KYPO — A PLATFORM FOR CYBER DEFENCE EXERCISES

Symposium on “M&S Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence” (MSG-133), Munich, Germany

15th October, 2015

Pavel ČELEDA, Jakub ČEGAN
Jan VYKOPAL, Daniel TOVARŇÁK

{celeda|cegan|jan.vykopal|danos}@mail.muni.cz

KYPO
BY CSIRT-MU

KYPO Vision & Goals

Vision

- Provide unique environment for **research and development** of new methods to protect **critical infrastructure** against **cyber attacks** in Czech Republic.

Goals

- Cloud infrastructure, threat detection & advanced visualization.
- Cyber security courses and exercises – hands-on.

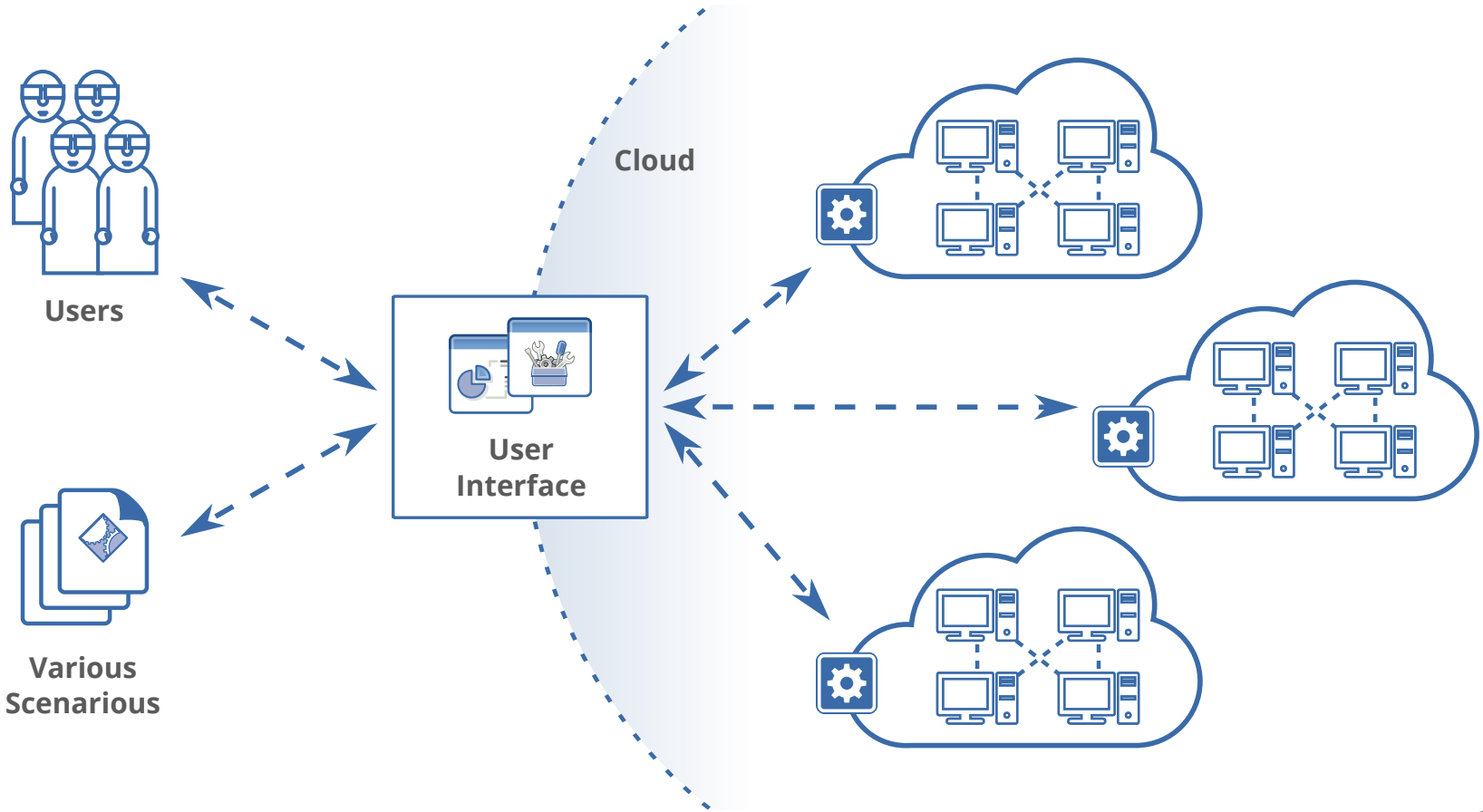
Contribution

- Increase readiness of Czech Republic in cyber research.
- Advance training methods for security teams (CERT/CSIRT).

