SPRÁVA ŽELEZNIC

Příspěvek do konference SZT

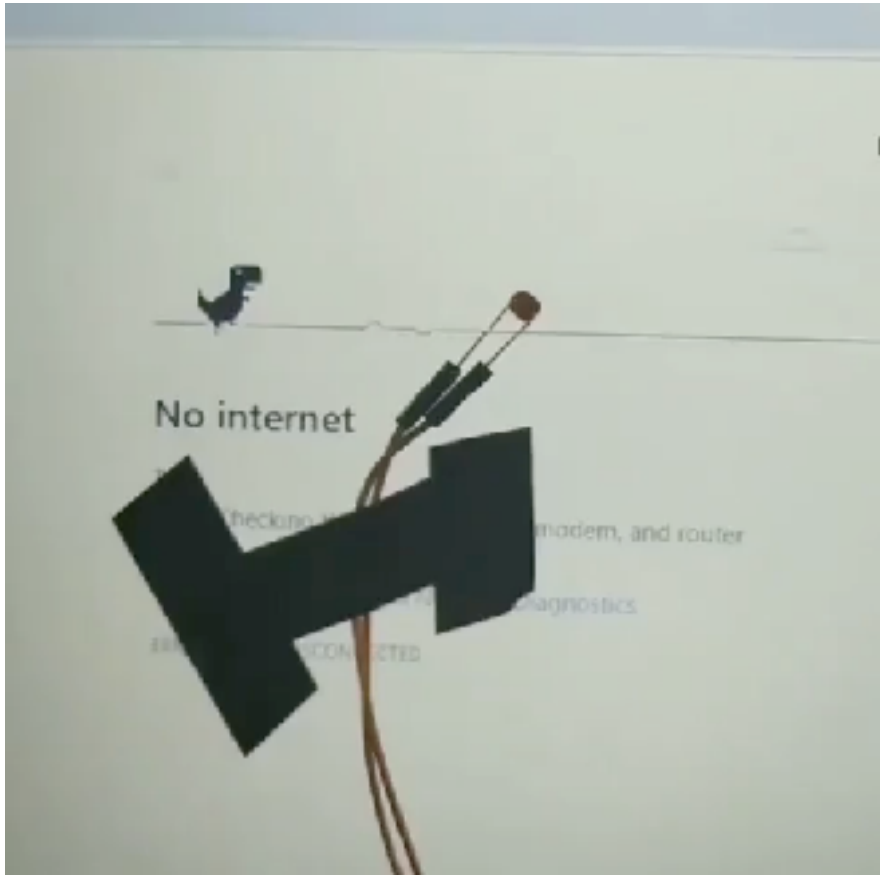
Koncepce datových sítí SŽ

Ing. Vladimír HORA
GŘ SŽ O14 OTSA

Olomouc, 4.10.2021

Typy datových sítí v SŽ

- 5 vrstev sítě
- ~8000 segmentů sítě
- ~14000 uživatelů
- ~32000 IP adres v TDS
- ~80000 ACL
- end of life technologie



