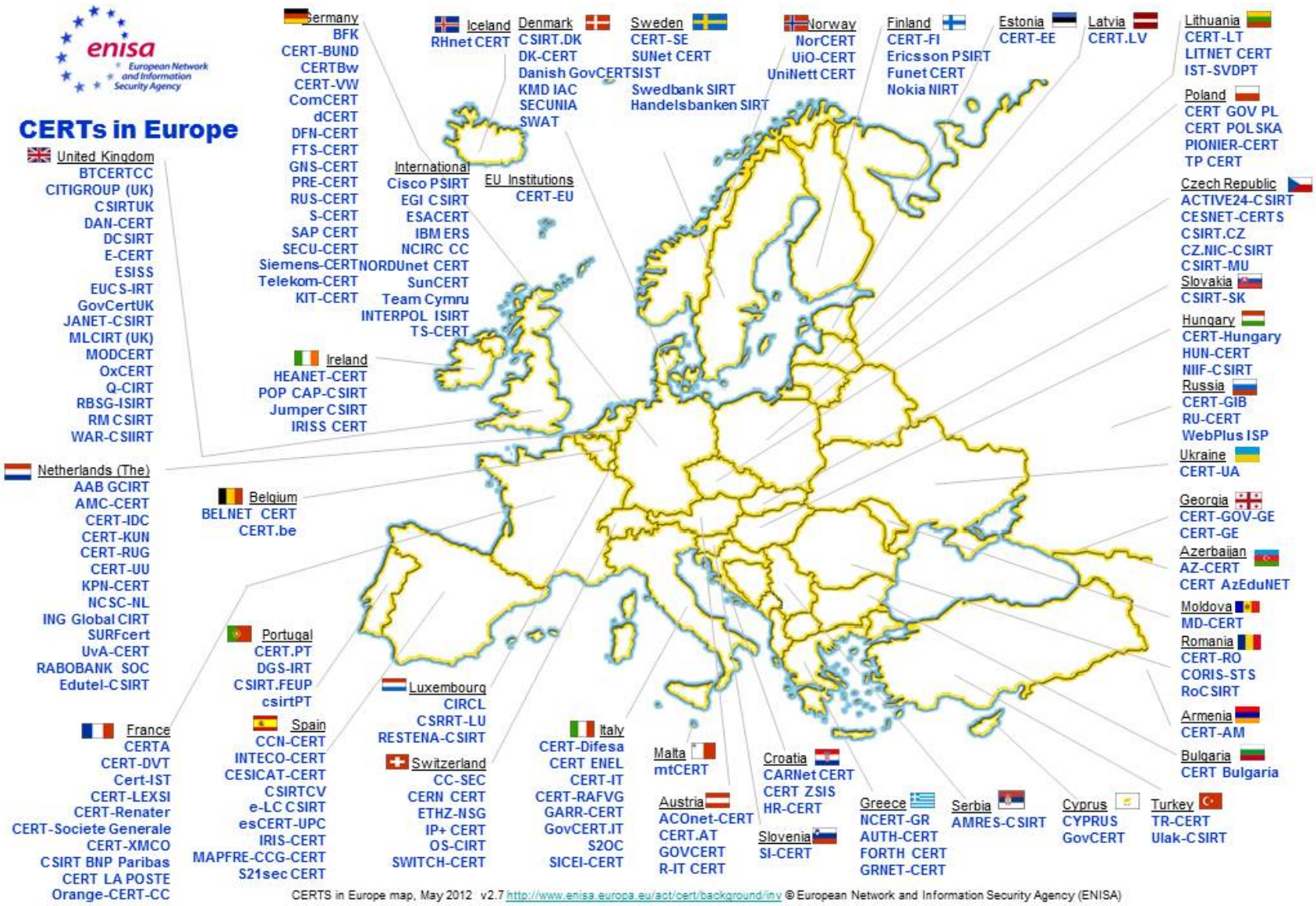
Vládní CERT tým

Radim Ošťádal
GovCERT.CZ

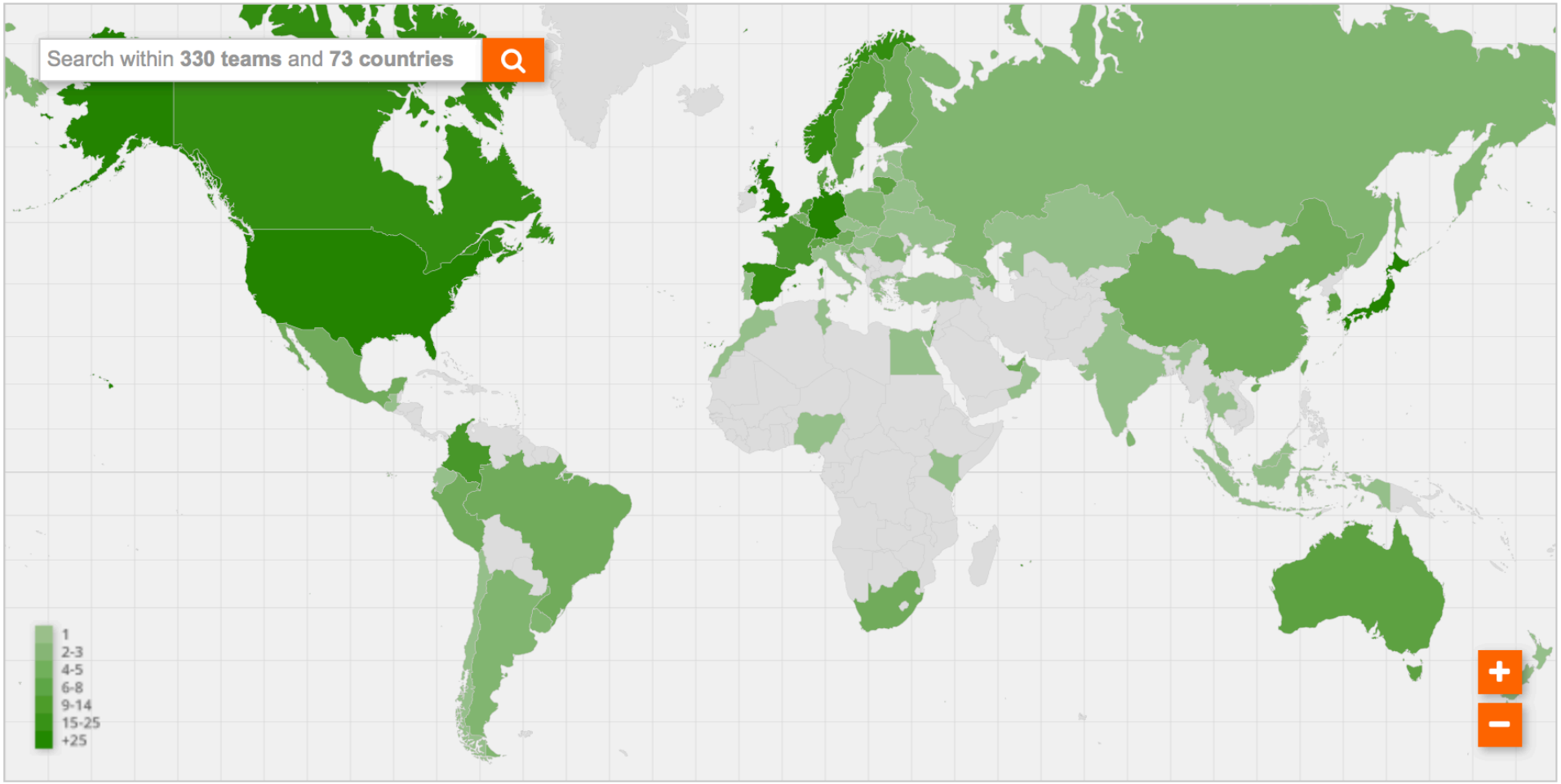
Národní centrum
kybernetické
bezpečnosti

CERT obecně

- Terminologie: CERT vs. CSIRT
  - CERT: Computer Emergency Response Team
  - CSIRT: Computer Security Incident Response Team
- Velká paleta poskytovaných služeb
- Komunitní přístup, spolupráce na dobrovolné bázi
- Zastřešující organizace:
  - Trusted Introducer (TI)
  - Forum of Incident Response and Security Teams (FIRST)
  - European Network and Information Security Agency (ENISA)



