Establishing a CSIRT

Computer Security Incident Response Team as Integral Part of Campus Security

Jan Soukal, CSIRT-MU

soukal@ics.muni.cz, http://csirt.muni.cz

April 25, 2014

About CSIRTs

- **Computer Security Incident Response Team**
- **A team typically represents a central contact and coordination point for an organization.**
- **CSIRT-MU, CESNET-CERTS, GovCERT.CZ, etc.**

CSIRT-MU

- A security team of Masaryk University, operated by the Institute of Computer Science.
- 2009 – established.
- 2011 – accredited by the Trusted Introducer.
- More info at http://csirt.muni.cz

CSIRT-MU

Resources

- Before 2009 – 0.2 FTE,
- Today – 14 FTEs.

Constituency & Network

- up to 45.000 users,
- Up to 20.000 active computers per day,
- 147.251.0.0/16, 2001:718:801::/48,
- domain muni.cz.

Establishing a CSIRT

Challenges and opportunities based on a 5-year evolution of the CSIRT-MU.

Starting position

- Support from the management is essential for a new-born security team.
- Clearly defined responsibility and authority should be assigned to the team.
- The majority of issues is "political" rather than technical when establishing a CSIRT.

Activities

Basic

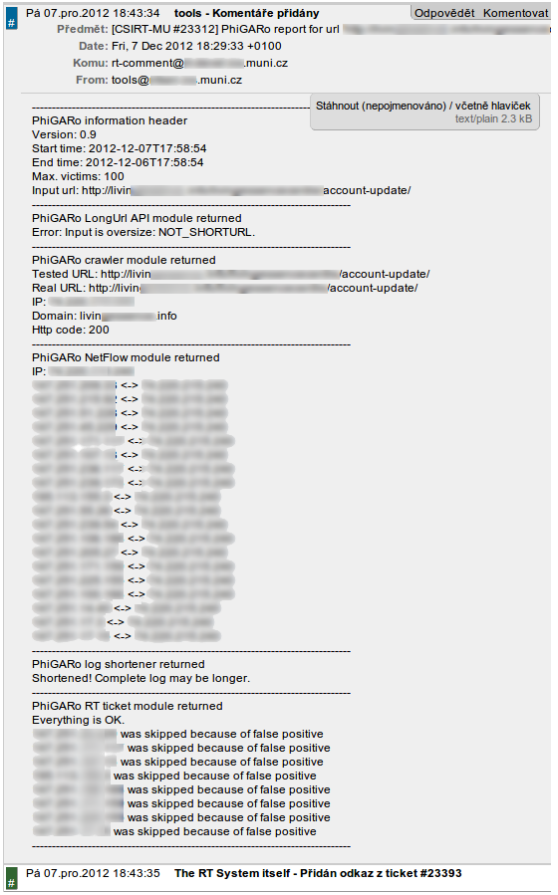
1. Incident handling of reported and detected threats.
2. Cooperation with CSIRT teams and other organizations.
3. Education of own users.

Extended

- Network traffic monitoring to detect threats.
- R&D to be state-of-the-art.

Incident Handling

1. An unified abuse contact to collect incident reports.
2. A ticketing system to manage communication.
   - Request Tracker
3. Clarity of communication.

