GREYCORTEX

Implementácia bezpečnostného dohľadu v organizáciách štátnej a verejnej správy

Martin Senčák, Beset, Bratislava
Vladimír Sedláček, Greycortex, Brno

KDO JE GREYCORTEX – 1/3

- Jsme evropská firma
  - profesionálové počítačové bezpečnosti
  - vytváříme produkt pro bezpečnější svět sítí (Internet) a propojených zařízení (SCADA, IoT)
  - pro firmy, instituce, silové složky, kritickou infrastrukturu, komunální podniky
- Máme zkušenosti
  - z AVG, Comguard a.s., TrustPort International, Acision
  - s výstavbou a správou počítačových sítí
  - tvorbou software pro analýzu a dopravu zpráv v telekomunikačních sítích
  - analýzou škodlivého software, managementem bezpečnosti

GREYCORTEX

KDO JE GREYCORTEX – 2/3

- Zviditelňujeme
  - strukturu sítě a datových komunikací
  - škodlivou nežádoucí komunikaci na síti (anomálie, porušení politik, útoky, unik dat, …)
- Využíváme
  - hloubkovou inspekci paketů (DPI)
  - statistickou analýzu
  - pokročilou signaturní detekci
  - reputační systémy
  - strojové učení (ML)
- Spolupracujeme s výzkumnými centry
  - VUT
  - CCDCOE

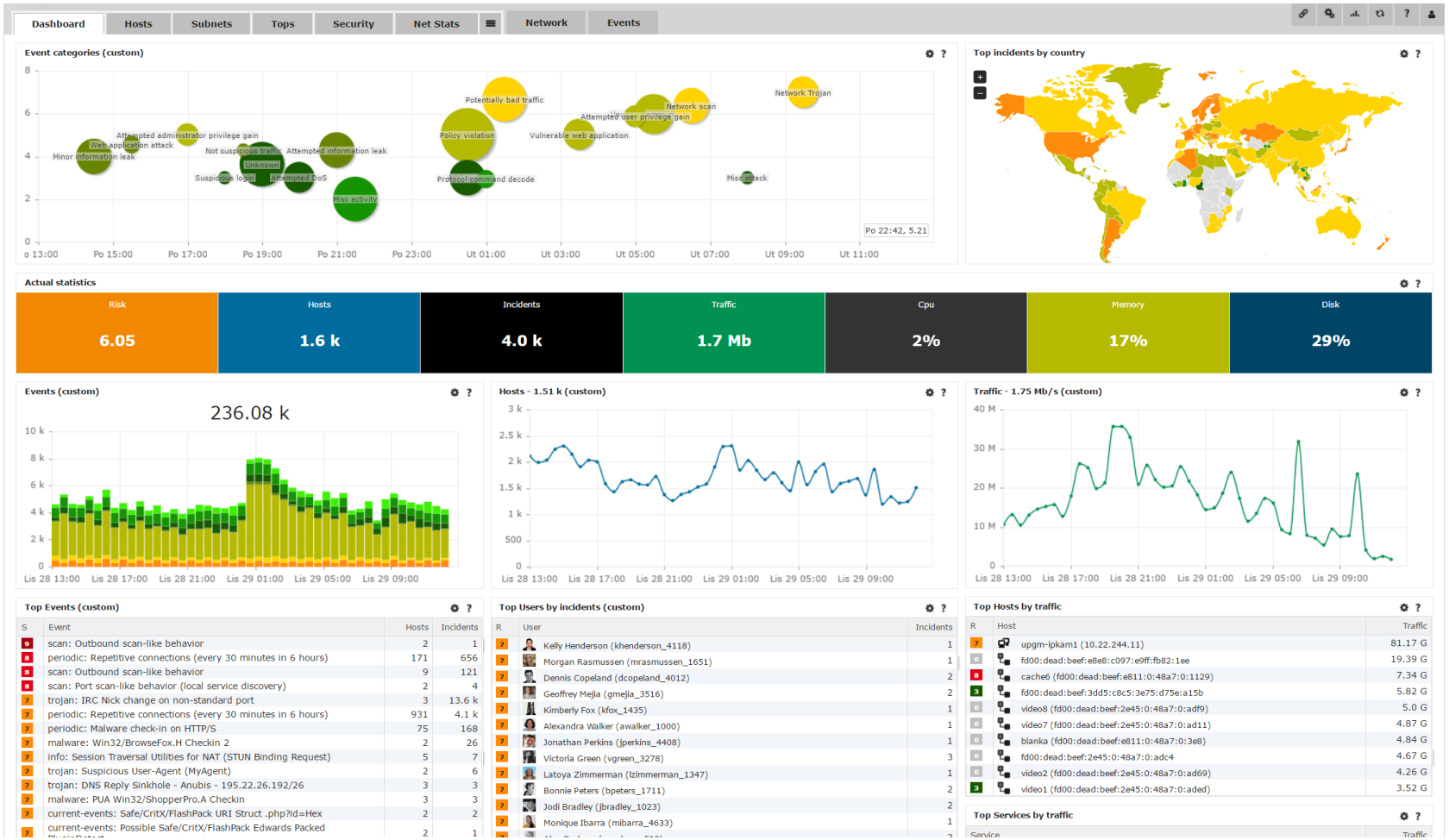
GREYCORTEX

KDO JE GREYCORTEX – 3/3

- Patříme
  - mezi klíčové dodavatele technologie v segmentu analýzy síťového provozu (NTA), spolu s firmami jako je Cisco, Darktrace, Fidelis Cybersecurity, Plixer a další
    - Podle analytické společnosti Gartner (viz Market Guide for Network Traffic Analysis, Published: 28 February 2019 ID: G00381265)
  - po Brexitu zůstaneme jediným výrobcem NTA software v EU

