FLAB: Forenzní laboratoř

Andrea Kropáčová
CESNET, z. s. p. o.

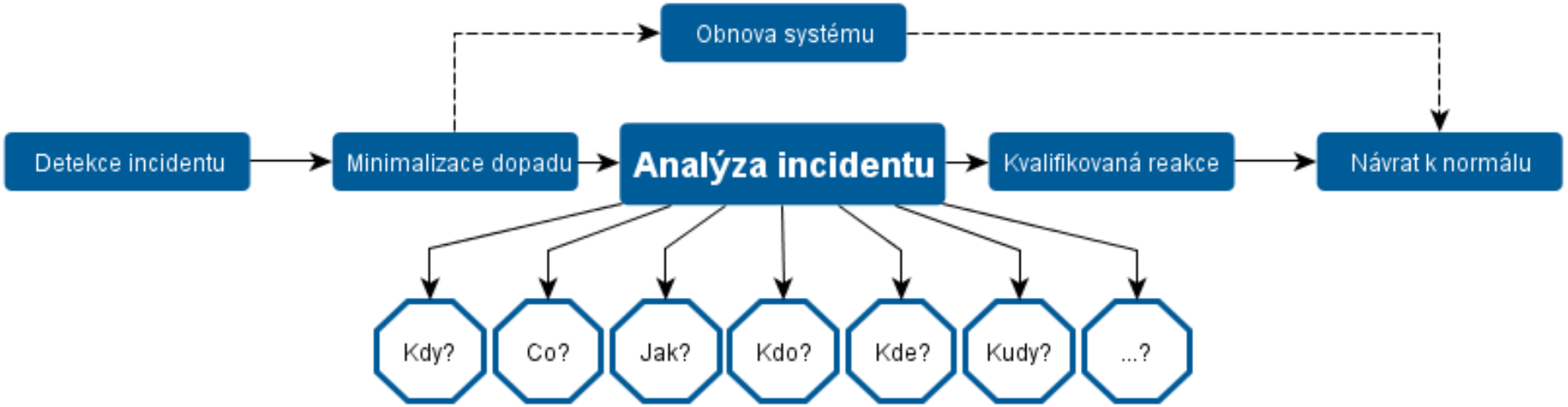
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
OP Výzkum a vývoj pro inovace

- https://flab.cesnet.cz/
- Založena v roce 2011...
- ... jako podpůrné pracoviště pro bezpečnostní tým CESNET-CERTS
  - analýza incidentů a hrozeb
  - zvládání incidentů

- **Dnes nabízí komplex služeb**
  - analýza bezpečnostního incidentu
  - penetrační testy sítě a služeb
  - zátěžové testy (odolnost proti DoS) sítě a služeb
  - *odborná analýza technologie, konzultace, školení*

Analýza bezpečnostního incidentu

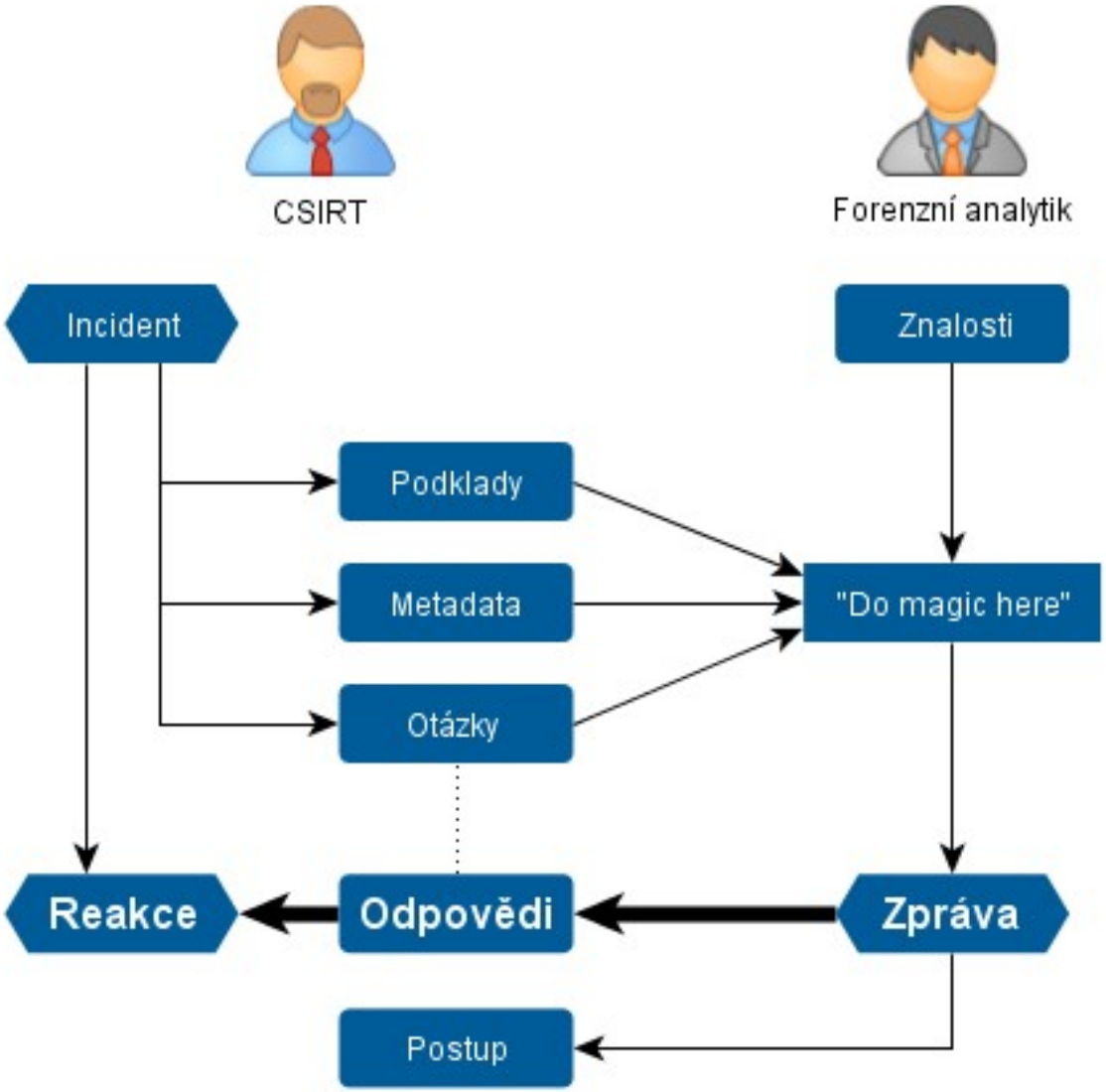
- CSIRT tým
  - Základní služba = reakce na incident



