

# Ochrana nemocničných dát a správne zálohovanie

Ako sa pripraviť na zálohovanie v roku 2023

Jan Rys | IXPERTA

[www.ixperta.com](http://www.ixperta.com)



## Vytvárame IT riešenia na mieru



**30+  
rokov  
skúseností**



**250+  
zamestnancov**

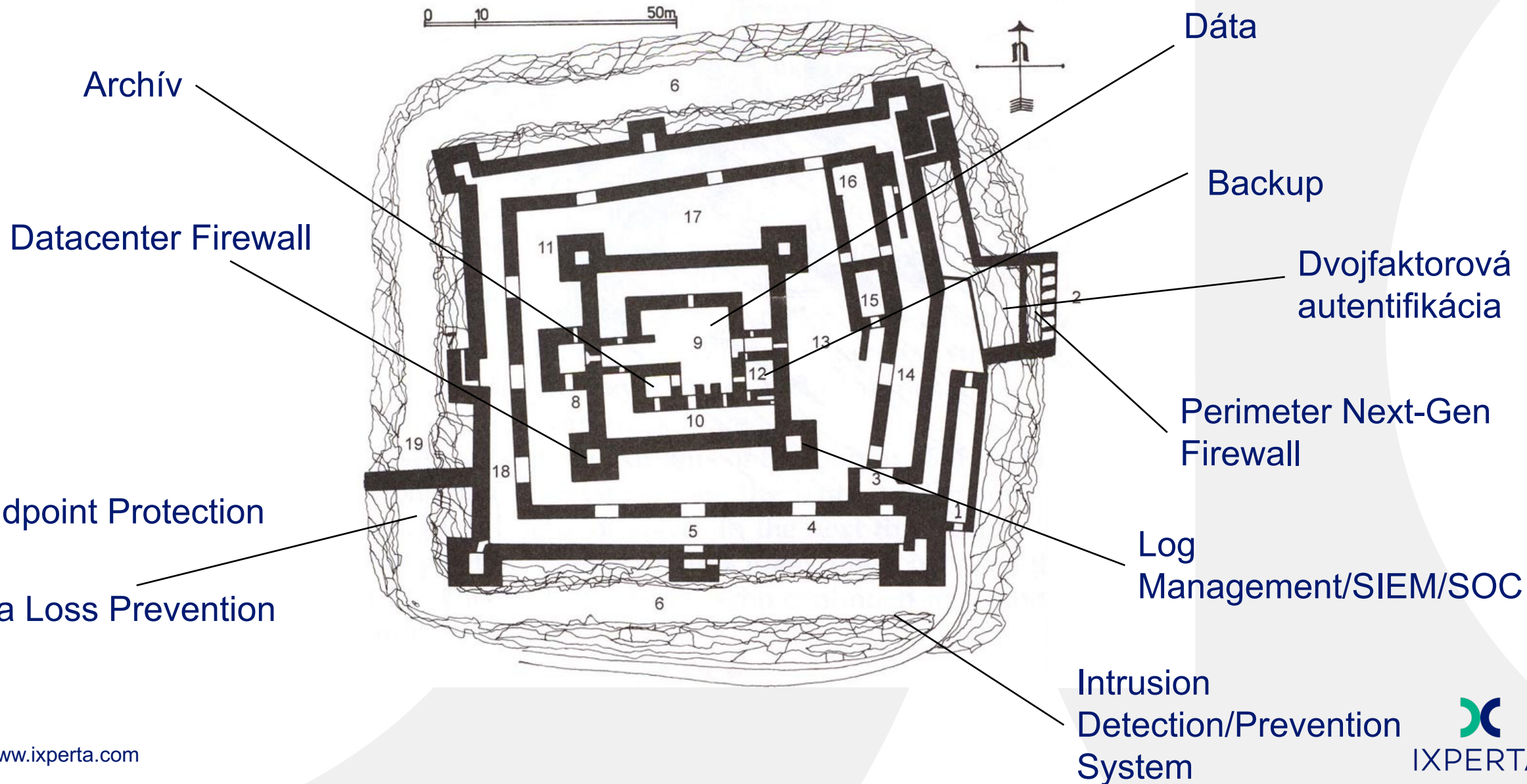


**6  
pobočiek v  
troch  
krajinách**



**lokálna  
spoločnosť**

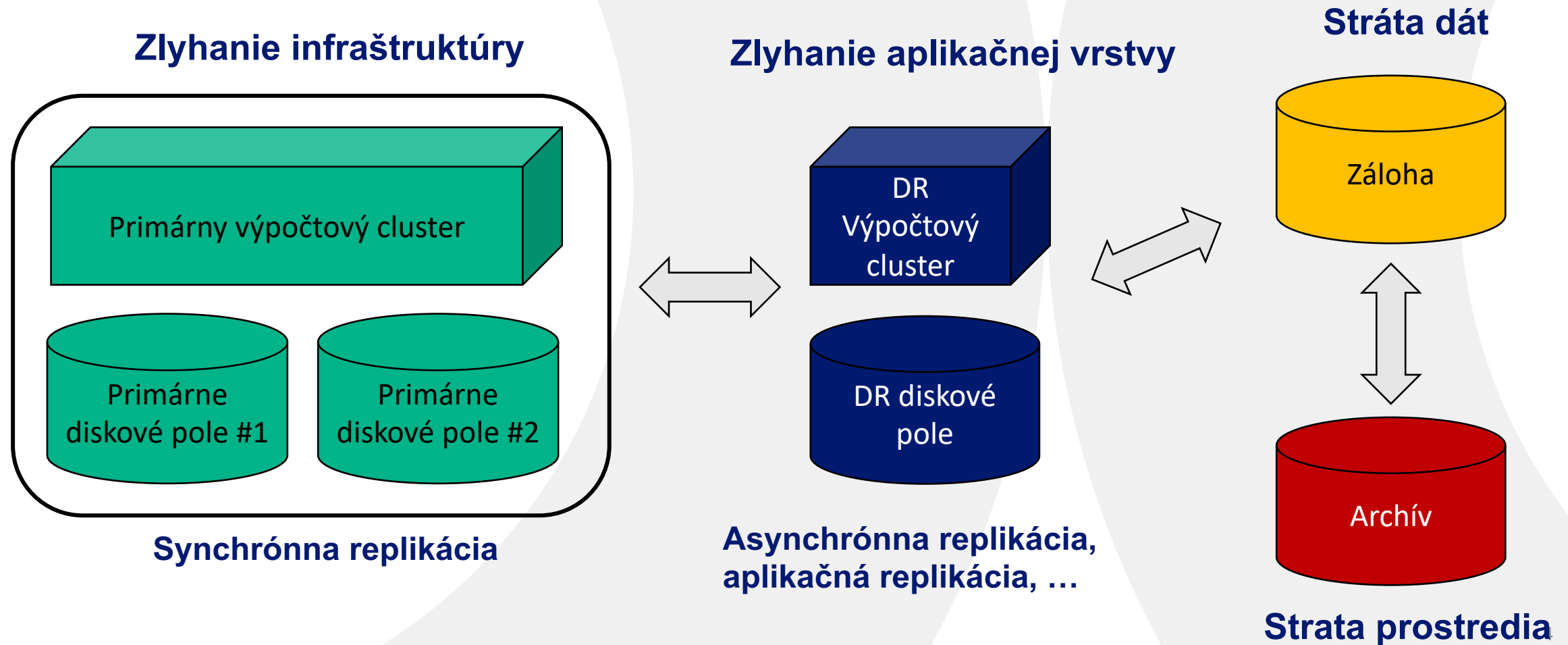
# Ako sa poučiť z histórie?