GREYCORTEX

RYCHLÝ SITUAČNÍ PŘEHLED



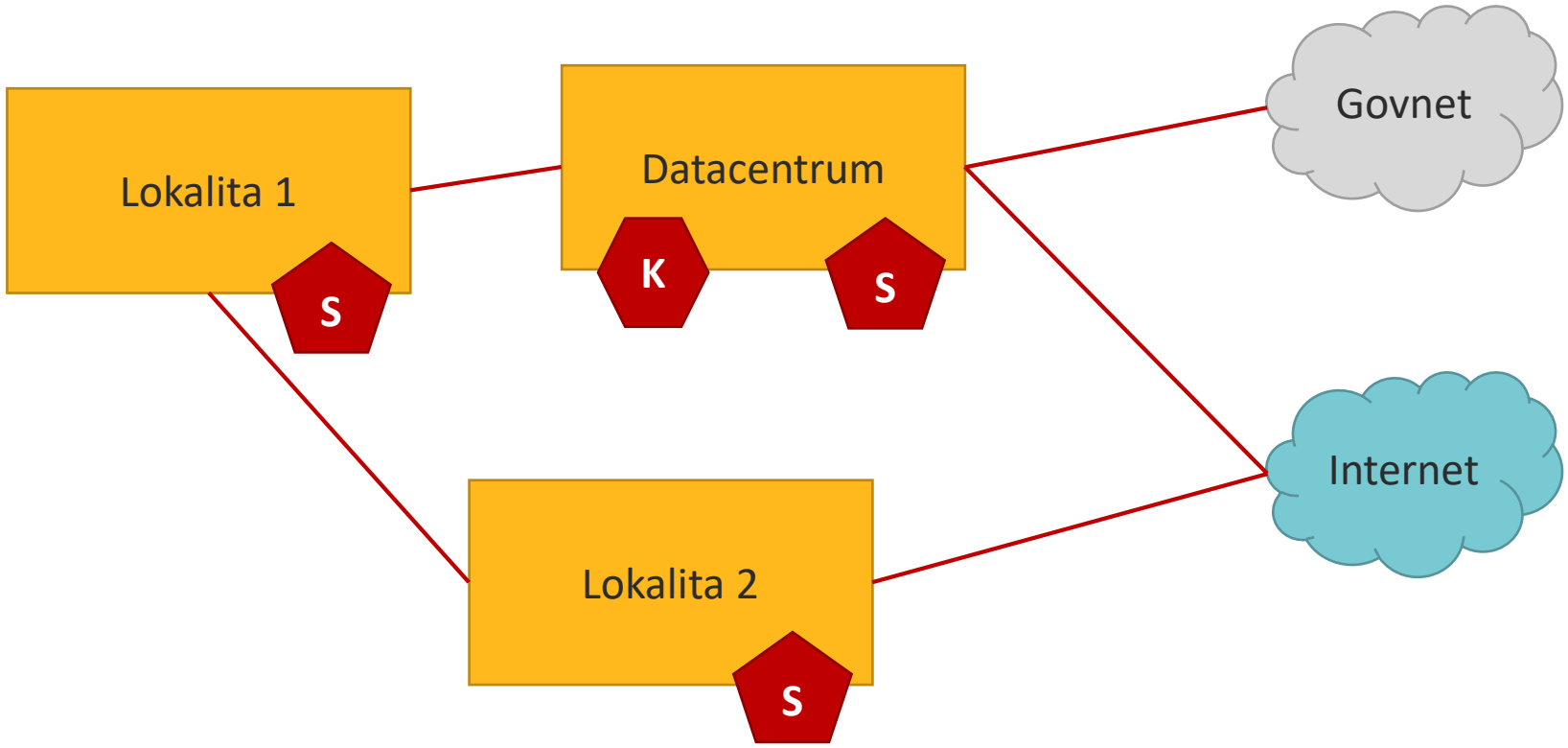
GREYCORTEX

Příklady nasazení

Dohled nad bezpečností sítě s GREYCORTEX Mendel

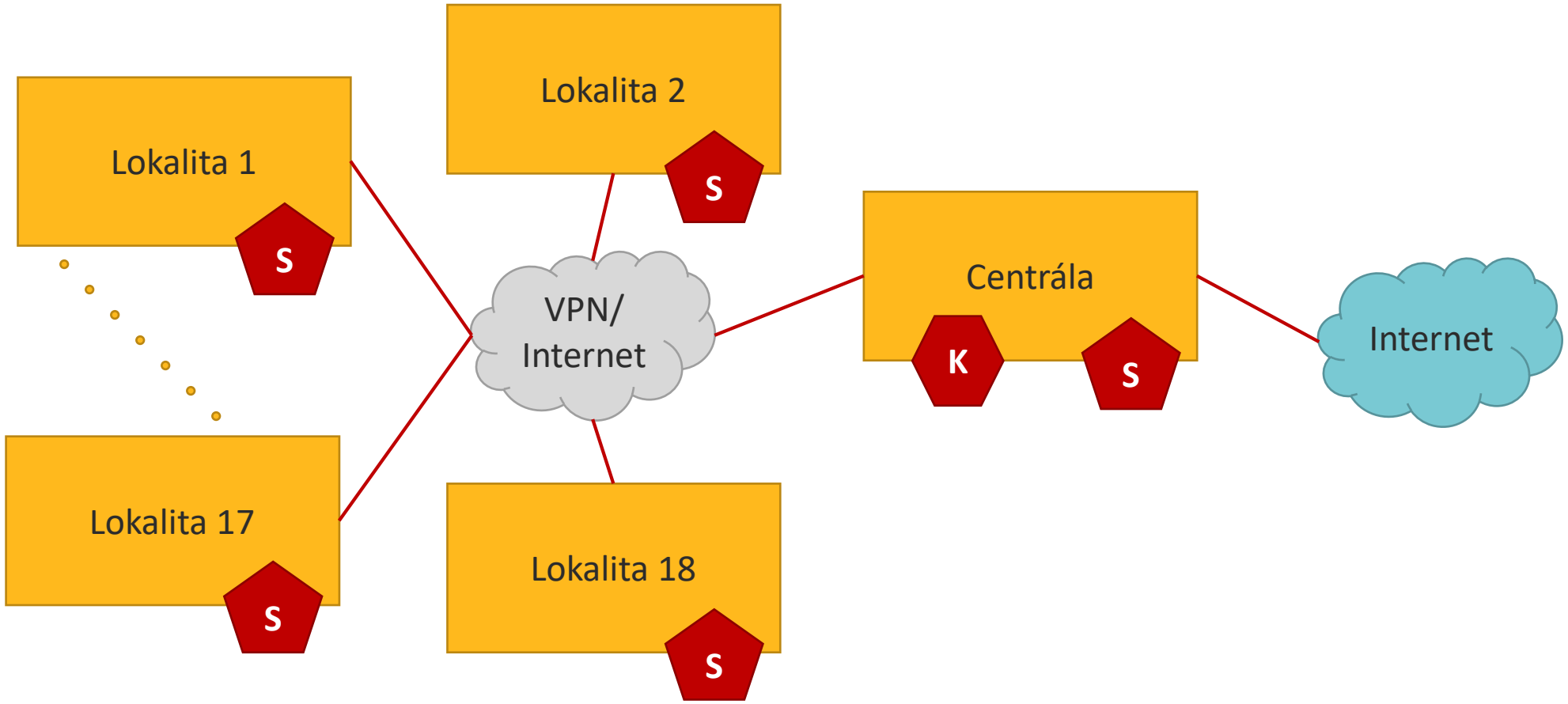
GREYCORTEX

VÍCE LOKALIT, JEDNO MĚSTO



