Obor činnosti

Finančné služby

Výzvy

Rozšíriť možnosti predošlého systému pre monitorovanie sieťovej prevádzky, ktorému končila životnosť.

Integrovať nové riešenie s existujúcim SIEM systémom pre manažment bezpečnosti IT.

Posilniť a zjednodušiť manažment bezpečnosti a prevádzky IT.

Prínosy riešenia

Identifikácia chýb konfigurácií, neplatných bezpečnostných certifikátov a iných prevádzkových a bezpečnostných problémov.

Zjednodušenie prípadného nahlasovania bezpečnostných udalostí príslušným autoritám.

Rozšírenie viditeľnosti do sieťovej prevádzky, vrátane šifrovanej internetovej komunikácie.

Zjednodušenie interpretácie dát zo sieťovej prevádzky vďaka zrozumiteľnej vizualizácii.

Nasadené produkty

Flowmon sonda s kolektorom

Flowmon ADS (IDS)

Systémy pre monitorovanie prevádzky počítačových sietí sú dnes nevyhnutnou súčasťou IT infraštruktúry každej organizácie, ktorá chce mať detailný prehľad o dátovej komunikácii, aby mohla efektívne riešiť prevádzkové a bezpečnostné problémy, ale aby tiež vedela splniť čoraz prísnejšie legislatívne požiadavky. Výnimkou nie je ani OTP Banka, ktorá v minulosti využívala ucelené bezpečnostné riešenie od spoločnosti IBM pozostávajúce z monitorovacej sondy, kolektora a softvéru pre manažment bezpečnostných informácií a udalostí (SIEM - Security Information and Event Management).

VÝCHODISKÁ

Keď sa existujúca sonda a kolektor ocitli na pokraji životnosti a výrobca pre ňu ukončoval podporu, rozhodlo sa oddelenie bezpečnosti IT v banke preveriť, aké možnosti pre monitorovanie sieťovej prevádzky sú v súčasnosti na trhu dostupné. „Hľadali sme riešenie s rozšírenou funkcionalitou, ktoré by sme zároveň vedeli bez problémov integrovať so SIEM systémom pre manažment bezpečnosti IT," spomína Peter Magula, vedúci oddelenia bezpečnosti IT v OTP Banke.

Obidvom kritériám vyhovuje riešenie od spoločnosti Flowmon, ktoré oproti predošlému nástroju prináša lepšiu viditeľnosť do siete a takisto rozšírenú analýzu sieťovej prevádzky s vyhľadávaním anomálií. Oddelenie bezpečnosti IT v banke zaujímala predovšetkým viditeľnosť do sieťových a aplikačných protokolov, a to najmä v súvislosti s rastúcim objemom zašifrovanej prevádzky, v ktorej je prakticky nemožné zaručiť bezpečnosť komunikácie bez špecializovaných nástrojov, ako je sonda s integrovaným kolektorom od Flowmonu.

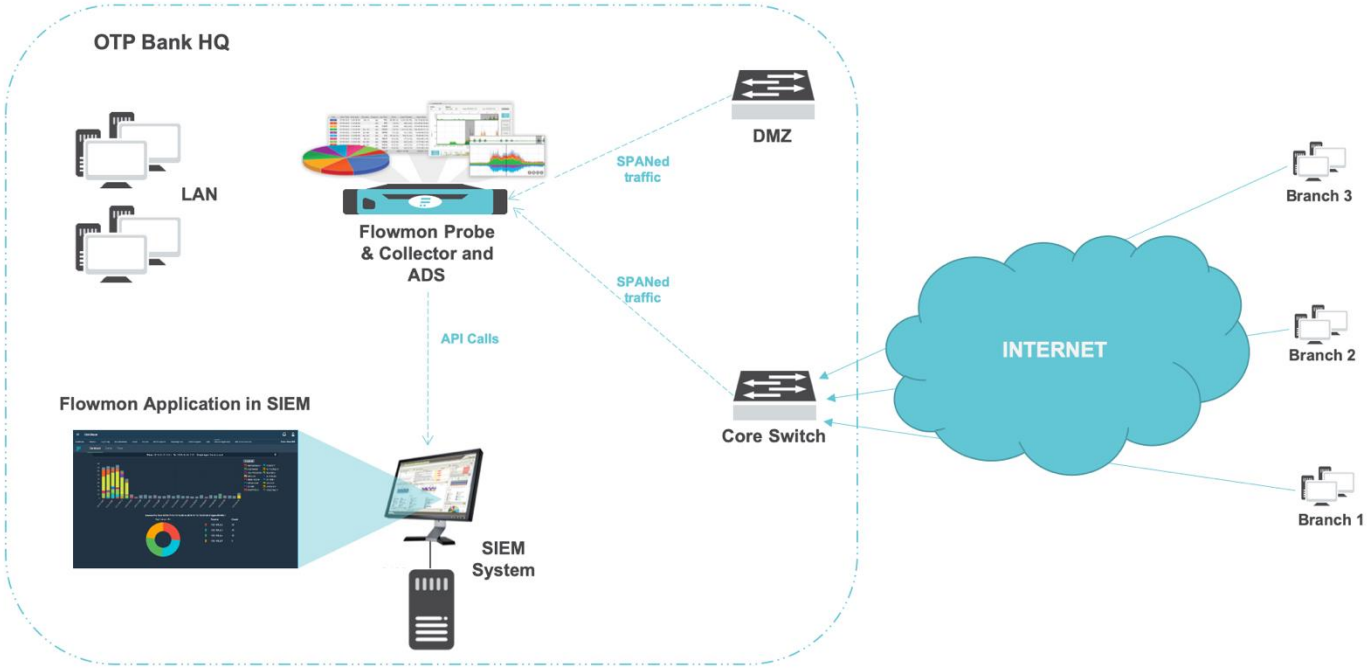
Správnosť voľby ešte pred samotnou implementáciou potvrdil manažmentu OTP Banky „proof of concept", pri konečnom výbere však zohral podľa Petra Magulu rolu aj dynamický vývoj riešení Flowmonu, lokálna podpora a „živá komunita", ktorá sa okolo produktov českej firmy vytvorila.