# Definícia východzieho stavu

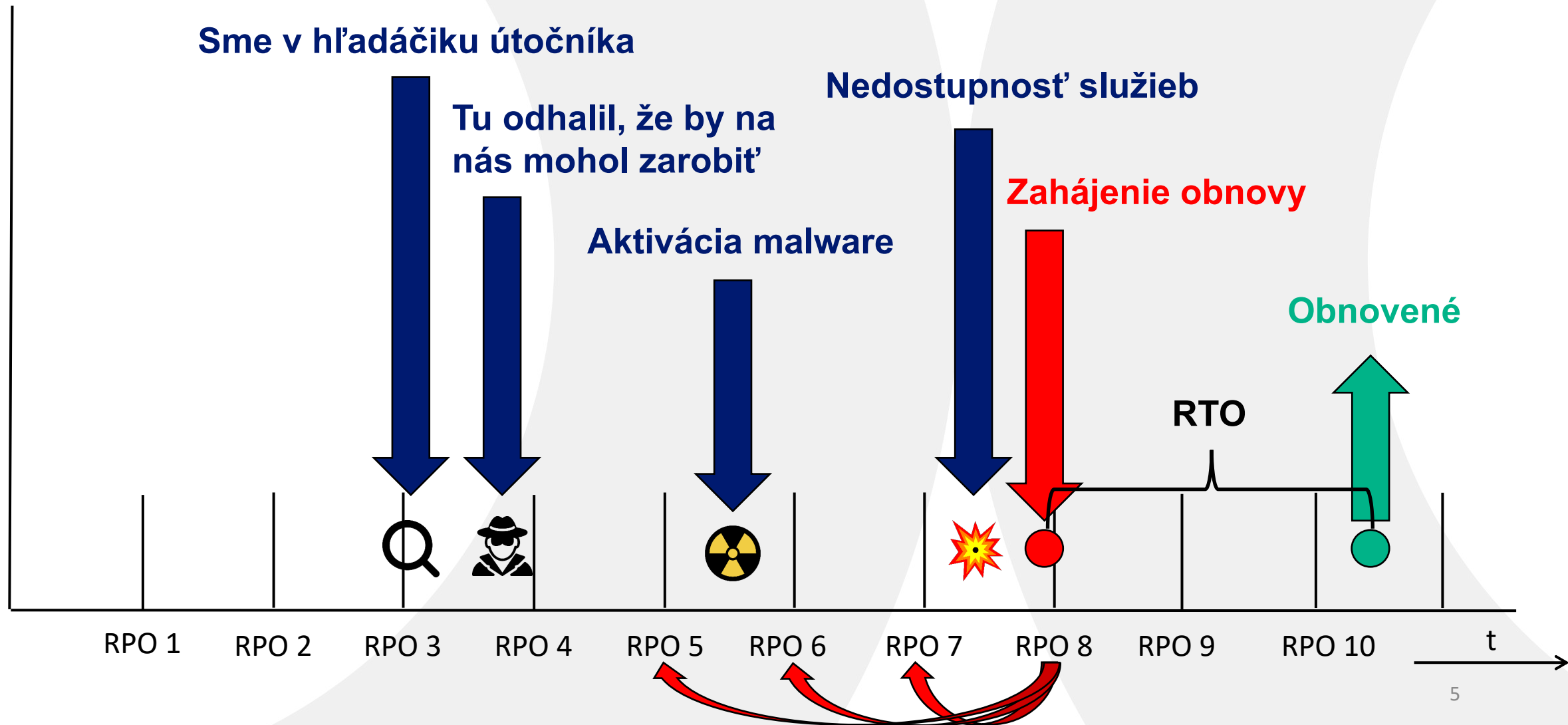
Technické riešenia v oblasti kybernetickej bezpečnosti sú protiopatrenia

Musíme si položiť otázku proti akému riziku dané protiopatrenia budujeme



# Anatómia zálohovania

## Respektíve anatómia obnovy



# Ako vieme, ktoré RPO je „zdravé“

Od kybernetickej bezpečnosti k aplikačnej konzistencii

## Dátová konzistencia ≠ Aplikačná konzistencia

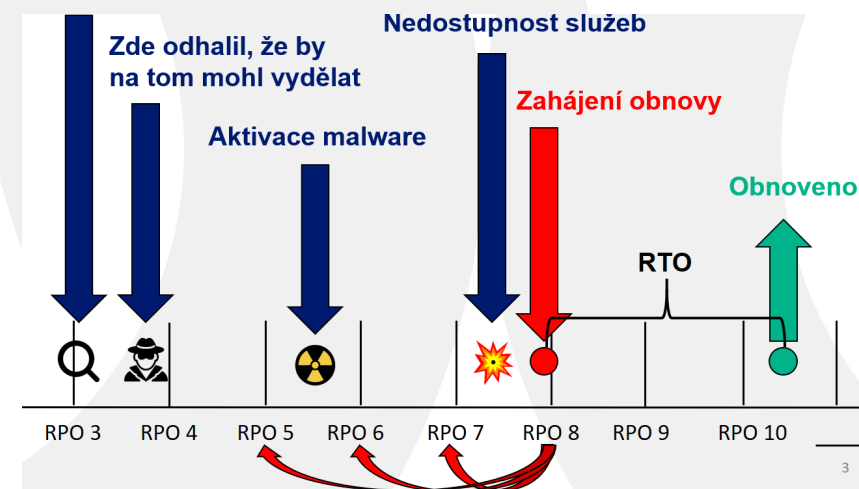
Dátová konzistencia je jednoducho overiteľná automatickými technickými prostriedkami. Aplikačnú konzistenciu je najvhodnejšie overiť pomocou cvičného obnovenia zo zálohy. Dátová konzistencia automaticky neznamená aplikačnú konzistenciu.

