

# Detekce a náprava

---

Pavel Kácha  
CESNET, z. s. p. o.

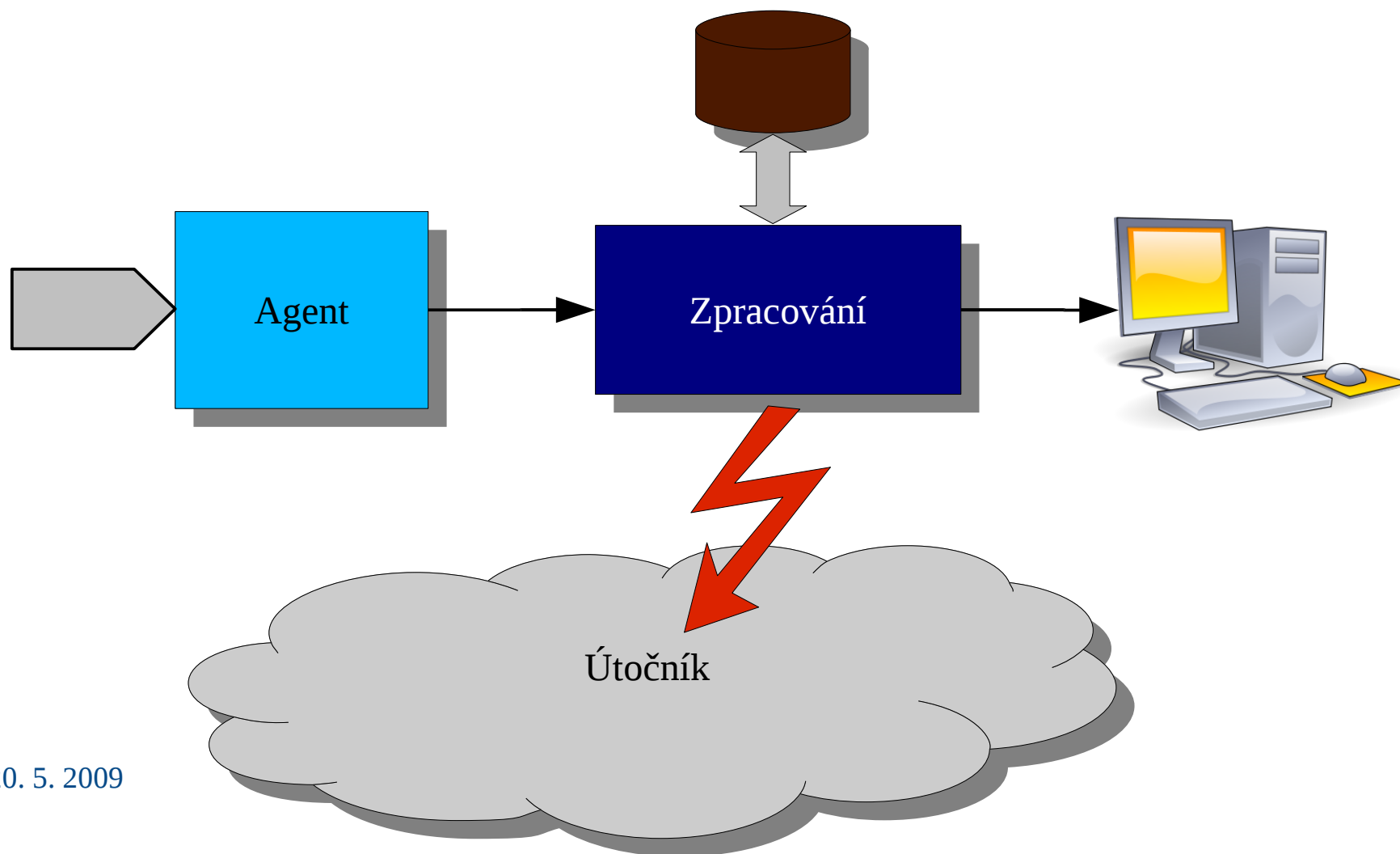
- **Zneužití slabiny systémového software**  
V dnešní době převážně červi a script-kiddies.
- **Využití slabého hesla nebo klíče**  
Slovníkové SSH útoky probíhají prakticky nepřetržitě.  
Slabé SSH klíče a certifikáty Debianího *openssl*.
- **Zneužití slabiny webové aplikace**  
Cross Site Scripting (XSS)  
SQL injection  
Defacement, phishing
- **Zneužití uživatelského účtu**  
Díky slabému heslu nebo krádeži identity.