VYJADRENIE ZÁKAZNÍKA

Peter Magula, vedúci oddelenia bezpečnosti IT v OTP Banke: *„Hľadali sme riešenie s rozšírenou funkcionalitou, ktoré by sme zároveň vedeli bez problémov integrovať so SIEM systémom pre manažment bezpečnosti IT."*

RIEŠENIE

Inštaláciu riešenia v OTP Banke mal na starosti integrátor, spoločnosť EMM, ktorá úzko spolupracovala s lokálnym tímom Flowmonu. Úvodná analýza, návrh riešenia aj samotné nasadenie prebehli rýchlo a hladko, v priebehu niekoľkých dní.



„Drobné technické problémy, napríklad v súvislosti s integráciou do aplikácie SIEM, sa podarili vždy promptne vyriešiť s technickou podporou IBM alebo Flowmonu," dodáva P. Magula. S dodatkom, že najdôležitejšia a najdlhšia časť projektu nasleduje až po nasadení riešenia, keď začnú prichádzať prvé dáta zo sieťovej prevádzky. Vtedy treba systém doladiť a nastaviť politiky tak, aby administrátori zbytočne nedostávali falošné poplachy. Detailnejšie ladenie vrátane zaškoľovania v réžii EMM a Flowmou trvalo zhruba dva týždne.

Okrem starostlivého doladenia by P. Magula potenciálnym záujemcom o riešenie Flowmonu odporučil myslieť pri výbere na prípadné budúce zmeny či rozšírenia infraštruktúry. V prípade OTP Banky to napríklad znamenalo, že sonda je pripravená na pripojenie cez metalické a zároveň optické porty, na ktoré mieni banka v blízkej budúcnosti prejsť.

SÚČASNÝ STAV A VÝSLEDKY

Riešenie od Flowmonu pozostávajúce zo sondy s integrovaným kolektorom a modulom ADS (Anomaly Detection System) dnes pomáha OTP Banke identifikovať a riešiť rozličné bezpečnostné a prevádzkové problémy súvisiace s dátovou komunikáciou, ktorá prechádza cez centrálu v Bratislave, čo zahŕňa aj internetové pripojenia všetkých pobočiek. Ihneď po nasadení napríklad analýza šifrovanej prevádzky poukázala na používanie zastaraných SSL protokolov a šifrovacích setov, ktoré už v banke nie sú schválené.

Oddelenie IT bezpečnosti tiež identifikovalo v infraštruktúre banky dva servery, ktoré sa pokúšali pripájať do materskej spoločnosti na nejestvujúce sieťové porty funkčných serverov, či konkrétne aplikácie a servery spôsobujúce zahlcovanie

komunikačnej linky, konkrétne VPN tunela medzi bankou a tretím subjektom. „Odhalili sme tak zbytočnú komunikáciu, ktorá mohla predstavovať zvýšené prevádzkové, či bezpečnostné riziko," dodáva P. Magula.

