Zákazníci SWANu majú k dispozícii špičkovú ochranu proti internetovým útokom a podrobný prehľad o prevádzke svojich sietí. Nie je to tak dávno, čo predstavitelia niektorých bánk výpadok internetového bankovníctva zľahčovali tvrdením, že klienti v takom prípade nemajú problém urobiť potrebné transakcie osobne na pobočke. Dnes je táto doba nenávratne preč.

Obor činnosti

Poskytovateľ internetového pripojenia

Výzvy

Rozšírením ponuky služieb s pridanou hodnotou prispieť k upevneniu popredného postavenia na trhu ISP

Zaistenie ochrany zákazníkov pred rozličnými typmi DDoS útokov

Poskytnúť viaceré úrovne služieb od potrieb zákazníka

Prínosy riešenia

Jednotný nástroj pre monitorovanie a analýzu prevádzky internej ISP siete, peeringových a tranzitných liniek

Multitenantný prístup dovoľuje implementovanie bezpečnosti ako služby (SaaS)

Natívna integrácia s riešením F5 prináša automatizáciu pri mitigácii DDoS útokov

Nasadené produkty

Flowmon Collector

Flowmon DDoS Defender

F5 BIG IP AFM

VÝCHODISKÁ

Banky, internetoví obchodníci, mediálne spoločnosti, aj verejná správa a organizácie z mnohých iných odvetví si uvedomujú, že znefunkčnenie internetového pripojenia môže v dnešnej digitálnej dobe priniesť rozsiahle škody.

Nie je ťažké predstaviť si, čo znamená odstavenie webu kybernetickým útokom typu DDoS pre veľký e-shop, ktorý v najsilnejšom predajnom období vybaví desiatky tisíc objednávok denne. Rizikom však nie sú len priame finančné straty – výpadok môže priniesť aj iné nepríjemnosti, napríklad poškodiť reputáciu značky či lojalitu zákazníkov.

SWAN je druhým najväčším poskytovateľom telekomunikačných služieb pre korporátnych zákazníkov na Slovensku, preto neprekvapuje, že sa v posledných rokoch podnikoví zákazníci čoraz častejšie pýtali na možnosti lepšie zabezpečiť svoju infraštruktúru pred rastúcimi hrozbami, ale tiež na zvýšenie viditeľnosti do siete, aby mohli identifikovať rozličné anomálie či technické problémy a zefektívniť jej prevádzku.

S dovtedy používanými technológiami síce operátor, ktorý vznikol spojením dvoch dlhoročných stabilných hráčov na slovenskom telekomunikačnom trhu SWAN a BENESTRA, vedel DDoS útoky detegovať, ale jeho možnosti chrániť klientov boli veľmi obmedzené. A doplnkové služby, ako je prehľad o sieťovej prevádzke zákazníka s možnosťou identifikácie iných bezpečnostných rizík, nedokázal poskytovať vôbec.

Augustín Revák, CTO , SWAN:

