

Zákazník:



Obor činnosti:

Prodej drogistického zboží

Výzvy:

- ▶ rozsáhlá počítačová síť s více než 100 poboček
- ▶ 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 Probe 2000
- ▶ Flowmon ADS Standard

dm drogerie markt s.r.o. Slovensko je součástí obchodního řetězce dm drogerie markt, který je jeden z nejvýznamnějších prodejců drogistického zboží ve střední a východní Evropě.

Infrastruktura

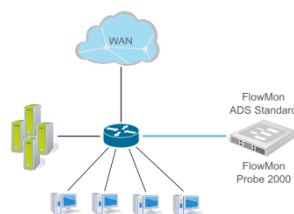
Síť v areálu dm drogerie markt s.r.o. Slovensko má kaskádovanou hvězdicovou prochází veškerý příchozí a odchozí provoz a komunikace mezi klienty a servery.

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 rozkrývání vnitřních i vnějších útoků
- ▶ Měřit využívání jednotlivých služeb
- ▶ 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



události a reporty.

Zařízení **Flowmon Probe 2000** obsahující dva monitorovací vstupy je připojeno ke SPAN portu na dvou centrálních switchích, které do těchto dvou monitorovacích portů zrcadlí veškerý provoz na síti.

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

Hodnocení uživatele

Ing. Ján Slivarich, Vedoucí ISM Technika, zhodnotil nasazení řešení takto:

*"Řešení Flowmon ADS jsme nasadili s cílem zvýšit bezpečnost a kontrolu nad naší infrastrukturou. Dříve jsme neměli k dispozici žádný systém pro monitorování anomálií na počítačové síti. Některé incidenty jsme řešili analýzou logů, které máme k dispozici na vyžádání z centrály dm drogerie markt. Pokud jsme chtěli zkontrolovat určité datové toky, které se nám jevily jako podezřelé, nezbývalo nám než se vydat trnitou cestou manuální analýzy. 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 automaticky provádí behaviorální analýzu, budeme schopni provoz na síti kompletně rozkrýt, odhalit problémy a útoky v reálném čase a tím pádem na ně pružně reagovat."*