- **Vím, za co jsem zodpovědný**  
Jasně rozdělená a definovaná zodpovědnost, v případě problému je každému jasné, kdo co řeší.
- **Vím, co na mém serveru a na mé síti běží**  
Omezená množina strojů a služeb  
Otevřené porty  
Jednoznačná autentizace a autorizace
- **Vím, co to dělá**  
Logování  
Periodické ukládání stavu  
Monitorování systémových prostředků, provozu, změn v systému
- **Nevím-li to, dostatečně to omezím a monitoruji**  
Firewall, DHCP  
Omezená práva  
Sandboxing uživatelských aplikací

- **Logová hlášení aktivních démonů**  
Postfix, Bind, Apache, SSHd...
- **Autentizační a autorizační záznamy**  
Přihlášení ke službám, síťové autorizace (DHCP, WPA)  
Důležité akce  
(Pozor na prokazatelnost uživatelské zodpovědnosti: komu kdy bylo uživatelské jméno přiděleno, souhlas s podmínkami, podpis)
- **Zprávy o hardware**  
Smart  
Teploty  
HW RAID
- **Události na síti**  
ARP, DHCP  
Přístupy na uzavřené porty  
Síťový IDS

- Jako online zdroj informací
  - Dostávají se ke mně vůbec aktuální informace?  
Logwatch, Swatch, Logcheck
  - Loguji dostatečně?  
Logování čeho je u mých démonů defaultně vypnuté?  
Stačí mi informace k dohledání viníka?  
(DHCP přidělí IP k MAC. Stačí mi to k dohledání zásuvky?)
- Pro post-mortem analýzu
  - Dá se mým logům věřit?  
Logování po síti na bezpečné místo  
Průběžný kontrolní hash logu
  - Jsou informace dostatečné bez živého stavu stroje?  
Síťová vrstva zaloguje *pid*. Víím po týdnu, který to byl démon?  
V které zásuvce byla MAC přidělená DHCP včera?

- Systém pro detekci průniků
  - Přesněji – pro detekci útoků



# NIDS (network)

- Sledování síťového provozu, detekce (síťová vrstva)
  - Scan, sweep
  - (D)DOS
  - Pokusy o přetečení zásobníku, injekci shellkódu
  - Jiné detekce anomálií, např. na základě statistik provozu
- Typické
  - *Snort, Bro*
    - Cca stovky Mb/s, na rychlejší síť třeba HW podpora (Několik projektů v rámci CESNETu.)
  - *LaBrea*

- Kontrola logů
  - *Swatch, Logcheck*
- Kontrola integrity souborového systému
  - *Samhain, Tripwire, Aide, Integrit*
- Aktivní antivirus
- Hledání rootkitů
  - *chkrootkit, rkhunter*
- Detekce anomálií
  - Promiskuitní mód, skryté procesy
- Kombinace
  - *Ossec, Monit, Aanval*

- **Být připraven**  
Dostatek informací  
Disaster Recovery Plan, Business Continuity Plan
- **Identifikovat útok**  
Ověření údajů ze stížnosti, IDS, logů, stavu systému
- **Omezit dopady**  
Odpojení od sítě, ořezání provozu, nouzový režim, obecně zastavení útoku
- **Zjistit rozsah**  
Zkompromitované autentizační údaje uživatelů?  
Podnikové informace?  
Návaznost na další systémy?

- **Obnovit provoz**

Obnovení ze záloh

Uzavření vektoru útoku (aktualizace, změna hesel)

- **Analýza**

Forenzní analýza na uloženém stavu systému

Zhodnocení škod

- **Reflexe**

Jak?

Proč?

Zvládli jsme?

Šlo to lépe?

- Kodifikace postupů a příprava pro případ mimořádné události

Je lepší (a levnější) mít připravený plán, než teprve po útoku začít zjišťovat, co vše je vlastně potřeba dělat.