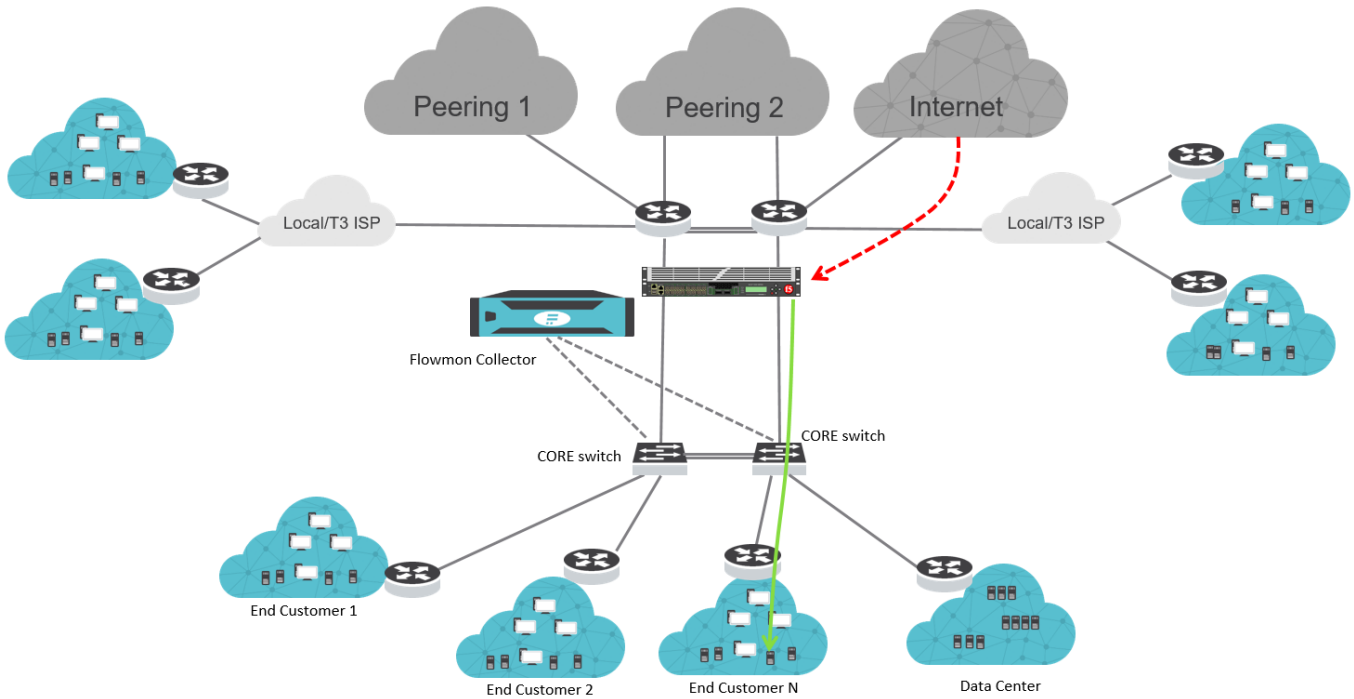
„Keďže internetové pripojenie je dnes komodita, SWAN tiež hľadá neustále spôsoby, ako okrem konektivity ponúknuť zákazníkom doplnkové služby s pridanou hodnotou, ktoré zvýšia lojalitu a umožnia dostať naše riešenia medzi ešte väčšie množstvo zákazníkov. Vďaka tomu vieme ponúknuť pokročilú ochranu sieťovej prevádzky nie len top hráčom na trhu ale aj stredne veľkým firmám, ktoré tiež potrebujú možnosť odhaľovať bezpečnostné riziká a odrážať DDoS útoky."

RIEŠENIE

Operátor preto začal vyvíjať nový typ služby, ktorá by organizáciám umožnila jednoducho monitorovať dátové toky v rámci internetovej konektivity, analyzovať správanie siete a chrániť sa pred nebezpečnými DDoS útokmi. Tie spôsobujú zahltenie infraštruktúry do takej miery, že spomalia alebo úplné znefunkčnia web, server či dátové pripojenie.

SWAN sa pri vývoji riešenia rozhodol využiť technológie spoločností Flowmon Networks a F5 Networks, ktoré v oblastiach monitoringu a analýzy sieťovej prevádzky, ako aj zabezpečenia pred kybernetickými hrozbami, poskytujú optimálny pomer ceny a hodnoty. Flowmon kolektor zbiera a ukladá štatistiky o sieťovej prevádzke a vďaka pokročilej analýze chránených segmentov zabezpečuje rýchlu detekciu DDoS útokov. Využíva k tomu štatistiky o sieťovej prevádzke (IPFIX/NetFlow), ktoré odhaľujú, kto a ako využíva sieťové služby. Ak Flowmon odhalí DDoS útok, zaistí konfiguráciu BIG IP AFM spoločnosti F5 pre jeho mitigáciu. Zároveň informuje smerovače v sieti, že prevádzka pre daný chránený segment má byť presmerovaná do mitigačného zariadenia F5, ktoré sa aj vďaka včasnej konfigurácii okamžite postará o vyčistenie útoku. Znamená to, že chybný obsah sa zahodí a zákazník dostane len legitímny obsah. Keď Flowmon identifikuje koniec útoku, zaistí návrat do pôvodného stavu a vymaže konfiguráciu zo zariadenia F5. Počas niekoľkomesačného projektu bolo potrebné odviesť množstvo integračnej práce, prispôsobovať technológie zo strany dodávateľov a optimalizovať celý koncept tak, aby vyhovel prísnym nárokom zákazníkov a umožnil vybrať každému z nich vyhovujúcu úroveň služby.

