TRENDY V OBLASTI BEZPEČNOSTI DATOVÝCH CENTER

JIŘÍ HROMADNÍK, FUBAR A.S.
CDCDP, ATD

KLÍČOVÉ OBLASTI BEZPEČNOSTI DATOVÝCH CENTER

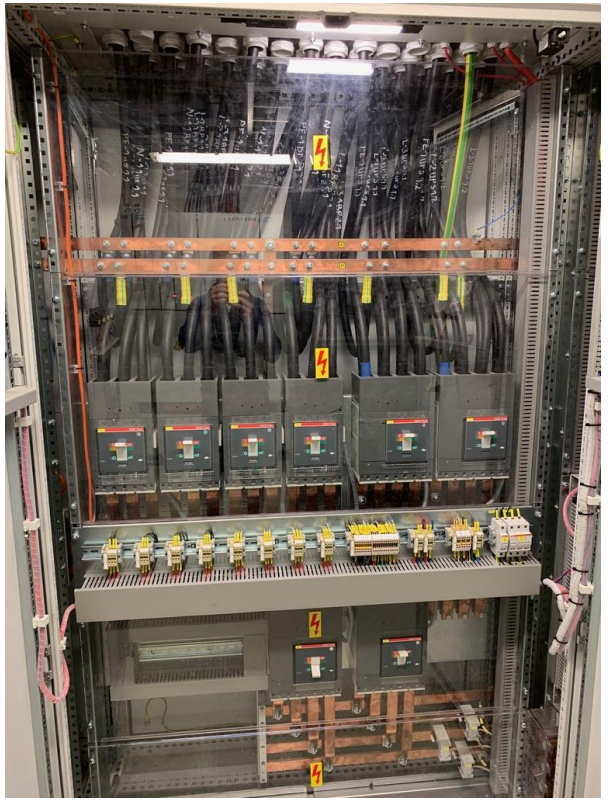
- Fyzická bezpečnost
- Kybernetická bezpečnost
- Bezpečnostní procesy
- Business Continuity a Disaster Recovery

FYZICKÁ BEZPEČNOST DATOVÝCH CENTER

- Tato oblast bude detailně pokryta v rámci následujících přednášek

KYBERNETICKÁ BEZPEČNOST

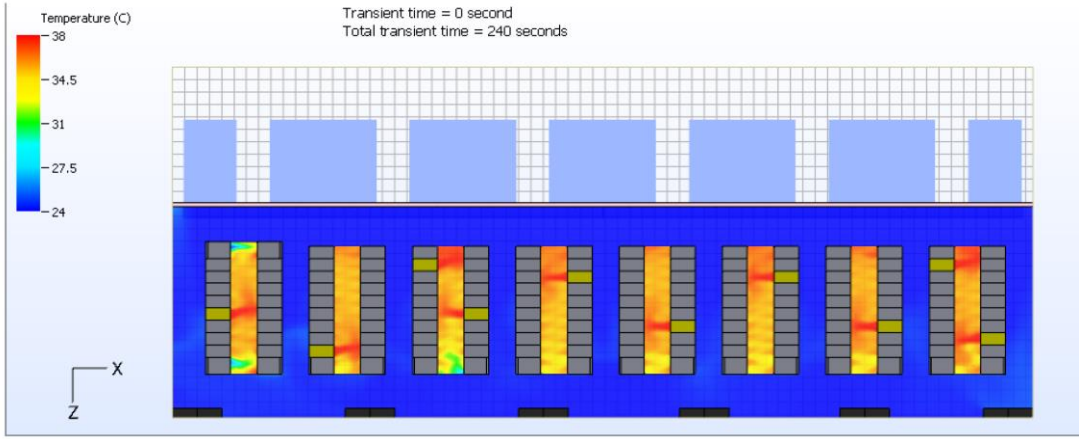
- Proč se věnovat v oblasti DC facility (budova + non-IT) kybernetické bezpečnosti?