- Potřeba získat informace
  - Podklady pro rozhodování ⇒ přesné a důvěryhodné
  - Detailní (forenzní) analýza

Analýza bezpečnostního incidentu

- Schéma spolupráce CSIRT – FLAB
  - **CSIRT**
    - Incident (problém)
    - Potřeba informací
      - Otázky
    - Umí poskytnout
      - Podklady
      - Informace
  - **Forenzní analytik**
    - Znalosti
    - Analýza
    - → **Odpovědi**
    - → Postup



Penetrační testy

- Hledání chyb a zranitelností
  - nikoliv potvrzení bezchybnosti (audit)

- Co by mělo být v centru zájmu správců
  - lze infrastrukturu zneužít pro další útoky?
  - lze získat, poškodit, smazat data, systémy, služby? (integrita, dostupnost, důvěrnost)
  - lze získat autentizační údaje uživatelů?
  - existují v prostředí zneužitelné zranitelnosti?
  - kde udělal administrátor chybu při konfiguraci?
  - co by mělo/mohlo být zabezpečeno lépe a efektivněji?
  - ...

Penetrační testy

- Průběh:
  1. fáze: **zadání**: specifikace požadavků, očekávání, rozsahu prací
  2. fáze: **aktivity v síti zadavatele**
     - scan sítě
     - sběr dat
     - testování specifikovaných služeb
  3. fáze: **následné zpracování**
     - dat, nálezů a zjištění
     - návrh a formulace doporučení

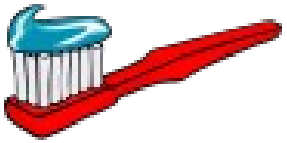
     ⇒ vytvoření a validace závěrečné zprávy
- Závěrečná zpráva
  - přehled provedených testů
  - zhodnocení výsledků
  - doporučení nápravy

Zátěžové testy

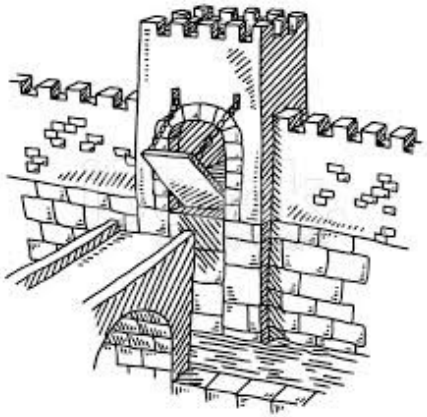
- Testování odolnosti služby (www, DNS)
- Sekundární efekt – testování odolnosti sítě a obranných prvků
- Průběh
  - specifikace: cíle, požadavky a očekávání, pravidla, režim
  - průzkum terénu (ve spolupráci se správcem testované sítě)
  - návrh průběhu testů
  - kalibrace nástrojů a prostředí
  - výběr termínu
  - provedení testů
  - vyhodnocení výsledků
- Závěrečná zpráva
  - přehled provedených testů
  - vyhodnocení výsledků
  - doporučení vhodných úprav

Pět „pé“

- **Prevention**



- **Protection**



- **Progress**

....

... *vrrrmmmm* ...

- **Preparedness**

- **Painless**

Penetrační testování od FLABu je druhá nejlepší věc, kterou lze udělat pro zabezpečení infrastruktury datových úložišť CESNET.

Tou první by bylo odpojit ji od sítě.

David Antoš, vedoucí oddělení datových úložišť CESNET

Děkuji za pozornost!

Andrea Kropáčová, andrea@cesnet.cz