LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Případová studie - LOGmanager pro Město Karviná

O zákazníkovi

Karviná je statutární město v Moravskoslezském kraji. Nachází se na území historického Těšínského Slezska, 18 km východně od Ostravy na řece Olši. Žije zde přibližně 54 tisíc obyvatel s významnou slovenskou a polskou menšinou. Je universitním, turistickým, lázeňským a ekonomickým centrem východního Ostravska se spádovou oblastí s více jak 200 000 obyvateli.

Původní stav

V Karviné má IT oddělení magistrátu ve své správě řadu technologií od různých výrobců: Informační systém městského úřadu je tvořen více dílčími provozně ekonomickými a technologickými systémy a aplikacemi s různou mírou vzájemné provázanosti. Mezi tyto systémy patří například spisová služba, ekonomický systém, personální a mzdový systém, mapové aplikace…

Dále je město Karviná zřizovatelem řady organizací, které provozují další, často velmi různorodé systémy. Každý ze systémů magistrátu generuje velké množství důležitých informací (logů) o své činnosti, o svém stavu a o činnosti jejich uživatelů. Jeden každý systém přitom ukládá logy jiným způsobem, v jiném formátu a na různou dobu. V případě výskytu problému by roztříštěnost ukládání logů znamenala velmi složitou identifikaci a také by se tím významně prodloužila doba nutná k jeho vyřešení.

Záměr projektu

Cílem projektu bylo sjednocení ukládání logů na externím zabezpečeném systému, který nebude umožňovat jejich mazání: ať již pracovníky magistrátu, jejich dodavateli nebo případnými útočníky. Pracovníci IT oddělení magistrátu by získali komplexní přehled, co se v jeho infrastruktuře děje. Ve většině provozovaných aplikací jsou uložena osobní data občanů, zaměstnanců magistrátu atd. Od května roku 2018 navíc platí evropská regulace GDPR, kdy každý správce osobních údajů musí na požádání (a pod značnými pokutami) prokázat, kdo přistupoval k osobním údajům, která má ve svých systémech a co s nimi dělal. Toto samozřejmě systém LOGmanager splňuje.

Výběr řešení

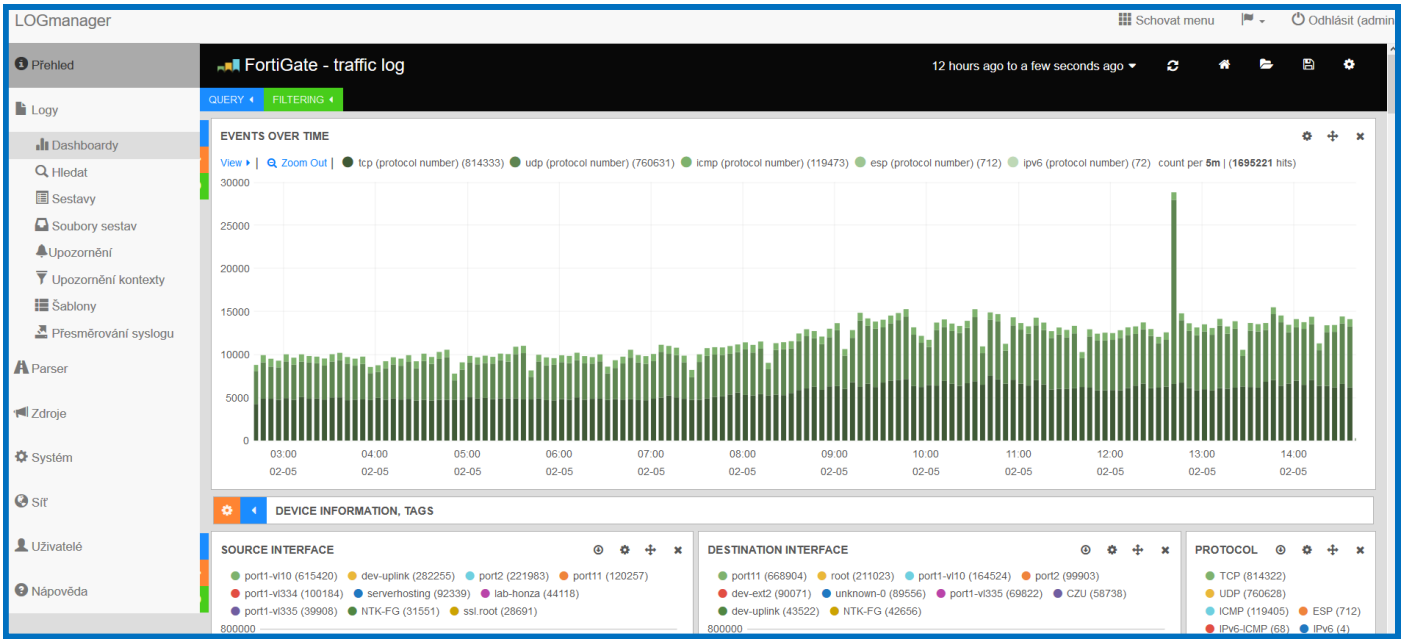
Výše popsané bylo třeba vyřešit nejen pro IT systémy magistrátu, ale i pro Městskou policii, základní a mateřské školy a další příspěvkové organizace města. Proto byly součástí projektu i LOGmanager Forwardery, které umožnují zabezpečený (zašifrovaný) přenos dat i po pomalých, zarušených nebo nestabilních linkách, procházejí i přes (vícenásobný) NAT a případně řeší i překrývající se IP adresní rozsahy u jednotlivých organizací. Zákazníka oslovily i další vlastnosti a výhody LOGmanageru:

- centrální úložiště logů s rychlým vyhledáváním, dlouhodobým uložením a pokročilými funkcemi typu alerty, korelace, tresholdy, reporty;
- jednoduchost ovládání, rychlost nasazení, český produkt v českém jazyce, skvělá dokumentace;
- nemožnost smazat logy;
- sběr logů z podřízených organizací;
- možnost jemného nastavení přístupových práv k datům, a to jak po funkčních celcích (např. pouze k Windows serverům u všech organizací) anebo po jednotlivých organizacích (správce sítě v jedné škole vidí jen svoje data).

PŘÍNOS PRO ZÁKAZNÍKA A OCEŇOVANÉ VLASTNOSTI

Po nasazení LOGmanageru jsou události sbírány z 50 virtuálních serverů, dvou VMware datacenter, databáze Oracle, firewallu a virtuálního kontroleru. Celá integrace a konfigurace systému pro centralizovaný sběr a analýzu událostí byla hotová velmi brzy.

LOGmanager svým sjednocením ukládání logů a jejich zabezpečením dokonale splnil očekávání zadavatele. Díky systému upozorňování jsou IT pracovníci magistrátu včas informováni o kritických událostech. Vyřešil zároveň i legislativní regulace v podobě GDPR. Zákazník také oceňuje jednoduchost upgradu systému, analytické možnosti a přístup k webinářům, které obsahují informace o změnách a novinkách i spoustu dalších technických informací od tvůrců LOGmanageru .



INFORMACE O VÝROBCI A DALŠÍ REFERENCE

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Do vydání tohoto referenčního listu nalezl LOGmanager více jak 140 spokojených zákazníků a na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější reference přímo z oblasti Vaší činnosti nás neváhejte poptat. Certifikovaným partnerem realizujícím tento projekt byla firma AUTOCONT a.s..