SOITRON GROUP

Obor činnosti

Informačné technológie a integrácia systémov

Výzvy

Vyššie nároky firiem a verejnej správy na bezpečnosť a dostupnosť kritických služieb a IT infraštruktúry

Aplikácia novej legislatívy – GDPR a NISD

Prínosy riešenia

Rozšírenie poskytovaných služieb o prediktívny monitoring, alerting a reporting

Skrátenie reakčnej doby vďaka rýchlej diagnostike a analýze problémov s dopadom na dostupnosť a bezpečnosť kritických služieb

Nasadené produkty

Flowmon sonda

Flowmon kolektor

Flowmon ADS

Flowmon APM

Flowmon Traffic Recorder

Keďže význam počítačových sietí rastie a zároveň pribúdajú sofistikované kybernetické útoky, čoraz viac firiem potrebuje nielen nasadiť pokročilú technológiu pre lepšiu viditeľnosť dátových tokov v sieti a detekciu anomálií, ale pomôcť tiež s analýzou a vyhodnocovaním výstupov sieťového monitoringu. Spolupráca Soitron Group s Flowmon Networks prináša zákazníkom kombináciu špičkových bezpečnostných technológií s odborným poradenstvom pri diagnostike a vyhodnocovaní potenciálnych hrozieb pre IT infraštruktúru aj firemné procesy.

KEĎ SIEŤ NABERÁ VÝZNAM

Keď spoločnosť Soitron nedávno nasadila v istej výrobnej fabrike systém pre monitorovanie sieťovej prevádzky od firmy Flowmon Networks, ako najzávažnejší problém v sieti zákazníka sa podarilo odhaliť prebiehajúci útok na takzvaný SSH server vedený cez verejnú IP adresu.

IT oddelenie fabriky zostalo po upozornení odborníkmi Soitronu prekvapené. Informatici boli totiž presvedčení, že žiadny SSH server v internete sprístupnený nemajú. Na okamih sa zdalo, že Flowmon hlási falošný poplach.

Spoločné pátranie IT administrátorov výrobného podniku s odborníkmi Soitronu však ukázalo, že monitorovací systém sa nemýlil. IT oddelenie totiž počas predošlej implementácie informačného systému naozaj vytvorilo pre externého dodávateľa SSH prístup, a neskôr pozabudlo na jeho zablokovanie. V čase nasadenia Flowmonu sa už niekto pokúšal túto zraniteľnosť zneužiť a vlámať sa do počítačovej siete fabriky.

Spoločnosť Soitron sa venuje poskytovaniu vzdialeného dohľadu nad prevádzkou IT infraštruktúry. Disponuje dohľadovým centrom, cez ktoré monitoruje na strane zákazníkov zariadenia ako sú záložné zdroje či „storage“ systémy, prípadne operačné systémy a virtualizačné platformy. Sledovanie infraštruktúry je však odjakživa zamerané výhradne na prevádzku. Čiže na sledovanie či zariadenia fungujú a či pracujú tak ako majú, či nie sú napríklad preťažené, alebo či nedošlo k poruche niektorého komponentu.

V poslednom období však rastie význam počítačových sietí. Aj zdroje, ktoré bývali v minulosti izolované, ako sú napríklad ICS/ SCADA systémy, začínajú byť online, aby využili potenciál internetu vecí. Zároveň dochádza k centralizácii počítačových zdrojov – čoraz viac softvéru beží na serveroch a bez spoľahlivej a rýchlej sieťovej konektivity sa tak aplikácie spúšťané na koncových zariadeniach stávajú nepoužiteľné. Popri rastúcom význame sietí narastá aj množstvo a sofistikovanosť kybernetických útokov, na čo reaguje legislatíva sprísňovaním nárokov, ktoré musia organizácie dodržiavať, najmä z pohľadu ochrany osobných údajov svojich klientov. Čoraz častejšie sa preto obracajú na systémy pre monitorovanie sieťovej prevádzky, ako poskytuje spoločnosť Flowmon Networks, ktoré umožňujú lepšie identifikovať a pochopiť, čo sa v počítačových sieťach deje.

CESTA K VYŠŠEJ BEZPEČNOSTI

Špecialisti Soitronu si začali uvedomovať, že v niektorých podnikoch aj verejnej správe nemusí samotné nasadenie technológie postačovať. Niekedy totiž na strane používateľa chýbajú kapacity pre sledovanie a vyhodnocovanie výsledkov sieťového monitoringu. Preto by bolo užitočné, keby zákazníkom vedel s diagnostikou siete pomôcť osvedčený dodávateľ s rozsiahlou expertízou.

