Případovka

AUTOCONT

# Bezpečnost informačních systémů nemocnice

## PROFIL ZÁKAZNÍKA

Psychiatrická nemocnice v Opavě je zdravotnické zařízení, jejímž zřizovatelem je Ministerstvo zdravotnictví ČR. Jde o nemocnici určenou pro diagnostiku a léčbu celého spektra duševních chorob včetně dětské psychiatrie.

Disponuje 863 lůžky, na kterých se ročně odléčí 6 500 pacientů. Nemocnice nabízí komplexní, vysoce odbornou psychiatrickou, psychologickou i sociálně-zdravotní péči. Provádí rovněž ochranné ústavní léčby, dále se podílí na vědecko-výzkumné činnosti, zabezpečuje doškolování vlastních pracovníků, provádí zdravotně výchovnou a osvětovou činnost.

PSYCHIATRICKÁ NEMOCNICE V OPAVĚ

## OBDOBÍ REALIZACE

Srpen - listopad 2019

*„Z důvodu dlouhodobé podfinancovanosti zdravotnictví, kdy prostředky z úhradové vyhlášky postačují pouze na provoz, a ne na rozvoj nemocnice, byli jsme i v oblasti úrovně ICT značně daleko za světem, a to i přesto, že jsme zpracovateli osobních a citlivých osobních údajů. Teprve výzva IROP 10 nám umožnila získat dostatečné finanční prostředky a dostat se, zavedením nových trendů práce s využitím moderních technologií a informačních systémů, v oblasti bezpečnosti IT do 21. století."*

Stanislav Taťoun, vedoucí oddělení ICT

## Výchozí situace a cíle projektu

Cílem rozsáhlého projektu, realizovaného v rámci Integrovaného regionálního operačního programu (IROP) bylo povýšení stávajícího IT prostředí na úroveň odpovídající aktuálním požadavkům legislativy, kybernetické bezpečnosti a zajišťujícího efektivitu zdravotnického personálu. Bylo nutno zvýšit odolnost informačních systémů proti kybernetickým hrozbám, sjednotit ověřování uživatelů a centralizovat jejich správu, dále zavést správu servisních požadavků včetně centrálního katalogu služeb a zabezpečit ukládání a řízení životního cyklu dokumentů. V neposlední řadě si projekt kladl za cíl modernizovat poštovní a komunikační služby.

K zajištění výše uvedených cílů bylo zapotřebí vybudovat moderní a výkonné datové centrum, odolné proti výpadkům, zajišťující infrastrukturu pro nové i stávající informační systémy na dalších minimálně 5 let.

## PŘÍNOSY

- Uživatelské přístupy a oprávnění pod kontrolou
- Efektivní a bezpečný přístup ke zdravotní dokumentaci
- Rychlejší přihlašování pomocí bezkontaktních karet
- Virtuální pracovní plocha následuje uživatele (Follow Me Desktop)
- Řízení oběhu dokumentů včetně silného šifrování
- Snadná úprava workflow při změnách interních procesů
- Bezvýpadkový provoz informačních systémů díky virtualizaci
- Tenký klient redukuje náročnost správy koncových zařízení na minimum
- Centrální sběr logů SIEM monitoruje a spravuje bezpečnostní události
- Dohledová služba SOC přináší prevenci ochrany proti útokům
- Rychlá reakce IT na změny požadované uživateli
- Uvolnění rukou internímu IT, větší prostor věnovat se správě klíčových systémů

# Popis řešení

Realizací tohoto projektu došlo k rozšíření technologické infrastruktury, prostředků pro bezpečnou komunikaci, sdílení dokumentů, možnosti základní manažerské kontroly hospodaření pomocí společného datového skladu, prvků pro elektronické zpracování interních procesů a zvýšení komfortu uživatelů informačních systémů a zvýšení bezpečnosti prostředí v souvislosti s naplněním požadavků zákona a vyhlášky o kybernetické bezpečnosti.

Pro zajištění odolnosti systémů nemocnice vůči kybernetickým útokům, kyberkriminalitě a možným ztrátám z toho plynoucích, bylo nutné povýšit jak organizační, tak i procesní a technickou odolnost.

Realizace projektu zahrnovala tyto oblasti:

- Řízení uživatelských identit (IdM)
- Dvoufaktorové (dvoufázové) ověřování uživatelů a Single Sign-On (SSO)
- Monitorování privilegovaných účtů (PAM)
- Správa servisních požadavků (ServiceDesk, Asset Management)
- Správa bezpečnostních informací a událostí (SIEM)
- Řízení oběhu dokumentů vč. silného šifrování (DMS)
- Zabezpečení přístupu k síti dle standardu 802.1x
- Aplikační bezpečnost a vysoká dostupnosti infrastruktury
- Centralizace komunikačních kanálů (e-mail, IM, videokonference)

Velký důraz byl kladen na špičkové zabezpečení jak samotné infrastruktury (firewally, sondy), tak i na aplikační bezpečnosti (web application firewally, analyzery) tak, aby se zabránilo krádežím citlivých či jinak zajímavých údajů, případně způsobení nedostupnosti provozovaných aplikací.

Kvalita zabezpečení byla několikrát testována penetračními testy prováděné externím dodavatelem.

Při realizaci projektu byly použity technologie partnerů Alvao, AT&T Cybersecurity, Citrix, Fortinet, Hewlett Packard Enterprise, Imprivata, Microsoft, ObserveIT, StarWind, Veeam, VMware.

Společnost AUTOCONT a.s. doplnila dodané produkty a technologie o další služby, nezbytné pro zajištění provozu celého systému po dobu pětileté udržitelnosti, jako jsou:

- Vzdálený dohled a vzdálená údržba
- Bezpečnostní dohled (SOC)
- Vzdělávání administrátorů