

Check Point

Naše veřejnost Vás zná jako dlouholetého country managera Nortel Networks. Co Vás přimělo po tolika letech opustit svět networkingu a pustit se do světa bezpečnosti?

Nortel je firma známá především jako dodavatel telekomunikačních a síťových řešení pro podniky a telekomunikační operátory. Během osmi let, po které jsem v Nortelu působil, jsem vnímal jak problematika bezpečnosti stále více penetruje do všech oblastí IT a telekomunikací. V okamžiku, kdy jsem začal uvažovat o možné změně mého dalšího působení, byla pro mě oblast bezpečnosti rozhodně velmi zajímavá.

Bezesporu se jedná o velmi perspektivní a dynamicky se rozvíjející prostředí, ve kterém je Check Point vnímán jako celosvětově uznávaný lídr jak z pohledu tržního podílu, tak i technologických inovací. To se týká především trhu VPN a korporátních firewallů, kde firma zaujímá 1. místo s 32% podílem na světovém trhu. Takže v okamžiku, kdy se objevila příležitost pracovat pro Check Point, nebylo rozhodování příliš těžké.

Snad každý IT odborník zná pojem „Check Point firewall“. Ne každý však ví, že Check Point je rovněž dodavatelem řady dalších řešení integrujících více aspektů síťové bezpečnosti. Je vůbec možné v krátkosti popsat celý rozsah produktového portfolia Check Pointu?

Obecně Check Point nabízí v rámci produktové řady NGX širokou škálu bezpečnostních řešení pro ochranu perimetru sítě, vnitřních sítí, webových aplikací, i koncových bodů v síti. Naše řešení chrání jak online komunikaci s externím světem, tak interní informace v podnikových sítích, pobočkách, partnerských extranetech a u vzdálených pracovníků.

Zásadním bezpečnostním prvkem pro zajištění bezpečnosti dat z naší nabídky je rodina produktů „VPN-1“ pro ochranu perimetru sítě před útoky zevnějšku. Mnohé společnosti, zejména finanční ústavy jdou ve snaze zabezpečit údaje svých klientů dál a z naší nabídky využívají např. produkt „Integrity Clientless Security“. Tento systém kontroluje, zda lidé, kteří se připojují k bankovnímu účtu nebo objednávají zboží, používají bezpečný počítač. Pokud jejich systém nesplňuje stanovené podmínky, nelze se ke službě přihlásit. V zásadě tak banky mohou přenést zodpovědnost tam, kam potřebují – na koncového uživatele.

Větší rizika však představují útoky, které přicházejí zevnitř, v případech, kdy zaměstnanec přinese např. na nezabezpečeném notebooku nebo PDA škodlivý software do podnikového prostředí a tím tak doslova obejde firewall. Abychom mohli dosáhnout efektivní bezpečnosti potřebujeme dvě věci. Tou první je moderní firewall, který dokáže rychle reagovat na nové hrozby. Musí být schopen rozpoznávat potenciálně nebezpečný software i jednotlivé datové pakety nejen podle vzorků známých hrozeb, ale i podle charakteristik jejich chování. A tou druhou jsou nástroje, které dokáží vynutit dodržování bezpečnostních pravidel na všech zařízeních v podnikové síti. To znamená, že se k datům dostanou pouze ta zařízení, která mají nainstalován aktuální SW, aktualizovaný antivir a antispyware. Pokud nebudou využívány oba dva prvky zabezpečení, není třeba utrácet ani za firewall - škodlivý software se do firmy dostane zevnitř a firewall tak bude k ničemu. Z tohoto důvodu pokládáme za velmi důležitou součást celkové bezpečnostní koncepce naše řešení „Integrity“, které nabízí kontrolu jak nad perimetrem, tak i koncovými stanicemi.