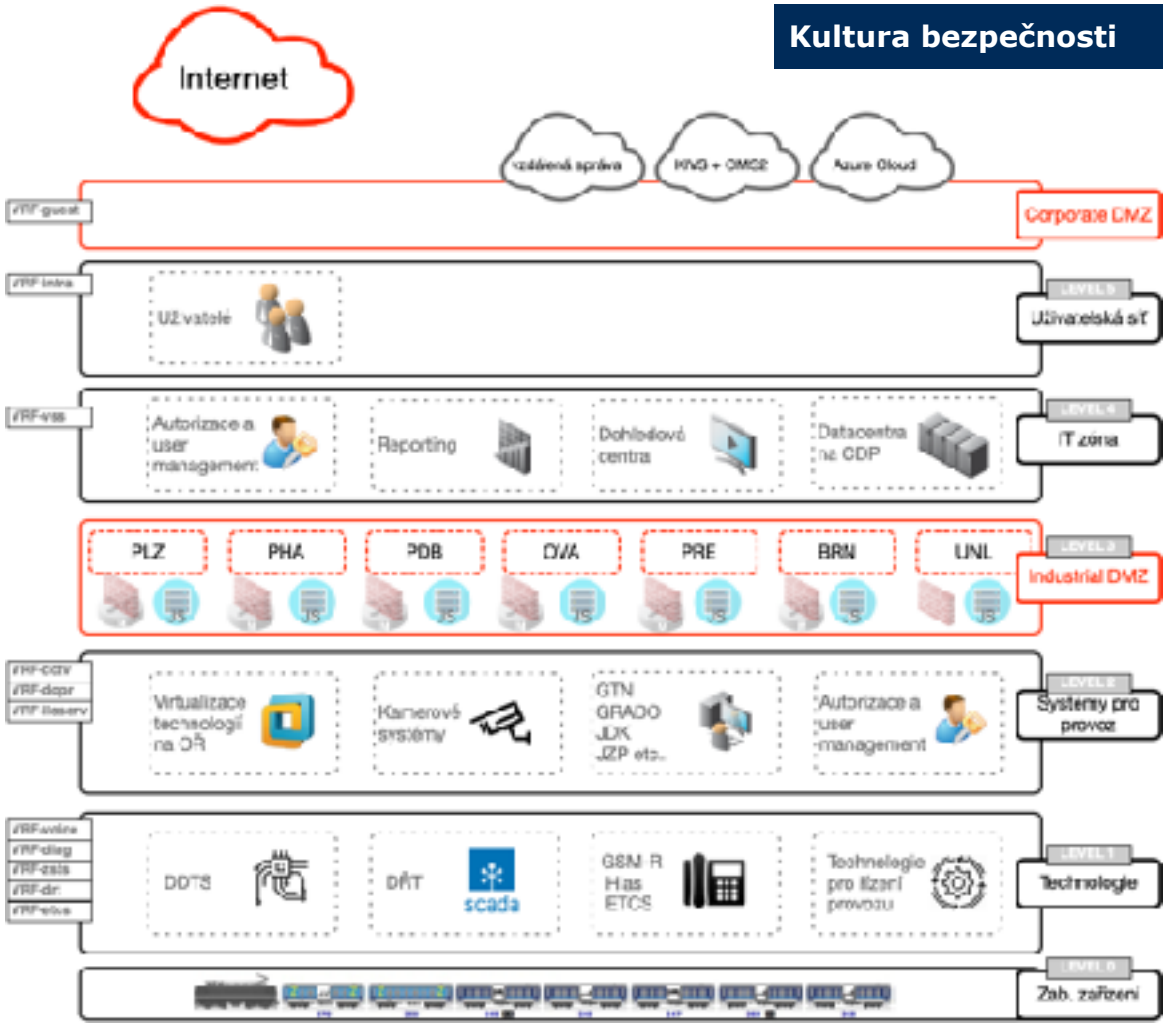
Definice IT a OT v SŽ

- IT/OT paradigma – definuje základní charakteristiky síťového prostředí v SŽ
- Co je to konvergence IT/OT

IT/OT Konvergence

- Segmentace
- Stanovení bodu konvergence
- Implementace ISA/IEC 63443
- Stanovení bezpečnostních zón
- Nastavení pravidel pro komunikaci

