Řešení pro monitoring síťového provozu na portálu Seznam.cz

Je možné mít dostatečný přehled o fungování sítě, v níž „tečou“ obrovské objemy dat, a nic neopomenout? Jak optimálně sladit provozní a bezpečnostní aspekty?

Fungování společnosti Seznam.cz včetně veškerých služeb poskytovaných internetovým uživatelům v současnosti zajišťují dvě datová centra s několika tisíci servery. Každé datové centrum je k internetu připojeno rychlostí 60 Gb/s. Je zřejmé, že správné fungování obou datových center včetně funkčního připojení k internetu je pro firmu vhledem k jejímu zaměření a rozsahu nabízených služeb zcela zásadní. Proto jsou tak důležité faktory propustnosti, spolehlivosti nebo ochrany proti útokům. V logice věci pak je efektivní monitorování datových toků a analýzy chování sítě poskytující detailní přehled o síťových komunikacích a umožňující automatickou detekci případných anomálií a hrozeb v síti. Při takovém objemu provozu a datových toků se rozhodně nejedná o triviální úkol.

Výchozí situace

Zákazník původně prováděl monitoring své sítě poměrně jednoduchými nástroji. Pracovníci odpovědní za provoz sítě monitorovali síťové přepínače a porty, vytvářeli si k tomu různé grafy apod. Opakovaně však naráželi na problém, jak ve vysokorychlostní síti získaná data zpracovat a dlouhodobě uchovat pro zpětnou analýzu.

Když se začali zabývat možností výběru řešení pro pokročilý monitoring síťového provozu, základním zadáním bylo, aby řešení dokázalo vytvářet grafy na základě různých filtrů, např. podle IP adres, portů, protokolů, a vytvářet tak grafickou prezentaci toho, co se v síti z provozního pohledu děje. Chtěli mít také možnost dohledávat výpisy síťové komunikace až dva týdny zpětně. To je v případě tak intenzivního provozu náročná úloha – dat je obrovské množství a z toho vyplývá požadavek na zpracování minimálně 20 Gb/s síťového provozu. Kromě této „provozní“ části (grafy, pohled do sítě, přehled o tom, co se v ní děje) chtěl mít zákazník možnost automatické analýzy a odhalování anomálií nebo útoků zvenčí – to byla druhá, „bezpečnostní“ část projektu.

Hlavní požadavky:

- dlouhodobé uchovávání informací o komunikaci v síťovém provozu,
- analýza o zobrazování informací ve formě rozličných výstupů (přehledové a koláčové grafy, tabulky, reporty, detailní výpisy komunikací apod.),
- detekce nežádoucích stavů, anomálií či přímo útoků.

Zákazník se v zásadě rozhodoval mezi dvěma typy možného řešení. Jedním byla paketová analýza, tj. pohled do celého provozu. Pozitivem je možnost sledovat síť kompletně až do obsahu paketů, resp. obsahu komunikace. Tímto způsobem lze hledat určité signatury útoků nebo zakázaných aplikací včetně možnosti paketovou komunikaci uchovávat. Vzhledem k tomu, jak rozsáhlou má Seznam.cz síť, si posléze vyhodnotil, že takové řešení by bylo extrémně drahé.

Proto byla zvolena druhá cesta – inspekce síťových toků, kdy provoz sítě není reprezentován celými pakety, ale jen

záznamy o komunikaci (IP adresa, port-port a k tomu informace o přenesených paketech, bytech atd.). Každá taková komunikace se vejde do jednoho záznamu, a tak i zpracování, ať už z pohledu uložení dat nebo vyhodnocování, je podstatně méně náročné na hardware. Řešení může být výrazně levnější a pro potřeby monitoringu dobře škálovatelné.

Zvolené řešení

Jako nejvhodnější bylo zvoleno řešení FlowMon firmy INVEA-TECH. V případě této české společnosti zákazník ocenil kromě podobné firemní filozofie i skutečnost, že vyvíjí hardware i software a její produkty patří mezi absolutní špičku v NetFlow segmentu. Seznam.cz rovněž kvituje možnost komunikovat se specialisty INVEA-TECH přímo – reakce na požadavky zákazníka je mnohem rychlejší, než kdyby se jednalo např. o velkého zahraničního výrobce s obvykle ročními cykly vývoje softwaru. Požadavky jsou do řešení zapracovány promptně, ať už jde o drobné „vady na kráse“ nebo rozvoj funkčnosti včetně nápadů, co by se dalo zlepšit či optimalizovat.