CERTS in Europe map, May 2012 v2.7 http://www.enisa.europa.eu/act/cert/background/inv © European Network and Information Security Agency (ENISA)


Search within 330 teams and 73 countries
1
2-3
4-5
6-8
9-14
15-25
+25

CERT služby

- Rozsáhlé množství služeb:
  - Alerts & Warnings
  - Incident Handling
  - Vulnerability Handling
  - Artifact Handling
  - Announcements
  - Technology Watch
  - Audits/Assessments
  - Configure and Maintain Tools, Applications, Infrastructure
  - Intrusion Detection
  - Information Dissemination
  - Risk Analysis
  - Business Continuity Planning
  - Security Consulting
  - Awareness Building
  - Education/Training
  - Product Evaluation
  - Security Tool Development

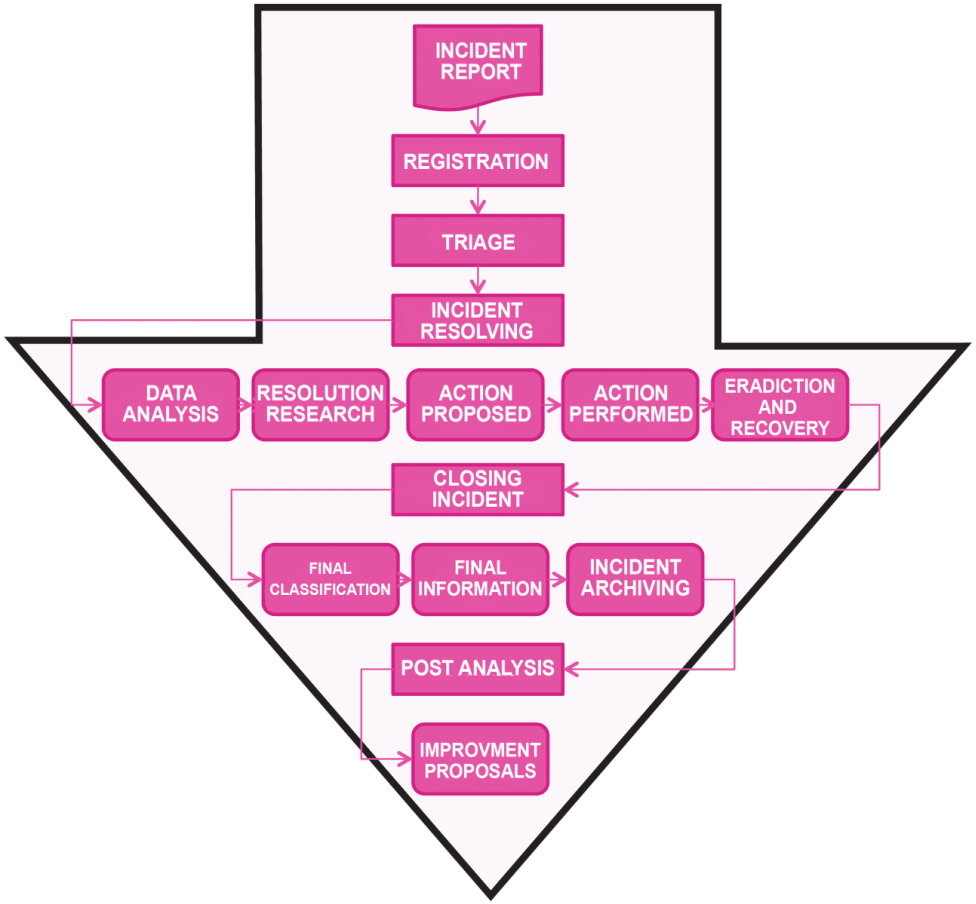
Vládní CERT tým

- Veřejný sektor a kritická informační infrastruktura
- Členění týmu:
  - Reaktivní oddělení
  - Vývoj a bezpečnostní testování
  - Oddělení síťové analýzy
  - Analytické oddělení
- Základní služby:
  - Proaktivní: koordinační činnost v rámci komunity a informační HUB
  - Detekční: schopnosti detekce anomálií
  - Reaktivní: reakce na incidenty, zpracování artefaktů
- Kontakt:
  - http://www.govcert.cz
  - cert@nbu.cz, cert.incident@nbu.cz (PGP)