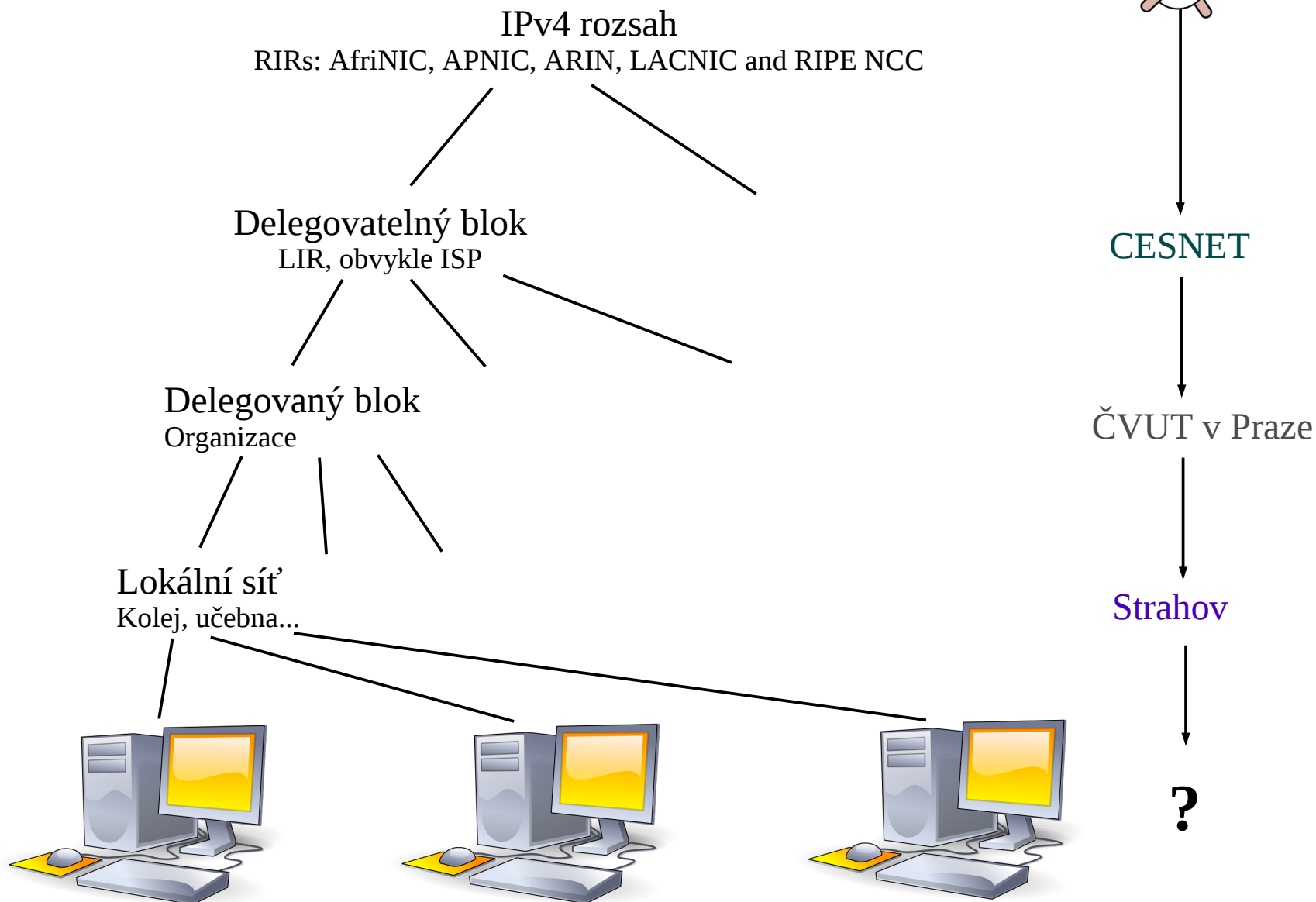
- Business Continuity Planning

- Plány pro zachování fungování organizace
- Kontinuita činností v případě výpadku služeb
- Náhradní nouzová řešení

