Zákazník:

MVV Energie CZ

Obor činnosti:

Energetický průmysl

Výzvy:

- Systémový dohled toků uvnitř infrastruktury i přístupu do internetu.
- Detekce a prevence úniků dát.
- Vyhodnocení využívání jednotlivých datových linek
- Automatická detekce anomálií a možnost vytvářet evidenci incidentů.

Přínosy řešení:

- Efektivnější správa a dohled sítě s přehledem nad využitím jednotlivých linek.
- Zvýšení bezpečnosti počítačové sítě s automatickou detekci anomálií.
- Automatický reporting pro účely kontrolních orgánů.

Nasazené produkty:

- FlowMon Probe
- FlowMon ADS Business

MVV Energie CZ je dynamicky se rozvíjející energetická skupina, kterou tvoří patnáct dceřiných společností působících v patnácti městech České republiky, především na Moravě, v severních Čechách a na Vysočině. Společnosti se zaměřují na výrobu a distribuci tepla a elektřiny a také vodohospodářství.

Infrastruktura

Divize IS/IT provozuje centralizovanou IT infrastrukturu pro všechny společnosti holdingu MVV Energie CZ s důrazem na bezpečnost, ale také na náklady související s poskytováním IT služeb.

Infrastruktura je vybudována z farmy terminálových serverů (Windows Server), ke kterým přistupují uživatelé z jednotlivých lokalit SW/HW tenkými klienty, z klasických PC nebo notebooků. S centrální infrastrukturou dále komunikují samostatné tiskové servery, tiskárny či síťové scannery a v některých případech i místní technologické sítě nebo jejich části. Požadavkem divize IS/IT proto bylo zajistit si systémový dohled datových toků uvnitř infrastruktury i přístupu do Internetu, v obou případech zejména se zaměřením na kontrolu bezpečnostních politik a pravidel vynucených jinými technickými prostředky i bezpečnostními směrnicemi dle ISMS.

Další požadavky zákazníka

Mezi hlavní požadavky zákazníka patřila **detekce a prevence** úniků dat, používání nedovoleného programového vybavení, připojování cizích zařízení a jiného škodlivého jednání na síti LAN/WAN. Dále pak **zvýšení bezpečnosti** a rychlé odhalení možných hrozeb, **vyhodnocení reálného využívání WAN** (respektive kapacit jednotlivých datových linek a komunikačních prostředků a automatická detekce trendů), **automatický reporting** pro účely kontrolních orgánů společnosti, automatická **detekce bezpečnostních incidentů**, možnost vytvářet evidenci incidentů a kontrolní nástroj pro vyhodnocování kvality externě dodávané služby WAN konektivity.

Technické řešení sondou Flowmon/ADS

Požadavky zákazníka byly naplněny nasazením čtyřportové sondy Flowmon, která je připojena do sítě za využití TAPů. Zákazník hojně využívá různých pohledů na monitorovaný provoz (profily) i automatických reportů. Pro automatickou detekci anomálií je používán systém Flowmon ADS.

Hodnocení uživatele

Ing. Jan Regner, manažer divize IS/IT společnosti MVV Energie CZ a.s. hodnotí Flowmon: *„Spolupráce s firmou Flowmon Netwokrs trvá již od roku 2008, kdy jsme poprvé implementovali její řešení pro kontrolu datových toků Flowmon Probe, s cílem systémově kontrolovat a dohledovat provoz na WAN síti. Díky výborným zkušenostem s tímto nástrojem a dalšímu požadavku na celkové zvýšení úrovně bezpečnosti (zejména pak na možnost detekce nežádoucího chování na síti LAN) jsme se rozhodli rozšířit náš monitoring také o ADS. Kvitujeme zejména to, že řešení Flowmon se úspěšně daří držet krok se stále novými bezpečnostními hrozbami, což nám umožňuje rychle a efektivně vyhodnotit potencionální rizika. Zároveň můžeme věnovat více času podpoře ostatních aktivit, které jsou důležité pro další rozvoj skupiny MVV.“*