## APT nie je možné odhaliť pomocou AV kontroly súborov záloh

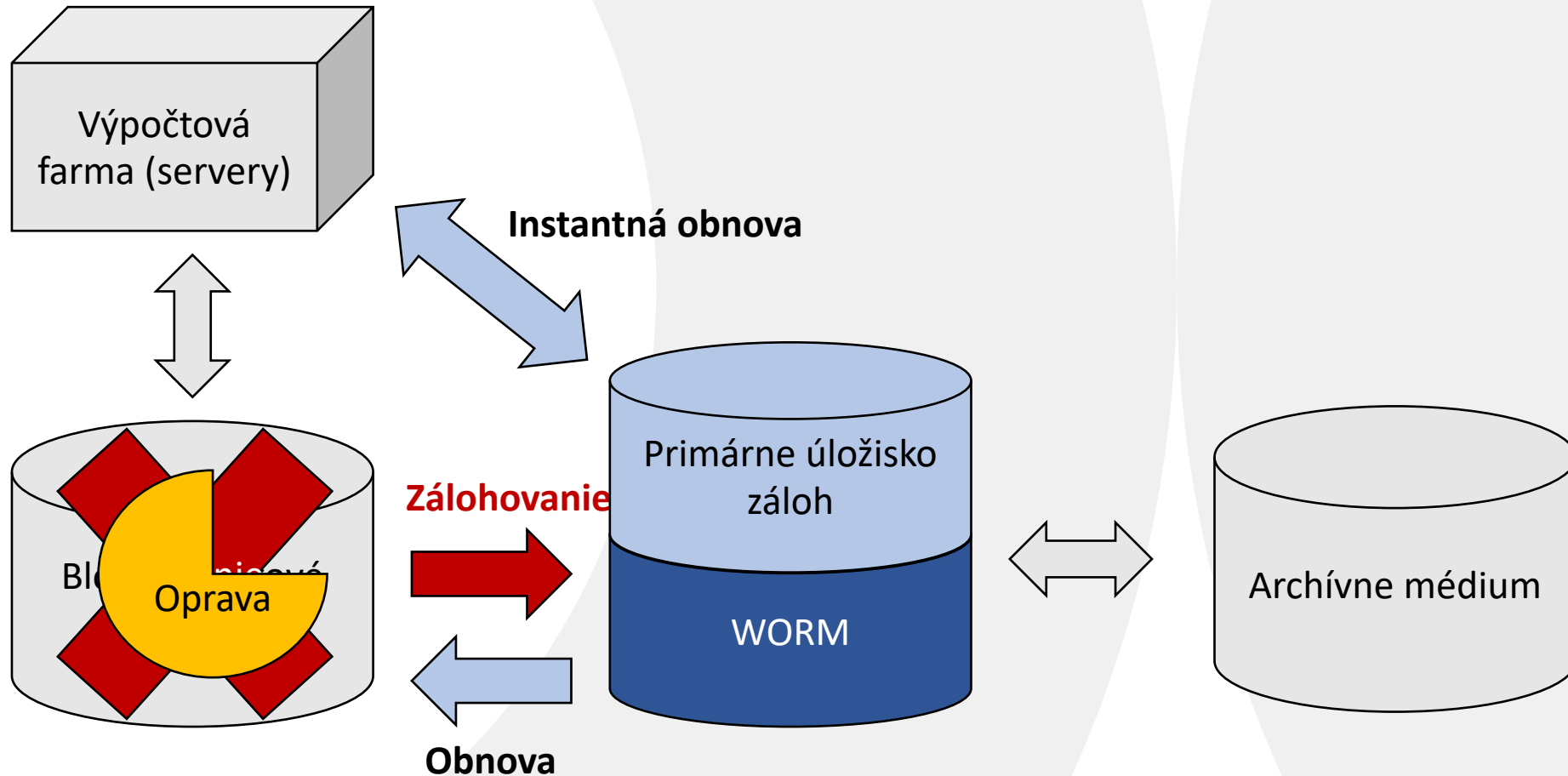
AV/EDR kontrola na bežiacich platformách je obvykle omedzená systémovými zdrojmi. APT nie je možné s istotou odhaliť len z dát a metadát záloh. Najlepšia cesta k odhaleniu APT je z bežiacej testovacej obnovy v sand-box prostredí.

