LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Případová studie Telco Pro Services a.s., člen skupiny ČEZ

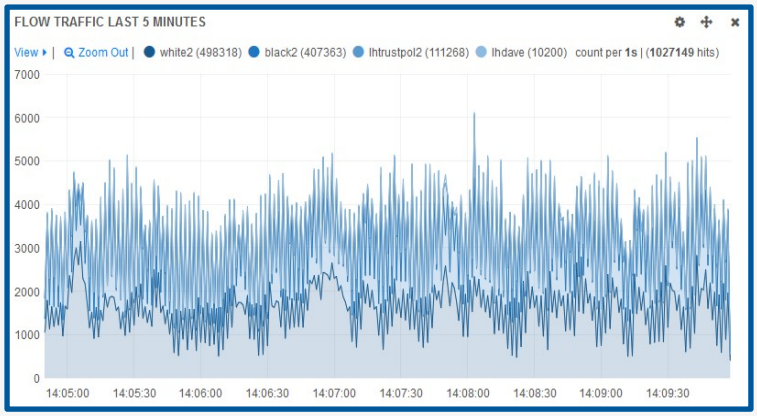
O zákazníkovi

Společnost Telco Pro Services, a. s., člen Skupiny ČEZ, je telekomunikačním operátorem působícím na českém telekomunikačním trhu, jehož podnikatelská činnost je zaměřena na poskytování telekomunikačních služeb zákazníkům s převažujícím podílem dodávky společnostem ze Skupiny ČEZ. Produktové portfolio zahrnuje jak služby veřejných elektronických komunikací, tak i služby zákaznicky orientované, postavené dle individuálních požadavků zákazníků. Společnost vlastní a provozuje rozsáhlé telekomunikační systémy vytvářející technickou základnu pro široké spektrum hlasových a datových služeb. Podstatný podíl tvoří telekomunikace přizpůsobené zákazníkům ze sektoru energetiky, využívané mimo jiné pro průmyslové systémy sloužících pro podporu dispečerského řízení výroby a distribuce elektrické energie.

Co zákazník řeší a proč?

Společnost Telco Pro Services, a. s., je telekomunikační operátor disponující rozsáhlou infrastrukturou, jak na bázi klasických TDM přenosových a hlasových systémů (PDH/SDH, síť digitálních ústředen včetně tranzitních), tak i moderních datových sítí na platformě univerzálních multiservisních architektur (MPLS). Převážně poskytuje následující služby:

- Veřejně dostupné služby elektronických komunikací
- Datové a hlasové služby v podnikových sítích
- Datové komunikace pro ovládání řídicích systémů
- Pronájem datových okruhů, služby pro operátory a ISP
- Správa technologií (v majetku) zákazníků



LOGmanager byl primárně vybrán pro zajištění povinností plynoucích ze zákona 181/2014Sb a slouží jako podpůrné aktivum prvků infrastruktury provozovaných společnostní. Provozní události, které jsou jednotlivými systémy zasílány na LOGmanager, jsou v něm uchovávány v podobě provozních záznamů a zároveň systém přijatá data dále poskytuje do prostředí korporátního SIEM řešení. Tím je zajištěno technicky předání provozních záznamů pro vyhodnocování kybernetických bezpečnostních událostí a incidentů.

Implementace LOGmanageru v prostředí Telco Pro Services a.s.

Rychlost implementace a univerzálnost systému LOGmanager pro použití nezávisle na infrastrukturních zdrojích, ze kterých jsou data zasílána, umožnila rychlý rozvoj a rozšíření záběru řešení napříč celou heterogenní infrastrukturou. Zákazník poskytnuté řešení dlouhodobě testoval, takže vzhledem k pozitivním zkušenostem s provozem systému a jeho schopnosti s daty pracovat na úrovni intuitivního grafického rozhraní, bylo řešení plošně nasazeno na veškerou provozovanou infrastrukturu. Pokrývá tak nyní plně potřeby sběru provozních událostí z telekomunikačních, bezpečnostních i podpůrných systémů. Jednoduše konstruovanou logikou pravidel byl zákazník schopen zajistit pro jednotlivé technologie samostatně definované struktury událostí s definovanými pravidly, které umožňují sledovat a notifikovat relevantní události, kterým je z provozního pohledu nutno věnovat pozornost.