Počet relevantných bezpečnostných a prevádzkových problémov, ktoré riešenie pomohlo banke identifikovať, postupne narastal popri dolaďovaní systému. Zodpovední pracovníci OTP Banky však oceňujú nielen samotnú funkcionalitu, ale aj celkový komfort, ktorý riešenie od Flowmonu do starostlivosti o bezpečnosť IT prináša.

Administrátor OTP Banky vidí dáta zbierané Flowmonom zo sieťovej prevádzky priamo v SIEM systéme s možnosťou detailnej vizualizácie týchto dát. Vďaka tomu majú odborníci na bezpečnosť a prevádzku IT oveľa lepší prehľad o tom, čo sa v sieti deje a dokážu tak aj ľahšie identifikovať prípadné anomálie či incidenty.

Intrusion Detection System (IDS) integrovaný priamo v sonde a kolektore Flowmonu prináša oddeleniu bezpečnosti IT ďalšie uľahčenie života . Keďže túto funkcionalitu si firmy často zabezpečujú samostatným hardvérom, OTP Banka sa vďaka integrácii tejto funkcionality do riešenia Flowmon ADS vyhla starostiam s konfiguráciou a prevádzkou ďalšieho zariadenia. Naviac je možné korelovať informácie z ADS a IDS v jednom ucelenom rozhraní, čo zvyšuje informačný a vizualizačný efekt pri forénznych analýzach.

POHĽAD DO BUDÚCNOSTI

Pri pohľade do budúcnosti považuje P. Magula za dôležité zachovať si prehľad o aktuálne využívaných bezpečnostných šifrovacích certifikátoch a protokoloch. Práve vďaka sonde Flowmonu odborníci na bezpečnosť v OTP Banke vždy vedia, ktorým certifikátom skončila platnosť a kedy centrála banky alebo medzinárodná autorita, akou je napríklad Internet Engineering Task Force (IETF), vydá odporúčania nepoužívať určité štandardy, okamžite dokážu zistiť, či a kde sú stále v prevádzke.

„Naša sonda pritom dokáže skúmať vo vnútornej sieti zákazníka aj certifikáty, ktoré nie sú pod jeho správou a automaticky upozorňovať oddelenia bezpečnosti na potenciálne rizikovú internetovú komunikáciu, a to bez potreby čokoľvek inštalovať na koncové zariadenia," Roman Čupka, hlavný konzultant pre strednú a východnú Európu a country manažér pre Slovensko v spoločnosti Flowmon.

V budúcnosti poslúži riešenie Flowmonu OTP Banke aj pri napĺňaní zákonných povinností. Sonda poskytuje profily špeciálne prispôsobené miestnym požiadavkám regulátorov, preto banka dokáže vďaka rozšírenej viditeľnosti do siete a vizualizácii dát prevádzkové a bezpečnostné incidenty nielen rýchlo identifikovať, ale ich aj efektívne nahlasovať.

OTP Banka navyše môže v budúcnosti rozšíriť Flowmon sondy a ďalšie doplňujúce funkcionality na iné útvary akým je v súčasnosti oddelenie bezpečnosti IT. Kým väčšina technologických nástrojov pre zabezpečenie správy a bezpečnosti IT je určená iba pre jedno oddelenie, riešenie Flowmon môže v organizácii využiť napríklad aj tím sieťových, či technologických špecialistov na monitorovanie výkonnosti siete, dostupnosti aplikácií, či iných kritických služieb.

O OTP BANKE

V súčasnosti OTP Banka Slovensko disponuje sieťou 58 pobočiek po celom Slovensku. Ústredie banky je v Bratislave. OTP Banka Slovensko disponuje systémom komplexného hodnotenia podnikateľských zámerov klienta v súlade so svetovými štandardmi a implementovaným platobným a zúčtovacím systémom PROFILE, ktorým sa zabezpečuje on-line prepojenie všetkých pobočiek OTP Banka Slovensko, a.s. Banka je v súčasnosti napojená na SWIFT, REUTERS, TELERATE.

Rozhodujúci objem v obchodnej činnosti banky predstavujú bankové produkty a služby poskytované klientom na slovenskom trhu. Štruktúra produktov a služieb zodpovedá požiadavkám rozhodujúcich segmentov trhu, ktoré banka obsluhuje. OTP Banka Slovensko ponúka svoje produkty a služby fyzickým aj právnickým osobám. OTP Banka Slovensko je univerzálnou bankou rodinného typu, preto aj ponuka produktov a služieb je prispôsobená požiadavkám viacerých generácií (od najmladšej až po dôchodcov), a tiež náročnosti jednotlivých klientov.