HASIČSKÝ ZÁCHRANNÝ SBOR JIHOČESKÉHO KRAJE

Obor činnosti

Státní správa

Výzvy

Správa infrastruktury s 1000 IP zařízení ve 20 lokalitách kraje

Efektivní správa a dohled nad rozsáhlou síťovou infrastrukturou

Zvýšení bezpečnosti a rychlé odhalování síťových útoků

Přínosy řešení

Získání viditelnosti do síťového provozu ve všech lokalitách

Zvýšení bezpečnosti sítě a automatická detekce incidentů a anomálií

Efektivnější správa a dohled sítě

Práce v uživatelsky přívětivém prostředí

Nasazené produkty

Flowmon Probe 4000 SFP
Flowmon Probes 1000 VA
Flowmon Collector R5-3000
Flowmon ADS Business

HZS zajišťuje ochranu životů a zdraví obyvatel České republiky. Aby mohl tyto cíle naplňovat, je správná funkčnost a zabezpečení informačních technologií, které využívá, klíčová. "*Bezpečnostní analýza ukázala, že antivir a firewall na perimetru sítě již nedostačují," říká Jakub Mauric, pracovník ICT.* HZS JČK se proto rozhodl implementovat řešení Flowmon.

POŽADAVKY ZÁKAZNÍKA

ICT infrastruktura HZS Jihočeského kraje prošla v posledních několika letech výraznou proměnou v téměř všech svých oblastech od datové sítě – přes virtualizaci serverů a zálohování, až po nastavení některých nezbytných procesů. Důraz byl kladen zejména na rychlost, bezpečnost a dostupnost. Zavedení pokročilého systému monitoringu sítě, vizualizace a zabezpečení bylo vnímáno jako další nezbytný krok. Cílem byla nejen ochrana vlastního perimetru, ale také dohled nad vnitřním prostředím. Pro naplnění cílů se zákazník rozhodl pořídit řešení Flowmon, které umožnilo:

- Monitoring a viditelnost provozu fyzické i virtuální sítě.
- Poskytnutí informací pro kapacitní plánování linek k jednotlivým geograficky rozmístěným lokalitám.
- Detekce anomálií v síťovém provozu a dalších hrozeb.

Největším přínosem pro zákazníka byla implementace Flowmon ADS, modulu pro behaviorální analýzu sítě. Zákazník oceňuje jednoduché ladění false positive a tím snížení počtu detekovaných událostí na nižší desítky, které je možné při daných lidských kapacitách analyzovat. Modul tak umožnil zákazníkovi detekovat anomálie, které jsou nedetekovatelné pomocí tradičních bezpečnostních řešení, jako je firewall nebo IDS.

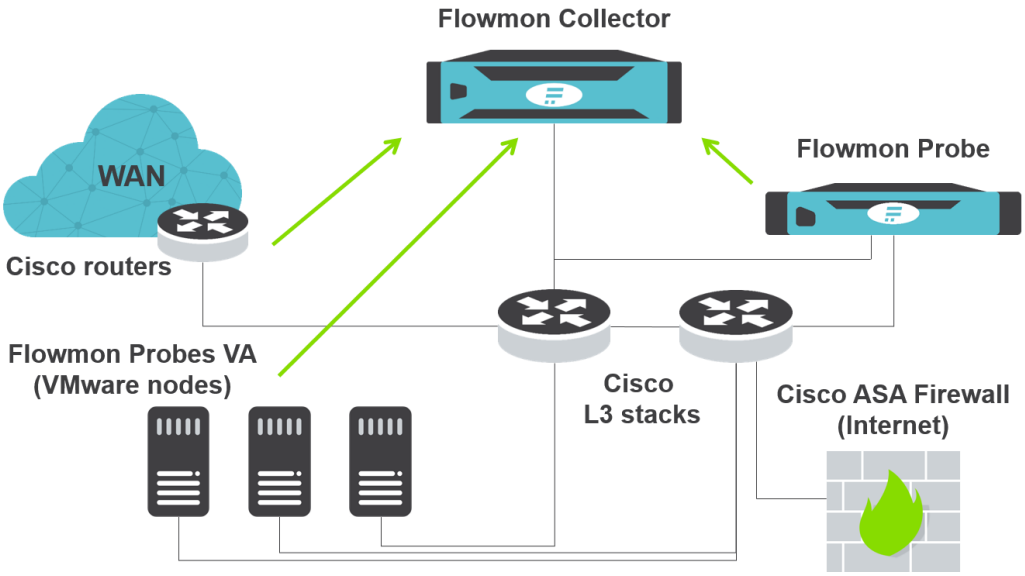
VYJÁDŘENÍ ZÁKAZNÍKA

Jakub Mauric, pracovník oddělení komunikačních a informačních systémů HZS Jihočeského kraje hodnotí nasazené řešení Flowmon:

Flowmon se ukázal jako velmi vhodný doplňkový nástroj pro dohled moha síťových parametrů a událostí (např. odezva, datové toky, anomálie). Bezpečnostní analýza ICT infrastruktury HZS Jihočeského kraje prokazatelně ukázala, že v dnešní době již pouhé antivirové řešení a firewall na perimetru sítě nedostačují. Osobně považuji modul Flowmon ADS za nezbytnou základní komponentu, která teprve odemyká skutečný potenciál celého řešení."

NASAZENÉ ŘEŠENÍ

Nasazené řešení se skládá z jednoho fyzického 3TB kolektoru, tří virtuálních jednoportových sond a jedné fyzické čtyřportové SFP sondy. Do fyzické sondy je zrcadlen provoz dvou Cisco L3 stohů, každá z virtuálních sond sbírá data z jednoho VMware nodu s tím, že HZS Jihočeského kraje používá základní vSwitch. Jako další zdroje informací slouží směrovače Cisco s protokolem IPFIX. Kombinací těchto zdrojů dat je zákazník schopen pokrýt drtivou většinu důležitých datových toků v kraji. Datové toky jsou na kolektoru analyzovány pomocí rozšiřujícího modulu Flowmon ADS pro behaviorální analýzu sítě a detekci anomálií.



O ORGANIZACI

HZS Jihočeské kraje je organizační součástí Hasičského záchranného sboru ČR. Základním posláním HZS ČR je chránit životy, zdraví obyvatel a majetek před požáry a poskytovat účinnou pomoc při mimořádných událostech, ať již se jedná o živelní pohromy, průmyslové havárie či teroristické útoky. Zároveň je základní složkou integrovaného záchranného systému (IZS).