# Vládní CERT

GovCERT.CZ

Ondřej Šrámek

10. 10. 2017

# Obsah

# Obsah

Co je Vládní **CERT**?

Jakými **technickými** kapacitami disponujeme?

S kým **spolupracujeme**?

Dlouhodobé **projekty**

**Aktuální** situace a **trendy**

# GovCERT.CZ

# GovCERT.CZ

| | |
|---|---|
| řeší | incidenty v kritických a významných systémech |
| proaktivní služby | sdílení informací, testování, vzdělávání, podpora |
| reaktivní služby | zvládání incidentů, koordinace, analýza artefaktů |
| detekční služby | síťové anomálie, otevřené zdroje |

# Technické kapacity

# Technické kapacity

**Správa** systémů, **penetrační** testování

Vývoj bezpečnostních **nástrojů**

Analýza **síťového** provozu

**Forenzní** zkoumání, analýza **malware**, **reverzní** inženýrství

**ICS**/**SCADA** systémy

# Spolupráce

# Spolupracujeme s . . .

| | |
|---|---|
| mezinárodními skupinami | CSIRT network, TF-CSIRT a FIRST |
| evropskou. . . | EU, ENISA |
| | NATO, CCD COE |
| | Policie ČR |
| | Bezpečnostní složky ČR |
| vzdělávací instituce | MUNI, VUT, UPOL,. . . |

# Projekty

# Dlouhodobé projekty

Rozmístění síťových **sond** ve státní správě

**ICS**/**SCADA** laboratoř

**Forenzní** laboratoř

**Penetrační** testování

kybernetické cvičení **Cyber Czech** (technické i tabletop)

# Aktuální výzvy a hrozby

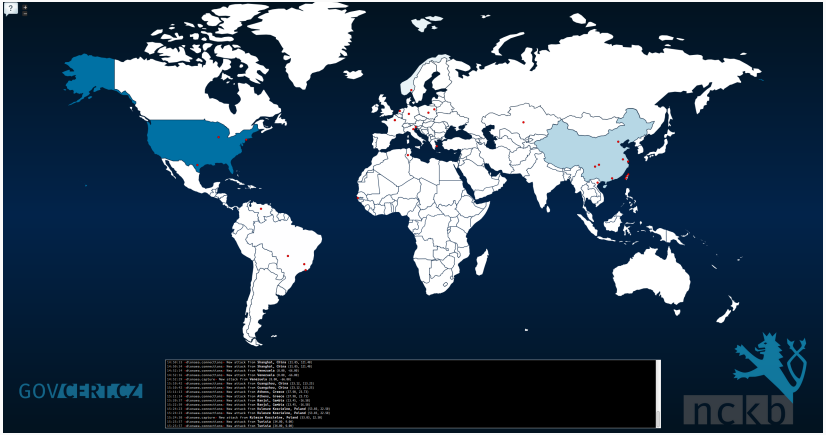
# Aktuální výzvy

| | |
|---|---|
| soukromí vs. ochrana | HTTP > HTTPs (Let's Encrypt) |
| IoT | hodinky, mobil, pračka, lednice, auto,... |
| život online | (pracovní) mobilní telefon/notebook s LTE |
| zdroje v ICT | nedostatek lidských zdrojů (správci/analytici) |
| Internet | je rychlejší a rychlejší |

