# CSIRT-MU

## Computer security at Masaryk University


**Jan Soukal**
**soukal@ics.muni.cz**

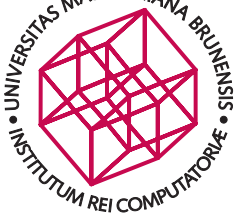
**April 11, 2014**

# What can you expect?


## I am going to:

- show how a computer security is managed at Masaryk University,
- describe activities of the CSIRT-MU in detail,
- point out typical benefits and/or issues you should expect when establishing a CSIRT team.

# CSIRT-MU




## Overview

- **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam of Masaryk University.
- Established in 2009.
- Accredited by the Trusted Introducer in Februrary 2011.
- Operated by the Institute of Computer Science, Masaryk University.
- `http://csirt.muni.cz/`

# CSIRT-MU

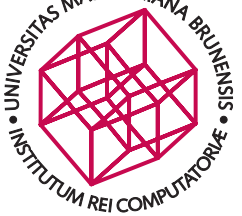
## Constituency

- All users of the Masaryk University's network – 40.000 users per day.

## Network

- Up to 20.000 active computers per day,
- 147.251.0.0/16,
- domain muni.cz.

# CSIRT-MU




- Team members are not local administrators.

## Goals

- To create trustworthy central contact point for the MU's network,
- to manage and prevent computer security incidents in the MU's network,
- to help increase security level of IT infrastructure at the MU,
- to increase elementary IT security knowledge among ordinary users at the MU.

# CSIRT-MU

## Activities

1. **Network traffic monitoring** – to see what's going on,
2. **Incident Handling** – to manage detected threats,
3. **Research** – to keep pace with attackers,
4. **Development** – to develop tools that suit our needs,
5. **Cooperation** – to share expertise and experience,
6. **Education** – mitigation of risks.

# CSIRT-MU


## Structure

1. **CSIRT-MU group** – operational tasks,
2. **Network Traffic Analysis Group** – research and development,
3. **Incident Analysis Group** – forensics experts.

## Resources

- **Operational, cca 4 FTEs.**
- **Research, cca 10 FTEs** – greatly depends on projects.

# Network traffic monitoring

## Purpose of monitoring

- You need to know what is happening in your network.
- You can detect threats and attacks or investigate reported events.
- You protect your users.
- (Czech) law aspect – you do your best to secure the network.

- No personal data is collected, just network flows are analyzed.

# Network traffic monitoring

## Users and the network

- 40.000 users per day,
- Up to 20.000 active computers per day,
- IPv4 range of 147.251.0.0/16,
- domain muni.cz.

## Monitoring infrastrucure

- 24 FlowMon probes,
- 3 main FlowMon collectors,
- IPFIX format.

# Network traffic monitoring

## Anomaly detection

- Analysis of traffic data allows you to detect malicious activities.
- We have developed and implemented several methods:
  - "generic" attacks detection – RDP and SSH brute-force, port scanning, etc.,
  - suspicious activities detection – communication with C&C, etc.,
  - even misconfigured or unsecured computers can be detected – open administration interfaces, etc.
- However, detected anomalies still have to be handled somehow...

# Incident Handling


- CSIRT-MU is the central security authority in the MU's network.
- The main task is to coordinate resolution of security incidents.

## Request Tracker – Ticketing system

- Operated by one or more incident handlers.
- No personal e-mails. One single contact instead.
- All issues are tracked and archived.
- Detection tools send reports to RT via e-mail.

# Incident Handling

## Security incident resolution

- Rougly 1.000 incidents per week – vast majority are "generic" incidents.
- Automated resolution of generic incidents is crucial.
- Specialists can focus on difficult and unusual cases.
- Example: PhiGARo anti-phishing tool – decreasing time needed for resolution from hours to minutes.

# Incident Handling

## Typical issues and Lessons learned

- **Clear responsibility** – list of responsible administrators, IT security directives, etc.
- **Communication issues** – either local admins and users often see the CSIRT team as an "enemy".
- **Vulnerable users** – low IT security knowledge, BYODs full of malware, etc.
- **People often do not care about security until something goes wrong.**

# Research

## Importance of research projects

- Setting trends rather than following them.
- Allows team to have more specialists and to raise their own.
- Increasing team's reputation.
- Creating precious contacts and relationships.
- Wider funding options.

## Risks

- Project-based funding is not reliable in a long term.

# Research

## Partners and Projects

- NSA, NCSC (Govcert) – C4e, CPG.
- Czech Ministry of Defense, U.S. Army – CIRC, CYBER, CAMNEP.
- Ministry of Interior – Security of optical components.
- Faculty of Informatics, other universities, etc.
- Other CSIRT teams – Project WARDEN.

