Zákazník

SLOVENSKÁ sporiteľňa

Obor činnosti

Finančné služby

Výzvy

- *Rozsiahla WAN sieť čítajúca viac ako 150 pobočkových zariadení, 100+ nezávislých LAN sietí a dve dátové centrá*
- *Existujúci monitoring nebol schopný poskytnúť v dostatočnej kvalite a efektivite potrebné informácie pre správu siete a sieťovú bezpečnosť*
- *Nedostatok informácií o prevádzke a udalostiach vyskytujúcich sa na vnútornej sieti*

Prínosy riešenia

- *Viditeľnosť do siete vrátane detailného prehľadu o chovaní užívateľov a zariadeniach v sieti*
- *Zvýšenie bezpečnosti počítačovej siete a s tým súvisiaca kontrola prístupov k ICT zdrojom.*
- *Efektívnejšia správa a dohľad nad sieťou*
- *Pomoc pri troubleshootingu a riešení problémov v sieti*

Nasadené produkty

- *Flowmon kolektor*
- *Flowmon sondy*
- *Flowmon ADS*

Kontakt

www.slsp.sk

Slovenská Sporiteľňa

Slovenská Sporiteľňa má najdlhšu tradíciou sporiteľníctva na Slovensku. V roku 2001 sa spoločnost začlenila do silnej finančnej skupiny Erste Bank der oesterreichischen Sparkassen AG. Slovenská Sporiteľňa patrí k najväčším bankám v krajine s počtom klientov takmer 2,4 milióna a počtom zamestnancov približne 4 tisíc. Je lídrom na trhu v celkových aktivitách, poskytnutých retailových úveroch a vkladoch. Drží tak isto prvenstvo v počte bankomatov a pobočiek, kde do dnešného dňa prevádzkuje 292 pobočiek a 17 firemných centier.

Situácia

Sieťové oddelenie spoločnosti rieši na dennej báze desiatky úkonov týkajúcich sa bežnej správy IT infrastruktury. Z pohľadu bezpečnosti chýbala nutná viditeľnosť v existujúcej sieťovej infraštruktúre.Vzhľadom ktomu vznikla požiadavka na implementáciu monitoringu dátovej komunikáce spĺňajúcej nasledujúce požiadavky:

- kompletní monitoring WAN siete (pobočková sieť po celom Slovensku),
- detailný monitoring LAN siete vrátane dvoch dátových centier a DMZ,
- efektívnejšia správa a dohľad nad sieťou, pomoc pri troubleshootingu a riešení problémov,
- potreba analýzy a vyhodnocovania sieťovej prevádzky pre potreby detekcie bezpečnostných udalostí a anomálií.

Riešenie Flowmon

Požiadavky spoločnosti boli vyriešené vďaka distribuovanému Flowmon riešeniu skladajúceho sa z:

- centrálneho 12TB Flowmon kolektoru,
- štyroch virtuálnych Flowmon sond implementovaných v lokalitách s nutnosťou monitoringu QoS/VoIP parametrov alebo neschopnosťou zariadení posielania Netflow,
- 25 aktívnych prvkov zasielajúcich NetFlow export dáta do centrálneho kolektora.

Vyššie uvedené riešenie je plne zintegrované s interným SIEM systémom pomocou syslog správ za účelom jednotného miesta zberu a vyhodnocovania bezpečnostných incidentov. Nad Flowmon logikou jsou nasadené viaceré korelačné pravidlá a ďalej sa s Flowmon výstupom pracuje v zmysle existujúcich procesov Incident manažmentu.

Vyjádrenie zákazníka

Ján Adamovský, CISO spoločnosti Slovenská Sporiteľňa, hodnotí nasadenie riešenia Flowmon:

„Flowmon nám priniesol viditeľnosť na sieťovej úrovni, ktorá nám predtým chýbala. Vďaka integrácii do štandardného procesu riadenia bezpečnostných incidentov sme zvýšili našu schopnosť incidenty včaš identifikovať a vhodne na ne reagovať.“