

# CZECH CYBER DEFENCE EXERCISE

## LESSONS LEARNED

26th January, 2016

TLP Code: WHITE

Jan Vykopal, Ondřej Mokoš

vykopal@ics.muni.cz,  
o.mokos@nbu.cz

CSIRT-MU, GovCERT.CZ



**KYPO**

BY CSIRT-MU

# Background I

## Prevention is better than cure

- Many cyber exercises have emerged in recent years.
- ENISA: Cyber Europe
- NATO: Cyber Coalition, Locked Shields.
- ...
  
- Players from Czech Republic are regular participants.
- Czech Rep. adopted Act on Cyber Security in 2014.
- Need for **national** exercise covering Czech specifics.



# Background II

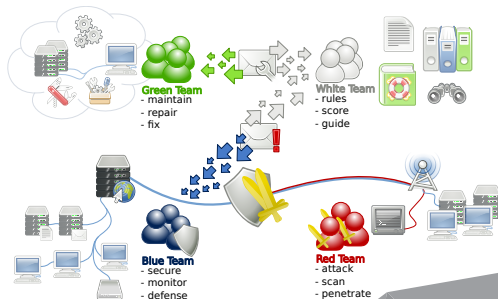
## Cyber Czech 2014

- First Czech exercise for security officers of public administration organizations.
- Organized by Czech National Cyber Security Centre (NCSC).
- One-day **table top** based on real well-known attacks that hit Czech Rep. in 2013 (DDoS, phishing campaigns).
- Covered technical, organizational and legal aspects.
- **Successful event, but some practices may not work in real life.**



# Cyber Czech 2015

- First Czech **technical** exercise for system administrators.
- Organized by Czech NCSC and Masaryk University, Brno.
- Inspired by Locked Shields exercise.
- Two-day **hands-on** defence exercise (Red vs. Blue teams).
- Leverages cloud-based **KYPO Cyber Exercise&Research platform** developed by CSIRT-MU.



# Design of the exercise I

## Overview

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

## Goals:

- Demonstrate most common vulnerabilities, attacks and tactics.
- Intentionally overwhelm players (not too much for not too long).
- Promote healthy competition.



# Design of the exercise II

## Participants are provided with:

- a background story to introduce them to the situation,
- network topology including “their” network that will be defended,
- network architecture and current setup,
- access credentials.



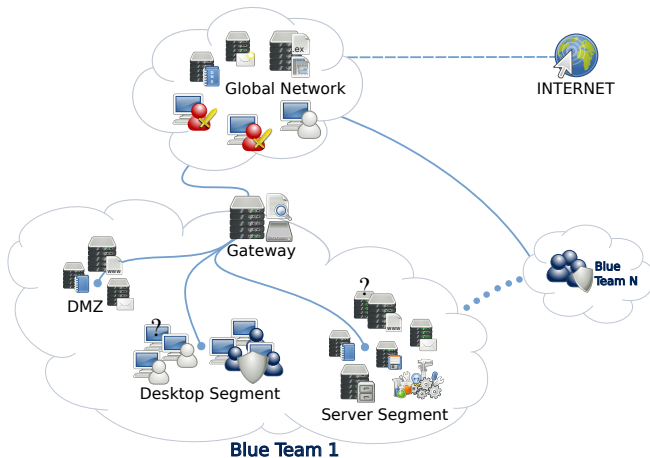
# Design of the exercise III

## Scenario

- Contains all planned actions of attackers and assignments for defenders prepared by the organizers.
- Attackers exploit specific vulnerabilities left in the compromised network in a fixed order.
- The completion of each successful attack is recorded by the attackers.
- Participants should also answer media requests.
- Some legal aspects were covered as well.



# Design of the exercise IV





# Design of the exercise V

## Attacks

- Attacks were carried out in multiple stages.
  - Reconnaissance, scanning
  - DMZ
  - Desktops
  - Servers
- Pivoting, DNS cache poisoning, command injections, backdoors

