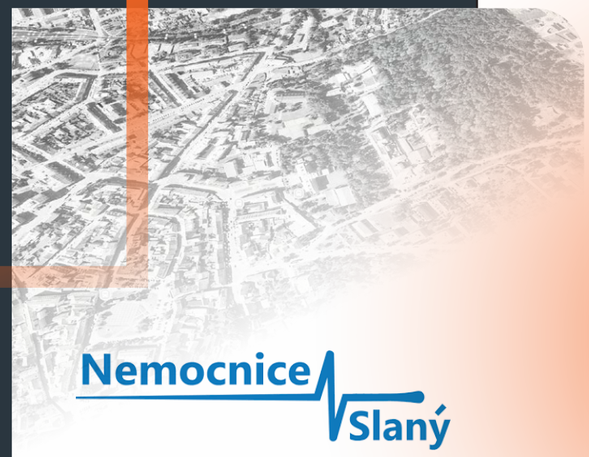
storage one

Případová studie
kybernetická bezpečnost v Nemocnici Slaný

storageone.cz

„Investice do kybernetické bezpečnosti ve zdravotnictví jsou dnes nutností, ne nadstandardem. Kybernetická bezpečnost má přímý dopad na ochranu citlivých dat pacientů i na plynulý provoz nemocnice.“

MUDr. Štěpán Votoček,
ředitel Nemocnice Slaný



Nemocnice Slaný

Zákazník

Nemocnice Slaný, založená v roce 1884, je klíčovým zdravotnickým zařízením Středočeského kraje. Disponuje 314 lůžky a pečuje o přibližně 100 000 obyvatel spádové oblasti. Nemocnice zaměstnává přibližně 400 pracovníků a poskytuje zdravotní péči v oborech chirurgie, gynekologie, interního lékařství a neonatologie. S ročním obratem v rozmezí 300 až 350 milionů Kč nemocnice kontinuálně investuje do modernizace a rozšiřování svých služeb. Nemocnice Slaný spojuje dlouholetou tradici s moderními technologiemi, což z ní činí nepostradatelnou součást místní zdravotnické infrastruktury. Rostoucí počet kybernetických hrozeb a stále vyšší nároky na dostupnost systémů však nemocnici postavily před důležitou otázku: jak zajistit, aby IT infrastruktura nebyla slabým článkem, ale naopak oporou celého provozu.

Výchozí stav

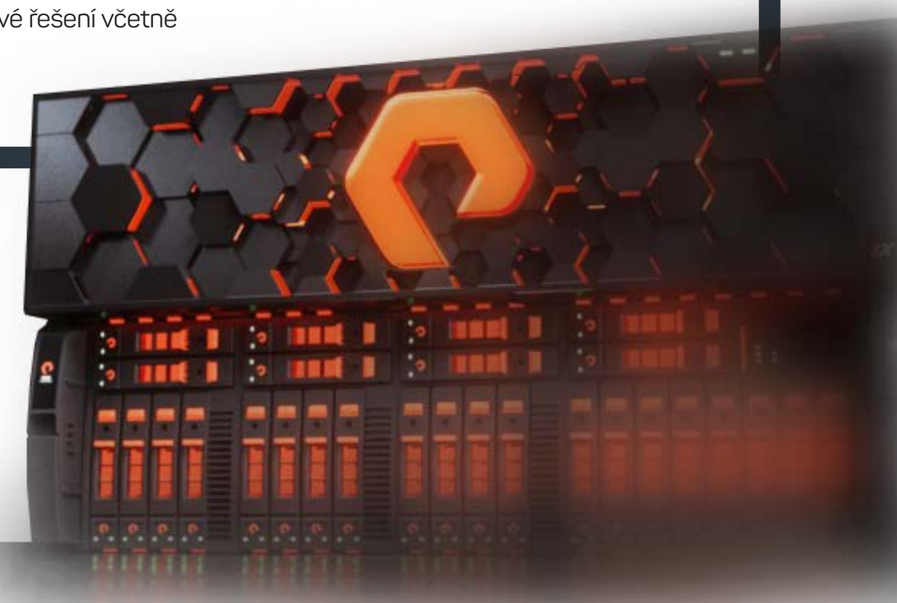
Nemocnice provozovala svou IT infrastrukturu na třech serverech Dell PowerEdge FC630 s virtualizační platformou VMware ESXi. Prostředí zahrnovalo 44 virtuálních serverů a přibližně 9 TB produkčních dat. Celý provoz byl tak závislý na jediném diskovém poli NetApp FAS2650, které představovalo zásadní Single Point of Failure. Výpadek diskového pole mohl znamenat zastavení klíčových systémů napříč celou nemocnicí. Současně chyběla moderní ochrana proti ransomwaru, immutable snapshoty, automatizovaná orchestrací disaster recovery, air-gap izolace záloh i plně redundantní síťová infrastruktura. V kontextu zdravotnictví šlo o rizika, která již nebylo možné dále přehlížet.