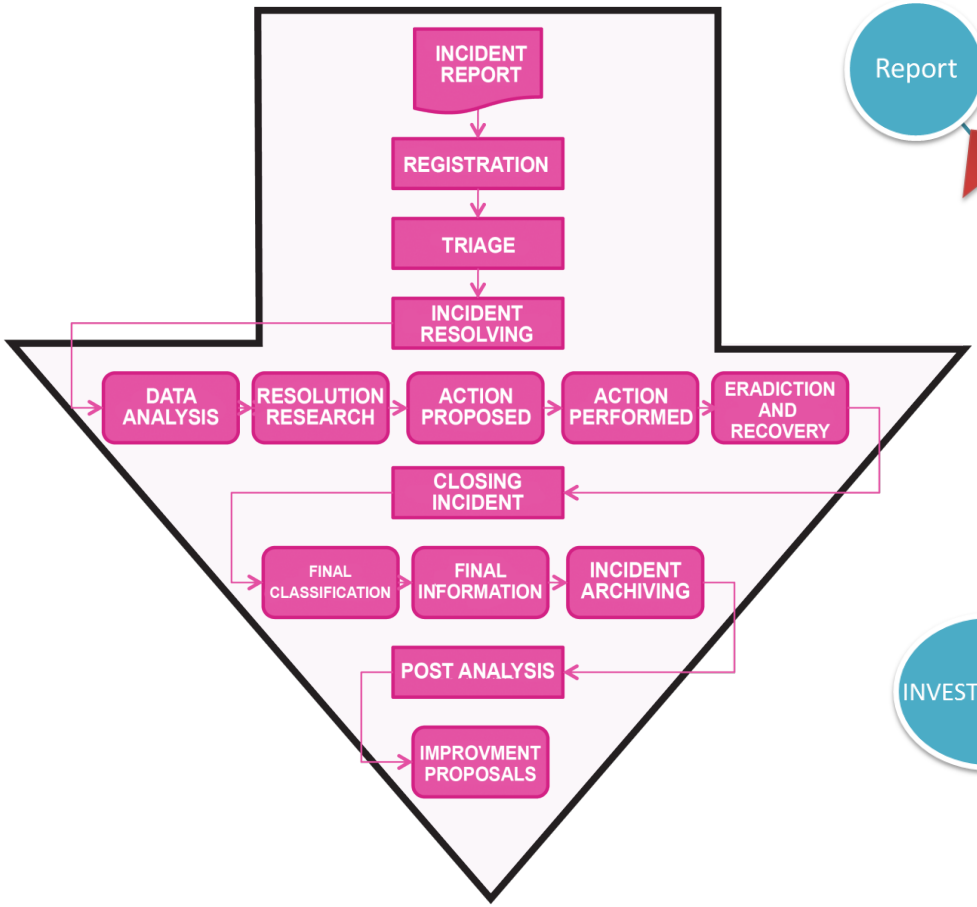
Zaměření týmu

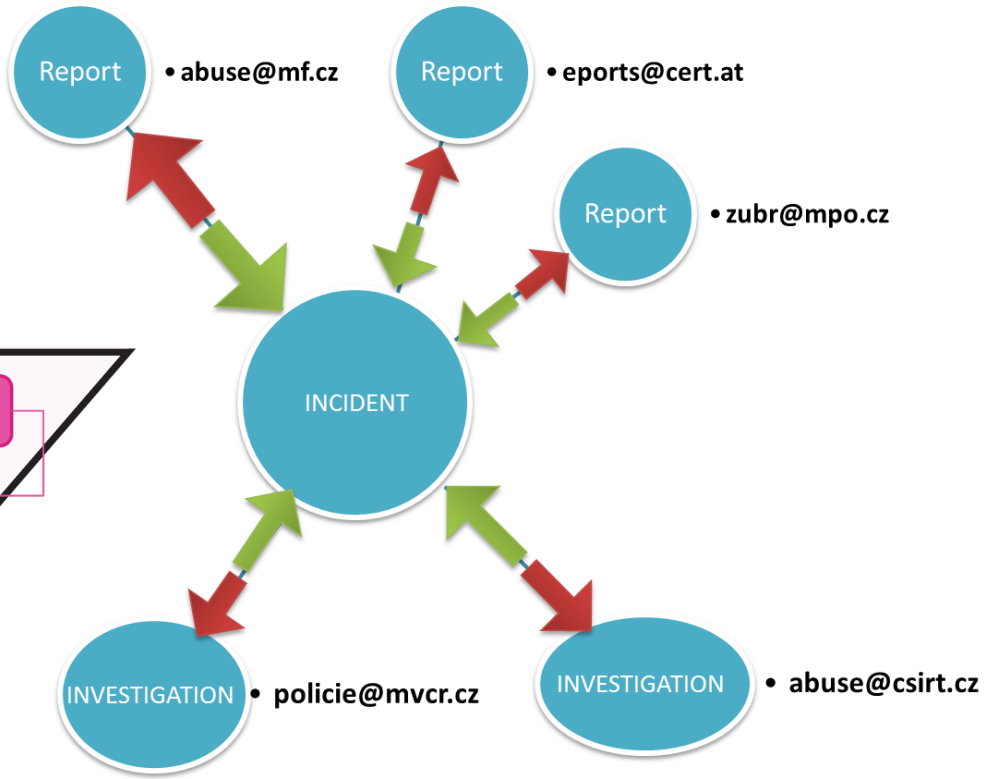
- **SCADA/ICS systémy**
- **Penetrační testování**
- **Forenzní činnost**
- **Analýza malwaru a reverzní inženýrství**
- Virtualizované prostředí a cloudová řešení
- Bezpečné programování a databázové systémy
- Operační systémy UNIXového typu
- Operační systémy Windows
- Síťová bezpečnost a analýza síťového provozu
- Honeypoty