„Doteraz sme analýzy bezpečnostných hrozieb či incidentov na diaľku nerobili, s rastúcim významom počítačových sietí a tým aj potrebou ich zabezpečenia, však začína byť táto otázka aktuálna. Platí to obzvlášť vtedy, keď zákazník nedisponuje potrebnými odbornými a neraz ani časovými kapacitami na hĺbkový monitoring a diagnostiku svojich sietí,“ vysvetľuje Štefan Porubčan zo spoločnosti Soitron. Inými slovami, nech je zariadenie akokoľvek kvalitné, jeho potenciál zostáva nevyužitý, ak sa mu niekto kompetentný dostatočne nevenuje.

Ako by malo skĺbenie špičkových bezpečnostných technológií s expertízou Soitronu vyzerať? Spoločnosť Soitron nasadí a nakonfiguruje v sieti zákazníka Flowmon kolektor, na ktorom sa ukladajú dátové toky či už z existujúcej infraštruktúry, alebo Flowmon sond. Systém pre monitorovanie siete u zákazníka zahlási okamžite všetky detekované bezpečnostné incidenty alebo anomálie, ktoré by mohli predstavovať bezpečnostnú hrozbu, do dohľadového centra Soitronu s nepretržitou službou. Odborníci firmy následne vyhodnotia, či ide o závažnú udalosť a treba zareagovať ihneď, alebo nejde o nič akútne a zákazníka stačí na nezrovnalosť upozorniť v rámci týždenného či mesačného review.

CUSTOMER TESTIMONIAL

Štefan Porubčan, Security Business Unit Manager spoločnosti Soitron.

„Vďaka produktom spoločnosti Flowmon Networks sme vytvorili službu s jedinečnou pridanou hodnotou. Okrem nepretržitého monitoringu prevádzkových, bezpečnostných a výkonnostných parametrov siete doplňujú experti z dohľadového centra o rychlú a zrozumiteľnú interpretáciu incidentov, ktoré identifikujú pokročilé technologie od Flowmon Networks. V menších a strdných podnikoch často nemajú dedikované sieťové a bezpečnostné oddelenia, ale univerzálne IT oddelneie s obmedzenými kapacitami. Nechceme preto zákazníkovi iba sprostredkovať hlásenia, ale pomôcť ich aj interpretovať a čo najrýchlejšie vyriešiť,“ vysvetľuje Š. Porubčan.

Zákazník teda dostane zrozumiteľný výsledok analýzy, ktorý mu na jednej strane povie čo sa deje a na druhej strane odporučí, ako reagovať. Rozmenené na drobné, dostane podrobnú informáciu či hrozí napríklad únik dát, prípadne narušenie ich integrity, aké systémy či firemné procesy sú vystavené riziku, alebo či je povedzme ohrozená dostupnosť služieb, lebo niekto zahlcuje linku. Z toho vyplynú odporúčania krokov, ktoré treba urobiť na eliminovanie rizík, čo môže byť napríklad izolácia staníc do

karantény, rekonfigurácia sieťových zariadení, alebo nasadenie nového bezpečnostného riešenia.

"Ak Soitron u klienta sieť aj prevádzkuje, čiže má zariadenia infraštruktúry pod svojou správou, dokáže v rámci supportu pri niektorých incidentoch aj zakročiť a problém vyriešiť. Ak si organizácia spravuje sieť sama, alebo sa problémy týkajú napríklad desktopových staníc, o ktoré sa stará iný dodávateľ, tak dostane odporúčanie pre ďalší postup," dodáva Š. Porubčan.

LEGISLATÍVNY TLAK

Lepšia viditeľnosť do sieťovej dátovej prevádzky vrátane identifikácie anomálií – a to bez ohľadu na to či jej výsledky bude organizácia interpretovať interne alebo s externou pomocou – bude v nastávajúcom období naberať na význame aj v súvislosti s legislatívnymi zmenami, ako sú zavedenie naradenia pre ochranu osobných údajov (GDPR) alebo pripravovaný Zákon o kybernetickej bezpečnosti na základe smernice EU. *„Nová legislatíva kladie na organizácie nároky, ktoré sa nedajú splniť bez adekvátnych technických prostriedkov, s ktorými treba vedieť pracovať. Preto som presvedčený, že nová služba spoločnosti Soitron, ktorá využíva aj naše technológie, bude pre zákazníkov atraktívna a prínosná,"* dodáva Roman Čupka, regionálny manažér spoločnosti Flowmon Networks.

O SPOLOČNOSTI

Soitron patrí k popredným nadnárodným technologickým spoločnostiam so zameraním na dodávky technologickej infraštruktúry, sieťových služieb a outsourcingu. Firma so slovenskými koreňmi a pobočkami v šiestich krajinách, ktorá je partnerom Flowmon Networks, prostredníctvom svojho dohľadového centra dlhodobo dozerá na prevádzku hardvéru popredných podnikov aj organizácií verejnej správy.