Zákazník:

Odvětví

Vysoké školství a vědecké výzkumy

- *Druhá největší univerzita v České republice*
- *9 fakult a více než 200 kateder, ústavů a klinik*

Výzva:

- *5000+ zaměstnanců*
- *40 000+ studentů*
- *15 000+ počítačů*
- *Desítky lokací*
- *Stovky serverů*
- *Konektivita 2x10Gbps*
- *10Gbps univerzitní páteřní síť*
- *Viditelnost do sítě*
- *Síťová bezpečnost*
- *Zpracování a správa incidentů*

Řešení:

- *Flowmon sondy*
- *Flowmon kolektory*
- *Flowmon ADS*

Benefity:

- *Výtečná viditelnost do sítě a reportování*
- *Automatická detekce anomálií a porušení univerzitních politik*
- *Automatizace CSIRT procesů a úkolů*
- *Použití Flowmon řešení pro účely výzkumu a výuky*

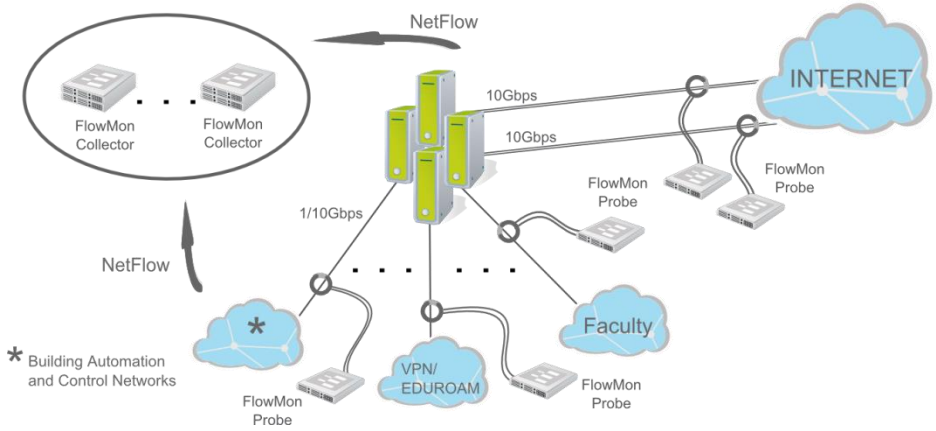
Masarykova univerzita je druhou největší univerzitou v České republice a vůdčí moravskou univerzitou. Aktuálně disponuje devíti fakultami a více než dvěma stovkami kateder, ústavů a klinik. Masarykova univerzita je uznávanou výzkumnou univerzitou a jednou z nejrychleji rostoucích vysokoškolských vzdělávacích institucí ve střední Evropě.

Infrastruktura

IT infrastruktura Masarykovy univerzity, s jejími devíti fakultami a kampusem, je rozmístěná na území celého Brna a blízkého okolí. Páteřní síť běží na 10Gbps a je spravována ústavem výpočetní techniky. Bezpečnost na síti je garantována skupinou CSIRT-MU – akreditovaným členem TERENA (European security community Trusted Introducer). Skupina CSIRT-MU je odpovědná za monitoring příchozího a odchozího provozu do sítě internet, spojení mezi fakultami a páteřní sítí, technologických sítí, VPN sítí, eduroam a kritických serverů.

Implementace

CSIRT-MU k zabezpečení monitoringu všech kritických bodů v univerzitní síti provozuje 25 Flowmon sond. Aby se mohla garantovat redundance a oddělení produkčních kolektorů od vývojových či testovacích, jsou informace a statistiky o provozu na síti uložené na šesti různých kolektorech. Celková kapacita kolektorů činí 40 TB. Flowmon ADS zpracovává statistiky o síťovém provozu z vybraných sond (např. provoz z/do sítě internet a vybrané fakulty) a automaticky detekuje bezpečnostní rizika a narušení univerzitních politik. Proces zpracování a správy incidentů je automatizovaný, takže všechny události jsou reportovány do systému správy incidentů Request Tracker spravovaného skupinou CSIRT-MU.



Hodnocení uživatele

Jan Vykopal, vedoucí týmu CSIRT-MU shrnul zkušenosti s řešením Flowmon ve službách Computer Security Incident Response týmu následovně:

„Přestože rádi vytváříme nové bezpečností monitorovací nástroje, pro monitorování naší infrastruktury i rutinní provoz univerzitního CSIRT týmu potřebujeme systém, na který se můžeme spolehnout. Navíc se díky profesionální podpoře řešení Flowmon můžeme soustředit na jádro naší práce."

Computer Security Incident Response Team
Masarykovy univerzity, ***http://www.muni.cz/csirt***