Zákazník:

BVV Veletrhy Brno

Obor činnosti:

Pořádání veletrhů a konferencí

Výzvy:

- *rozsáhlá počítačová síť s více než 60 aktivními prvky*
- *kompletní pokrytí areálu wi-fi sítí*
- *sběr statistik o provozu pouze jako suma přenesených dat přes rozhraní aktivních prvků*
- *pracné dohledávání a prokazování útoků a problémů v síti manuální analýzou dat*

Přínosy řešení:

- *optimální vzhledem k potřebám zákazníka*
- *vynikající poměr cena/výkon*
- *lehce rozšiřitelné, přizpůsobitelné aktuálním potřebám*
- *významné snížení nákladů na správu sítě*
- *viditelnost do sítě, důraz na chování uživatelů a zařízení*
- *automatizace procesů správy sítě a bezpečnosti*

Nasazené produkty:

- *Flowmon ADS Standard*
- *Flowmon Probe 2000*

Veletrhy Brno, a. s. jsou nejvýznamnější veletržní správou ve střední Evropě, hlavní činností společnosti je pořádání veletrhů a výstav. K dalším aktivitám patří výstavba veletržních expozic, pronájem všech prostor brněnského výstaviště, pořádání doprovodných programů k veletrhům a zajištění veškerých služeb, které s realizací veletrhů souvisí.

Infrastruktura

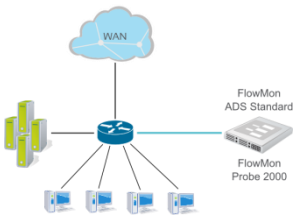
Síť v areálu brněnského výstaviště má kaskádovanou hvězdicovou strukturu. Hlavním prvkem této sítě je centrální switch, přes který prochází veškerý příchozí a odchozí provoz a komunikace mezi klienty a servery. Druhý významný switch, ke kterému je připojen mimo jiné i externí webový server, je umístěn v DMZ.

Síťová infrastruktura je postavena výhradně na aktivních prvcích firmy Cisco. Díky tomu je možné v případě potřeby kdykoliv řešení **Flowmon** rozšířit a využít schopnosti zařízení Cisco ke generování statistik o datových tocích – NetFlow a tato data zpracovávat nasazeným **Flowmon ADS**.

Požadavky zákazníka

- Účinně kontrolovat dodržování bezpečnostních směrnic a předpisů
- Vlastnit nástroj pro odhalení a rychlé rozkrytí vnitřních i vnějších útoků
- Detekovat úniky citlivých informací, sociální inženýrství
- Dokladovat skutečnou kvalitu služeb, zpoždění sítě a služeb
- Eliminovat nežádoucích aplikace, sdílení obsahu
- Detekovat infikovaná zařízení v síti
- Průběžně optimalizovat konfiguraci sítě a síťových zařízení

Nasazení řešení Flowmon ADS



Zařízení **Flowmon Probe 2000** obsahující dva monitorovací vstupy je připojeno ke SPAN portu centrálního switche a SPAN portu switche v DMZ, které do těchto dvou monitorovacích portů zrcadlí veškerý provoz na síti.

Flowmon ADS Standard průběžně a zcela automaticky analyzuje nasbíraná data, generuje události a reporty.

Hodnocení uživatele

Ing. Heršálek, systémový administrátor, zhodnotil nasazení řešení takto:

*"Dříve jsme monitorovali počítačovou síť naší společnosti tak, že jsme sbírali pouze informace o objemech přenesených dat na IP vrstvě a klíčových protokolů. Pokud jsme chtěli zkontrolovat určité datové toky, které se nám jevily jako podezřelé, nezbývalo nám než se vydat trnitou cestou manuální analýzy. Tato cesta se ukázala jako značně problematická, zejména kvůli extrémní časové náročnosti. Tímto způsobem nám taktéž mohli uniknout některé anomálie, či útoky, které byly rozloženy v delším čase, a probíhaly s menší intenzitou. Díky řešení **Flowmon ADS**, které behaviorální analýzu provádí automaticky, budeme schopni provoz na síti kompletně rozkrýt, odhalit problémy a útoky v reálném čase a tím pádem na ně pružně reagovat."*