Incident handling

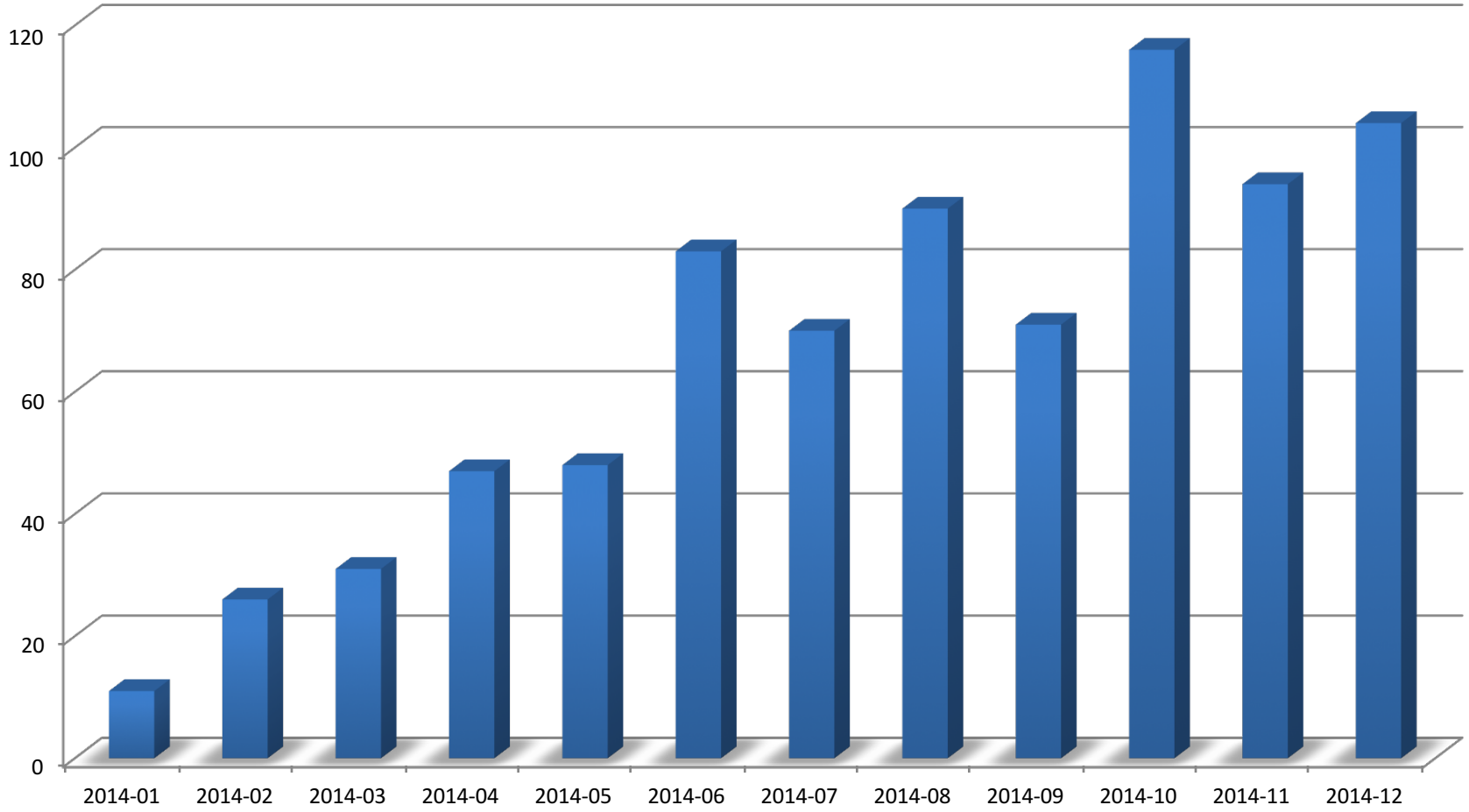


Incident handling





Hlášení incidentů za minulý rok



Aktuální trendy

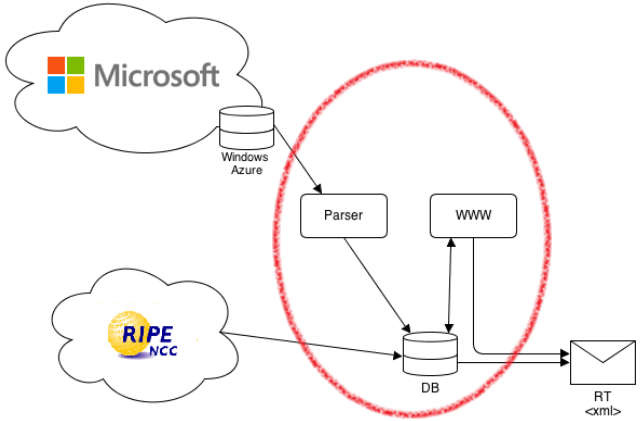
- Rozsáhlé phishingové kampaně
- Zvýšená hrozba špionážního malware
- Zvýšení počtu odhalených botnetů
- Útoky na routery v domácích a firemních sítích
- Snížení počtu DoS a DDoS útoků v rámci veřejného sektoru a KII

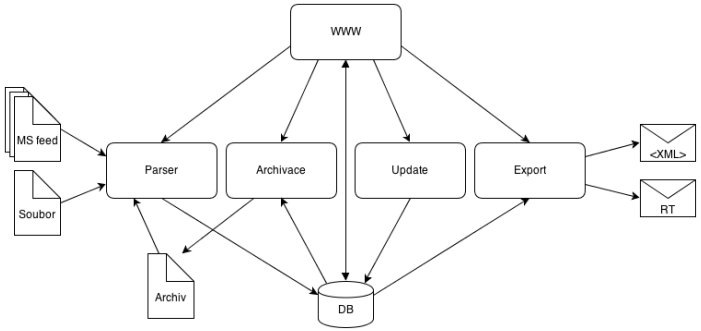
Sdílení informací

- Kybernetické incidenty
- Aktuální zranitelnosti a hrozby
- Vypracované analýzy (např. analýza malwaru)
- Sdílení nástrojů, technických schopností
- Strojově zpracovatelná data – *Indicators of Compromise* (IoC)
  - Shadowserver
  - Antivirové společnosti
  - Další CERT/CSIRT týmy