V neposlední řadě stojí za zmínku také naše produktová řada „ZoneAlarm“, která je jednou z nejrespektovanějších značek pro ochranu koncových bodů sítě, a která dnes chrání milióny počítačů proti hackerům, spyware a proti zcizení dat.

Efektivitu nasazení řešení Check Point navíc zvyšuje Open Platform for Security (OPSEC), což je oborový technologický rámec a sdružení, které Check Point založil v druhé polovině devadesátých let. OPSEC si klade za cíl integraci a interoperabilitu nejlepších řešení od stovek předních světových výrobců.

Check Point nenabízí jen bezpečnostní produkty, ale i služby pro koncové uživatele. Jak byste tyto služby charakterizoval a jak na ně může náš podnikový uživatel takřkajíc „dosáhnout“?

Check Point nabízí několik různých druhů služeb, které jsou našim zákazníkům dostupné prostřednictvím sítě našich autorizovaných partnerů. Jednak jsou to pochopitelně služby spojené s produktovou podporou, skrze které se snažíme, aby naši zákazníci měli vždy a všude okamžitý přístup k informacím či přímé podpoře. Dále máme k dispozici dedikovaný tým „Professional Services“, který zajišťuje hladkost celého průběhu implementace našich řešení - od analýzy, projektování, přes implementaci až po upgradu. Samořejmostí jsou školení, certifikace, různé druhy notifikací či program Early Availability.

Z hlediska přidané hodnoty k našim produktům jsou ale velmi důležité „SmartDefense Services“, což je v podstatě neustálý proud nejen aktualizací, ale též konfiguračních návodů a rad pro správce našich produktů, reagující na aktuální hrozby. Odstup mezi zveřejněním informace o bezpečnostním problému a prvním výskytem jeho zneužití se neustále zkracuje - dříve šlo o měsíce, dnes se ale jedná spíše o dny nebo hodiny. To nedává dostatek prostoru pro vytvoření a distribuci nových definičních souborů. Proto roste důležitost systémů, které dokáží analyzovat chování aplikací a síťového provozu a odhalit tak i nové hrozby.

Zkusím to vysvětlit na příkladu: ve chvíli, kdy se objevil „Slammer“, nebyl na tento rychle se šířící typ útoku nikdo připraven, ale poučili jsme se! Po „Slammeru“ přišel „Blaster“, který během prvního dne způsobil obrovské škody. Ne však firmám, které využívaly naši službu „SmartDefense“, která kromě definičních souborů již využívala také analýzu vzorců chování. „Blaster“ využíval port, který slouží k určité funkci, nestandardním způsobem. Takový provoz byl identifikován jako podezřelý a „SmartDefense“ proto rozhodla o blokování daného portu. Naši zákazníci byli v bezpečí.

Společnost Check Point vstoupila i na pole řešení zvaných SIEM (Security Information and Event Management). V čem je síla vašeho řešení?

Zahlcení daty z bezpečnostních zařízení a aplikací patří k největším problémům, kterým čelí IT oddělení velkých podniků po celém světě. Naše produkty „Eventia Suite“ ulehčují IT profesionálům práci tím, že data získávaná z různých bezpečnostních a síťových zařízení různých výrobců automaticky analyzují. Tento přístup dokáže uspořit čas strávený procházením výpisů až o 80%.

„Eventia Suite“ tvoří aplikace „Eventia Analyzer“ a „Eventia Reporter“. „Eventia Analyzer“ nabízí centralizovanou správu logů v reálném čase z bezpečnostních řešení od Check Pointu i dalších výrobců. Automaticky přitom řadí jednotlivá hlášení podle jejich důležitosti a informuje správce systému o nutnosti případného zásahu. Nástroje aplikace „Eventia Reporter“ potom poskytují konzistentní pohled na bezpečnostní data z osobních počítačů i aktivních síťových prvků.