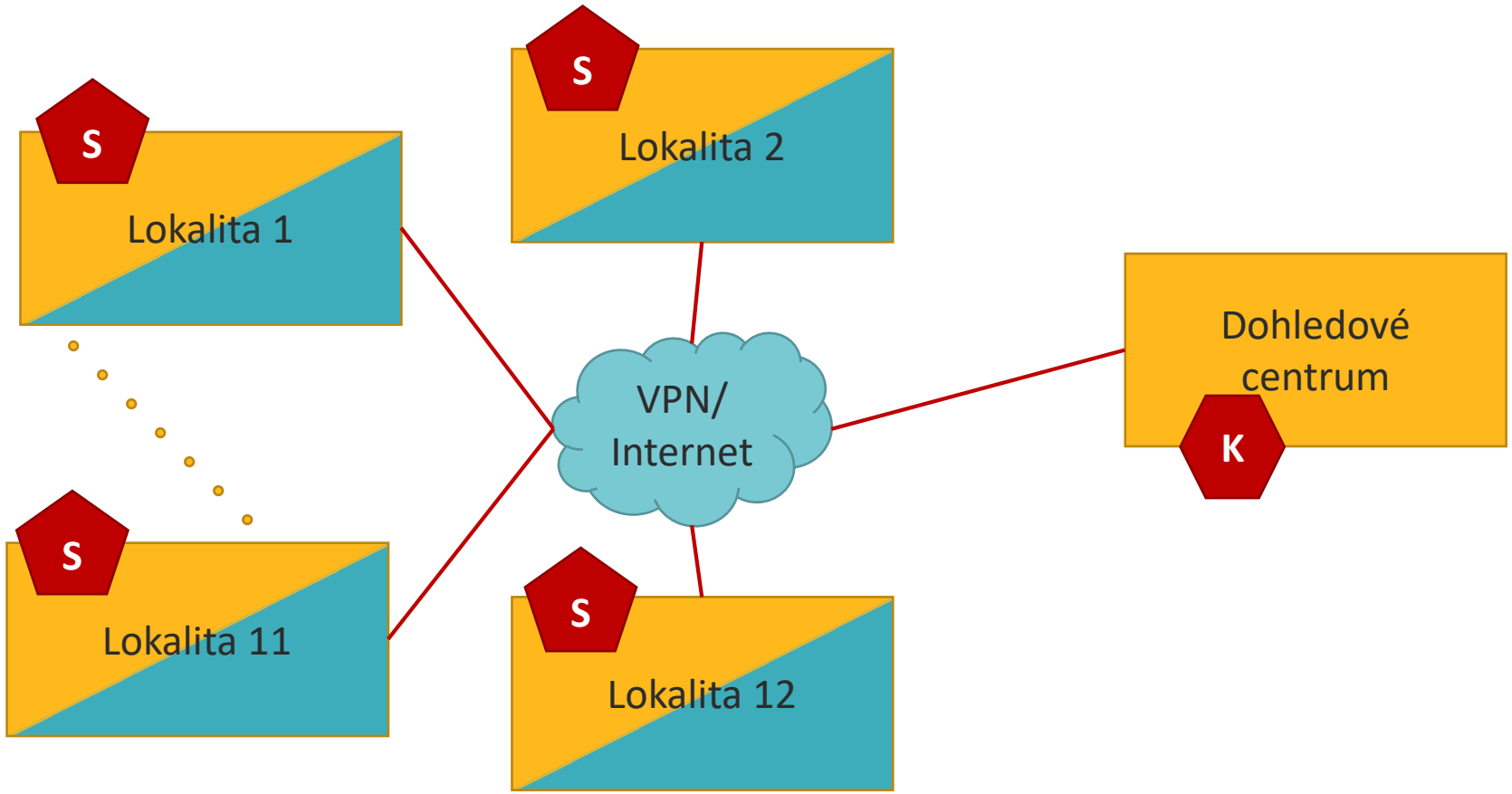
GREYCORTEX

CELONÁRODNÍ PŮSOBNOST



GREYCORTEX

SDÍLENÁ INFRASTRUKTURA



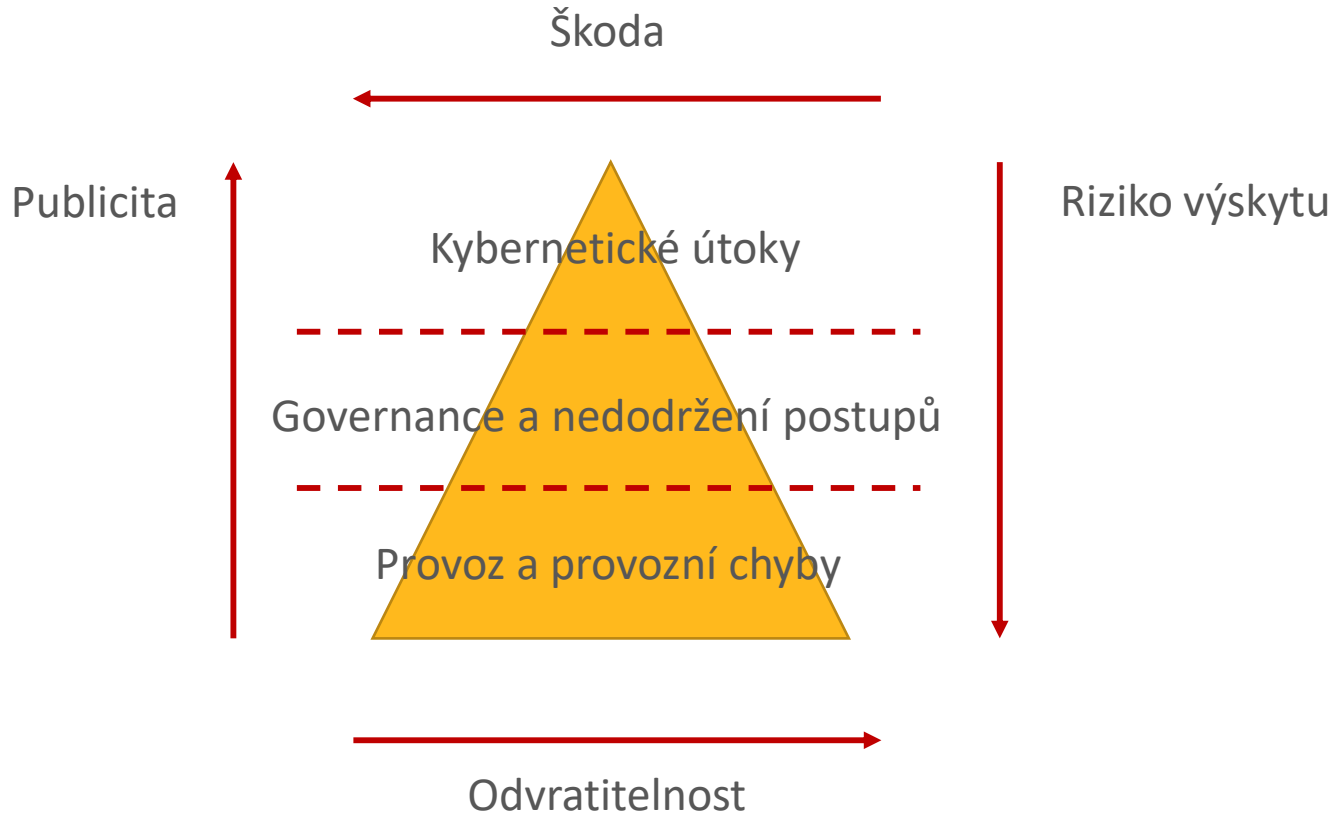
GREYCORTEX

Co jsme při nasazování našli

Tedy v prvních hodinách po zapojení

GREYCORTEX

OBVYKLÍ PODEZŘELÍ