„Na začiatku vývoja služby neexistovali natívne možnosti prepojenia technológií Flowmon a F5. Obaja dodávatelia robili postupne aj na základe tohto projektu v produktoch úpravy, ktoré dnes môžu využívať zákazníci po celom svete,“ hovorí Augustín Revák zo spoločnosti SWAN.



Architektúra riešenia

Výsledkom náročného projektu je nová služba Network Control, ktorá umožňuje zákazníkom spoločnosti SWAN podrobne monitorovať ich sieť, identifikovať bezpečnostné hrozby a odrážať kybernetické útoky, ktoré tradičné ochranné prostriedky ako sú firewall či antivírus nezastavia.

Služba je dostupná v troch úrovniach, pričom po štyroch mesiacoch od spustenia ju už využívali dve desiatky zákazníkov operátora z rozličných odvetví – od bankovníctva, cez mediálne spoločnosti, až po verejné inštitúcie. Samozrejme, riešenie používa pre účely ochrany a monitoringu aj samotný SWAN.

Úrovne služby

- **Basic** – základná úroveň služby ponúka sieťový monitoring, detekciu DDoS útokov, reporting, automatické upozornenia a služby dohľadového centra. V prípade útoku je možná jednoduchá mitigácia pomocou metódy RTBH (Remotely Triggered Black Hole), ktorá celú komunikáciu na zákazníka zahodí a tým ochráni jeho infraštruktúry pred zahltením.
- **Standard** – táto úroveň služby využíva BGP Flowspec a dynamickú signatúru útoku, pomocou ktorej špecifikuje chybnú komunikáciu a inštruuje smerovače, aby ju „zahodili“. Zákazník tak nepríde o prevádzku, ktorá nezodpovedala dynamickej signatúre útoku. Dynamická signatúra je navyše priebežne aktualizovaná, aby upravila mitigačnú stratégiu v prípade zmeny charakteristiky útoku.
- **Profi** – pokročilá úroveň ochrany kombinuje BGP Flowspec prístup na presmerovanie inkriminovanej komunikácie pre precízne vyčistenie pomocou F5 BIG IP AFM. Vďaka natívnej integrácii medzi Flowmon Networks a F5 Networks umožňuje v prípade útoku plnú automatizáciu vrátane automatickej konfigurácie mitigačného zariadenia pre okamžité vyčistenie útoku.

„*Na Slovensku síce nie sme jediný operátor, ktorý dokáže poskytovať ochranu voči DDoS útokom, Network Control sa však vyznačuje mimoriadnou flexibilitou a klientom tiež prináša vyššiu pridanú hodnotu v podobe monitoringu tokov dát, čiže detailnú viditeľnosť toho, čo sa v sieti deje. To výrazne uľahčuje prácu našim expertom pre dohľad nad poskytovanými sieťovými službami, ako aj bezpečnostnému oddeleniu,*“ konštatuje A. Revák zo SWANu

Network Control je všestranná a cenovo dostupná služba, určená verejným organizáciám a prakticky každej firme, pre ktorú je dôležitá dostupnosť webu a služieb poskytovaných zákazníkom cez internet. K cieľovej skupine patria napríklad aj menší lokálni poskytovatelia internetu.

„*Služby od spoločnosti SWAN využívame dlhodobo a sme veľmi radi, že môžeme v súčasnosti využívať i vylepšenú službu pre ochranu voči DDoS útokom, keďže ako finančná inštitúcia poskytujeme našim klientom služby s vysokou pridanou hodnotou a dôraz na bezpečnosť je z tohto pohľadu prvoradá*,“ dodáva Chief Security Officer Slovenskej Sporiteľne Ján Adamovský

SWAN vo svojej sieti vďaka nasadeným technológiám zaznamenáva bežne niekoľko závažných útokov denne. Pri špecifických udalostiach, ako sú napríklad voľby alebo významné športové podujatie, intenzita mnohonásobne narastá.