KYPO Architecture

KYPO
BY CSIRT-MU

KYPO Architecture



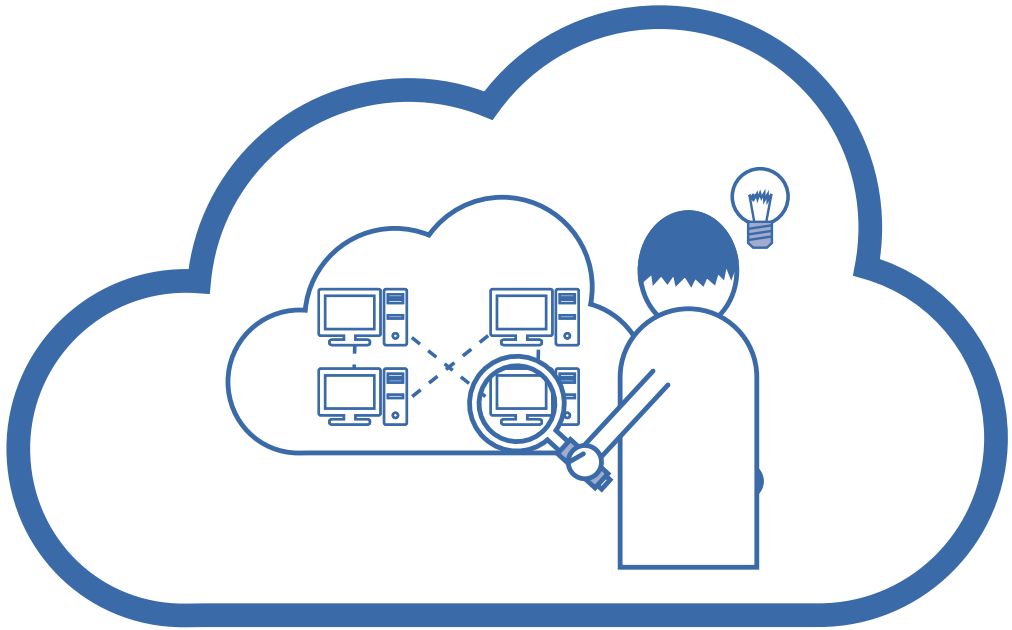
KYPO
BY CSIRT-MU

KYPO Use Cases

KYPO
BY CSIRT-MU

Cyber Research & Development

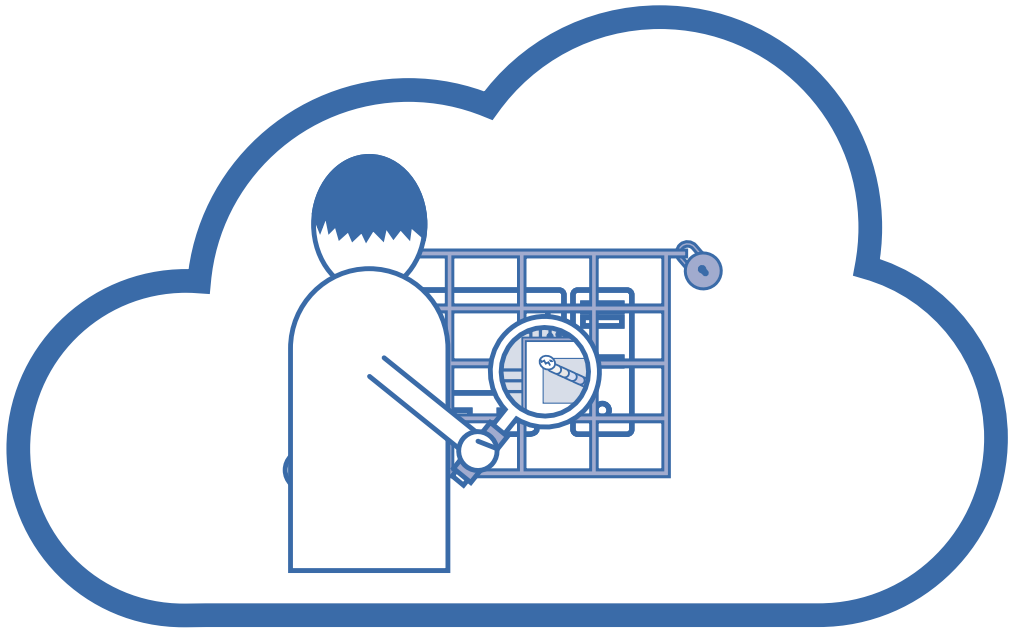
- Sandbox design makes experiments easily repeatable.
- Provides monitoring using NetFlow and packet capture (PCAP).
- Data is stored for further analysis or fast replay of experiment.



KYPO
BY CSIRT-MU

Forensics Analysis & Network Simulations