„Eventia Suite“ nyní nabízí užší integraci s produkty „SmartCenter“ (jednotná konzola pro správu bezpečnostních řešení Check Point pro podniky) a „Provider-1“ (jednotná konzola pro správu bezpečnostních řešení Check Point pro poskytovatele telekomunikačních služeb). Ti zákazníci, kteří již využívají „Eventia Analyzer“, mohou s novou verzí „Eventia Suite“ provádět hloubkové analýzy a vyšetřovat zdroje bezpečnostních problémů s podporou nových reportovacích nástrojů. Navíc, funkce dynamických aktualizací umožňuje rozšířit seznam podporovaných bezpečnostních zařízení a bezpečnostních událostí pro „Eventia Analyzer“ i výpisů pro „Eventia Reporter“ o nové záznamy bez čekání na novou revizi klíčových aplikací.

V nové pozici jste nyní několik měsíců. Určitě jste měl při nástupu řadu plánů a předsevzetí. Jak se Vám je daří uskutečňovat?

Počátečních plánů bylo a je mnoho zejména v dalším posílení naší pozice na důležitých trzích v celém regionu východní Evropy, mezi které samozřejmě patří i Česká republika. Jejich naplnění je úzce spjata s výsledky, které v celém regionu i v jednotlivých lokálních zemích dosahujeme.

Z tohoto pohledu mohu říci, že uplynulý rok byl pro celý region i všechny naše prioritní trhy v rámci regionu velice úspěšný. Vykázali jsme nárůst téměř 30% což znamená, že jsme pro Check Point jednoznačně nejrychleji rostoucím regionem v EMEA.

V průběhu minulého roku jsme otevřeli novou pobočku v Rumunsku a posílili naši kancelář v Rusku. Věřím, že velmi dobré výsledky v uplynulém roce a jasný plán dalšího rozvoje obchodu v celém regionu povedou k dalšímu posílení našich aktivit zejména v České republice, Polsku a Rusku a také k otevření 1-2 nových poboček v regionu.

Jakou roli vidíte u lokálních partnerů jako je Simac?

Check Point prodává veškerá řešení prostřednictvím autorizovaných partnerů, takže kvalitní lokální partnerská síť je pro nás klíčová.

Firmy jako je Simac, které mají vysoce kvalifikované specialisty v oblasti IT a bezpečnosti jsou pro nás velmi důležitými obchodními partnery. Kromě standardní podpory našich produktů v předprodejní fázi, během implementace a následné podpory, jsou schopny zákazníkovi nabídnout také další služby. Zejména mám na mysli integraci s dalšími řešeními v rámci již dříve zmíněného programu OPSEC (Open Platform for Security) včetně zajištění úzké návaznosti na stávající infrastrukturu zákazníka. Tak dochází k podstatnému rozšíření společné nabídky nad rámec standardních řešení Check Point a tím i k dalšímu zvýšení atraktivnosti naší nabídky.

Právě díky rozsáhlým zkušenostem Simacu s budováním infrastruktur podnikových sítí a díky kvalitnímu týmu IT a bezpečnostních specialistů je pro nás spolupráce s firmou Simac velice perspektivní.

Co byste popřál zákazníkům Simacu?

Začíná nový rok, takže zcela určitě pevné zdraví, hodně štěstí a spokojenosti jak v osobním, tak i v profesním životě a samozřejmě, aby podnikové sítě Vašich a v řadě případů i našich zákazníků úspěšně odolávaly případným útokům – jak jinak než za pomoci technologií Check Point.

Nyní (na konci roku 2006) dokončujeme akvizici společnosti NFR Security, což přinese našim zákazníkům nejvýkonnější dostupné nástroje ochrany před cílenými útoky hackerů v reálném čase. Současně spěje k úspěšnému konci akvizice společnosti Pointsec, která nabízí automatické nástroje pro šifrování dat poskytující zaručenou úroveň zabezpečení na koncových zařízeních. Check Point tím usiluje o začlenění vrstvy ochrany uložených dat do naší komplexní bezpečnostní nabídky.