Botnet Feed

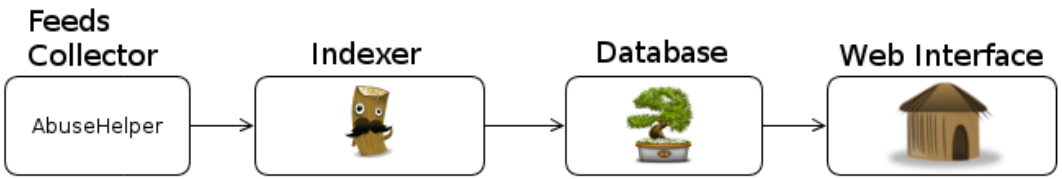
- Nástroj vyvíjený vládním CERT týmem
- Data od MS Digital Crimes Unit
- Komunikace směrem od strojů k C&C serverům botnetů
  - Potenciálně nakažené PC
  - Conficker, Zeus, ZeroAccess, …
- Strojově zpracováváme 250-300 tisíc záznamů denně
- Agregace dat a předání dalším organizacím





Projekty IHAP a MDM

- Incident Handling Automation Project
- Malicious Domain Manager
- Zpracování a normalizace dat cca 250 tisíc událostí za měsíc - brute-force, phishing, exploit, trojan, …
- Celkem získaných dat týkajících se ČR – 685 událostí
- Zdroje dat:
  - Výzkumné organizace
  - IDS/IPS, honeypoty
  - Akademické týmy
  - Black / grey listy



Honeypoty

- Členění podle zaměření:
  - Klientské (webový prohlížeč)
  - Serverové (server nabízející zranitelnou službu)
- Získané informace:
  - Zájmy a chování útočníka
  - Používané nástroje
  - Infikované stránky
- Thug
  - Málo interaktivní klientský honeypot
  - Analýza webu - škodlivý kód, infikované soubory (pdf, doc, …)
  - Možnost proaktivní detekce nakažených webových stránek
- Modern Honey Network
  - Framework pro správu a nasazení honeypotů
  - (Polo)Automatizované nasazení HN/P (Conpot, Dionaea, Glastopf, …)

Poskytované služby

- Pomoc s technickým řešením incidentu (incident handling)
- Navázání komunikace s jiným subjektem
- Možnost obrátit se na GovCERT.CZ s událostí, dotazem, ...
- Vulnerability management
- Varování ostatních potenciálních obětí dříve, než budou zasaženy, lesson learned
- Open Source Intelligence (OSINT)
- Proaktivní činnost – BotNet Feed, IHAP, honeypoty, ...
- Penetrační testování
- Analýza malwaru a reverzní inženýrství

Aktuální projekty

- Koordinační centrum pro české bezpečnostní týmy:
  - Videokonference se stálými i ad-hoc členy
  - Řešení rozsáhlých bezpečnostních útoků
  - Práce nad sdílenými dokumenty
- Nový webový portál:
  - Veřejná a neveřejná část
  - Neveřejné fórum pro bezpečnostní týmy a další organizace
  - Informace o incidentech a zranitelnostech
  - Vydávání varování

Aktuální projekty

- Laboratoř ICS/SCADA systémů
- Forenzní laboratoř
- Automatizované sdílení informací o incidentech:
  - System-to-system komunikace
  - Spolupráce se společností O2
- Budování testovacího prostředí
- Skenování zranitelností (OWASP)
- Provádění penetračních textů (externí, interní se plánují)
- Organizace a účast na národních i mezinárodních cvičeních