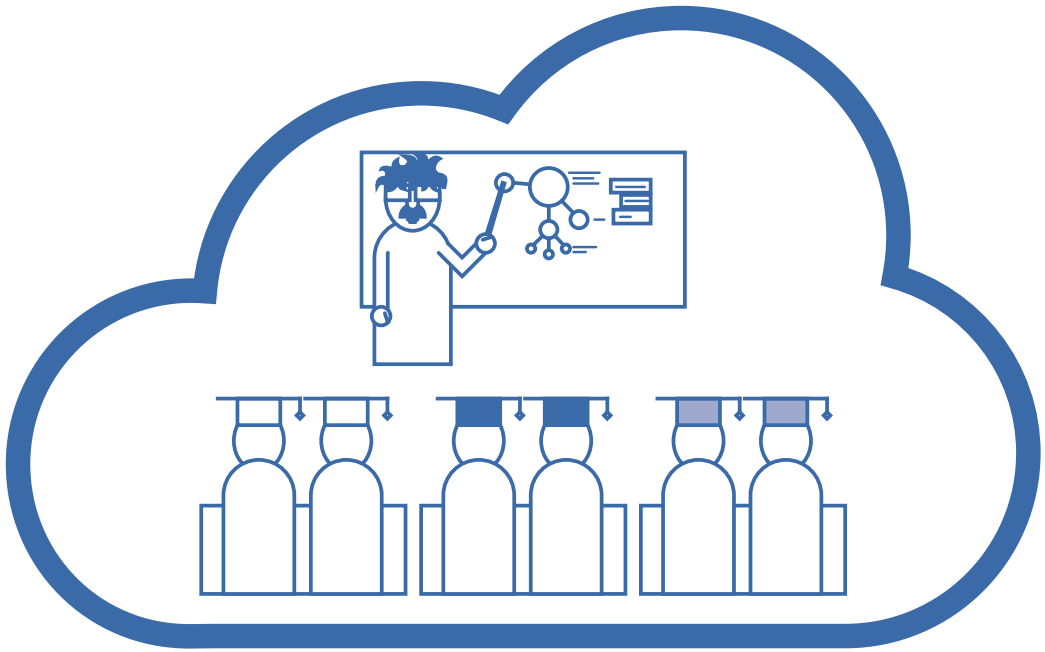
- Adjustments of the sandbox according to malware actions.
- Malware is kept in a safe isolated environment.
- Various tools can be used during the analysis in the sandbox.



KYPO
BY CSIRT-MU

Security Training & Exercises

- Covering skills needed by both users and ICT administrators.
- Main advantages are high rate of interactivity, built-in monitoring, and remote access to all computers for students.