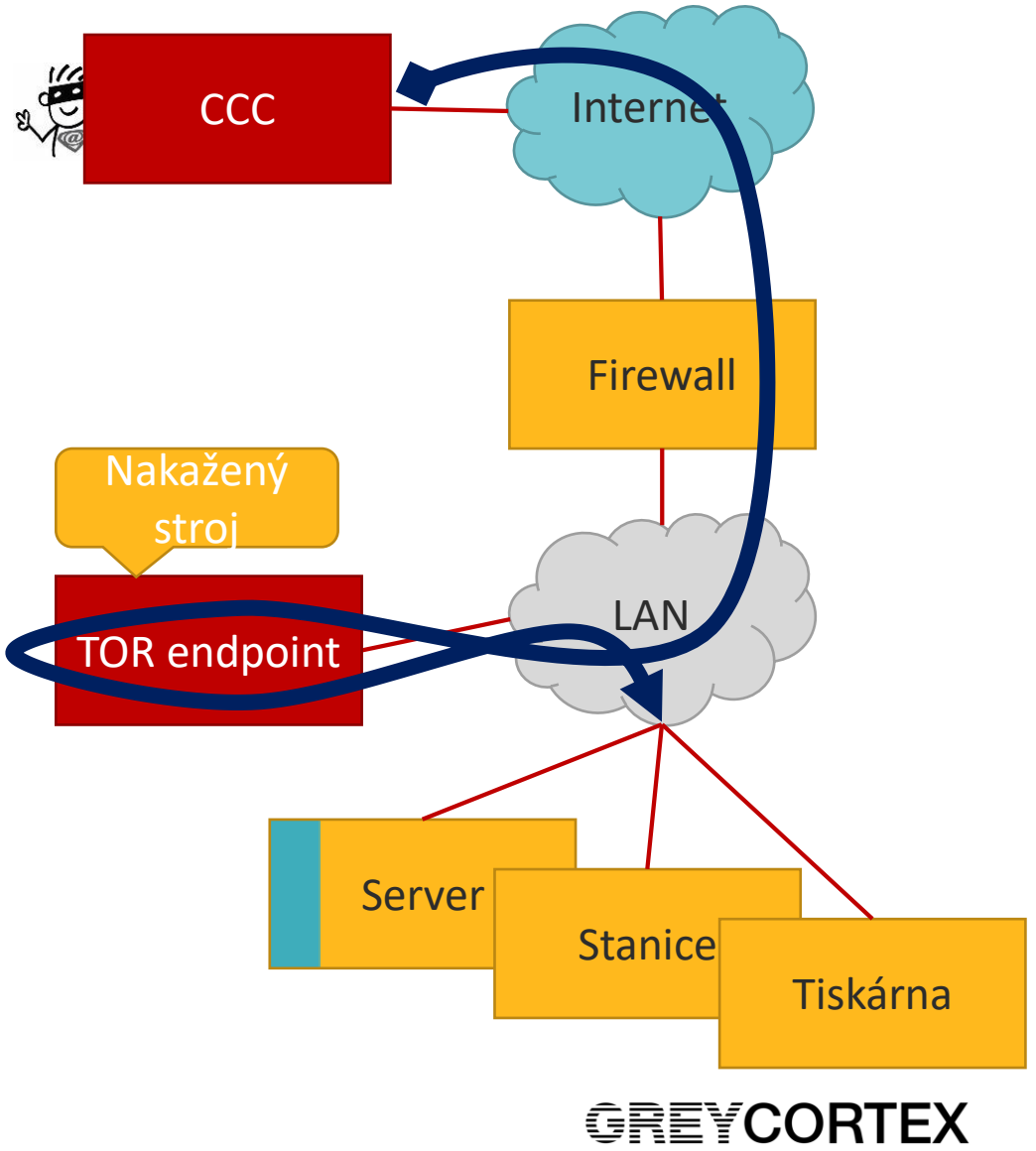


GREYCORTEX

ÚTOKY – 2/2

- Malware VPN Filter
  - TOR provoz **ve vnitřní síti**

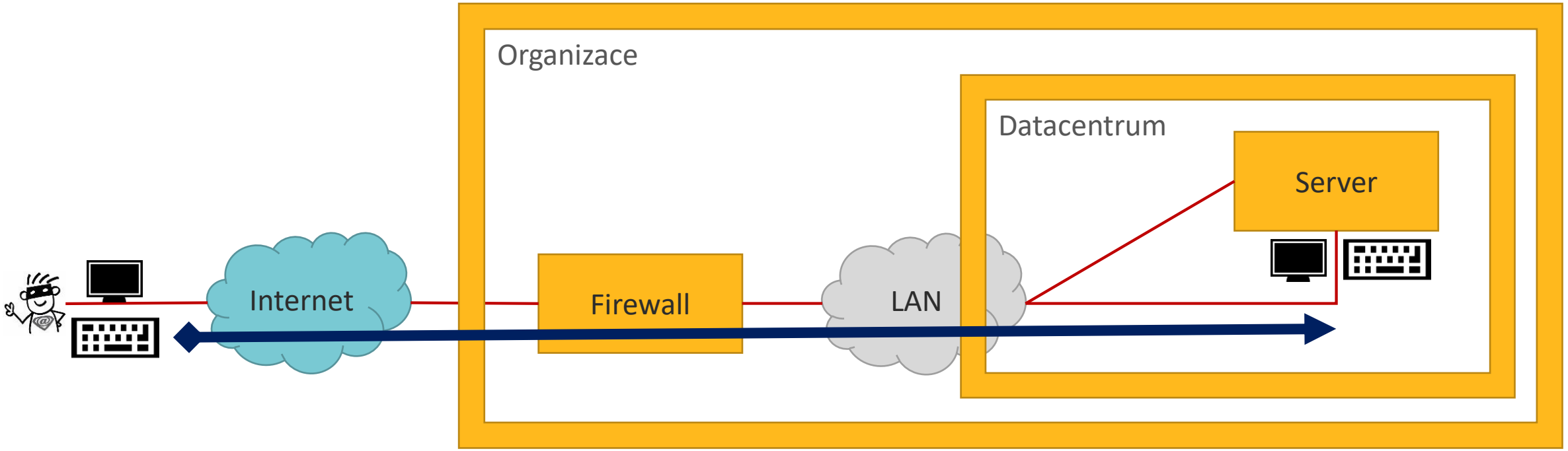
- Wannacry šifruje 25 PC
  - Přístupy na známá jména a adresy killswitch
  - TOR provoz **ve vnitřní síti**



