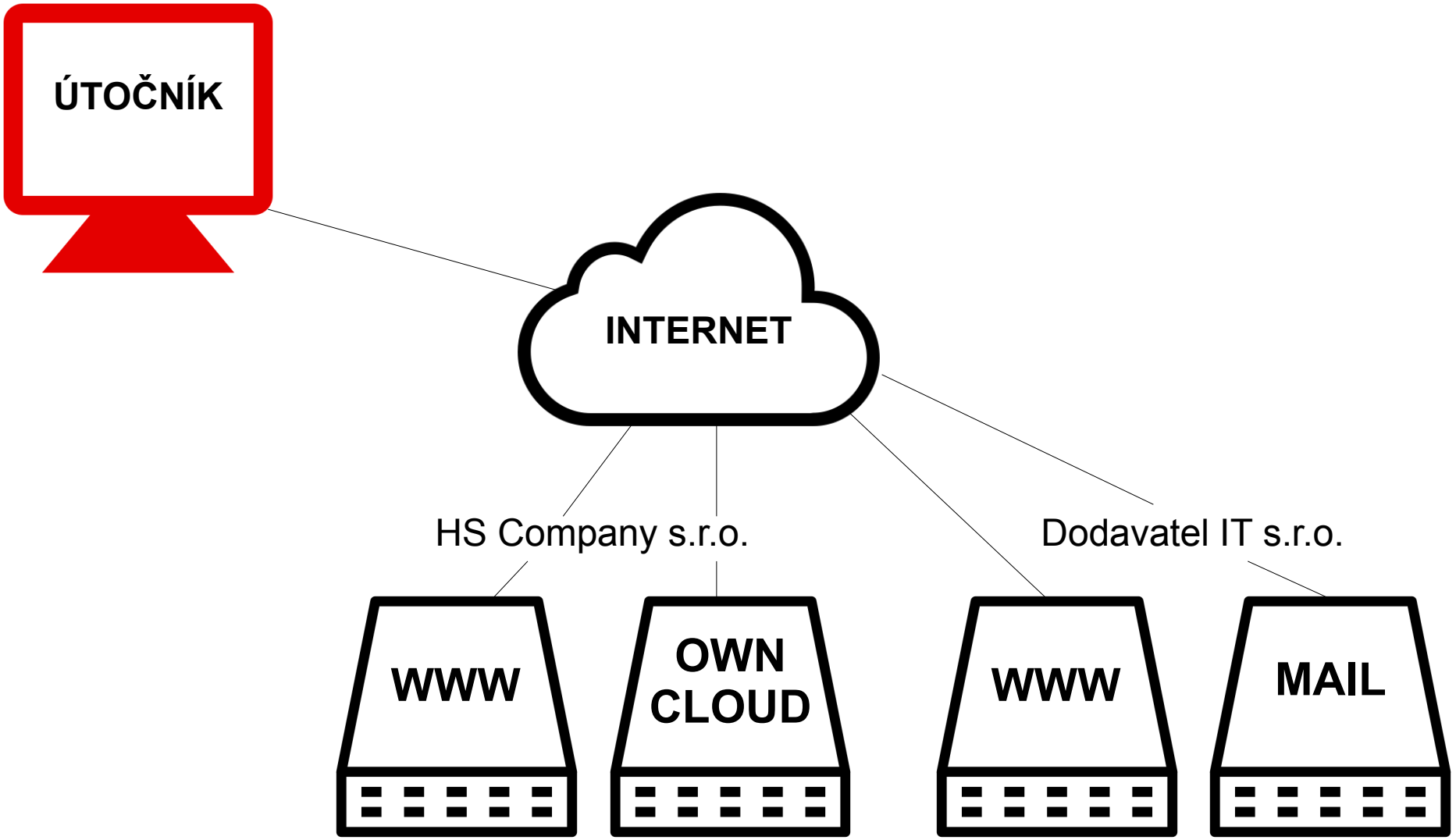
cesnet

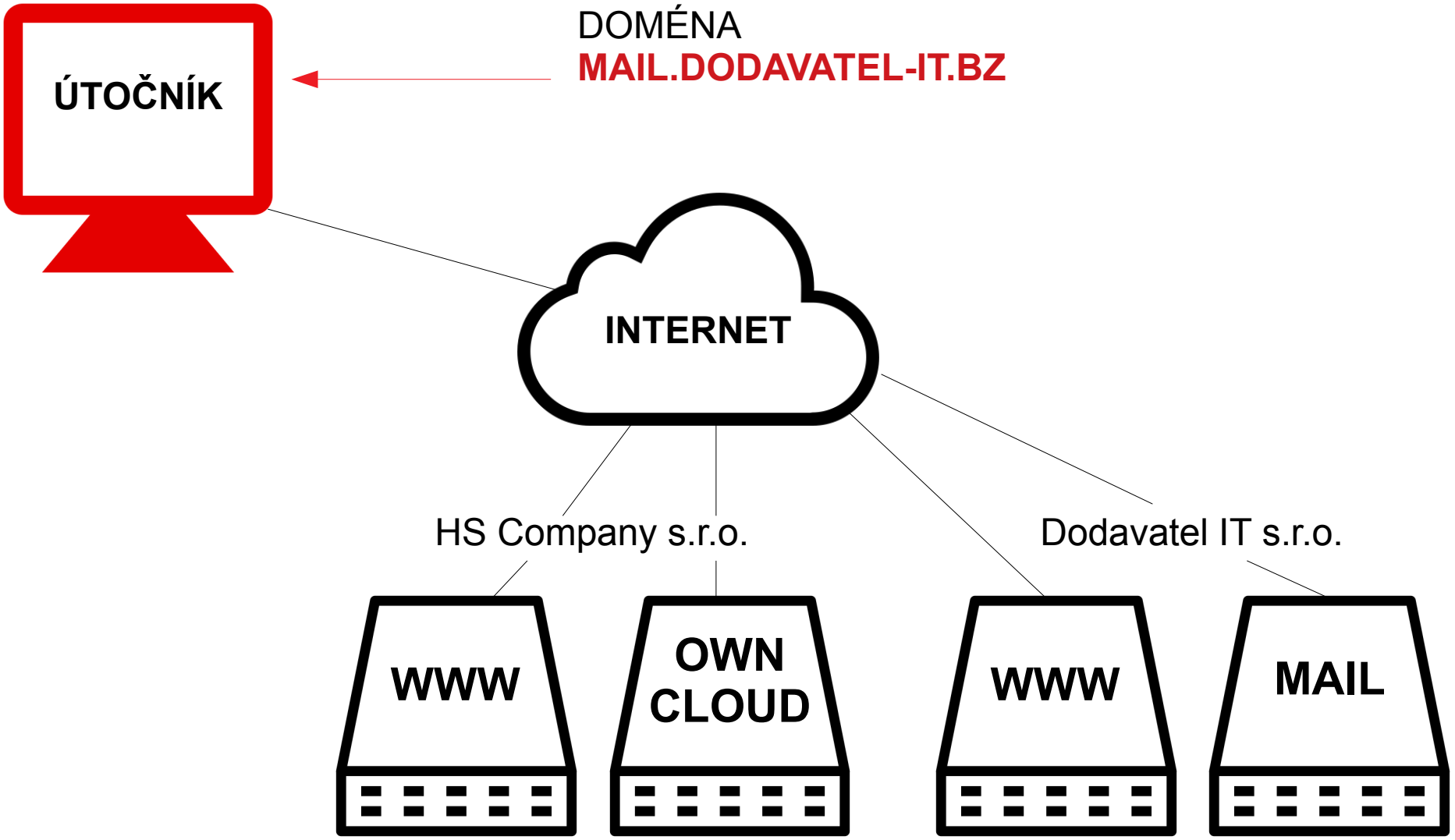
Hacking show 2
Tenká červená linie

Radomír Orkáč

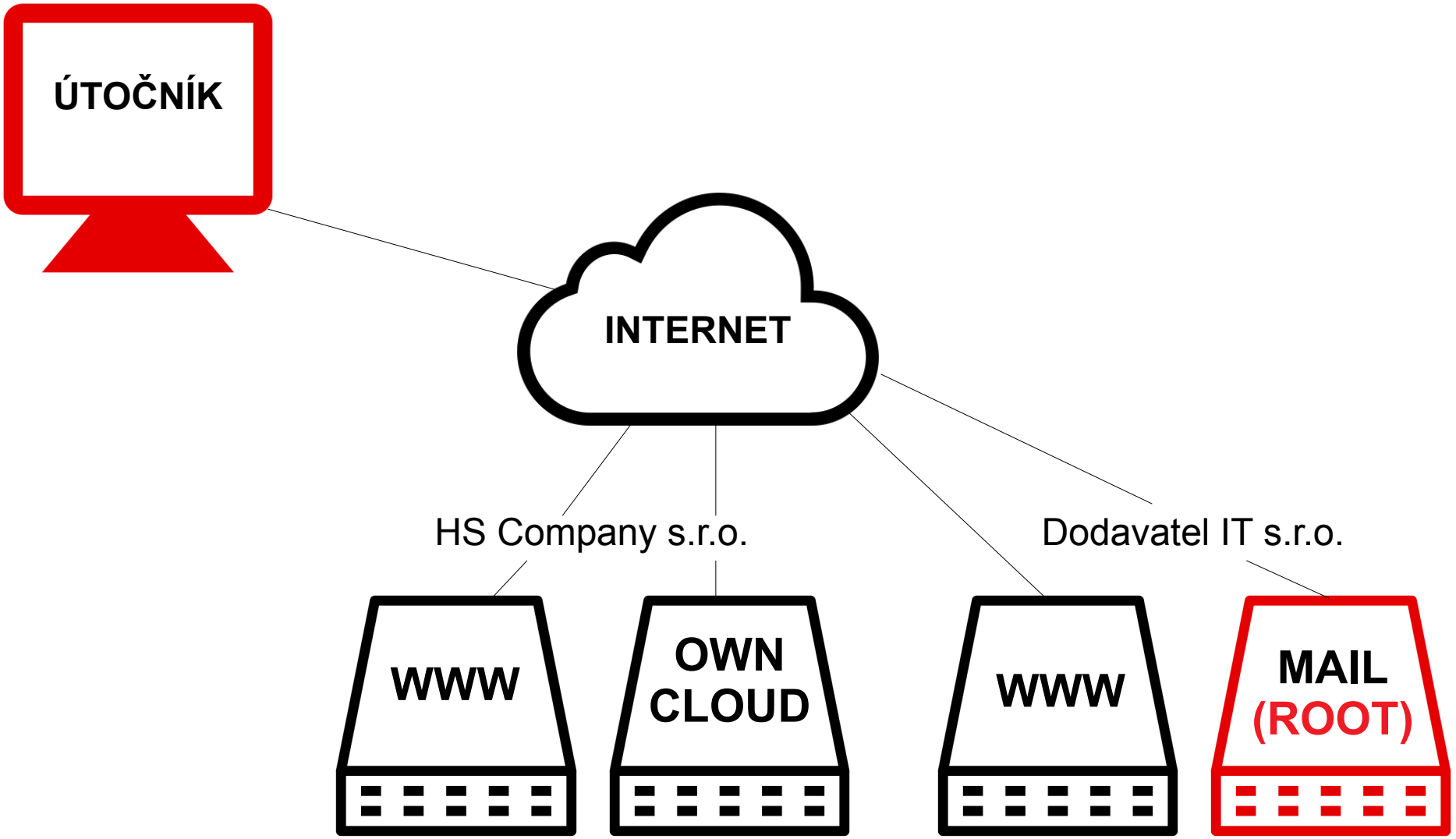
Sběr informací o cíli útoku



Sběr informací o cíli útoku



Útok na řetězec dodavatelů



Rekapitulace I.

- Sběr informací o cíli
  - Veřejně dostupné zdroje
    - Webová prezentace firmy
    - WHOIS databáze
  - Skenování cíle a okolí
- Útok na řetězec dodavatelů
  - Supply chain attack
  - Nejslabší článek = lidský faktor
    - Phishing
    - Špatná politika hesel

Rekapitulace II.

- Proniknutí do koncové sítě oběti
- Útoky na nízkých síťových vrstvách
  - Chybějící mechanismy prevence útoků
    - ARP inspection
- Zneužití procesu validace vlastnictví domény
  - Problém plně automatizovaného procesu
  - Nedostatečná ochrana CAA záznamy v DNS
- Využití získaného certifikátu
  - MITM, odposlech síťového provozu

Rekapitulace III.

- Polevení v bezpečnostní politice na interní síti
  - Bezpečnost primárně na perimetru sítě
- Opomínání záplatování systémů ve vnitřní síti
- Hvězdičkové (wildcard) certifikáty
  - Snadno zneužitelné
  - CAA záznamy nepomohou
- Pohodlí vs. bezpečnost
  - Přístup na ownCloud z Internetu

cesnet

???

https://flab.cesnet.cz

flab@cesnet.cz