KYPO
BY CSIRT-MU

The Design of a Cyber Defence Exercise

KYPO
BY CSIRT-MU

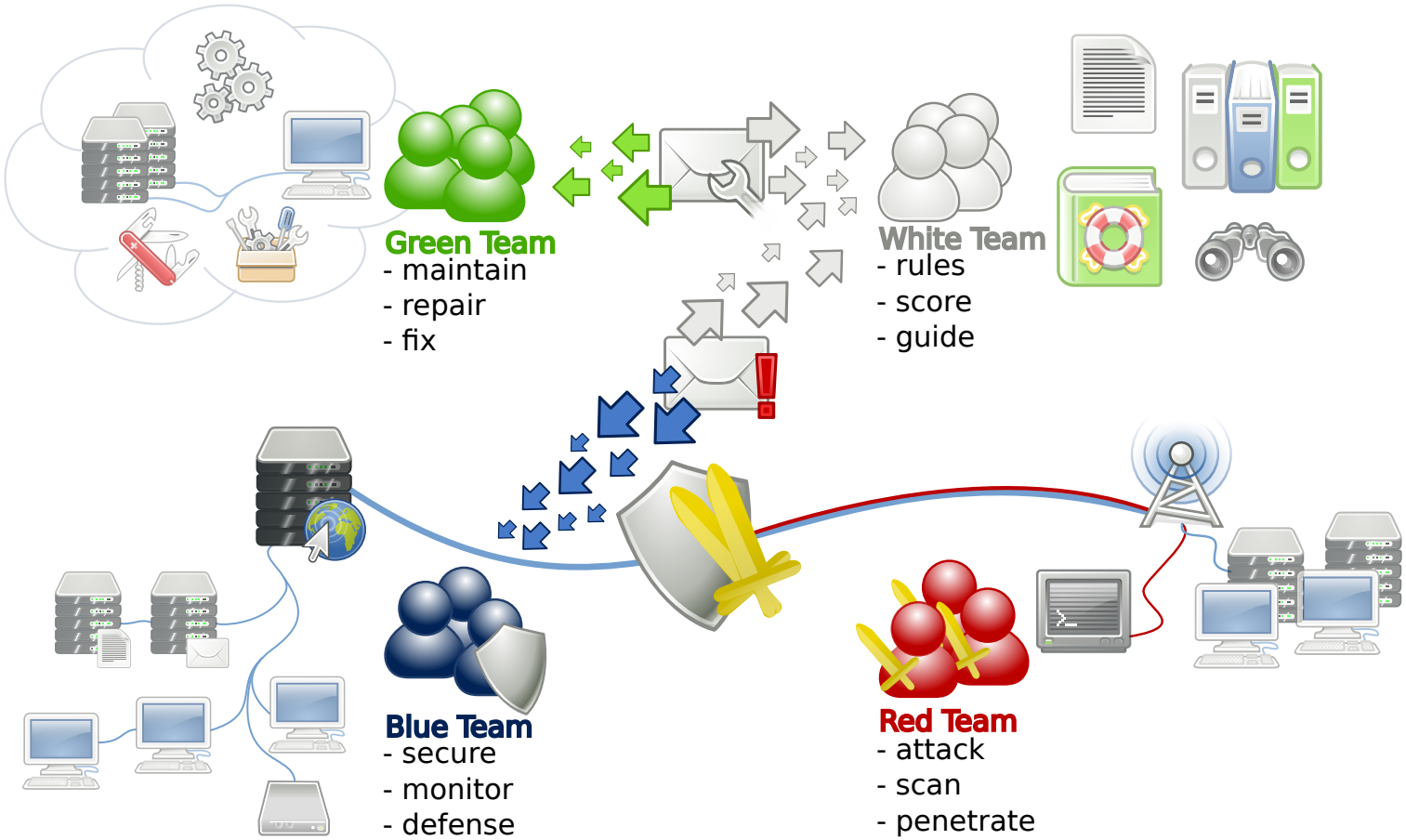
Cyber Exercise Design

Cyber Czech 2015 – October 6-7, 2015

Objectives

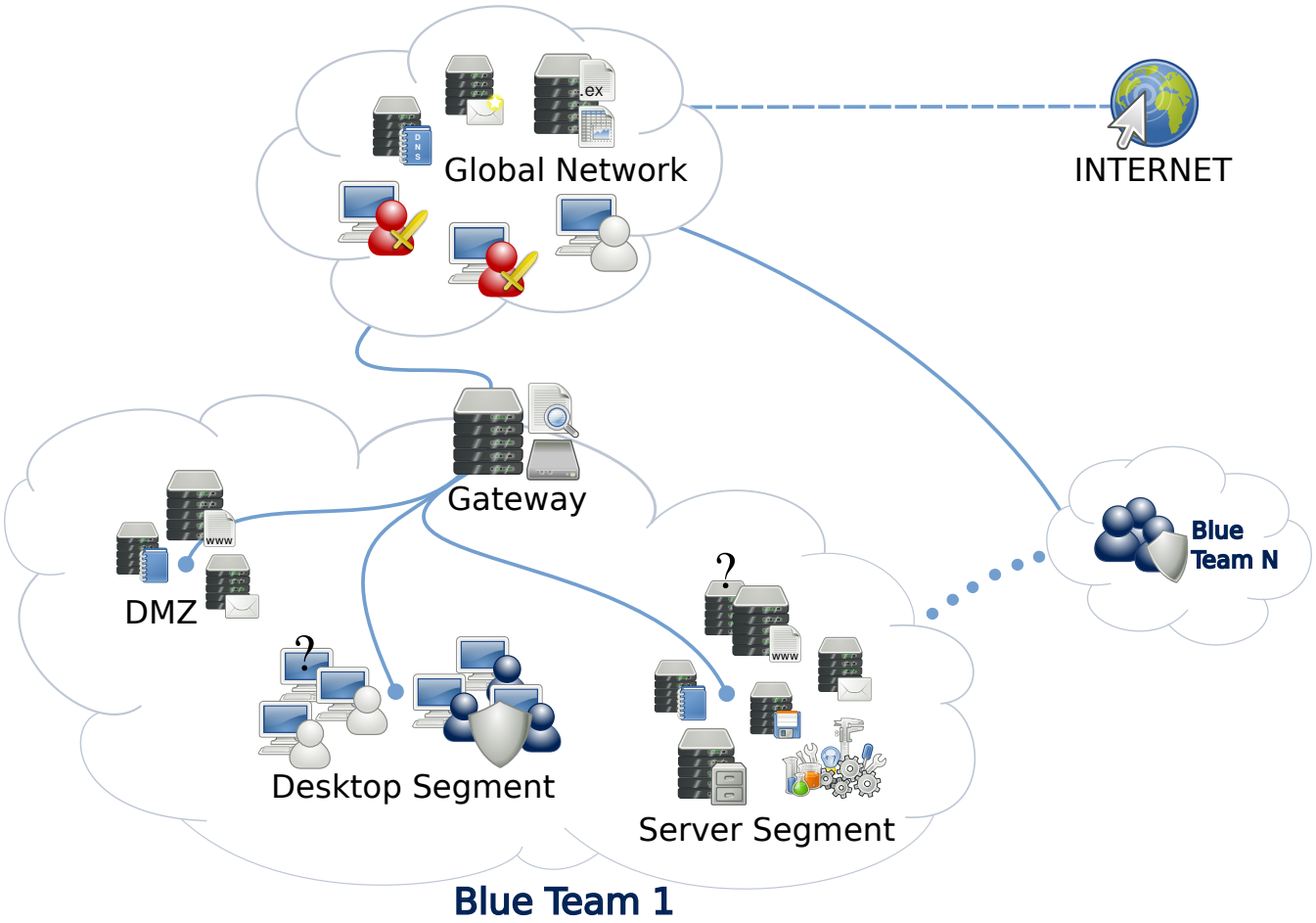
- Focused on defending critical information infrastructure.
- Participants are put into the role of CSIRT members sent into unknown organizations to recover compromised networks.
- They have to secure the simulated infrastructure, investigate attacks and cooperate with media and organizers.
- Attackers are skilled and coordinated with unclear motivations.