GREYCORTEX

KONFIGURAČNÍ CHYBY – 1/4

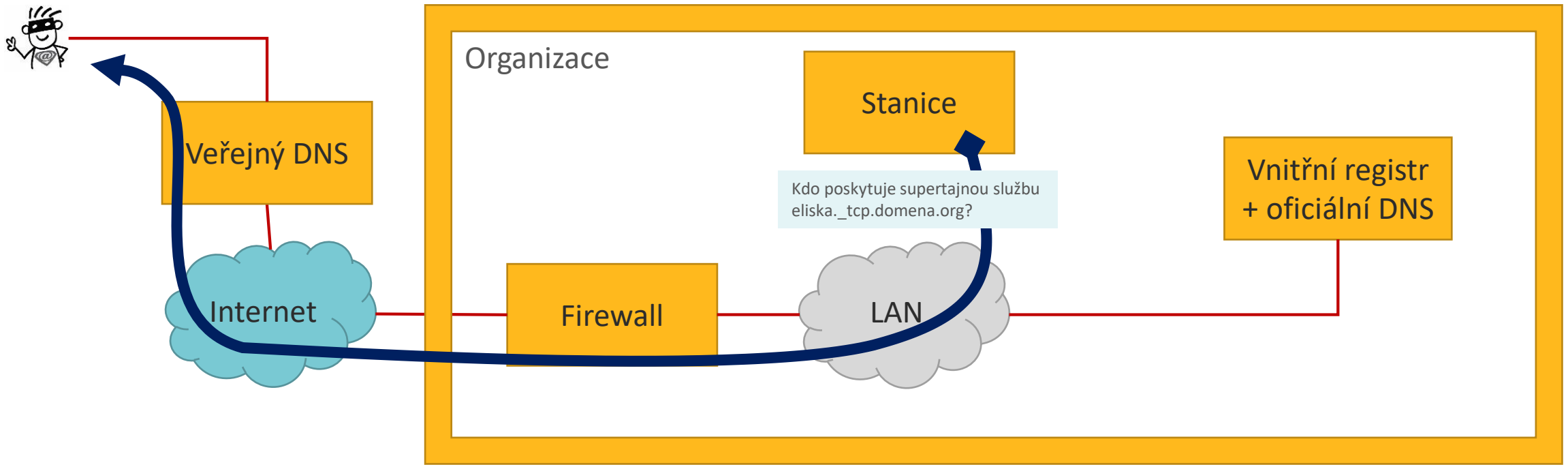
- Vzdálená konzola fyzického serveru byla přistupována z internetu
  - Porty otevřené na firewallu pro přístup z veřejné sítě (přímo, bez VPN či jiné ochrany)