„*Ochrana sietí bude pre organizácie v súvislosti s pribúdajúcimi sofistikovanými hrozbami, ale aj čoraz prísnejšou legislatívou, v budúcnosti čoraz naliehavejšia,*“ hovorí Roman Čupka, country manažér Flowmon Networks na Slovensku a konzultant pre región CEE.

Prirodzene, s rastúcim dopytom porastú aj príjmy operátora zo služby Network Control, hoci Augustín Revák upozorňuje, že hlavným očakávaním nie je ani tak významný prírastok výnosov, ale nadštandardná služba, ktorá presvedčí zákazníkov k dlhodobej spolupráci práve so SWANom.

Zákazníci na službe oceňujú nielen vyššiu ochranu proti kybernetickým útokom, ale aj možnosť získať lepšiu viditeľnosť do vlastnej siete, ktorú zabezpečujú technológie Flowmon. „*Vďaka lepšej viditeľnosti má zákazník úplný prehľad o tom, čo sa v jeho sieti deje. Môže diagnostikovať dôvody preťaženia, neštandardné správanie aplikácií, alebo nadmerné sťahovanie dát,*“ dodáva R. Čupka.

Na základe analýzy prevádzky v sieti vie potom zákazník podniknúť opatrenia, ktoré povedú k efektívnejšiemu využitiu sieťových zdrojov. Cez službu Managed Security, ktorú SWAN svojím zákazníkom poskytuje, dokáže napríklad regulovať prístup k niektorým aplikáciám či internetovým službám, ktoré nadmerne zaťažujú sieť a prípadne tým ušetriť prostriedky na upgrade kapacity linky.

Michal Kaprinay, Operational Infrastructure Manager, Národná agentúra pre sieťové a elektronické služby, (National Agency for Network and Electronic Services) hodnotí službu ochrany pred DDoS útokmi takto:

“*V minulosti sme pre DDoS ochranu používali interné nástroje a kapacity, ktoré ale nebolo možné využiť pri sofistikovanejších volumetrických DDoS útokoch. SWAN nám umožnil službou Network Control identifikovať a odrážať útoky veľmi efektívne pri šetrení našich interných kapacít. Okrem toho máme prístup k reálnemu prostrediu pre viditeľnosť do siete rozšírenú o analýzy pre troubleshooting prevádzkovo-bezpečnostných problémov na sieti. Zefektívnili sme tak manažment nášho prostredia, ktoré poskytuje kritické služby ďalším organizáciám.*”

BUDÚCNOSŤ

Na základe dopytov zákazníkov SWAN už v súčasnosti pracuje na rozšírení služby Network Control o doplnkovú funkcionalitu založenú na systéme Flowmon ADS pre detekciu anomálií a podozrivého správania siete na základe behaviorálnych analýz.

Zákazníkom rozšírenie prinesie ešte podrobnejší pohľad do siete a umožní odhaliť aj veľmi špecifické a doteraz neznáme hrozby, napríklad vďaka identifikácií paketov, ktoré by sa v sieti vôbec nemali nachádzať, alebo prenosov dát, ktoré by vôbec nemali byť prenášané. Flowmon ADS zároveň vnáša do procesu identifikácie sieťových problémov viac inteligencie aj automatizácie, čo uľahčuje život administrátorom, ale aj klientom.

O SWAN

Telekomunikačný operátor SWAN poskytuje elektronické služby od roku 2000. Vybudoval vlastnú optickú sieť s európskymi parametrami a je najväčším čisto slovenským telekomunikačným operátorom a druhým najväčším poskytovateľom telekomunikačných služieb pre korporátnych zákazníkov na Slovensku. V roku 2018 sa SWAN spojil s celonárodným telekomunikačným operátorom BENESTRA, ktorý pôsobil na trhu od roku 1999. Vznikol tak operátor s rozsiahlou vlastnou infraštruktúrou a komplexným spektrom služieb a s ponukou najlepšej a najstabilnejšej národnej a medzinárodnej konektivity. www.swan.sk