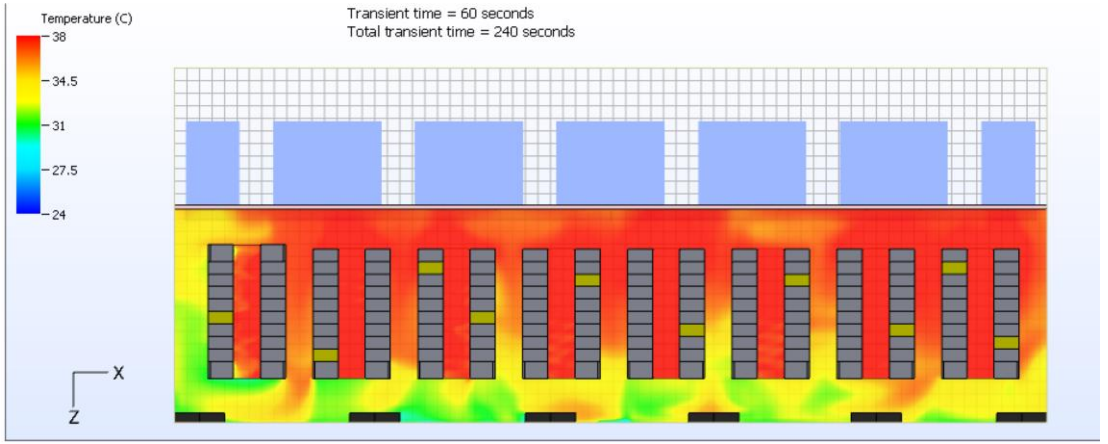


KYBERNETICKÝ ÚTOK NA NON-IT INFRASTRUKTURU

- **Stále častější útoky na systémy technické infrastruktury**
  - Energetická infrastruktura
  - Infrastruktura datových center
  - Dopravní infrastruktura

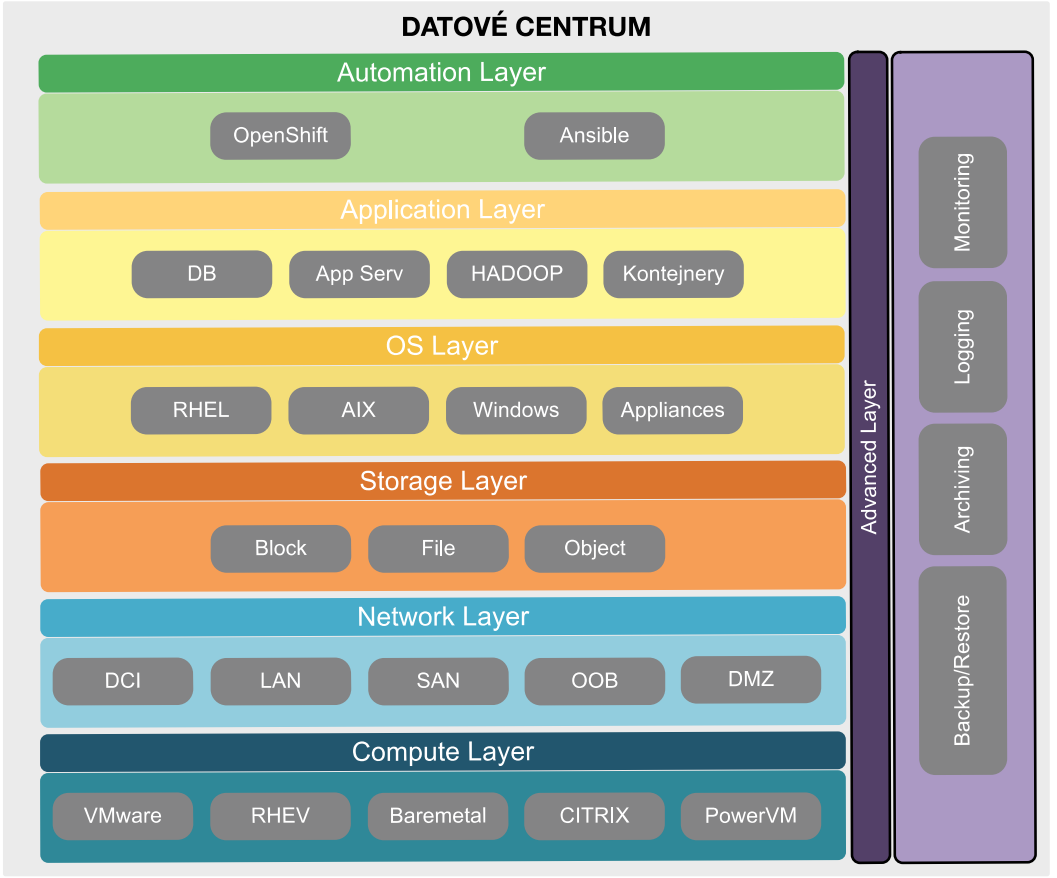
- **Typické útoky na datová centra**
  - Nápájecí infrastruktura
  - Chladící infrastruktura
  - Bezpečnostní infrastruktura