## Details

`http://www.muni.cz/ics/services/csirt/research`

# Research

## Key advantages

- Having CSIRT team allows you to battle-test results of your research in a "real life network".
- You can use results of your research in operational activities of your CSIRT team – just hitting two birds with one stone.

# Development

## Based on

- knowledge of our network – monitoring,
- operational experience – incident handling,
- possible threats and solutions – research.

## Goals

- Automation of generic incidents' resolution – our own extensions of the Request Tracker.
- Specialized tools fitting our needs.
- Proof-of-concept implementation of proposed methods.
- Identification and attraction of talented students.

# Development

## Our tools

- **RdpMonitor** – RDP brute-force attacks detection plugin for NfSen.
- **SSHMonitor** – SSH brute-force attacks detection plugin for NfSen.
- **PhiGARo** – tool for phishing incidents' management and resolution.
- **Honeyscan** – honeynet monitoring plugin for NfSen.
- **Time series solver** – network flow time series analysis tool.

## Download

`http://www.muni.cz/ics/services/csirt/tools`

# Cooperation

## Motivation

- **Sharing experience, expertise, tools and useful data is always a good choice** – there is no need to reinvent the wheel.
- **Having sufficient CSIRT-community around your team.**
- **Also we like to cooperate with students on their bachelor or diploma theses** – of course we try to attract the best of them to our team ;)

# Cooperation

## Partners

- **National Security Authority** – together we educate security experts.
- **CESNET-CERTS** – our "parent" NREN CSIRT team.
- **TEAM CYMRU** – exchange of honeypots' data, botnet C&C contacts, etc.
- **TF-CSIRT** – enhancing of large scale communication between CSIRT teams.
- **INVEA-TECH** – university spin-off.

# Education

## Motivation

- Educating your users should be less expensive than resolving "their" security incidents.
- You (CSIRT team) should be recognized by your users – users should know you.

# Education

## Activities

- **Educational web** `https://security.ics.muni.cz` – interactive animations, explanations and warnings.
- **Phishing at your own risk** – interactive anti-phishing workshop.
- **Seminars** – for instance "We know about you".