GREYCORTEX

KONFIGURAČNÍ CHYBY – 2/4

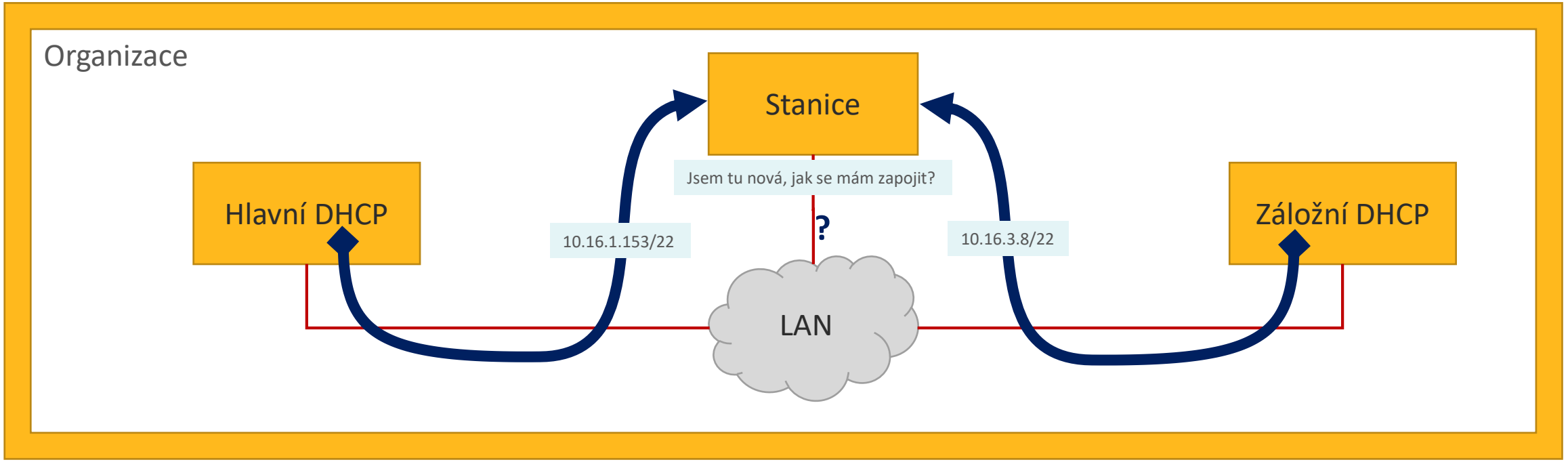
- Dotazy pracovních stanic směřovány přímo na veřejný DNS
  - Dotazy venku prozrazovaly jména a role stanic, náhradní postupy zjišťování ve vnitřní síti



GREYCORTEX

KONFIGURAČNÍ CHYBY – 3/4

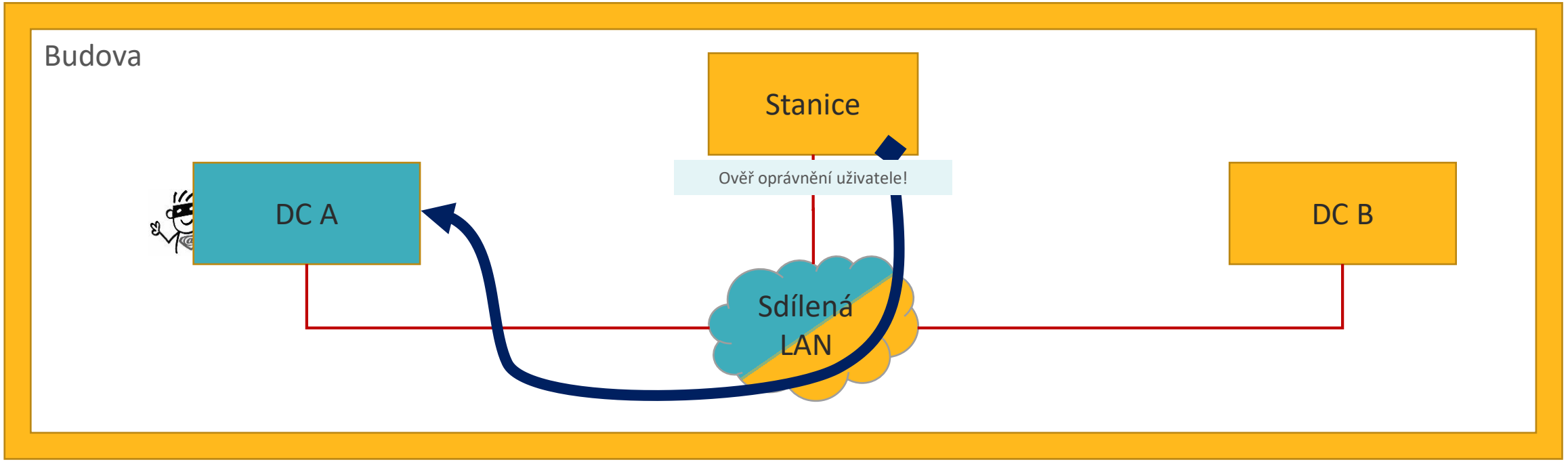
- Shodná konfigurace pro hlavní a záložní DHCP server, nesynchronní data
  - Jedna stanice dostávala dvě nabídky různých adres, dvě různé stanice dostávaly stejnou adresu