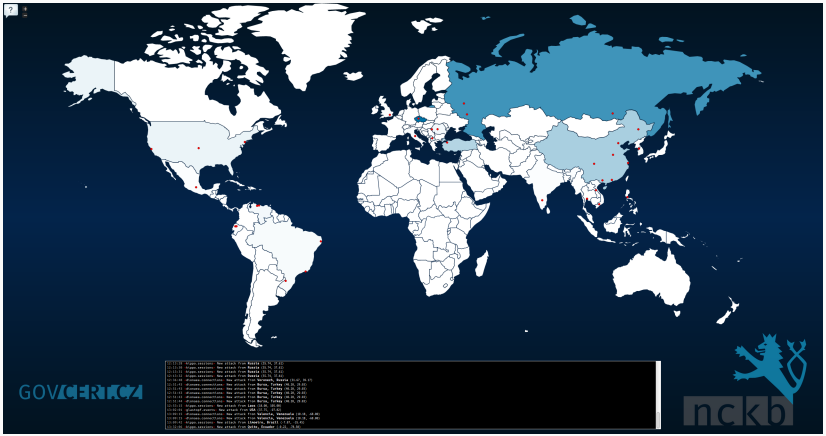
# Aktuální hrozby

| | |
|---|---|
| DoS/DDoS | hacktivismus<br>zničení konkurence (eshop, gaming,...) |
| (spear) phishing | malware > botnet/ransomware/exfill/...<br>cílená kampaň |
| scan | mapování otevřených portů/zranitelností |
| brute-force | telnet, ssh, rdp, pop(s), imap(s),... |
| „leak“ nástrojů | Equation Group, Vault7, Hacking Team,... |

# Aktuální hrozby z . . .

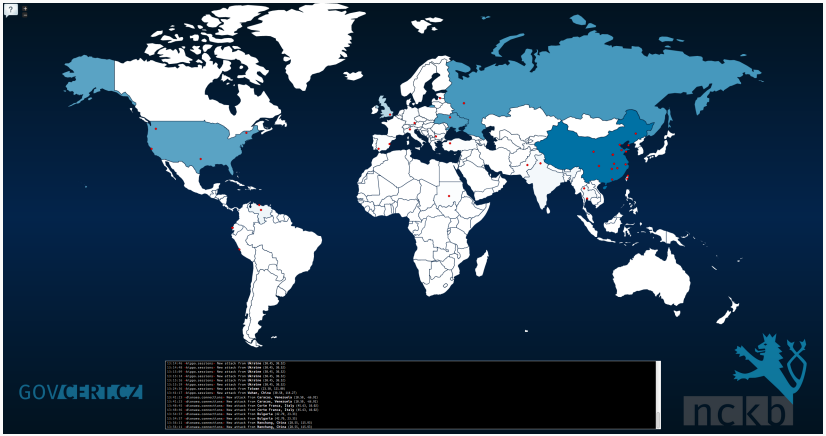


# Aktuální hrozby z . . .



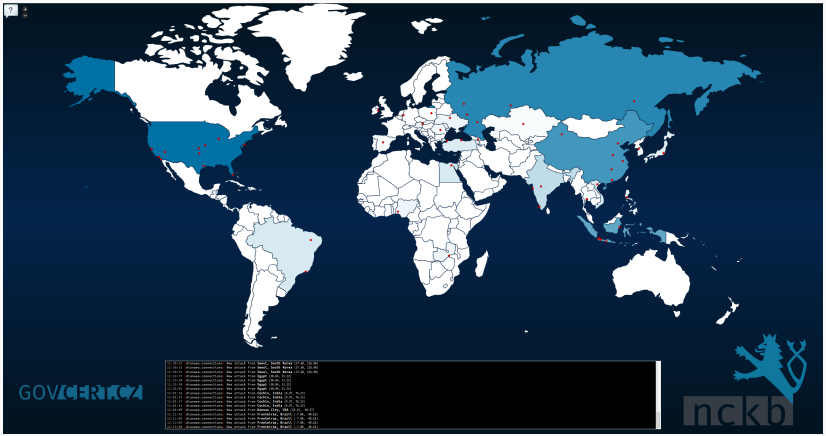
# Aktuální hrozby z . . .

# Aktuální hrozby z . . .



# Aktuální hrozby z . . .

# Aktuální hrozby z . . .



# Děkuji za pozornost!

**Otázky?**

GOVCERT.CZ 

**Ondřej Šrámek**

**veoducí oddělení Analýzy síťového provozu**

**o.sramek@nukib.cz**