## Vulnerabilities

- Vulnerable applications
- Misconfigurations
- User accounts
- Privileges



# Design of the exercise VI

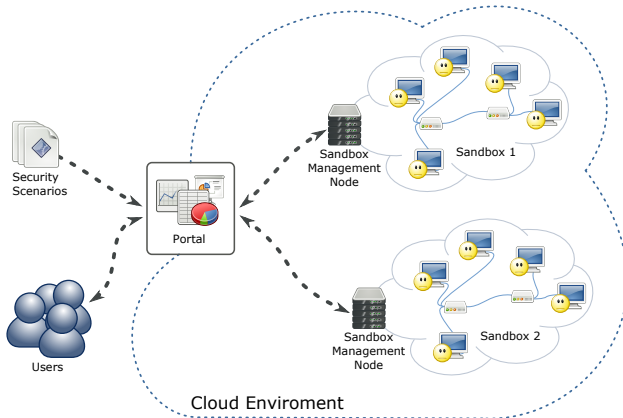
## Scoring

- Successful attacks or their mitigation.
- Availability of specified critical services.
  - The most critical is a control application of a steam generator.
  - Then services provided by servers in DMZ (web, mail).
- Quality of reporting to the CSIRT coordinator and media.



# Exercise infrastructure I

## KYPO Cyber Exercise&Research Platform



# Exercise infrastructure II

## Monitoring

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



# Exercise infrastructure III

## Scoring implementation

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



# Exercise infrastructure IV

## Physical facility

- All Blue team members (21 people) invited to KYPO Lab.
- 1 team = 4 people around a table with 3 desktops with access to KYPO platform.



## Exercise infrastructure V

- Printed hand-outs: exercise rules and description of "defended" network.
- Network topology is visualized in KYPO web portal.
- Near real-time scoreboard is displayed to all participants.
- White, Red and Green teams (~20 people) are seated in a separate room.
- Two representatives (PoC) of White team are available for questions and requests of Blue teams.
- Walkie-talkie are used for communication with PoCs and the rest of the organizers.



# Lessons learned I

Participants enjoyed realistic environment of the exercise.

## Preparation phase

- **Extremely** laborious, especially when more than one institution is involved (communication overhead, synchronization).
- Learning objectives ⇒ Scenario | Selection of participants ⇒ Attacks ⇒ Infrastructure ⇒ Scoring ⇒ Post-mortem evaluation
- Do not plan big on automation.
- Multiple exercise execution lowers the costs.





## Lessons learned II

- Although required skills for the exercise were announced, the level of participants' proficiency varied dramatically.
- Participants skills in dry run and execution may differ too.
- If you send out invitations asking for technical staff, you do not always get people from technical staff.



# Lessons learned III

## Exercise organization

- Players focused on technical part, those without PC did **not** act as coordinators.
- Toolset prepared for players to ease their tasks was not widely used.
- Players did not pay much attention to critical services (the steam generator).
- Some exercise elements was not used as expected – e.g., news portal.
- Duration of the familiarization phase was not sufficient.
- Not enough handouts (service description) for all players.



## Lessons learned IV

- Red team needs internal chat for coordination of their actions.
- Even slightly inaccurate timetable for attacks is very helpful.
- Weight of scoring components was unbalanced – e. g., simulated physical access was more expensive than penalty for service unavailability or successful attack.
- Players were very suspecting even though instructed that particular mails are not phishing attempts.
- Post-mortem detailed evaluation (after-action review) is an essential part of the exercise.
- It is a great place to share information. (Because people actually listen, provided they liked the exercise.)



# Lessons learned V

## Infrastructure

- Long and complex game password/names distract players.
- Deployment of hosts with Windows OS is not so easy as host with Linux OS.
- Configuration of some hosts was changed in last minutes but not documented.
- Not enough hosts for White team (common users, media).
- KYPO platform passed the stress test:
  - 5 independent sandboxes run for all teams at the same time
  - each sandbox contained about 25 interconnected hosts
  - 125 hosts in total



# Conclusion

- Cyber exercise employing realistic infrastructure is well-accepted.
- Its preparation is extremely laborious with respect to the number of participants.
- Dry run provides valuable feedback to all exercise components.
- Feedback from real testers is invaluable but still expect some surprise.
- Preparation should not start by focusing on technical aspects.
- First discuss learning objectives (including soft skills) and scoring possibilities.
- **Less is more.** Number of hosts/services/attacks vs. their realistic integration to the whole exercise.



# QUESTIONS AND ANSWERS

 [www.kypo.cz](http://www.kypo.cz)

Jan Vykopal, Ondřej Mokoš

 @csirtmu @GOVCERT\_CZ    [vykopal@ics.muni.cz](mailto:vykopal@ics.muni.cz), [o.mokos@nbu.cz](mailto:o.mokos@nbu.cz)

**GOVCERT.CZ**

