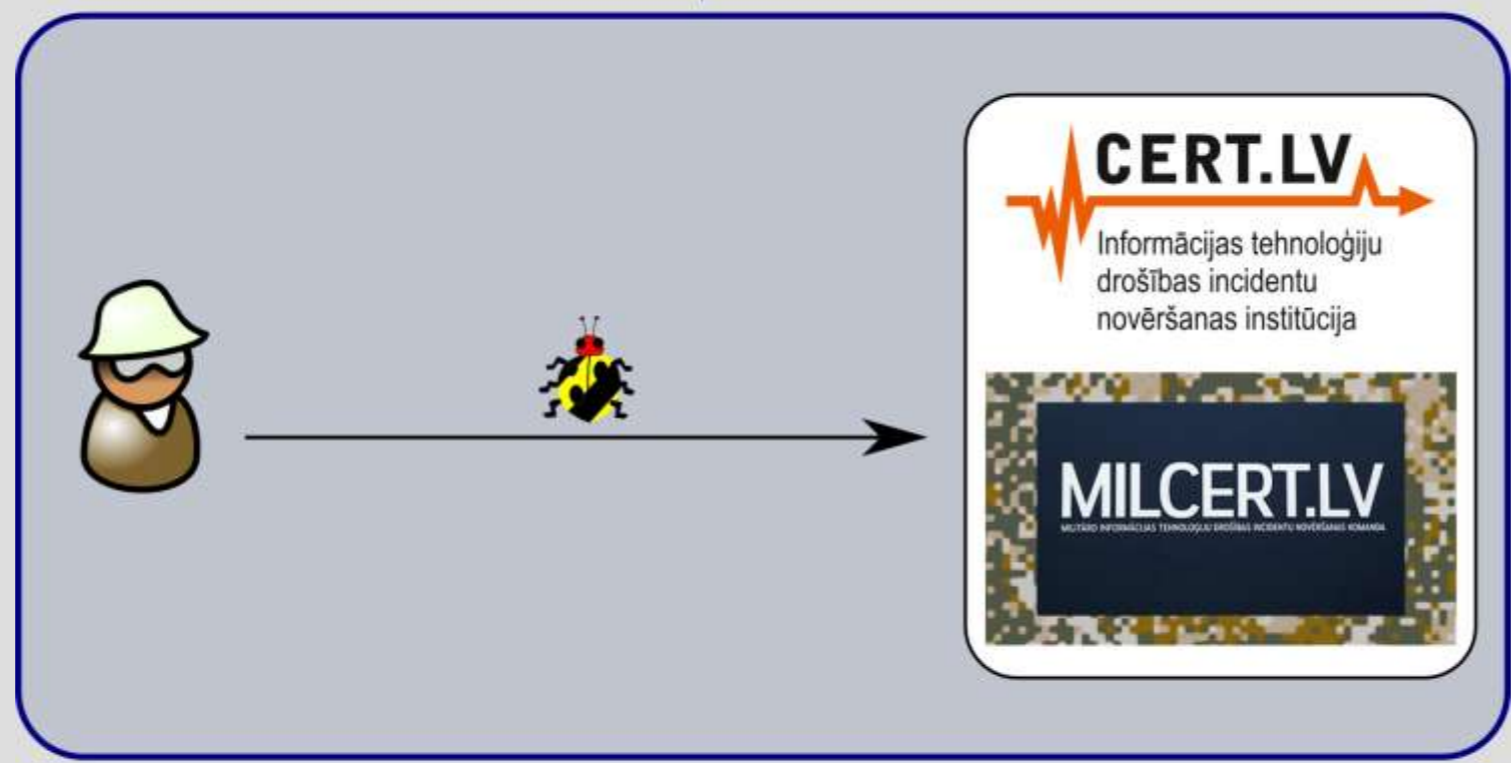
creates evidence in a verifiable manner
through audit trails and other means
necessary