Nasazené produkty společnosti INVEA-TECH:

- FlowMon sonda
- FlowMon kolektor
- FlowMon ADS

V první fázi projektu byla nasazena výkonná autonomní FlowMon sonda, která je zapojena prostřednictvím pasivních rozbočovačů (splitterů) mezi firewall a load balancer. Sonda sbírá data ze dvou optických 10 gigabitových linek a posílá je k uložení na FlowMon kolektor, jehož součástí je i systém FlowMon ADS – ten veškerá data analyzuje. Celková úložná kapacita kolektoru je 24 TB a umožňuje analýzu kompletních dat až několik měsíců zpětně. Statistické informace a reporty jsou dostupné i v řádu let. Systém FlowMon ADS neboli modul automatické detekce anomálií upozorňuje na každou podezřelou síťovou událost, sleduje např. zřetelné anomálie – skenování, DDOS útoky i různé další typy podivných síťových spojení, jež mohou znamenat provozní problémy nebo třeba pokus o útok, který lze v síťové vrstvě odhalit.

Volba uvedených produktů byla vcelku jednoznačná: FlowMon sonda díky svým technickým vlastnostem prakticky nemá na českém trhu konkurenci, navíc se vyznačuje výhodným poměrem cena/výkon. FlowMon kolektor byl vybrán ten nejvýkonnější, který výrobce nabízí, s ohledem na velikost sítě zákazníka a jeho požadavky týkající se uchovávání dat (min. 14 dní) v řádu x TB včetně dostatečného procesorového výkonu a paměti počítače (serveru) pro zpracování všech statistik. Součástí FlowMon kolektoru je standardně modul pro provozní monitoring sítě, zatímco funkcionalitu bezpečnostního monitoringu zajišťuje dodatečný plug-in FlowMon ADS, který byl na základě požadavku zákazníka v tomto řešení samozřejmě zahrnut.

Nasazení

Před vlastní implementací se uskutečnilo testovací nasazení navrženého řešení, tzv. proof of concept. Dostatečně průkazně se vyzkoušelo, že sonda i celé řešení vyhovují požadavkům zákazníka. Na základě toho se Seznam.cz definitivně rozhodl, že si pořídí uvedenou sondu a výkonný kolektor, aby mohl dostatečně dlouho uchovávat data, zpětně je zpracovávat, vyhledávat v nich atd. Samotná implementace byla poměrně rychlá. Trvala tři dny: první den zabrala příprava hardwaru a softwaru, druhý den zprovoznění a třetí den konfigurace modulu detekce anomálií včetně zaškolení administrátorů.

Počet datových toků, které směřují na kolektor, činí ve špičkách 100 až 120 tisíc za sekundu. Jde o enormní zátěž, jež nemá v Česku ekvivalent. Vzhledem k vysokému objemu provozu se v rámci použitého řešení využívá vzorkování (sampling), tedy nezpracovává se každý datový tok, ale podle stanovených kritérií jsou vybrány toky, které se systémem FlowMon ADS zpracovávají/analyzují. Do budoucna se zvažuje, jak toto vzorkování snížit a zpracovávat vyšší podíl datových toků.

Jak již bylo uvedeno, Seznam.cz má v současnosti dvě datová centra. Výše popsáno je nasazení pro jedno datové centrum. V následujícím kroku, a tedy v další části projektu, se realizovalo nasazení pro druhé z nich. V něm není použita sonda, ale data se sbírají z aktivního síťového prvku. I zde je však nasazen kolektor včetně modulu detekce anomálií podobně jako v prvním datovém centru. Cílem je v obou případech sledovat veškerý příchozí provoz na portálu Seznam.cz včetně všech dalších portálů a služeb poskytovaných uživatelům (Firmy.cz, Lidé.cz, Mapy.cz, videa, e-mailová pošta apod.).

Přínosy řešení

Mezi hlavní přínosy zvoleného a následně implementovaného řešení z pohledu provozních i bezpečnostních aspektů patří:

- komplexní přehled o komunikacích a využití jednotlivých portálů a služeb,
- možnost „vidět“ do sítě,
- detekce anomálií a útoků,
- získání podkladů pro optimalizaci poskytovaných služeb.