bod konvergence ->

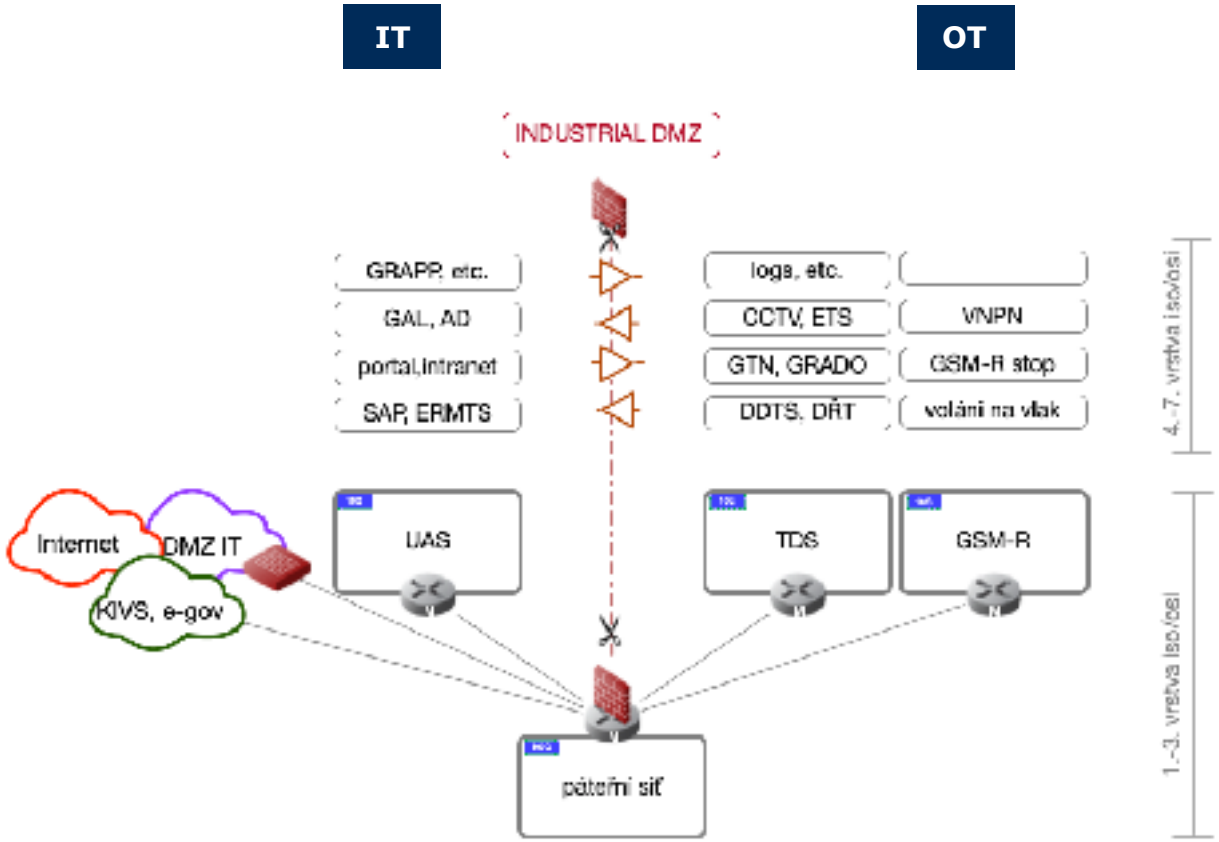


Infrastruktura SŽ

- Robustní infrastruktura pro IT i OT
- 1-3.5 vrstva sítě SŽ
  - **jádro (core) sítě sjednotit na MPLS**
  - **dedikované GSM-R služby**

- od 3. vrstvy

IT	OT
updating	hardening
blacklisting	whitelisting
tisíce uživatelů	stovky uživatelů
Manažerské výstupy	Sběr dat
Plochá síť	Segmentovaná síť
UAS	TDS
Progresivní přístup	Konzervativní přístup