# Education

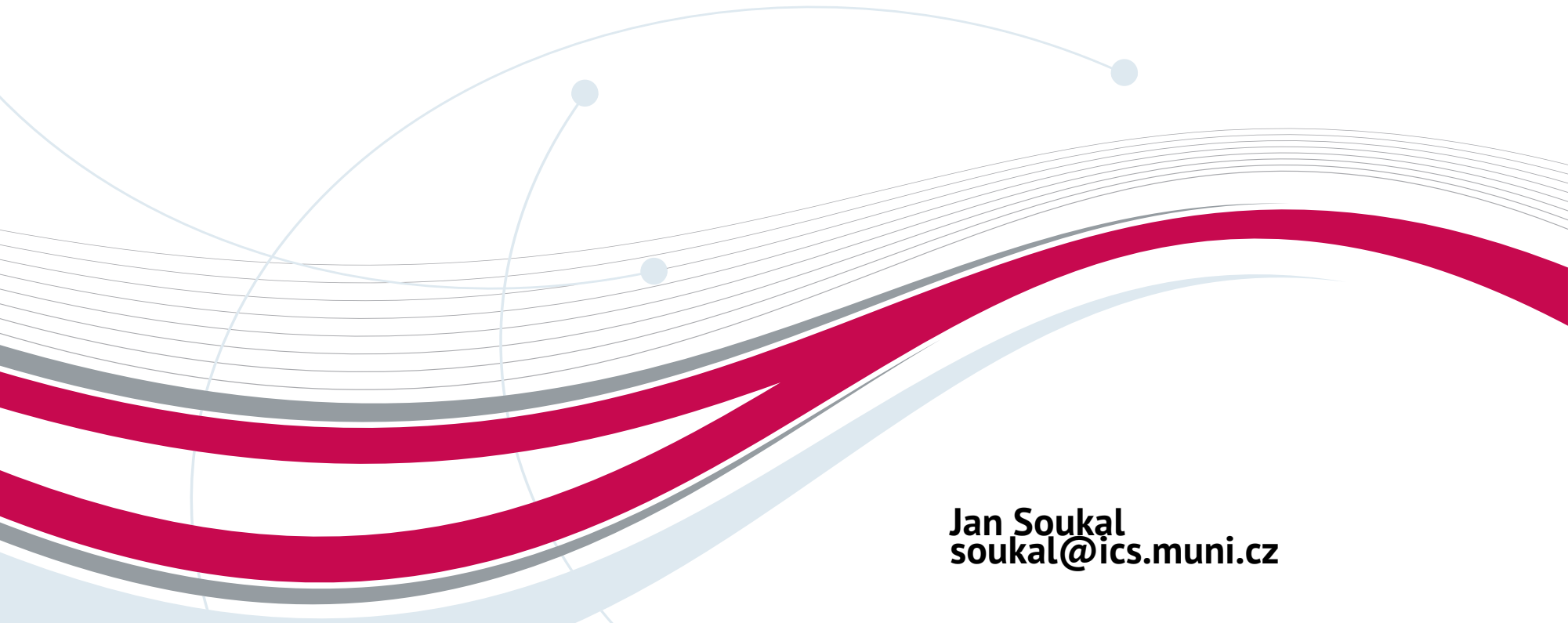
## Reality

- Educational activities have low impact while being very resource consuming.
- CSIRT team is recognized by local administrators but rarely by end users.

# Summary

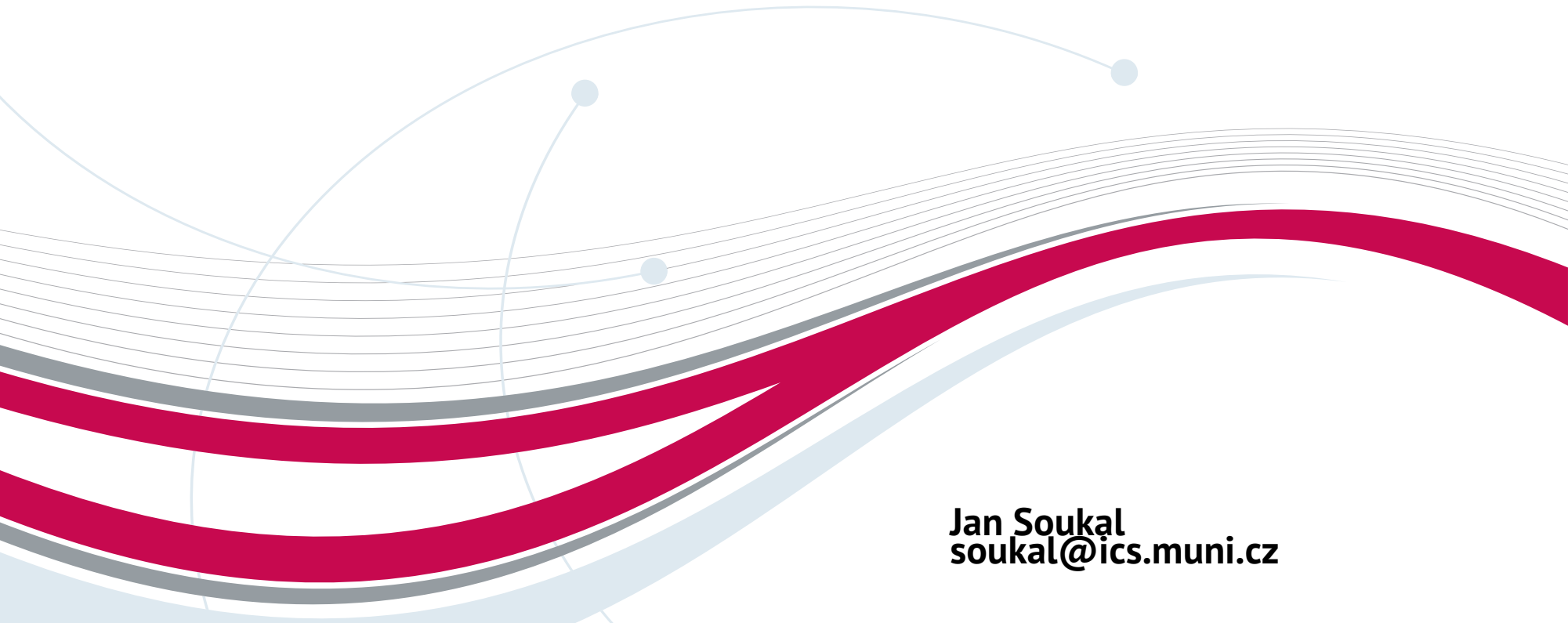

- It is possible to run CSIRT team in a campus network.
- Having an operational CSIRT team supported by network monitoring can greatly help you to extend your IT security research.
- And vice-versa, an operational CSIRT team can deeply benefit from security research.
- Having contacts in the field of IT security research is also essential.
- Think twice when planning educational activities.

# Questions & Answers



Jan Soukal
soukal@ics.muni.cz

**Thank you for your attention.**



**Jan Soukal**
**soukal@ics.muni.cz**