GREYCORTEX

KONFIGURAČNÍ CHYBY – 4/4

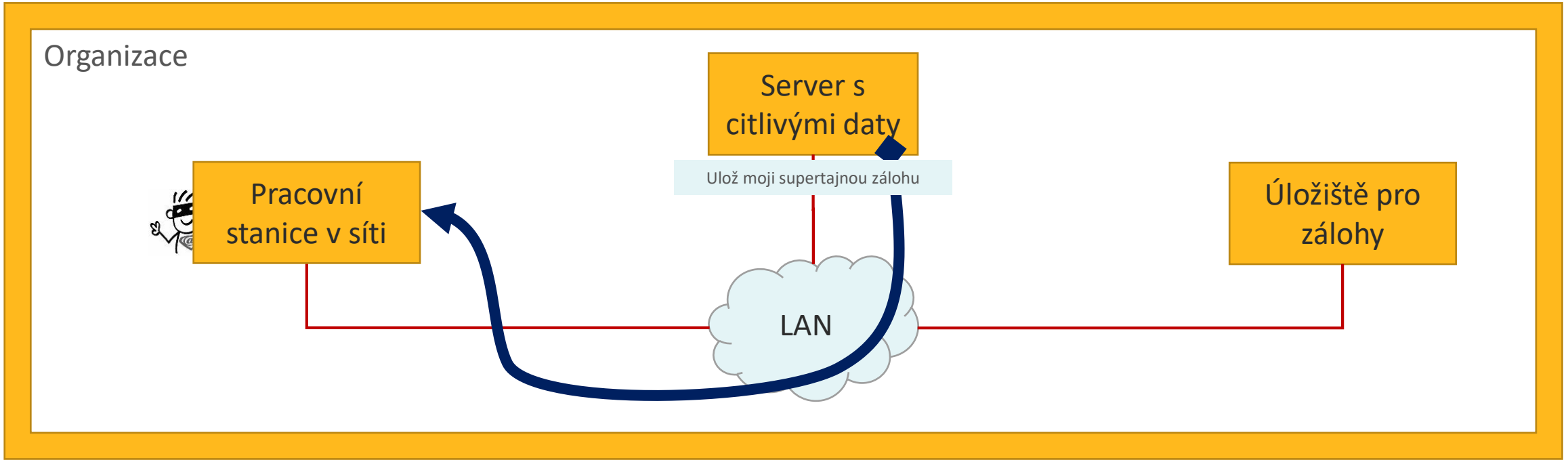
- Ve sdílené infrastruktuře se stanice jednoho subjektu připojovaly k DC druhého
  - Pomíchané nastavení bridge a routerů v různých VLANech