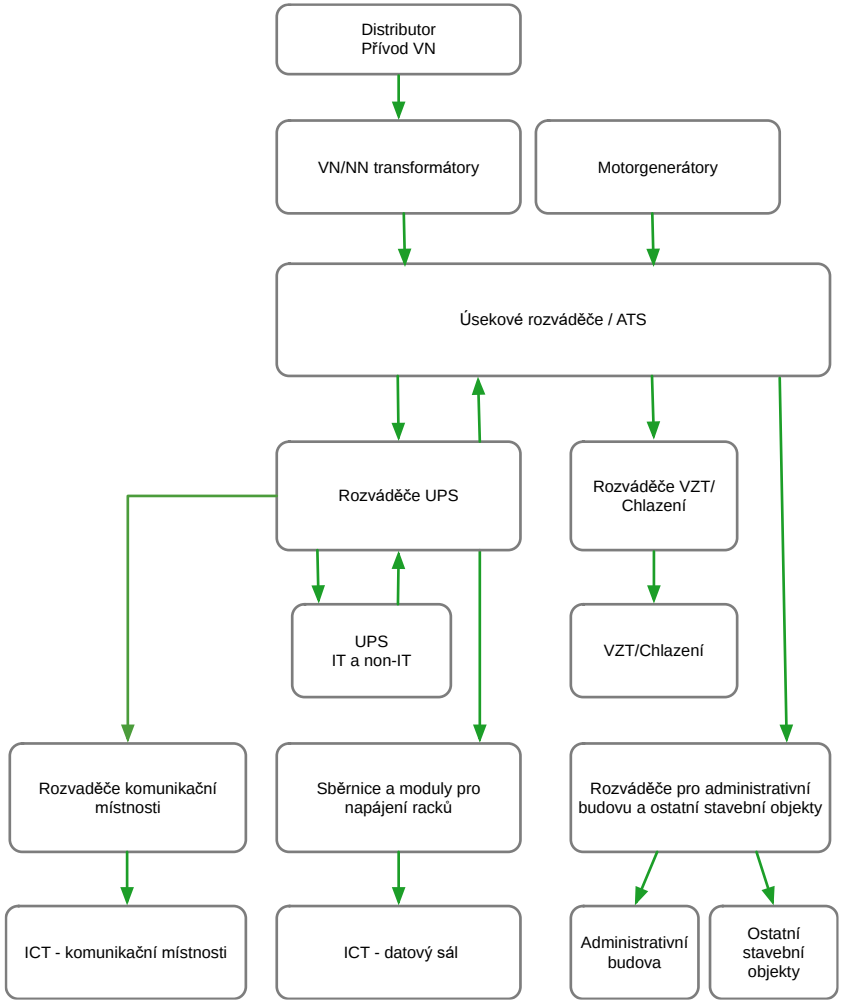


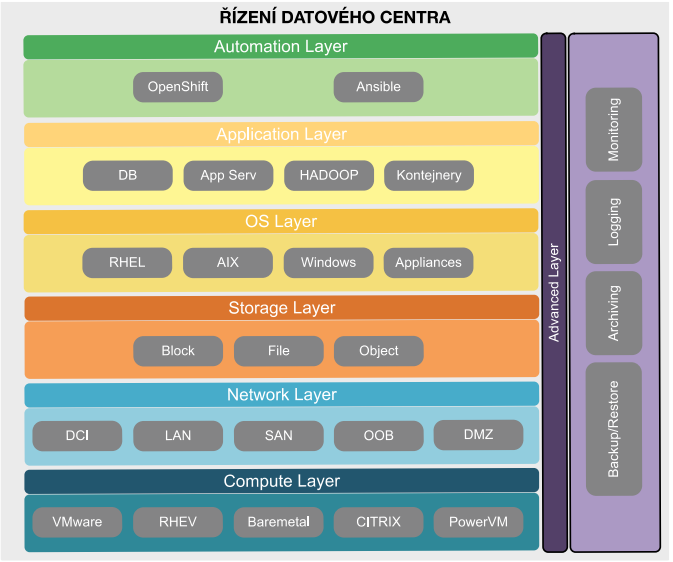
KYBERNETICKÁ BEZPEČNOST

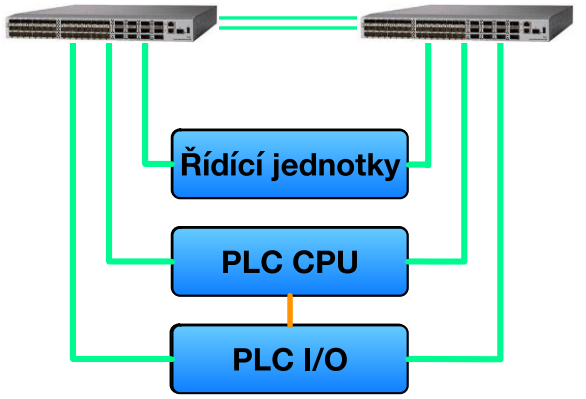
- Kybernetickou bezpečnost si v rámci DC spojujeme zejména s IT stackem



JAK SOUVISÍ KYBERNETICKÁ BEZPEČNOST S NON-IT







JAK SOUVISÍ KYBERNETICKÁ BEZPEČNOST S NON-IT

BEZPEČNOSTNÍ PROCESY

- **Non-IT systémy**
  - Inventory management
    - Přehled o verzích firmware a operačních systémů ve všech non-IT prvcích
    - Sledování bezpečnostních slabin a hardeningu ve spolupráci s výrobci
  - Servisní a update management
    - Kontrola bezpečných servisních zásahů
    - Řízený update management
- **IT Stack pro systémy řízení DC**
  - Hardening, bezpečnostní aktualizace firmware, VM/OS, DB a aplikační servery
  - HA a zálohování na bezpečné úložiště – nejlépe certifikovaná objektová storage
  - Striktní oddělení od IT systémů a zajištění bezpečnosti – FW, IPS, IDS, AD, AV…
- **Řídící a monitorovací nástroje**
  - Soulad se standardy vývoje bezpečných řídících a dohledových systémů
  - Striktní zabezpečení jako pro jakékoliv aplikace se vzdáleným přístupem a cloud aplikace

BUSINESS CONTINUITY A DISASTER RECOVERY

- **Související normy**
  - ISO 27031 - požadavky na informační a komunikační technologie pro zajištění kontinuity podnikání
  - ISO 22301:2020 - Security and Resilience – Business continuity management systems
- **Disaster Recovery plán pro DC facility – nutná návaznost na BC strategii**
  - CRAMM analýza a návaznost na BIA – například provázanost DCIM a CMDB
  - Plány eskalace při významné události a definice rozhodovacích bodů
  - Organizace obnovy po významné události
  - Nouzové postupy po významné události
- **Zajištění proti externím vlivům – např. mimořádné události**
  - Zajištění / posílení ochrany
  - Zajištění přístupu a fungování obsluhy a servisu
  - Zajištění dodávek nafty
  - Zajištění náhradních dílů

DĚKUJEME ZA POZORNOST