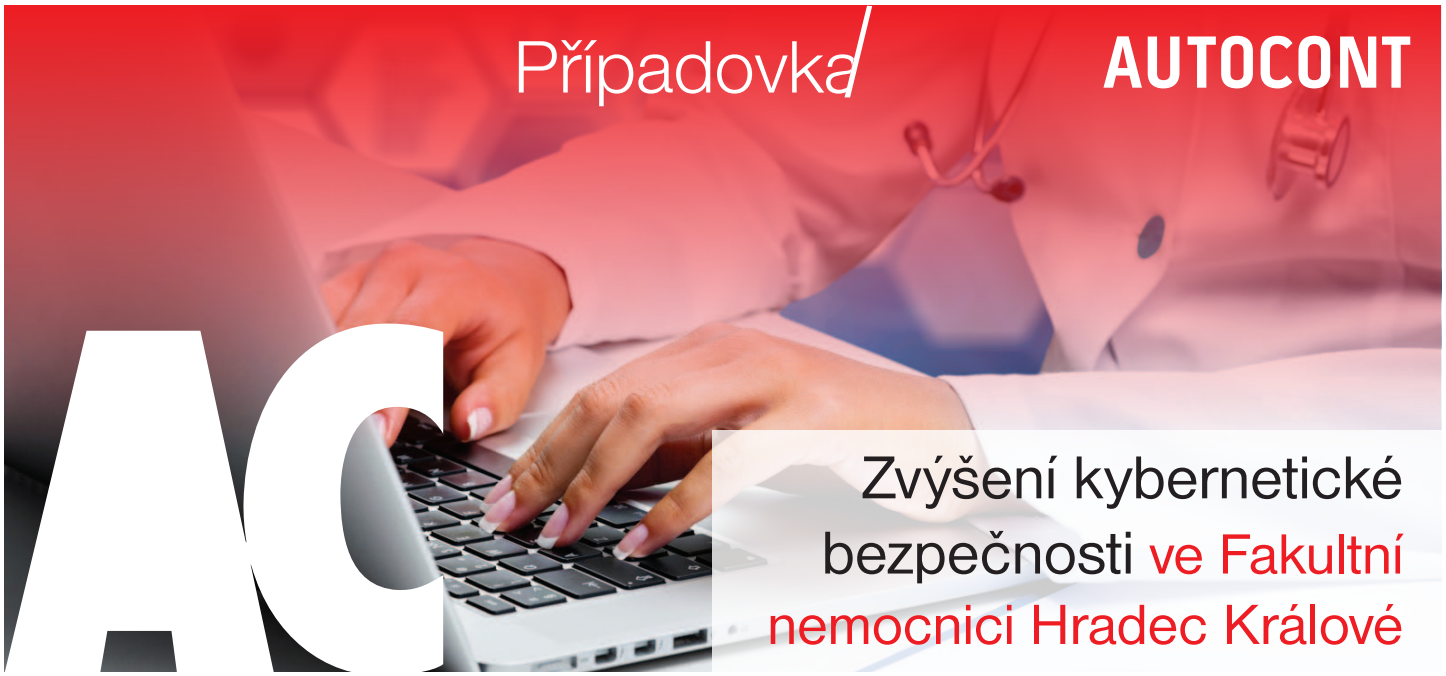

Případovka

AUTOCONT

Zvýšení kybernetické bezpečnosti ve Fakultní nemocnici Hradec Králové

PROFIL ZÁKAZNÍKA

Největší nemocnice Královéhradeckého kraje, ale i patřící k největším nemocnicím v ČR, jejímž zřizovatelem je Ministerstvo zdravotnictví. Jako fakultní nemocnice se podílí na výuce studentů Lékařské fakulty UK v Hradci Králové. Nemocnice se 4 500 pracovníky, disponuje téměř 1 400 lůžky a každoročně se postará přibližně o 40 000 pacientů. Vzhledem k řadě vysoce specializovaných pracovišť zajišťuje zdravotní péči pro obyvatele nejen Hradce Králové a příslušného kraje, ale v některých případech také dalších regionů republiky.