accesses data as little as necessary in order to
discover the vulnerability



↓  immediately, but no later than after 5 workdays



CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija



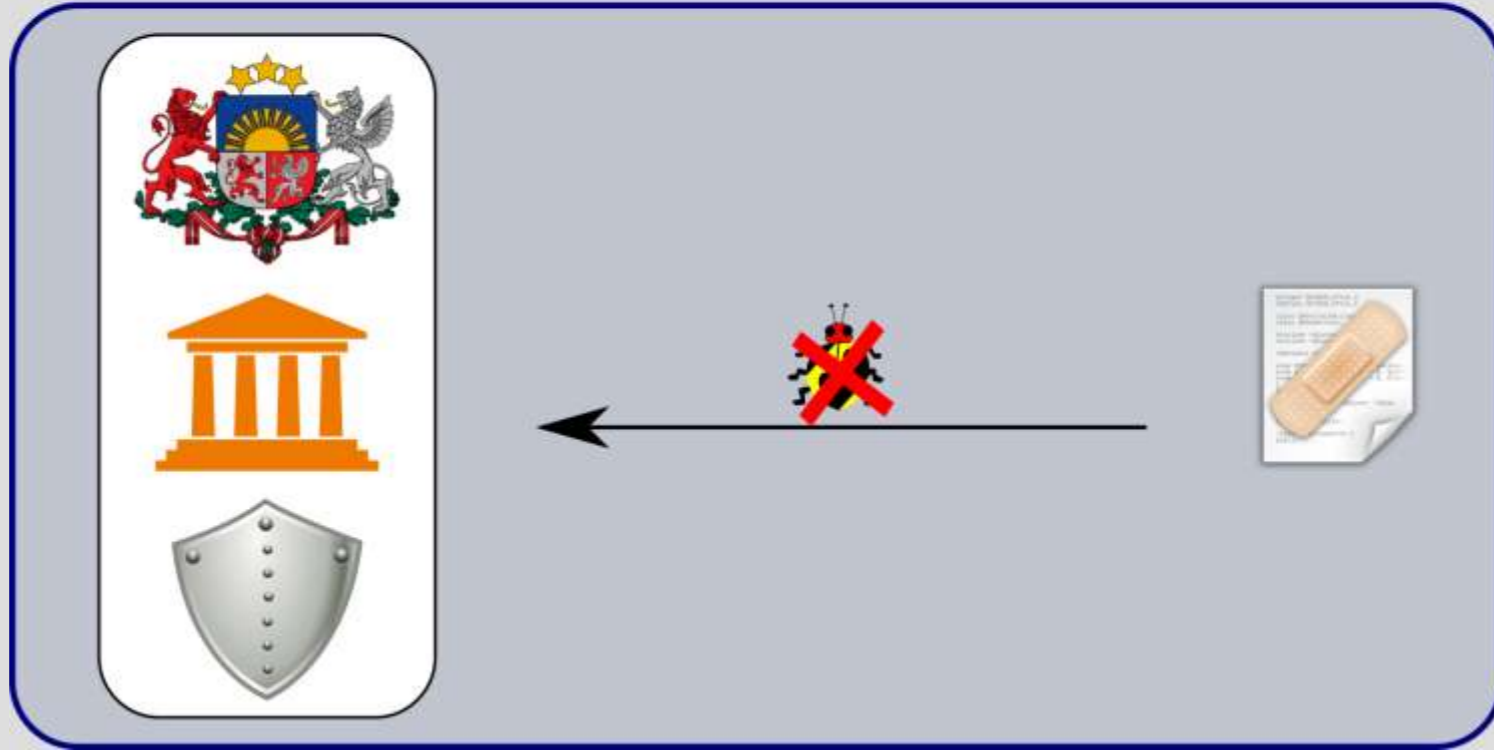
CERT.LV

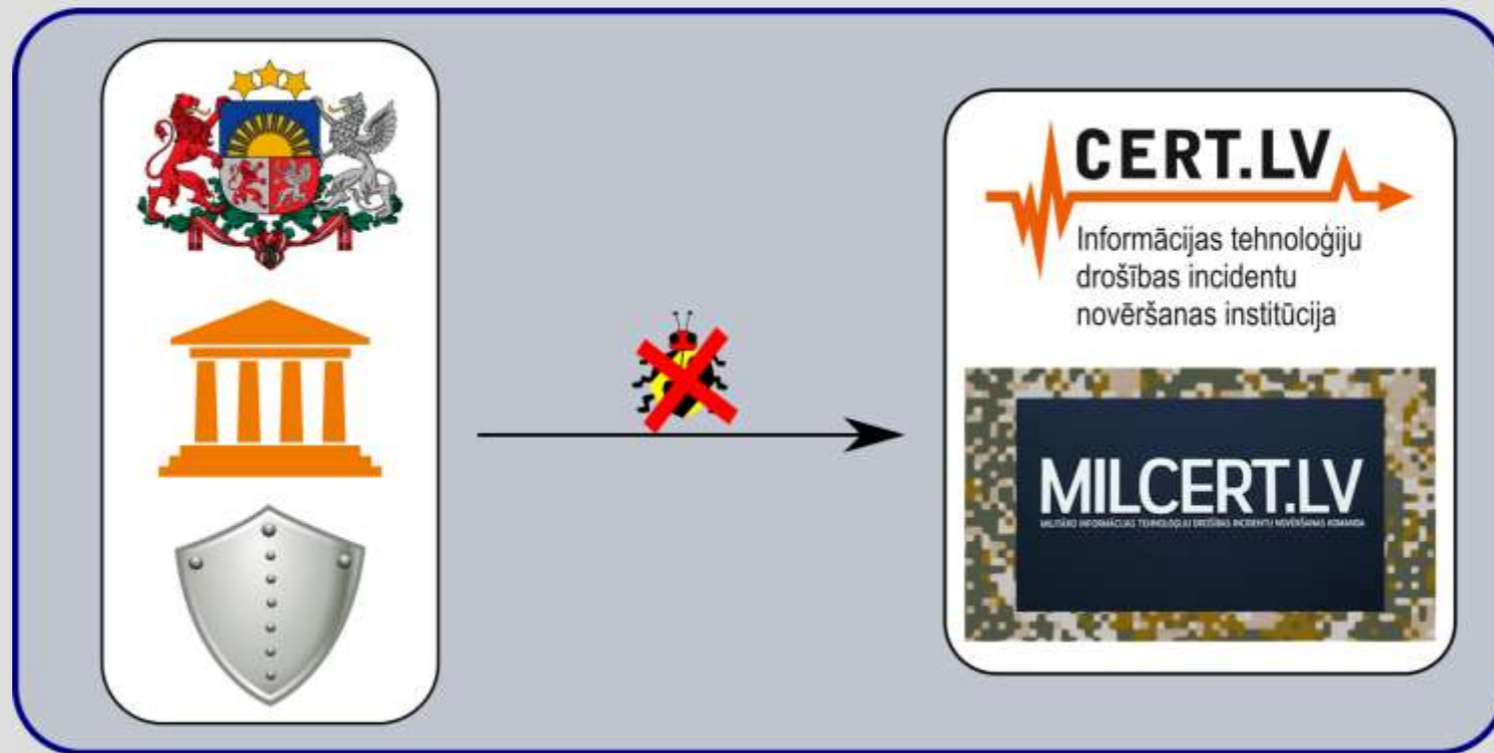
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