- Disaster Recovery Planning

- Plány pro obnovu činnosti
- HW, SW, data, ale i lidské zdroje

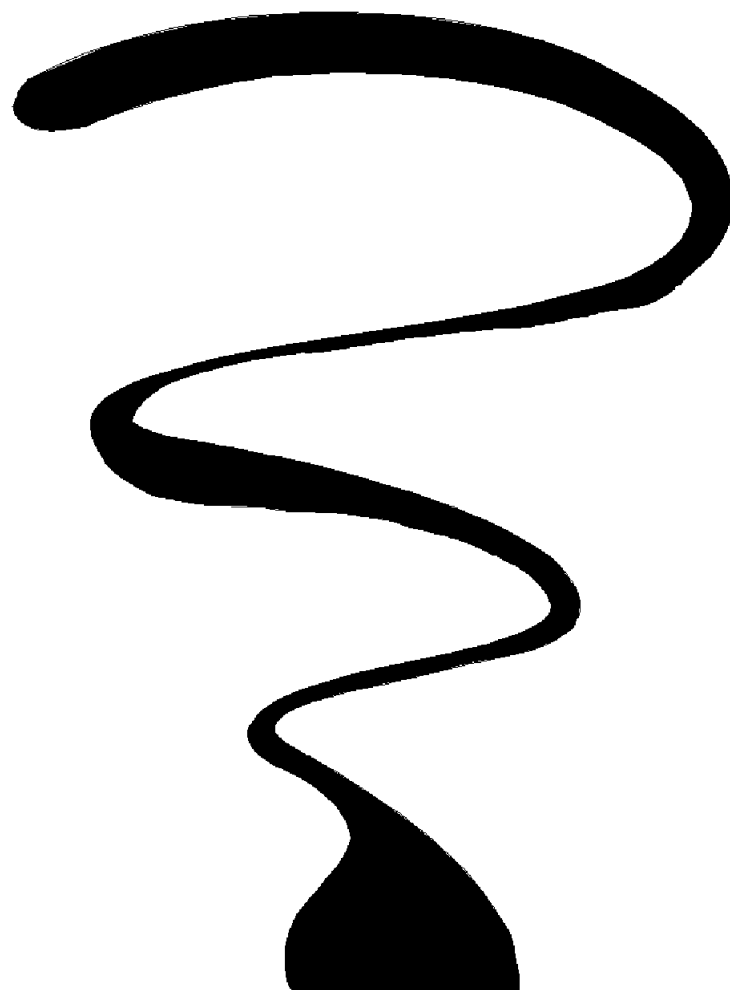
# Jak sem zapadá CSIRT



- CSIRT se stará o to, aby incidenty v jeho jurisdikci byly rychle a spolehlivě řešeny
- Má k dispozici nástroje na omezení dopadu při nedostatečné reakci
- Má ale zájem na spolupráci se správci v případě specifických incidentů
- Vždy je důležitá komunikace

- Komunikační kanály
  - Vazby na světovou komunitu bezpečnostních týmů
  - Může varovat další potenciální oběti
  - Konzultovat s dalšími napadenými
  - Koordinovat řešení a nápravu

# Dotazy?



Technické zprávy Cesnetu

<http://www.cesnet.cz/doc/techzpravy/>

Snort

<http://www.snort.org/>

Bro

<http://www.bro-ids.org/>

LaBrea

<http://labrea.sourceforge.net/>

Logcheck

<http://logcheck.org/>

Swatch

<http://swatch.sourceforge.net/>

Samhain

<http://www.la-samhna.de/samhain/>

Tripwire

<http://sourceforge.net/projects/tripwire/>

Aide

<http://www.cs.tut.fi/~rammer/aide.html>

Integrit

<http://integrit.sourceforge.net/texinfo/integrit.html>

Osiris

<http://osiris.shmoo.com/>

chkrootkit

<http://www.chkrootkit.org/>

rkhunter

[http://www.rootkit.nl/projects/rootkit\\_hunter.html](http://www.rootkit.nl/projects/rootkit_hunter.html)

Ossec

<http://www.ossec.net/>

Monit

<http://mmonit.com/monit/>

Prelude

<http://www.prelude-ids.com/en/welcome/index.html>

Aanval

<http://aanval.com/>

IDMEF

<http://www.ietf.org/rfc/rfc4765.txt>