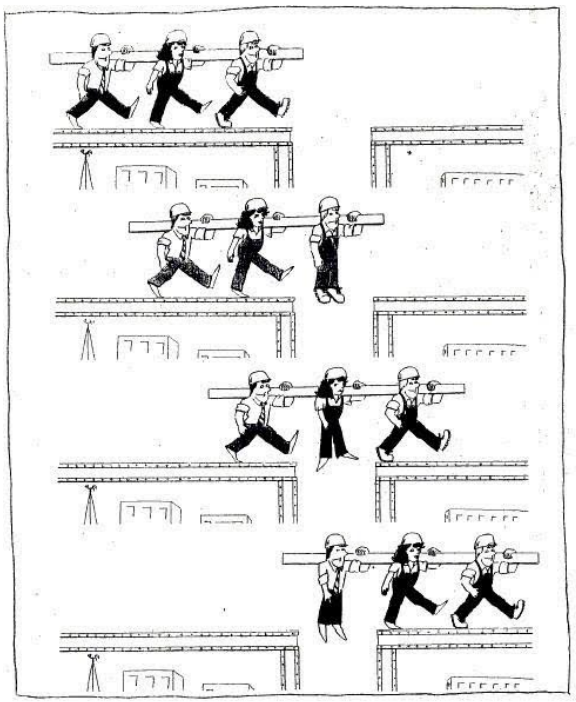


Policies and directives

- Clear responsibility must be given.
- "Who is responsible for what."
- The team should adopt crisis management and policies.

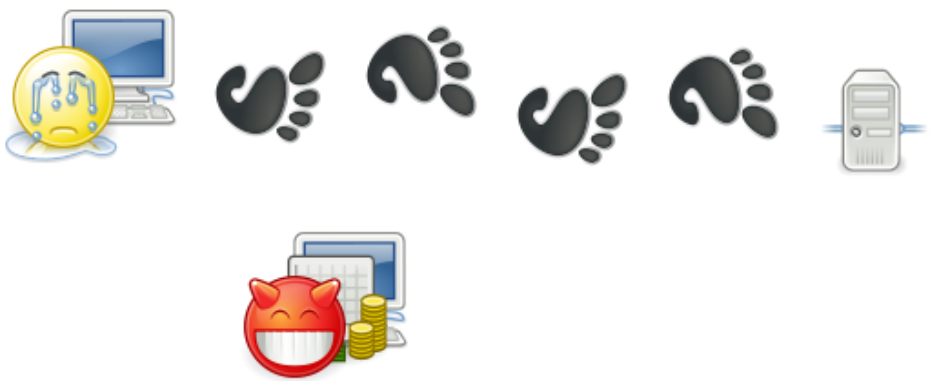
Cooperation

- Share experience, expertise, tools and useful data.
- Build sufficient CSIRT community around your team.
- Trusted Introducer, other security teams, etc.