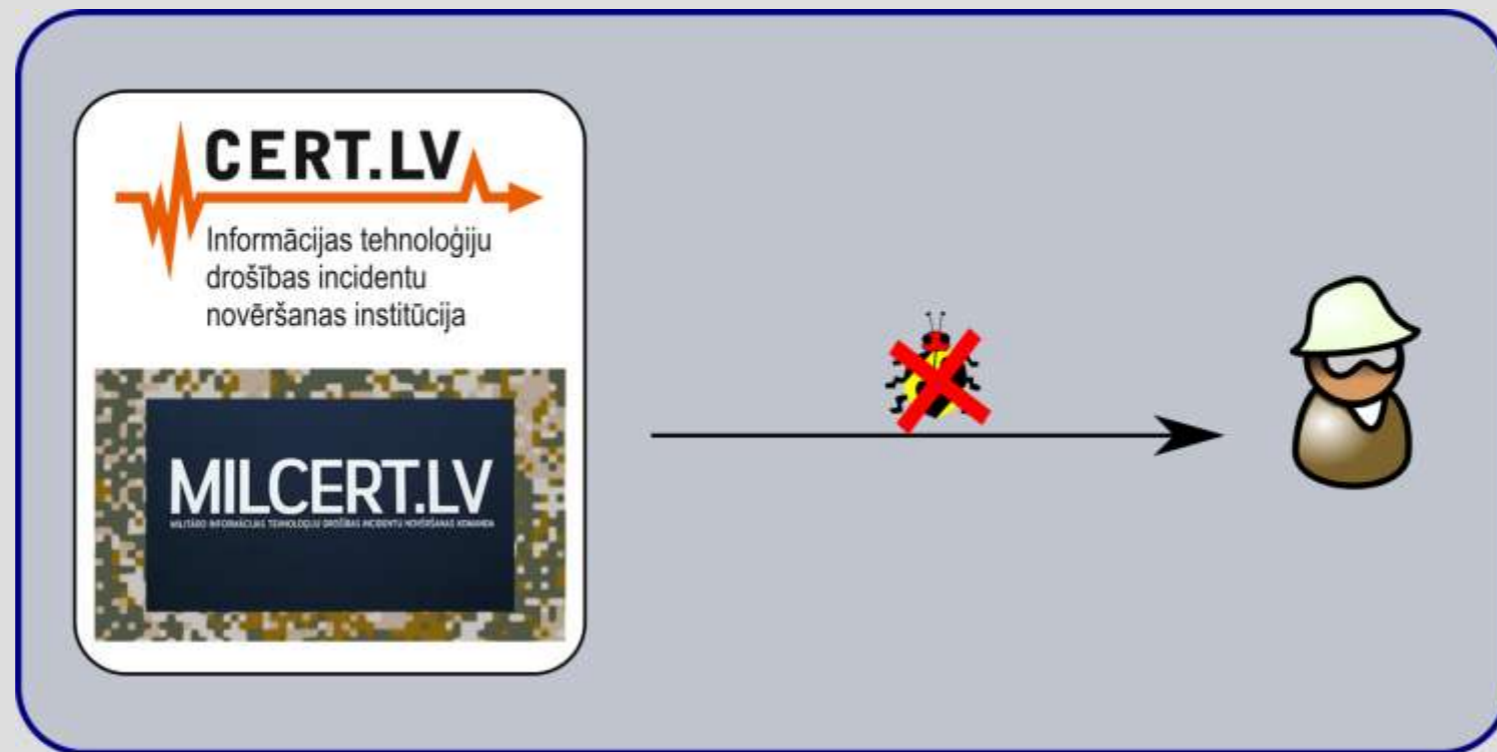




90 - 180
days







Discussion

Researcher is vulnerable

Legal responsibility for vendors
who do not fix bugs?

Security through obscurity is a
bad strategy

Educational challenges

What is the role of CSIRTs?

Owners have to have capacity
to react

Bug bounties

Naming and shaming should
not be one sided

Legal frameworks

What is the role of
governments?

Companies / institutions do not
want to pay for security



Thank you!

<https://www.cert.lv>