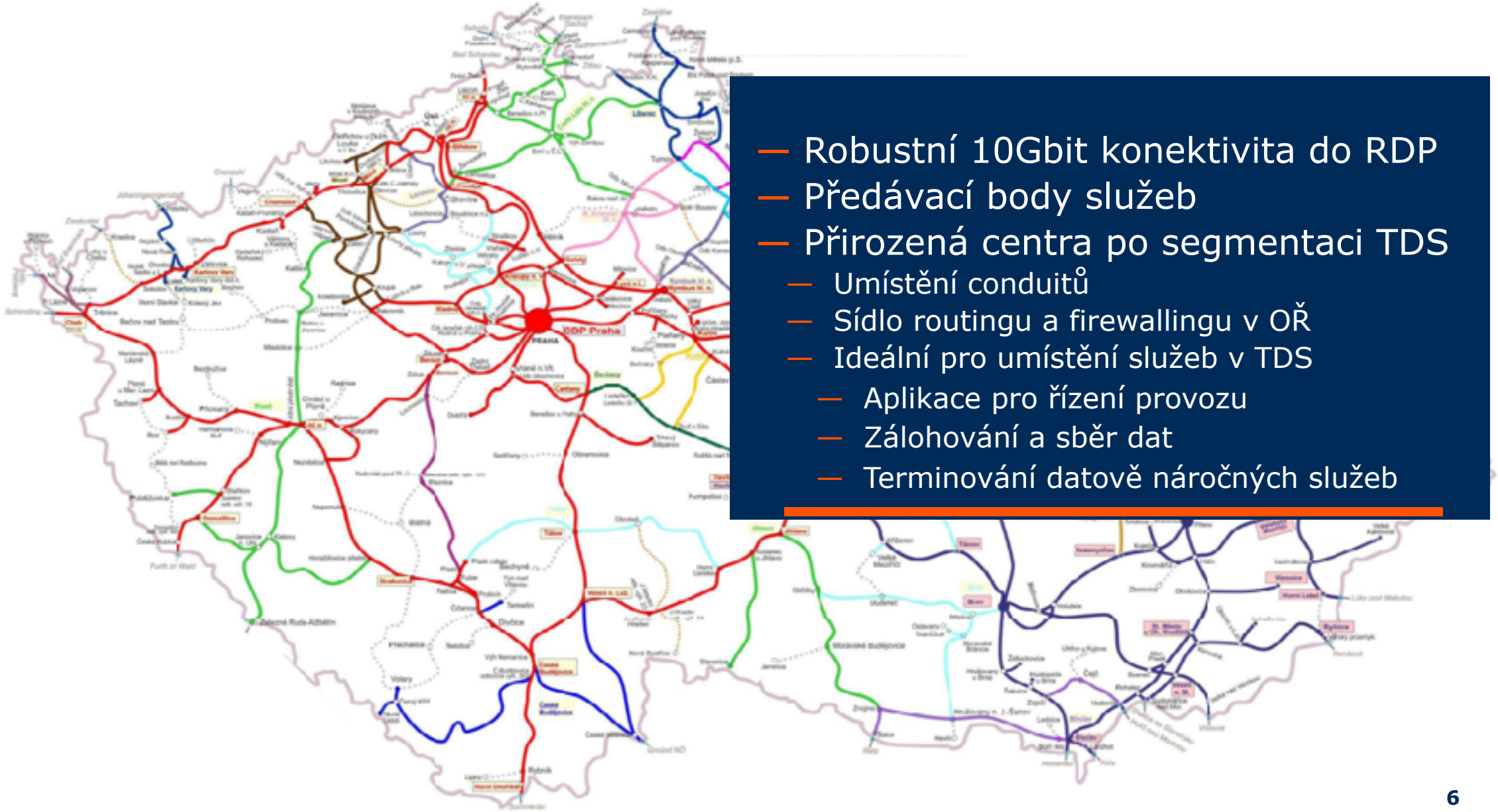


ISO/OSI model sítě SŽ

Infrastruktura SŽ - rozvoj

- Upgrade core sítě a segmentace TDS
- Robustní 10Gbit konektivita do RDP
- Implementace ISA/IEC 63443
- Hardening, industrial DMZ, Certifikační autorita
- OŘ TDS datová centra, Předávací body služeb
- Virtualizační farmy v TDS DC
- KIVS a CMS2, eGoverment
- IoT, secure LTE -> 5G
- Unifikace SW prostředí - API
- Migrace SDH/TDH -> MPLS
- Ústup od E1 a legacy služeb -> TCP/IP (TSN)
- Promyšlený sběr dat