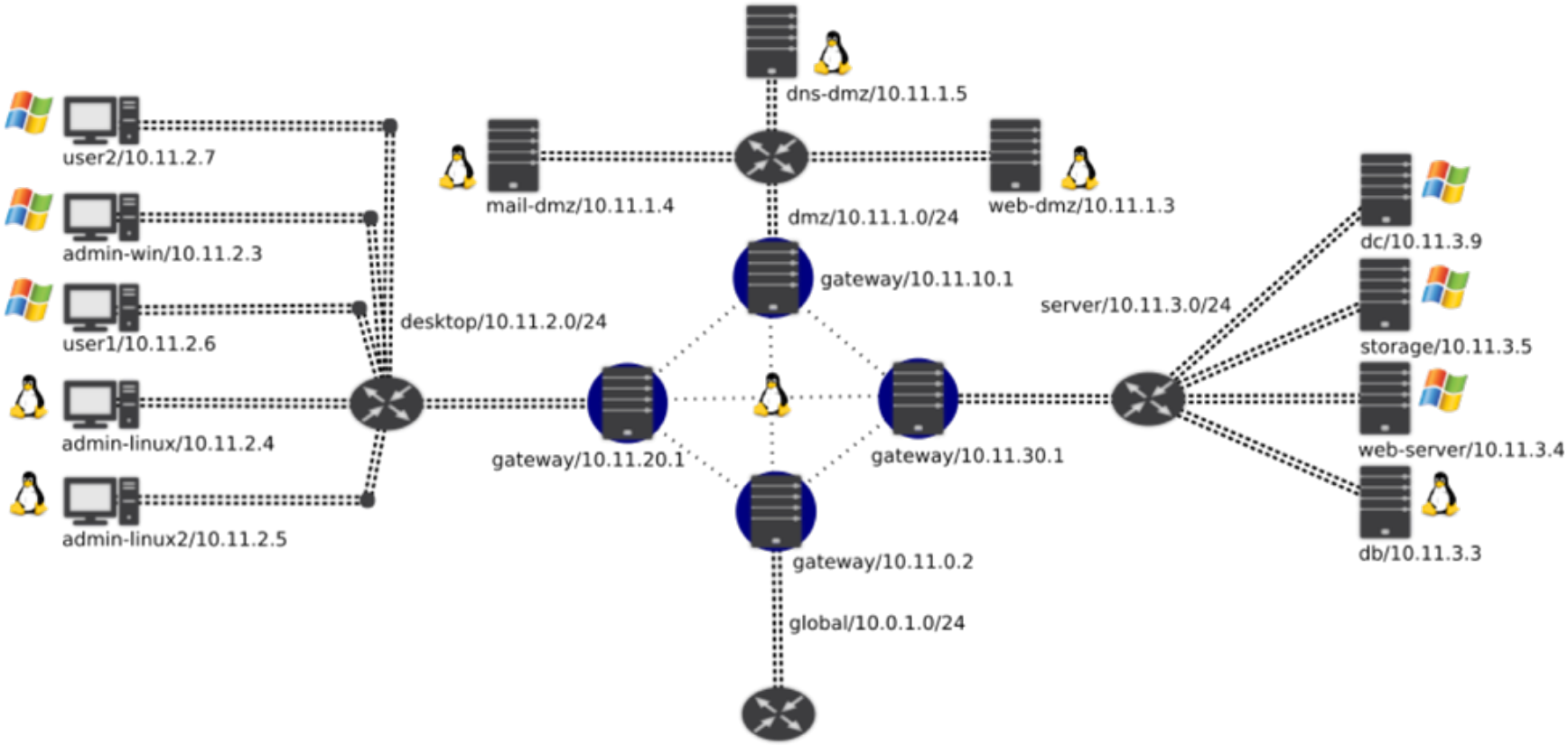
Technické Cyber Czech 2015

- První technické národní cvičení kybernetické bezp.
- Proběhlo 6.-7. října 2015
- Národní centrum kybernetické bezpečnosti ve spolupráci s Masarykovou univerzitou
- Red / Blue tým cvičení s více než 60 účastníky
- Příprava trvala přibližně 9 měsíců
- Scénář:
  - Česká republika oficiálně podporuje výstavbu nových jaderných elektráren
  - Kybernetické útoky na ministerstva a elektrárny
  - Skupina Dark Hackers
  - Týmy rychlé reakce byly vyslány do jednotlivých elektráren

Technické Cyber Czech 2015

- Simulované prostředí s 20 počítači a servery
- Prostředí obsahuje:
  - Zastaralé a nepatchované systémy a aplikace
  - Zranitelné služby a slabá uživatelská hesla
  - Defaultní konfigurace a instalace množství aplikací
  - Malware, logické bomby, …
  - Nejistota ohledně předchozích administrátorů

Technické Cyber Czech 2015



Technické Cyber Czech 2015

- Hodnocení jednotlivých týmů dostupné během celého cvičení
- Co se hodnotilo:
  - Automatické bodování dostupnosti
  - Záporné body za úspěšné útoky Červeného týmu
  - Zajištění použitelnosti prostředí pro jeho uživatele
  - Sdílení informací a spolupráce mezi jednotlivými týmy
  - Spolupráce a komunikace s médii
  - Právní scénář

Technické Cyber Czech 2015

Otázky?

Děkuji za pozornost!