OBDOBÍ REALIZACE

04/2019 - 10/2019

„Naše fakultní nemocnice provozuje mnoho infrastrukturních systémů a množství aplikací uchovávající citlivá data. Dlouhodobě nám chyběl nástroj, který by plnil funkci centrálního úložiště auditních záznamů o provozu a zároveň v reálném čase vyhodnocoval kybernetické bezpečnostní události a incidenty. Problém totiž není v úrovni zajištění samotných auditních dat, ale ve schopnosti je vyhodnotit v kontextu aktuálních kybernetických hrozeb. S přispěním výzvy integrovaného regionálního operačního programu, jsme si mohli dovolit pořídit jeden z nejúčinnějších SIEM nástrojů na komerčním trhu."

Ing. Miroslav Procházka, vedoucí oddělení IT FN HK

Výchozí situace a cíle projektu

Fakultní nemocnice Hradec Králové investuje nemalé prostředky do své výpočetní infrastruktury, a to včetně oblasti navýšení zabezpečení proti kybernetickým hrozbám. Doposud jí však chyběl centrální integrující prvek pro všechny technologie zaměřený právě na bezpečnost.

Řešení typu SIEM umožní podstatným způsobem zvýšit kybernetickou bezpečnost ve smyslu včasného odhalení závadného chování v systémech nebo v počítačové síti. SIEM v reálném čase vyhodnocuje data z celé ITC infrastruktury a včas rozpozná bezpečnostní hrozby. Umožní aktivně testovat zranitelnosti v infrastruktuře, buduje reputační databázi a zajišťuje funkci auditního úložiště logů a síťových toků.

PŘÍNOSY

- Významné a trvalé posílení v oblasti informovanosti, evidenci a řízení bezpečnostních rizik
- Zpracování a vizualizace bezpečnostních událostí v reálném čase
- Vybudování auditního úložiště logů s dlouhou retencí
- Nastavení správného bezpečnostního logování pro klíčové zdravotnické aplikace
- Nasazení skeneru zranitelností, integrovaného v SIEM řešení
- Plnění požadavků legislativy na kybernetickou bezpečnost pro provozovatele základní služby
- Zaškolení zaměstnanců pro identifikaci a zvládání kybernetických rizik
- Trvalá podpora v oblasti bezpečnosti po celou dobu udržitelnosti projektu

POUŽITÉ TECHNOLOGIE

IBM QRadar SIEM

Fakultní nemocnice Hradec Králové v minulosti nedisponovala žádným podobným systémem. V omezené míře se využívaly nástroje výrobců jednotlivých systémů. Cílem tedy bylo zaměřit se na tuto oblast a nasadit nástroj, kterým se problematika bezpečnosti dala řídit z jednoho místa. Rozhodování urychlila i možnost využít spolufinancování z dotačních prostředků EU, v rámci výzvy integrovaného regionálního operačního programu (výzva č. 10).

Zájem byl o nasazení řešení ve schématu vysoké dostupnosti, s průchodností v řádech několika tisíců záznamů za sekundu, aktivním skenerem zranitelností a auditním úložištěm s retencí až 18 měsíců, pro vybrané systémy.

Popis řešení

Společnost AUTOCONT a.s. dodala bezpečnostní řešení SIEM založené na produktu IBM QRadar, a to včetně jeho následné podpory. Systém SIEM byl dodán jako dvojice zařízení, zapojených ve schématu vysoké dostupnosti se synchronizovanými úložišti. SIEM má propustnost několik tisíc auditních logových záznamů (též. EPS), licence pro zpracování síťových Flow a též licence pro scanner zranitelností. Do QRadar SIEM je napojeno na 500 zdrojů událostí. Systém spolehlivě prověří více než 200 milionů událostí za den.

Pověření a zaškolení pracovníci mají nyní okamžitý přehled o bezpečnostní situaci v kyberprostoru nemocnice a díky integraci na IBM reputační databázi (X-Force) i o vnějších hrozbách. Ty zařízení QRadar rozpoznává právě na základě provázání s externí reputační databází.

Součástí Projektu byla dodávka technologických komponent, analýza, projekt nasazení, instalace, implementace, parametrizace, testy výkonu a funkcí v podobě simulace kybernetických útoků, školení, dokumentace a následná servisní a metodická podpora.

Kromě QRadar SIEM a Vulnerability Manager je možné za příplatek získat další funkcionality v podobě modulů QRadar Risk Manager, Network traffic capture nebo Incident Forensics modul. Tyto moduly poskytují funkcionality zaměřené na pokročilou analýzu sledování vektoru útoků nebo modelování, ve stylu „what-if“ analýz při plánování změn v síťové infrastruktuře nebo její konfiguraci.