Datová centra v TDS

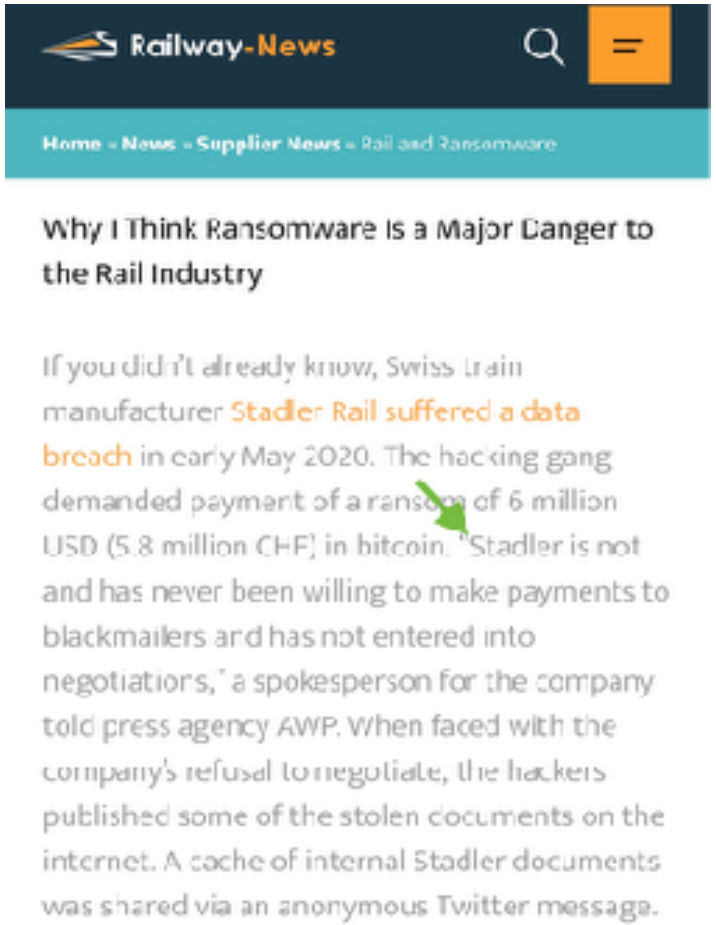


- Robustní 10Gbit konektivita do RDP
- Předávací body služeb
- Přirozená centra po segmentaci TDS
  - Umístění conduitů
  - Sídlo routingu a firewallingu v OŘ
  - Ideální pro umístění služeb v TDS
    - Aplikace pro řízení provozu
    - Zálohování a sběr dat
    - Terminování datově náročných služeb

Bezpečnost sítě

- Ransomware
  - **Kia Motors - únor 2021**
  - **CD Projekt Red - únor 2021**
  - **Acer - březen 2021**
  - **Colonial Pipeline - květen 2021 - 5mio$ hackers, 340mio$ ztráty**
  - **Maersk - červen 2021 - 300 mio$**
  - **Stadler Rail - květen 2020 ->**
- Ostatní kybernetické hrozby
- SecurityByObscurity řešení (bunker-like mentality)
- Roztříštěnost SW - neexistence API
- Vendor locky
- Diskomfort uživatelů - GUI

Průměrná doba odstávky 21 dnů



Diagnostika a Data mining - DDTS 2.0

- Souběh s aktuálními projekty – Logmanagement
- Infrastruktura generuje velké množství nevyužitých dat
- Datová analytika
  - **Data z DDTS**
  - **Data z logmanagementu**
  - **Data z technologií**
- DDTS jako jednotný notifikační kanál v TDS SŽ

Děkuji za pozornost

Koncepce datových sítí SŽ
Ing. Vladimír Hora
GŘ SŽ O14

horav@spravazeleznic.cz

© Správa železnic, státní organizace
Dlážděná 1003/7, 110 00 Praha 1