exe, a.s.
Slávičie údolie 6, 811 02 Bratislava
Tel.: 02 - 67 296 111, Fax: 02 - 67 296 666
www.exe.sk

Sieťové riešenie FlowMon v SPF

Pomáha okamžite odhaliť neoprávnené používanie siete

Situácia

Existujúci koncept bezpečnosti spolieha na bezpečný perimeter a rozdelenie prevádzky do samostatných virtuálnych LAN sietí v rámci fyzickej a virtuálnej infraštruktúry. Kompletnú firemnú sieť Slovenského pozemkového fondu tvorí jedno hlavné dátové centrum v sídle spoločnosti, záložné dátové centrum u poskytovateľa konektivity a MPLS sieť pokrývajúca do 30 lokalít v rámci SR. Na dátovej sieti organizácie sú prevádzkované služby slúžiace pracovníkom SPF - autentifikácia používateľov, intranetový portál, elektronická pošta, desktopová virtualizácia, dochádzkový systém, účtovníctvo, rôzne evidenčné a ekonomické systémy, systémy na spracovanie zmlúv a iných dokumentov, GIS, súborové a tlačové služby. Prevádzka týchto sietí však nie je detailne sledovaná a vyhodnocovaná na bezpečnostné hrozby. Monitoring sieťovej prevádzky je riešený iba z hľadiska vyťaženosti jednotlivých aktívnych sieťových prvkov.

Obchodné ciele

Prevádzka LAN / WAN siete si pri nasadzovaní a rozširovaní infraštruktúry vyžadovala efektívnejšie identifikovať anomálie a nežiaduce toky dát v sieti. Nasadzovaním množstva nových technológií v infraštruktúre SPF nebolo možné rýchlo reagovať na všetky konfiguračné požiadavky. SPF požadovalo zvýšiť bezpečnosť v LAN / WAN sieti a rýchlo odhaľovať možné hrozby. Taktiež množstvo nežiaducich aplikácií vyťažovalo prevádzku LAN / WAN siete a z pohľadu funkcie organizácie bola potreba zaviesť elimináciu zdieľania obsahu.

Prehľad riešenia:

Krajina
Slovenská republika

Odvetvie
právnická osoba, koná vo verejnom záujme.

Profil zákazníka
Slovenský pozemkový fond (SPF) je neštátna a nezisková organizácia zriadená zákonom č. 330/1991 Zb. o pozemkových úpravách, usporiadaní pozemkového vlastníctva, obvodných pozemkových úradoch, pozemkovom fonde a pozemkových spoločenstvách v znení neskorších predpisov.

SPF spravuje poľnohospodárske nehnuteľnosti vo vlastníctve SR a podiely spoločnej nehnuteľnosti vo vlastníctve SR a nakladá s poľnohospodárskymi pozemkami, ktorých vlastník nie je známy s podielmi spoločnej nehnuteľnosti, ktorých vlastník nie je známy. SPF môže nehnuteľnosti vo svojej správe a nakladaní okrem iného prenajímať, predávať (previesť

exe, a.s.
Slávičie údolie 6, 811 02 Bratislava
Tel.: 02 - 67 296 111, Fax: 02 - 67 296 666
www.exe.sk

Pre budúci rozvoj a efektivitu rozširovania infraštruktúry je potrebné mať nástroj na meranie využívania jednotlivých služieb. V neposlednom rade, SPF vyžaduje priebežne optimalizovať konfiguráciu LAN / WAN siete a aktívnych sieťových zariadení

Výzvy

- rozsiahla dátová sieť s viac ako 300 počítačmi vo viacerých lokalitách
- bezpečný perimeter, ale chýbajúci bezpečnostný monitoring prevádzky v rámci internej dátovej siete
- problematické vyhľadávanie a preukazovanie problémov a oprávnených prístupov vo firemnej sieti
- monitoring prístupu na zdroje LAN

Riešenie

Požiadavka SPF bola riešená v prvom rade ako jednorazový audit LAN / WAN siete za pomoci nasadenia 4-portovej sondy FlowMon Probe 4000, ktorá bola zapojená do centrálneho prepínača datacentra SPF. Zákazníkovi bola ako súčasť finálneho riešenia odporučená sonda FlowMon Probe 20000 s dvomi 10 Gb monitorovacími portami. Každý port bol napojený do jedného z dvoch centrálnych prepínačov. Na nich bolo nastavené zrkadlenie všetkej sieťovej prevádzky vstupujúcej do centrálnych prepínačov. Ako súčasť sondy sme implementovali aj voliteľný modul ADS (Anomaly Detection System), ktorý skúma správanie siete a hľadá potenciálne hrozby a anomálie, ktoré môžu ohroziť alebo obmedziť sieťovú prevádzku.

Hlavné prínosy riešenia

- Odhalenie neoprávneného používania firemnej siete
- Odhalenie potenciálne infikovaných pracovných staníc malwarom
- Odhalenie zariadení v sieti, ktoré nie sú v evidencii a ktoré môžu predstavovať potencionálnu bezpečnostnú hrozbu
- Identifikácia zariadení v sieti, ktoré majú nesprávne nastavené sieťové nastavenia (napr. DNS, NTP, SMTP...)

Citát

„Riešenie FlowMon nám poskytuje okamžitý prehľad o aktuálnej situácii v sieti ako aj možnosť dohľadať minulé udalosti. Zvolená technológia si poradí aj s bezpečnostnými hrozbami, ktoré ešte nie sú dostatočne známe. Vďaka rýchlemu zaškoleniu obsluhy a bezproblémovej implementácie môžeme využívať potenciál tejto technológie v plnom rozsahu vo veľmi krátkom čase.“

Roderik Plevka, SPF

Produkty a technológie

- FlowMon Probe 20000 SFP+
- FlowMon ADS Standard

vlastníctvo), zriadiť na ne vecné bremeno alebo uspokojiť nimi reštitučné nároky. Okrem toho SPF k nehnuteľnostiam v správe a nakladaní vydáva stanoviská k územným konaniam, k stavebným konaniam, k zmene druhu pozemku a k vydržaniu vlastníckeho práva.

Veľkosť spoločnosti

Počet PC – 306 ks
Počet serverov – 60 ~ 70 ks

Východisková situácia

Firemnú sieť SPF tvorí jedno hlavné dátové centrum v sídle spoločnosti, záložné dátové centrum u poskytovateľa konektivity a MPLS sieť pokrývajúca do 30 lokalít v rámci SR.

Riešenie

Prvá fáza riešenia bol jednorazový audit LAN / WAN siete. Ďalšia fáza bolo zapojenie a konfigurácia sondy FlowMon Probe 20000 s dvomi 10 Gb monitorovacími portami. Taktiež bol implementovaný modul ADS, ktorý skúma správanie siete a hľadá potenciálne hrozby a anomálie.

Profil partnera

exe, a.s. poskytuje od roku 1990 služby a riešenia v oblasti informačných technológií zákazníkom na troch kontinentoch. Zaoberá sa vývojom softvéru, projektovaním a implementáciou informačných systémov, lokalizáciou a globalizáciou softvéru a outsourcingovou podporou infraštruktúry. Je držiteľom certifikátov ISO 9001:2008, EN 15038, Microsoft Gold Certified Partner a mnohých ďalších.

Kontakty

Slovenský pozemkový fond
Búdková 36
Bratislava 817 15
Tel.: 02 - 20 941 111
www.pozfond.sk

exe, a.s.
Slávičie údolie 6
811 02 Bratislava
Tel.: 02 - 67 296 111
Fax: 02 - 67 296 666
www.exe.sk