

Krajská nemocnice

Case Study



Krajská nemocnice je jednou z největších soukromých nemocnic v České republice. Poskytuje péči v oblasti onkologie, chirurgie a mnoha dalších, nabízí svým klientům i rehabilitační služby. Nemocnice zaměstnává **téměř 1000 zaměstnanců**. **IT tým nemocnice má pouze tři členy**, přestože je její struktura složitá a rozsáhlá. Počítačová síť využívá řady běžných řešení pro zabezpečení sítě, včetně zabezpečení koncových zařízení, firewallů a má kvalitně členěnou strukturu sítě, včetně veřejné Wi-Fi pro pacienty, interního administrativního segmentu, segmentu pro VOIP a havarijní dispečink, interního segmentu zdravotnických dat a další.

„MENDEL nás opravdu příjemně překvapil. Využili jsme nabídku nasazení 30denní bezplatné verze a po jejím uplynutí jsme se rozhodli jej pořídit. MENDEL umožnil našemu týmu vyřešit obrovské množství problémů, a to okamžitě, bez nákladného a zdlouhavého hledání nových členů týmu.“ (CIO)

Výzvy a požadavky

Přestože byla síť dobře segmentovaná, čelili její správci několika zásadním potenciálním i existujícím hrozbám či problémům. IT týmu chyběla dostatečná viditelnost do sítě, nebyl schopen odhalit všechna zařízení přihlášená v síti, což vedlo k několika vzácným, ale přesto znepokojujícím bezpečnostním incidentům. Ačkoli tyto výsledky nevedly přímo ke ztrátě dat, byly samy o sobě alarmující. Síť navíc čelila chronickým potížím s výkonem. IT tým postrádal dostatek času a zdrojů pro řešení všech výše uvedených problémů.

Nemocnice hledala bezpečnostní řešení pro monitorování sítě - hlavním cílem bylo zajistit plnou funkčnost všech bezpečnostních nástrojů v síti, plnou viditelnost sítě, sledování a monitorování výkonu a zabezpečení důvěrných údajů o pacientech.

Výsledky

MENDEL poskytuje zabezpečení, viditelnost a reaguje na výzvy vyplývající z běžných požadavků lékařské praxe. IT tým zvládá díky MENDEL v původním složení starost o zabezpečení a plnou funkčnost sítě. Jako přidaná hodnota slouží schopnost organizace být v souladu se zákony a směrnicemi pro ochranu osobních dat (GDPR).

Výzvy:

- Omezená viditelnost zařízení a komunikace v síti
- Bezpečnostní incidenty hrozící ztrátou nebo ohrožením dat, byť vzácné
- Starší modely firewallů neposkytující dostatečné zabezpečení
- Nedostatek času, zdrojů a nástrojů pro zjišťování bezpečnostních incidentů
- Chronické problémy s výkonem sítě

Výsledky:

- Firma používá licenci s hardware MENDEL All-in-One
- MENDEL ve zkušebním provozu detekoval několik událostí ohrožujících bezpečnost veřejné i interní sítě
- Dalším potenciálně nebezpečným událostem se daří předcházet včasnou detekcí
- Podařilo se odhalit a odstranit původce problémů s výkonem
- MENDEL pokryl bezpečnostní mezeru dodatečnou integrací se stávajícími firewally
- Byla odhalena a následně upravena řada konfigurací, které zvyšovaly bezpečnostní riziko