Příklady odhalených útoků a anomálií BOX 1

- Modul FlowMon ADS odhalil ICMP flood, který zahlcoval síť. Jednalo se o špatnou konfiguraci, kdy si v cizí síti ověřovali dostupnost internetu pravidelným pingem na portál www.seznam.cz, nicméně v důsledku špatné konfigurace došlo k chování odpovídajícímu útoku ICMP flood.
- Modul FlowMon ADS pravidelně odhaluje útočníky pokoušející se o kompromitaci veřejně dostupných webů (firmy.cz, lide.cz).

Zákazník díky nasazenému řešení již odhalil různé typy útoků zvnějšku (viz Box 1) nebo interních anomálií, které byly způsobeny např. nevhodnou konfigurací některých částí sítě. V praxi se potvrdil obecný princip, že síť lze optimalizovat či rozvíjet teprve tehdy, je-li možné sledovat, co v ní reálně „teče" a jaké je její rozdělení z pohledu služeb, aplikací nebo jednotlivých serverových skupin. Když síťový administrátor může sledovat, jak postupně narůstá síťový provoz, nakolik se mění v určitých dnech či měsících, pak dokáže úspěšně predikovat, kdy bude potřeba posílit infrastrukturu, a může tak účinněji plánovat využití kapacit sítě. Jindy naopak díky detailnímu pohledu zjistí, že např. určitá špatná konfigurace způsobuje zbytečný provoz a zahlcení sítě. Následně pak může komunikační infrastrukturu (resp. její příslušnou část) odladit a fyzické posílení kapacity sítě v tomto případě není nutné.

Tomáš Dedek
tomas.dedek@iseco.cz

Eva Neduchal Podskalská
eva.neduchal@iseco.cz

Ing. Tomáš Dedek

Vystudoval technickou kybernetiku na ČVUT, řídil implementační projekty pro velké finanční instituce, pojišťovny, automobilový průmysl i státní sektor. Dnes působí jako senior konzultant a technický ředitel ve společnost ISECO.CZ.

Eva Neduchal Podskalská

Řídila collections v oblasti interních podvodů ve společnosti Provident Financial, poté byla členkou týmu řízení rizik v GE, věnovala se rozvoji obchodu a vedla marketing v české pobočce společnosti Bull. V současné době působí ve společnosti ISECO.CZ.

Gartner: Ochota vrcholových managementů investovat do IT bezpečnosti se zvyšuje

Asi 40 % velkých společností bude mít do roku 2018 formální plány pro případ, že by agresivní kyberútoky přerušily jejich činnost. V současné době nemá takové plány téměř nikdo. Změna souvisí s postojem vrcholových managementů, které se tímto tématem zabývají stále častěji, a to navzdory tomu, že reálně k takovým útokům dochází jen zřídka. Manažeři si totiž uvědomují rostoucí závislost svých organizací na informačních technologiích a s tím i to, že výpadek fungování organizace by byl mnohem delší než v minulosti. Uvádí se to ve studii, kterou na začátku letošního roku zveřejnila společnost Gartner.

Podle analytiků Gartner se změnilo především to, že i zaměstnanci v terénu přistupují prostřednictvím svých mobilních zařízení k informačním systémům a jsou na nich závislí. Navíc se stále více prosazuje internet věcí. Případný útok by tedy zasáhl daleko více zdrojů. Při posuzování následků je ovšem zapotřebí vnímat nejen škody na těch zdrojích, ale také dopady na podnikové procesy a na produkty či služby produkované organizací. Digitální byznys zpravidla počítá s tím, že veškeré informační zdroje a zařízení připojená k internetu jsou neustále dostupná. Výpadek kterékoliv části řetězce pak může přerušit celou transakci či proces, což bude mít okamžitý dopad na zákazníky, tvrdí Gartner.

Jedním z očekávaných důsledků je to, že bezpečnostní programy dostanou mnohem vyspělejší podobu. Manažeři informační bezpečnosti a kontinuity činnosti budou moci počítat s větší podporou vrcholových managementů, bude však na ně vyvíjen větší tlak, aby měli jasně připravená opatření, formalizované plány a přehledné reporty. Fakticky se jedná o plynulé pokračování trendu, který Gartner sleduje již od roku 2012, ale který zesílil s mobilitou a internetem věcí. Jak z výzkumu vyplývá, vrcholové managementy dnes vidí jasné důvody, proč investovat do počítačové bezpečnosti a proč přistupovat ke kybernetickým rizikům proaktivně. (ph)