V současné době je systém rutinně využíván provozními pracovníky a správci jednotlivých technologií, pro které byla připravena pravidla pro záchyt vybraných událostí, vlastní dashboardy a notifikační služba v závislosti na jejich požadavcích. Díky výkonu řešení je snadné vyhledávat v historických datech informace o prvních výskytech událostí, dohledat související informace z ostatní infrastruktury, hledat souvislosti. Jednotlivé týmy využívají své vlastní prostředí např. v oblasti správy firewall, monitoring konfiguračních změn prováděných na telekomunikačních zařízeních, podpora monitoringu a stavů HW platforem serverů, AAA infrastruktury a dalších.

PŘÍNOS PRO ZÁKAZNÍKA A OCEŇOVANÉ VLASTNOSTI

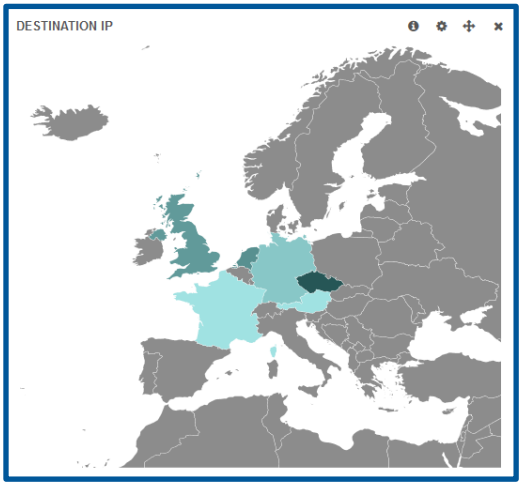
Systém splnil požadavek na zajištění tzv. forenzního skladu dat, kde jsou data s dostatečnou retencí uchována pro potřeby případného zpětného vyšetření událostí, případně zajištění důkazů v rámci vyšetřování kybernetických událostí a incidentů. Díky schopnosti řešení zajistit integritu a důvěrnosti dat je LOGmanager využíván jako důvěryhodný zdroj informací pro důkazní řízení.

Systém LOGmanager je provozován jako sdílený podpůrný systém pro celky infrastruktury a další provozní prostředí. Z důvodu operativního nasazení v reakci na povinnosti plynoucí ze zákona 181/2014Sb, byl systém vybudován s ohledem na svou schopnost zajistit plnou funkcionalitu sběru logů provozních událostí bez licenčního omezení, na výkon, srozumitelnost prostředí a rychlost nasazení. Zajištění spolehlivého prostředí pro sběr provozních událostí jednotlivých technologii KII a dalších provozovaných komunikačních systémů společnosti. Zajištění jednotného místa příjmu a předání informací o provozních událostech s dostatečnou kapacitou, výkonem a spolehlivostí.

LOGmanager se jako řešení v Telco Pro Services a.s. osvědčil natolik, že jsou v současné době realizovány projekty na rozvoj a rozšíření infrastruktury LOGmanageru o záložní systémy a další menší separátní dedikované instalace pro izolované části komunikační infrastruktury.

Zákazník oceňuje nejvíce následující vlastnosti

- ⇒ Diagnostika pádů nebo provozních problémů jednotlivých aplikací
- ⇒ Predikce a předcházení vzniku havárií, narušení bezpečnosti dat, přehled nad neobvyklými a podezřelými transakcemi, přístupy apod.
- ⇒ Možné sledování konfiguračních změn prováděných administrátory a operátory systému
- ⇒ Diagnostika a řešení bezpečnostních incidentů
- ⇒ Dohledání přístupů, uživatelských činností, plnění SLA, auditních požadavků apod.
- ⇒ Jsou k dispozici podklady pro forenzní analýzu při vyšetřování bezpečnostních incidentů
- ⇒ Monitoring a kontrola dodržování právních předpisů, regulací a norem.



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 130 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. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.