Rozhodnutí pro změnu

Nemocnice Slaný proto vypsala veřejnou zakázku na kompletní redesign IT infrastruktury. Cílem bylo odstranit kritická rizika, zajistit vysokou dostupnost dat, rychlou obnovu provozu a vybudovat prostředí odolné vůči kybernetickým hrozbám v souladu se zákonem o kybernetické bezpečnosti. Vítězem výběrového řízení se stal STORAGE ONE — systémový integrátor specializovaný na datovou infrastrukturu a kybernetickou bezpečnost.

Bod zlomu

Zvažovány byly dvě cesty – postupný upgrade současných komponent s nutností následné integrace jednotlivých dílčích částí řešení do jednoho funkčního celku, nebo komplexní projektová realizace v jednom kroku. Nemocnice se rozhodla pro druhou variantu - efektivní a systémové řešení včetně kompletní dokumentace, školení a akceptačních protokolů, a to v plánovaném čase, rozsahu i rozpočtu. Zásadní požadavky zákazníka: zajištění vysoké dostupnosti dat, minimalizace dopadů případného útoku a rychlá obnova provozu s maximální ochranou dat.



Řešení

Navrhli jsme a realizovali komplexní systémové řešení kombinující špičkový hardware Pure Storage, pokročilou ochranu dat Commvault a redundantní síťovou infrastrukturu HPE. Implementace probíhala ve dvou etapách během 12 měsíců.

Projekt realizoval více bezpečnostních technických opatření dle zákona o kybernetické bezpečnosti:

- **Ochrana před škodlivým kódem:** Implementace dvou diskových polí s možností vytvářet chráněné snapshoty dat, chráněné proti ransomware útokům. Využito je AI monitorování v sandbox prostředí.
- **Zajištění dostupnosti informací:** Disková pole propojena do redundantního metroclusteru s kruhovou síťovou topologií a arbitrací. Vysoká dostupnost je neustále sledována inteligentními systémy.
- **Zálohování a aplikační bezpečnost:** Pokročilý zálohovací systém zajišťuje minimální ztrátu dat (RPO) a rychlou obnovu (RTO). Obsahuje funkce jako Zero Trust přístup, air-gap a orchestraci obnovy.
- **Kryptografické zabezpečení:** Disková pole za provozu kryptují uložená data, čímž je omezena možnost exfiltrace dat nemocničních IS.

Odolnost a kontinuita provozu

Nové IT prostředí přineslo nemocnici výrazné posílení kybernetické odolnosti a provozní stability. Klíčové informační systémy – nemocniční, ekonomické, personální i laboratorní – dnes běží na infrastruktuře, která eliminuje Single Point of Failure a zajišťuje kontinuální provoz kritických systémů. Nemocnice Slaný tak získala moderní, bezpečné a škálovatelné IT prostředí, které splňuje současné legislativní požadavky a zároveň vytváří pevný základ pro další rozvoj digitálního zdravotnictví.

→ Ransomware ochrana

SafeMode + Commvault Threat Wise — immutable snapshoty s AI detekcí hrozeb v sandbox prostředí.

→ Nonstop dostupnost

ActiveCluster active-active — redundantní metrocluster s automatickým failoverem, 99.9999%.

→ Orchestrovaná DR

Automatické testování obnovy, validace záloh, Live Mount, Live Recovery a orchestrace DR.

→ Soulad s legislativou

Technická opatření dle zákona o kybernetické bezpečnosti a směrnice NIS2.

„Nové bezpečnostní prvky výrazně zvýšily naši odolnost vůči hrozbám, které mohou ovlivnit provoz nemocnice. Řešení naplnilo všechna očekávání."

Jakub Boček,
Vedoucí ICT, Nemocnice Slaný

Everpure™ formerly Pure Storage

Commvault®

Partnerství Pure Storage & Commvault v oblasti kybernetické odolnosti přináší unikátní kombinaci immutable úložiště s AI detekcí hrozeb ThreatWise a automatickou eskalací. Validovaný referenční design obou výrobců garantuje bezproblémovou integraci.

Shrnutí

Implementace

12 měsíců celkově
10 měsíců fyzická realizace
Celý projekt jsme zvládli za 10,5 pracovních dnů

Výsledky

99.9999% dostupnost dat
<1 ms latence úložiště
<15 min RTO Tier 0
0 RPO nulová ztráta dat

Využité produkty

Pure FlashArray //X20R4
Commvault Data Protection
HPE FlexFabric 5710