Zákazník:

Seznam.cz

Obor činnosti:

Provozovatel portálu českého internetu, katalogu firem a www stránek, řady informačních serverů a praktických služeb včetně emailové schránky

Výzvy:

- *monitorování příchozího provozu na veškeré provozované portály a služby*
- *velké množství uživatelů*
- *velké objemy dat*

Přínosy řešení:

- *přehled o komunikacích a využití jednotlivých portálů a služeb*
- *viditelnost do sítě*
- *detekce anomálií a útoků*
- *podklady pro optimalizaci poskytovaných služeb*

Nasazené produkty:

- *Flowmon Probe 40000*
- *Flowmon Collector*
- *Flowmon ADS*

Nasazení realizoval:

BULL s.r.o.
INVEA-TECH Platinum Partner

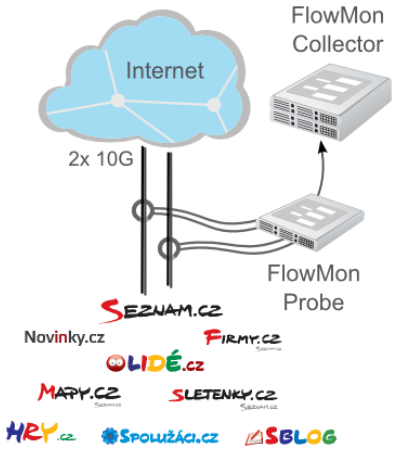
Seznam.cz je nejnavštěvovanější český internetový portál, jehož domovskou stránku denně navštíví přes 2,5 milionu uživatelů. Služby Seznam.cz jako fulltextové vyhledávání, katalog firem, e-mailová pošta či zpravodajství jsou běžnou součástí života českých uživatelů Internetu. Vizí společnosti Seznam.cz je pracovat na tom, aby Internet byl nejsilnější české médium a na něm Seznam.cz místem první volby.

Požadavky zákazníka

Společnost působí ve dvou datových centrech, ve kterých má umístěny tisíce serverů zajišťující chod poskytovaných internetových služeb. Každé datové centrum je do internetu připojeno rychlostí 50 Gb/s. Správné fungování datového centra a připojení do Internetu je pro společnost vzhledem k jejímu zaměření zcela klíčové, proto neustále pracuje na jeho zlepšování (zvyšování propustnosti, spolehlivosti či ochraně proti útokům). Proto bylo logickým krokem nasazení technologií monitorování datových toků a analýzy chování sítě, které poskytují detailní přehled o síťových komunikacích a umožňují automaticky detekovat útoky, anomálie a hrozby v síti. Mezi hlavní požadavky patřily:

- dlouhodobé uchovávání informací o komunikacích,
- analýza a zobrazování informací ve formě různých výstupů (přehledové a koláčové grafy, tabulky, reporty, detailní výpisy komunikací atd.),
- detekce nežádoucích stavů, anomálií či přímo útoků.

Nasazení řešení Flowmon společností BULL



Na základě průzkumu dostupných nástrojů se zákazník rozhodl pro řešení Flowmon, jehož nasazení bylo realizováno společností BULL ve spolupráci s výrobcem řešení společností INVEA-TECH.

Pro monitorování příchozího provozu na již agregovaných dvou 10Gbps linkách je použita 4-portová 10-gigabitová sonda Flowmon Probe 40000, která je zapojena prostřednictvím pasivních rozbočovačů (splitter). Sonda naměřená data posílá k uložení a analýze na Flowmon kolektor, který obsahuje také systém Flowmon ADS. Celková úložná kapacita kolektoru je 24TB a umožňuje analýzu kompletních dat až několik měsíců zpětně, statistické informace a reporty jsou pak dostupné až v řádu let. Systém Flowmon ADS veškerá data analyzuje a upozorňuje na jakoukoliv podezřelou síťovou událost, anomálii či přímo útok.

Hodnocení uživatele

Martin Doleček, manažer provozního oddělení, zhodnotil nasazení řešení takto:

"Řešení Flowmon nám doslova a do písmene otevřelo oči nad obrovskými objemy dat. Jednoduché a zároveň detailní ovládání je přímo šité jak pro síťové administrátory, tak pro manažery. Modul ADS, detekující anomálie, nás upozorňuje na interní neoptimality, ale i na každodenní útočné pokusy. Při rozhodování byl pro nás také klíčový profesionální a otevřený přístup, proto společnosti BULL a INVEA-TECH lze jen doporučit."