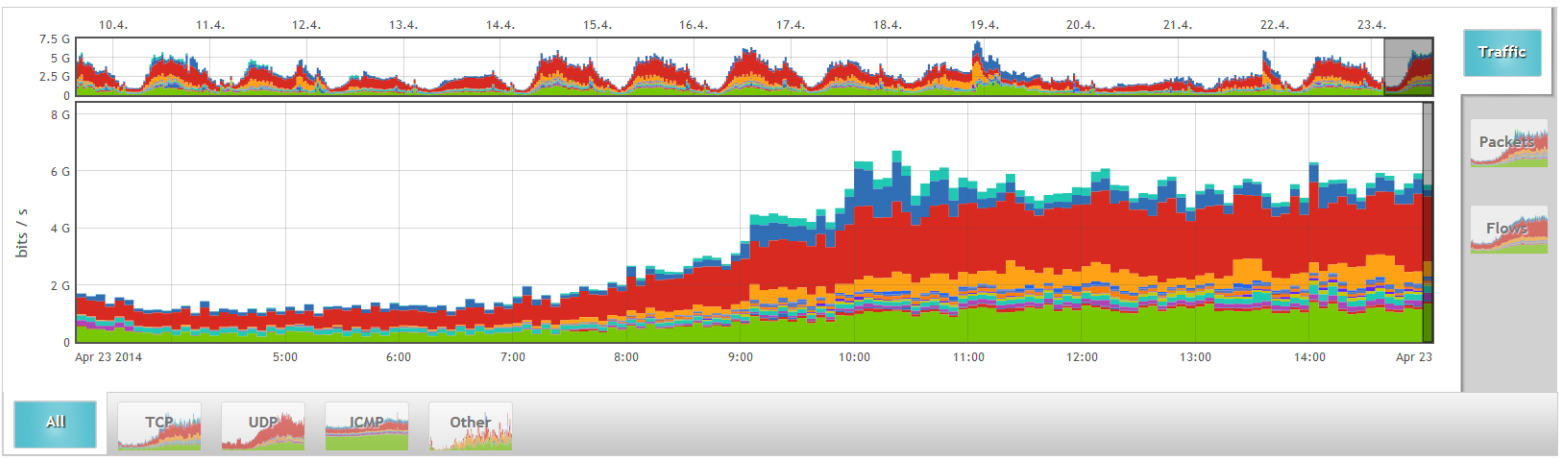
Education

- Educating users **should** be less expensive than resolving "their" incidents.
- Alerts and warnings, interactive web, workshops, ...
- But, educational activities have **low** impact while being very resource consuming.



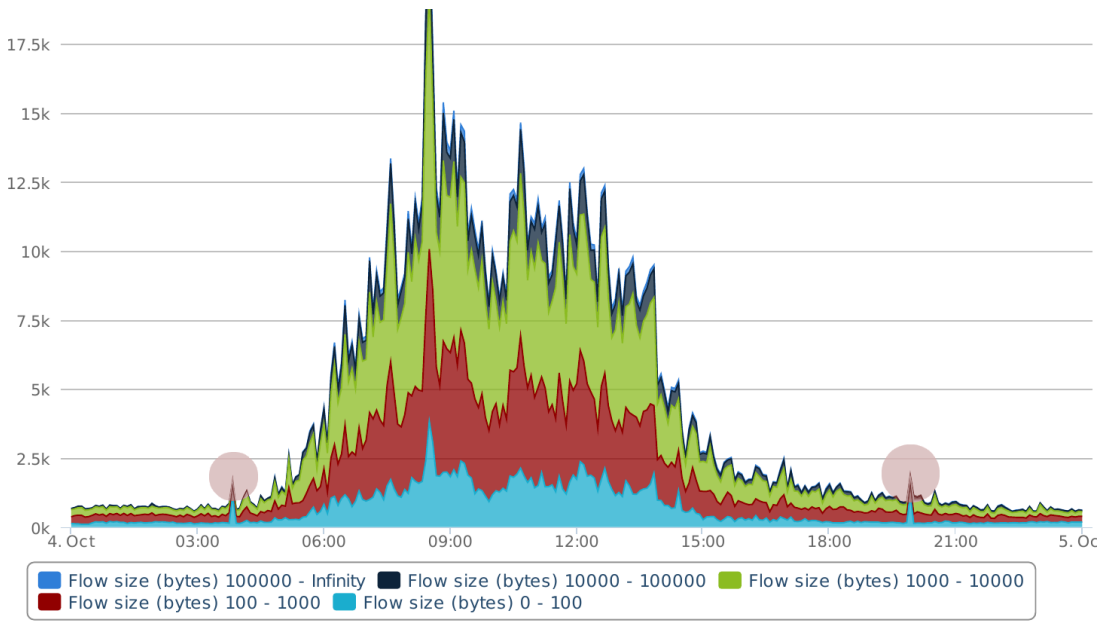
Network traffic monitoring

1. Log analysis and honeypot detections.
2. DPI – e.g. Heartbleed attempts detection.
3. Flow monitoring and analysis (NetFlow or IPFIX).



Research

- A way to be state-of-the-art.
- Considerably wider funding options.
- Possibility to battle-test proposed approaches.



Development

- Based on the knowledge of the network and operational experience.
- Involve students and try to attract those talented (at a university).

Summary

- The majority of issues is "political" rather than technical when establishing a CSIRT.
- Policies and directives are crucial.
- Setting up an unified abuse contact and communication is a tedious process.
- Think twice when planning educational activities.
- Use research as a funding scheme and reputation booster.

Thank you for your attention.

Jan Soukal, CSIRT-MU
soukal@ics.muni.cz, http://csirt.muni.cz