Roles



KYPO
BY CSIRT-MU

Technical Implementation



KYPO
BY CSIRT-MU

Monitoring Infrastructure

- Built-in network traffic monitoring (provided by the KYPO platform).
- Ad-hoc host-based monitoring (based on Syslog).
- Ad-hoc service monitoring based on Nagios (network- and host-based).
- Basis for the scoring system and post-mortem evaluation of the exercise.

Scoring Implementation

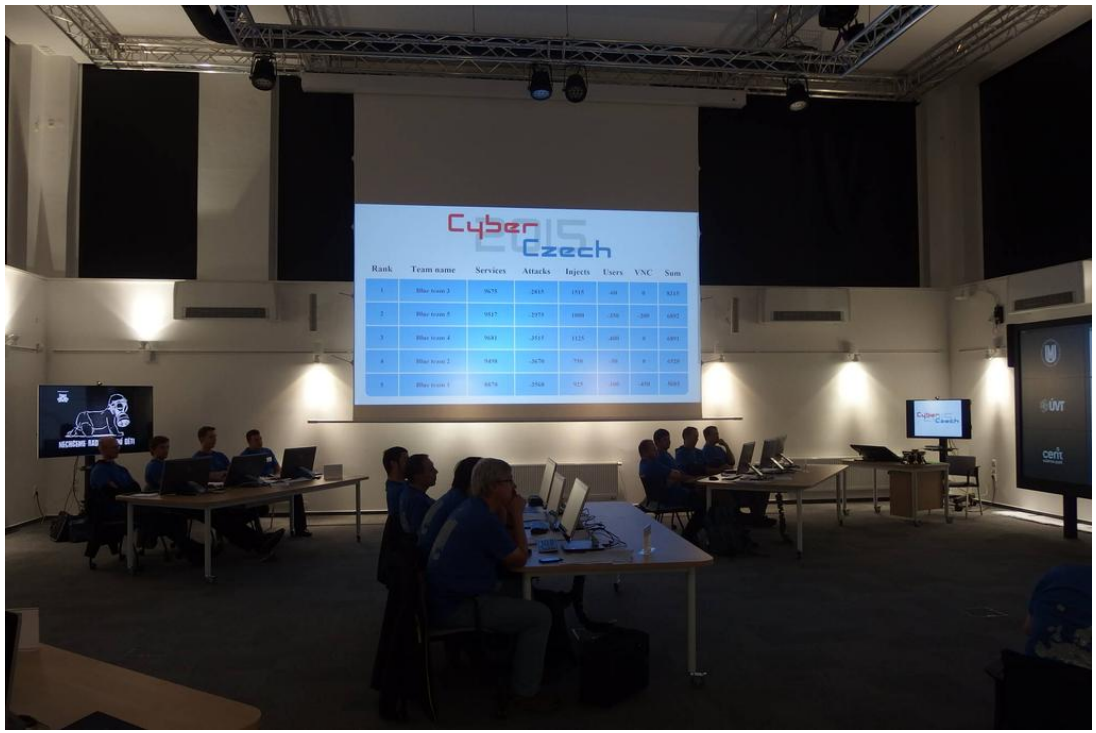
- Availability of requested services – based on Nagios monitoring.
- Resistance to prepared attacks – manually rated and entered by Red team members.
- Quality of reporting to the organizers and media – manually assessed by White team.
- Penalty for 10-minutes direct access to particular host simulating physical visit of a server room – entered by White team.

Physical Facility – KYPO Laboratory

KYPO
BY CSIRT-MU

Physical Facility – Cyber Czech 2015

- All Blue team members (20 people) invited to KYPO Lab.
- 1 team = 4 people around a table with 3 desktops.



KYPO
BY CSIRT-MU

Conclusion

KYPO
BY CSIRT-MU

KYPO – Cyber Exercise & Research Platform

Summary

- Largest (academic) cyber range in the Czech Republic.
- First Czech national cyber exercise – Cyber Czech 2015.
- Looking for R&D partners and cyber security practioners.

KYPO
BY CSIRT-MU

THANK YOU FOR YOUR ATTENTION.

www.kypo.cz

@csirtmu

Pavel Čeleda et al.

celeda@mail.muni.cz