## Primárne úložisko záloh môže plniť rolu DR úložiska

V prípade krízovej situácie je možné použiť výkon primárneho úložiska záloh a prostredí pre obnovu k zabezpečeniu funkcie DR prostredia.



# Nemeniteľné zálohy a instantná obnova



# Čo by ste mali očakávať od Vašej zálohovacej platformy?

## Záloha musí byť nemeniteľná

Tak aby sme mohli spoľahnúť, že jednotlivé RPO budú dostupné.

Pre záruku toho, že v zálohe bude to, čo očakávame, je nutné dodržať princíp troch A, kryptografia na zálohovacej ceste a uloženie dát do nemeniteľného snapshotu.

## Primárne úložisko záloh môže ponúknuť instantnú obnovu

Táto požiadavka je v rozpore s nemeniteľnosťou záloh. Tzn. musí ísť o separátnu kópiu dát. Reálne počítajme, že čistá kapacita primárneho úložiska záloh pre túto funkcionality je zhruba trikrát väčšia, ako pri tradičnom primárnom úložisku dát. Výkon úložiska musí byť akceptovateľný pre produkciu, napr. all-flash pole alebo scale-out.

## Riešenia musia byť integrovateľné

Ak chceme hľadať APT, tak nie je ekonomicky a časovo reálne testovať každé RPO ručne. Na testovanie je vhodné automatizovať niektoré testy a určiť vhodný pomer ručných a automatizovaných testov.

# Riešenie sa môže zdať technicky zložité

Máme riešenie pro korporáciu aj dynamickú firmu

## Chceme vybudovať on premise riešenie

Je nutné definovať požiadavky na RPO a RTO. Ak nemáme, nevadí. Pomôžeme Vám definovať vrátane katalógu služieb, analýzy rizík a definície vhodných protipatrení. Nasleduje investícia do technológií a ich integrácie. Aby riešenie naplnilo očakávanie, je potrebné nastaviť procesy pre zachovanie prevádzky a vykonanie obnov.

## Máme spoľahlivé produkčné prostredie, ale už nemáme priestor pre DR

Primárne prostredie je on-premise a zálohy sú v cloude poskytovateľa služby. Vy si môžete zvoliť služby, ktoré budeme na zálohách poskytovať: testovanie konzistencie, antivírusové testovanie, DR a pod. Alebo naopak - DR on premise a produkcia v cloude – rozhodnutie je na Vás.

## Ideme do cloudu

Technologické riešenia podľa potrieb. Pre každú inštanciu v našom cloude máme postavený separátny tenant, ktorý môže a nemusí používať centrálné služby. Každá služba sa vždy prispôsobuje požadovaným RPO, RTO.

## Úspešný príbeh



Nemocnica  
**Svätého Michala** a.s.

### Problém

- Sieťová vrstva bez vysokej dostupnosti
- Decentralizované úložisko dát – komplikované politiky zálohovania
- Minimálna ochrana perimetra
- Nesúlاد so ZoKB