GREYCORTEX

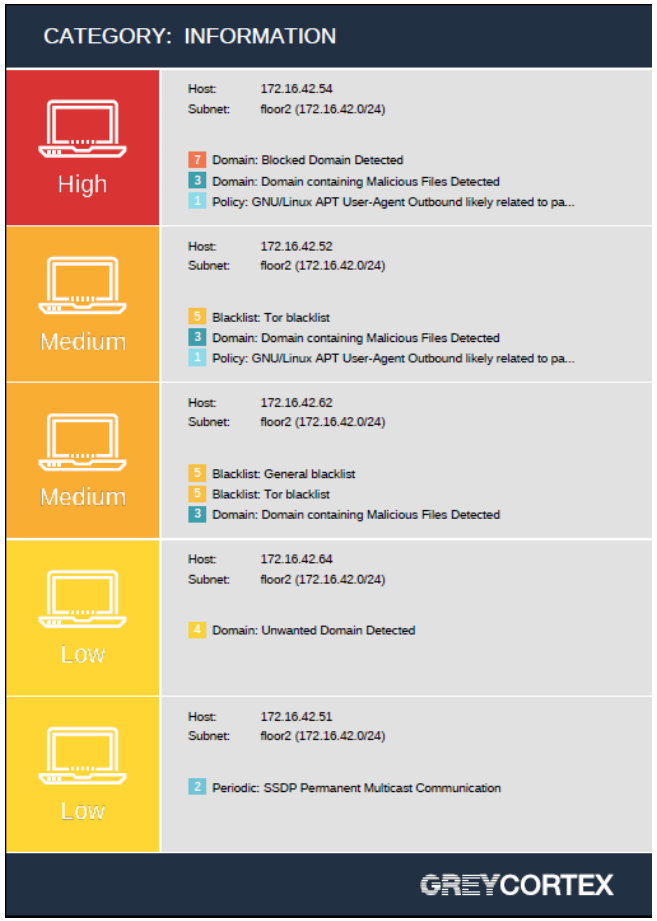
PROVOZNÍ CHYBY – 1/1

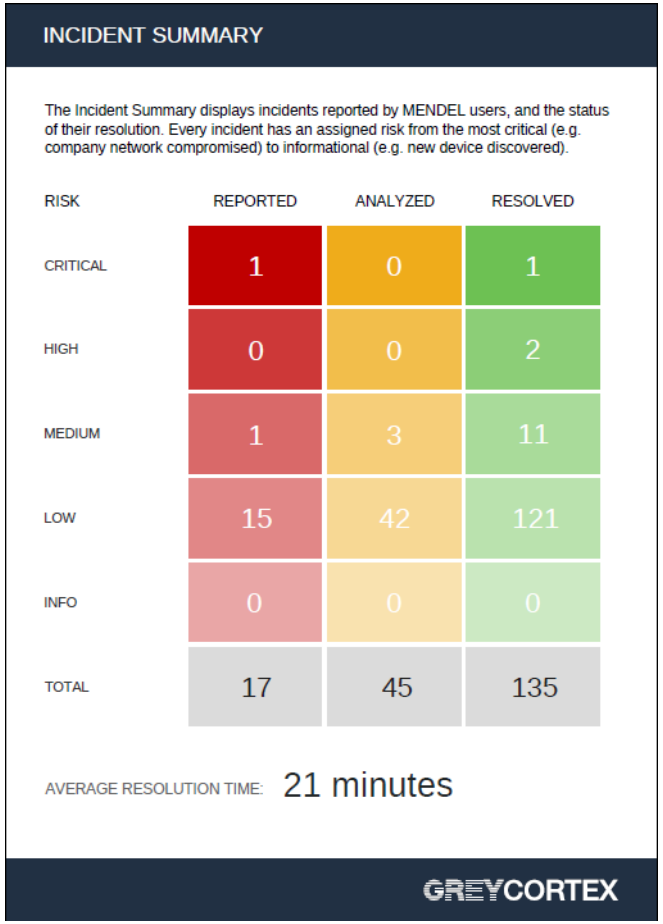
- Zálohování na špatný cíl
  - Server byl přesunut do jiné podsítě, nastavení zálohování nebylo opraveno a data se zapisovala na jiný stroj, který „zdědil“ IP adresu původního serveru



GREYCORTEX

MÁME NOVÉ PŘEHLEDNÉ REPORTY





GREYCORTEX

Doporučení a závěr

Co dál a jak se rozhodnout?

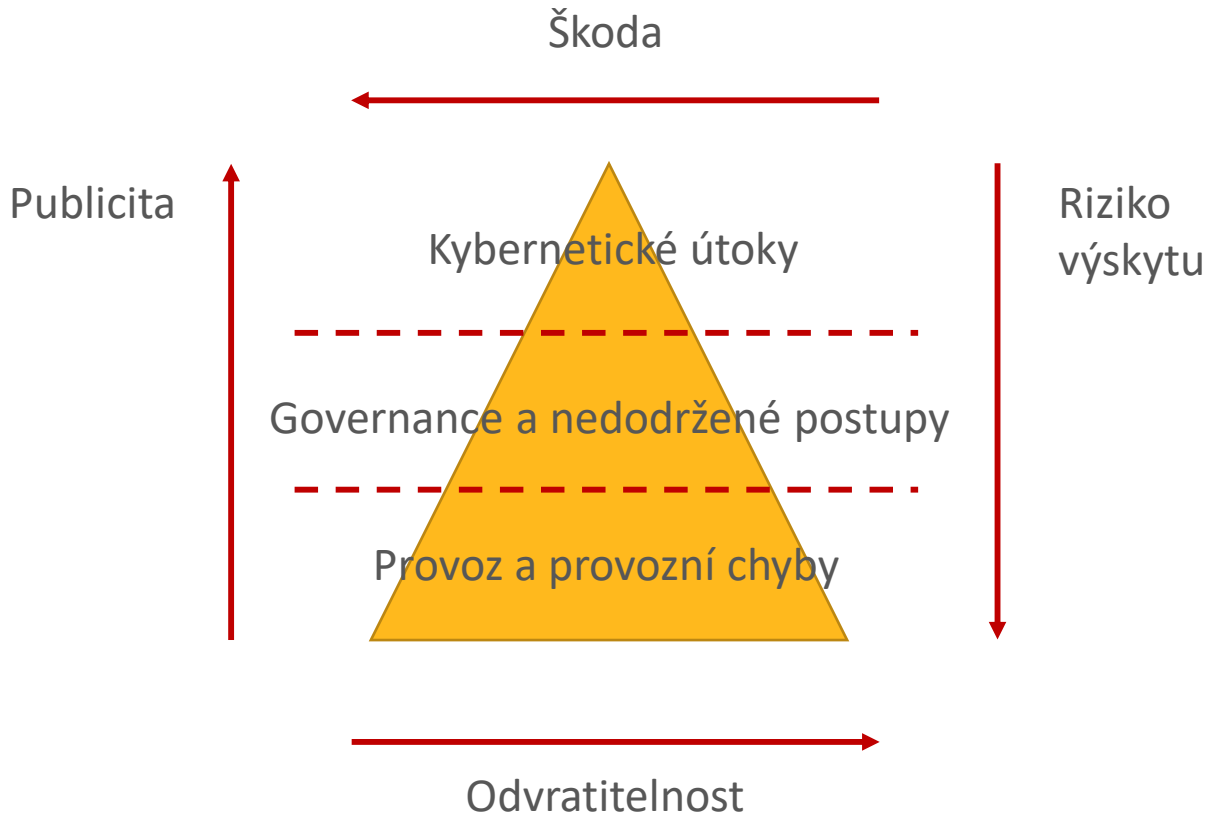
GREYCORTEX

CHRAŇTE SE

Zásady kalkulace škody a investic do ochrany:

- Nejde o to, *jestli* událost nastane,
  ale o to **kdy** k ní dojde a **jak velká** bude škoda
  (kolik bude činit ztráta a kolik bude stát náprava).
- Náklady ochranných opatření mají být **úměrné**
  velikosti škody a riziku výskytu události.
- Nelze vsadit na jediný druh ochrany,
  opatření je třeba **kombinovat**.
- Je třeba také trvale sledovat
  a ověřovat, jak daná opatření fungují.

(Shon Harris, CISSP study materials)



GREYCORTEX

PROVĚŘUJTE

Vladimír Sedláček
C|EH, Certified LiveWire Examiner, …
GREYCORTEX CTO
vladimir.sedlacek@greycortex.com

Co dál?

- Přijďte si pro více informací
- Vyzkoušejte nás
  - techniku a licenci zapůjčíme
  - nálezy vysvětlíme

Martin Senčák
Obchodný riaditeľ
+421 2/57275111
martin.sencak@beset.sk

Řadíme se ke světové špičce, ale domluvíte se s námi!

Děkuji za pozornost!

www.greycortex.com – další informace, příklady použití

info@greycortex.com – kontaktujte nás

www.youtube.com/greycortex – videa

GREYCORTEX