

Zákazník



**Raiffeisen
BANK**

Obor činnosti

Finanční služby

Výzvy

- ▶ Absence nástroje pro detailní přehled o dění v síti
- ▶ Řešení s využitím stávajících Cisco Nexus 7000 zařízení
- ▶ Uložení statistik na min. jeden měsíc
- ▶ Automatická detekce anomálií

Přínosy řešení

- ▶ Efektivnější správa a dohled sítě
- ▶ Zvýšení bezpečnosti počítačové sítě
- ▶ Záznam statistik na 2TB virtuálním kolektoru

Nasazené produkty

- ▶ Flowmon kolektor VA
- ▶ Flowmon ADS Business

Ve spolupráci s



U Plynárny 1002/97
101 00 Praha 10
Česká republika

www.alefnula.cz
sales@alef.com

O společnosti

Raiffeisenbank a.s. je jedna z největších a nejvýznamnějších bank na trhu v České republice. Nabízí široké spektrum služeb jak v oblasti osobních, tak firemních financí. Zakládá si především na kvalitě poskytovaných služeb a profesionálním přístupu ke klientům. V roce 2008 byla prohlášena za nejlepší banku v České republice.

Požadavky od IT oddělení Raiffeisenbank

Společnost Raiffeisenbank se potýkala s problémem v oblasti monitoringu datových toků. Ve svých datových centrech postrádala nástroje pro detailní přehled o dění v síti na úrovni komunikací. Jako zákazník banka požadovala řešení spočívající ve využití stávajících zařízení v síti a na nich podporovaných protokolů. Pro sběr a vyhodnocování informací bylo možné využít virtualizovaného datového centra, a tedy již pořízeného výpočetního výkonu. Požadavek na dobu pro uložení statistik o veškerých komunikacích byl minimálně jeden měsíc. Mezi dalšími požadavky byla schopnost automaticky detekovat a sledovat výskyt anomálií v monitorovaném provozu a následně na tyto anomálie upozorňovat.

Řešení

Společnost ALEF NULA ve spolupráci s Flowmon Networks navrhla řešení, které využívá protokol NetFlow spuštěný na stávajících síťových prvcích Cisco Nexus 7000. Použit byl protokol NetFlow ve verzi 9 a stávající předkonfigurované šablony pro IPv4 provoz. Na vybraných L2 VLAN sítích byl nakonfigurovaný monitoring provozu ve směru vstupu dat do L2 VLAN.

Veškeré informace o provozu jsou zasílány do Flowmon kolektoru o kapacitě 2TB, který je nasazen ve virtuálním prostředí datového centra. Flowmon kolektor ukládá, zobrazuje a analyzuje síťové statistiky ve formátu NetFlow a poskytuje uživatelům detailní informace o síťových komunikacích a jejich průběhu. Kromě základního modulu pro analýzu nasbíraných dat byl kolektor rozšířen o modul Flowmon ADS (Anomaly Detection System) ve variantě Business, který nad síťovými daty provádí automatickou detekci anomálií na síti a upozorňuje na každou podezřelou aktivitu či síťovou komunikaci. Nasazené řešení tedy slouží nejen pro zvýšení bezpečnosti počítačové sítě a detekci bezpečnostních anomálií, ale také pro detekci provozních problémů a událostí v síti.

Vyjádření zákazníka

Jan Krtička, vedoucí síťové infrastruktury

„V tak citlivém prostředí, jakým bezesporu bankovní datová síť je, je potřeba mít přehled nad bezpečnostními hrozbami, datovými toky a anomáliemi. Tuto kontrolu a vyšší bezpečnost nám přinesl právě produkt Flowmon. V konfiguraci s již stávající infrastrukturou Cisco a výpočetním výkonem v datových centrech jsme získali cenově výhodné řešení, které nám umožňuje detailní přehled provozu sítě, možnost zpětné analýzy a zefektivnění správy. Přínosem je i Flowmon ADS, který umožňuje detekci incidentů a hrozeb, odhalení infikovaných stanic a provozních problémů.“