### Cieľ

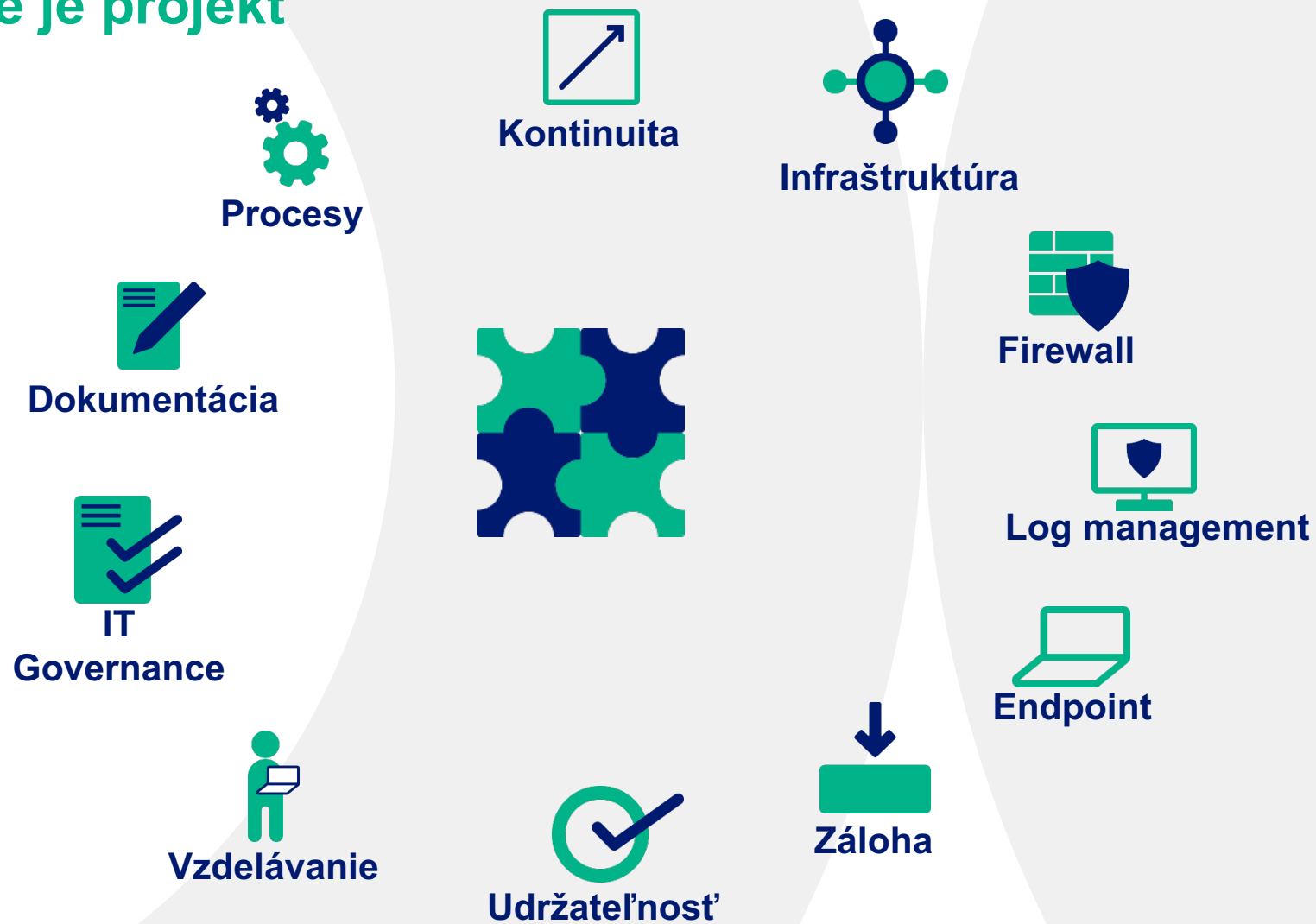
- Zvýšenie dostupnosti služieb
- Komplexná ochrana pred kybernetickými útokmi
- Nastavenie zálohovania, centralizácia dátových úložísk
- Postupné zvyšovanie súladu so ZoKB, reflektovanie zmien v súvislosti s NIS2



### Riešenie

- **Obnova centrálnych prepínačov, segmentácia siete**
- **Nasadenie Next-gen Firewallu na všetkých pobočkách**
- **Softvérovo definované úložisko, nastavenie zálohovacích politík**
- **Postupné odstraňovanie nálezov auditu**

## Bezpečnosť nie je projekt





**Ďakujem za pozornosť**

**Dovidenia na stretnutí  
Moderná nemocnica  
Hotel Jason, Vršatec  
7. – 8. decembra 2023**

**Jan Rys**  
**[jan.rys@ixperta.com](mailto:jan.rys@ixperta.com)**