Kontaktní informace
Pro více informací prosím kontaktujte:
Stanislav Přibyl
PRAM Consulting s.r.o.
T: +420 736 684 268
E: stanislav.pribyl@pram.cz

Jak odhalit i doposud neznámé útoky na podnikovou IT infrastrukturu?

Analýza chování podnikové sítě a detekce nežádoucích aktivit

Praha, Česká republika – 9. ledna 2015

Kybernetická bezpečnost je žhavým tématem posledních let a její význam v budoucnu ještě více poroste. Smůlou je, že ne všechny hrozby a incidenty lze odhalit přímo – například na základě jedné konkrétní události či zjištění známého vzorku kódu. Štěstím je, že řešení existují a jedním z nich jsou tzv. Network Behavior Analysis (NBA), tedy analýzy chování sítě včetně detekce vzorů využití sítě, které mohou souviset s nežádoucími či nelegitimními aktivitami. Jinými slovy, NBA umožňuje vyhledávat a analyzovat anomálie v komunikační infrastruktuře.

Obdobně jako jakákoli jiná technika založená na analýze i NBA potřebuje mít co analyzovat, tedy data. Rozhodnutí, jaká data je třeba sledovat nelze učinit od stolu bez znalosti konkrétní situace a vyjasnění si, v jaké oblasti organizace působí, co je pro ni kritické, které služby jsou zranitelné, jaké dopady může mít nefunkčnost vybraných částí podnikové informační architektury apod. Základem je vždy zjištění, co se vlastně v síti děje, jaký je objem přenášených dat a v rámci jakých služeb. Ve standardní pracovní den, o víkendech, během svátků, při vysokém vytížení zaměstnanců apod.

Sbíráme informace

Část informací je možné získat pomocí jiných monitorovacích nástrojů, například prostřednictvím protokolu SNMP. Nicméně tato úroveň není pro NBA dostatečná. Důležité je právě provázání analýzy typu dat, kontextu a ve finále ještě zohlednění typu dat tak, aby bylo možné zjistit, zda aktuální stav odpovídá typickému způsobu využívání sítě. Pro každý druh komunikace – bez ohledu na to, zda jde o NTP protokol pro synchronizaci času, DHCP protokol pro přidělování IP, ICMP protokol pro vykonávání kontrolních úkonů v IP sítích či jiné UDP/TCP datové přenosy – existují odhady, jaké chování takové komunikaci odpovídá. Tento odhad samozřejmě není neměnný a může se pomocí statistických metod přizpůsobovat reálné situaci v konkrétní organizaci.

Vím, jak bys měl komunikovat

Existuje tedy poměrně přesná představa o předpokládaném objemu přenosu konkrétního typu dat za jednotku času. V případě, kdy NBA na síti odhalí komunikaci, která překračuje běžné limity nebo probíhá netypickým způsobem, lze spustit potřebné kroky – od varování přes pokročilou analýzu s korelací dat s ohledem na čas, místo a další okolnosti až po aktivní zásah. Díky informacím o typu dat a jednotlivých účastnících komunikace je Network Behavior Analysis při zjišťování anomálií velmi úspěšnou technologií.

Analýzy chování sítě mohou být nejen součástí dlouhodobých bezpečnostních opatření, ale lze je v případě podezření na nežádoucí aktivity provést i nárazově. V obou případech jde mnohdy o pomyslné hledání jehly v kupce sena, miliardy protokolových záznamů nejsou výjimkou. Díky pokročilým analytickým postupům však bývá získání výsledků otázkou minut a hodin než týdnů. NBA je tak v mnohých případech významný nástroj poskytující a umožňující forenzní analýzu pro vyšetřování událostí, incidentů a útoků.

Pro finanční instituce i výrobní podniky

Řešení Network Behavior Analysis je vhodné pro všechny zákazníky, kteří si váží svých dat a nechtějí dopustit jejich ztrátu nebo kompromitaci. Samozřejmě, v případě několika málo počítačů by se jednalo o kanón na vrabce – NBA se ale při pravdivém počátečním vyhodnocení rizik vyplácí již od pár desítek síťových počítačů. Nejde přitom o technologii vhodnou pouze pro finanční a bankovní instituce, ale pro firmy napříč všemi vertikálami. V podmínkách České republiky získá NBA na významu i s účinností nového zákona o kybernetické bezpečnosti. Mezi zájemce o analýzu chování sítě patří ovšem i firmy, které nemusí plnit žádná zákonná bezpečnostní kritéria a jen chtějí mít přehled o tom, co vlastně se v jejich síti děje.

Smysluplný pohled na bezpečnost

Důležitost NBA roste i s ohledem na internet věcí a stále častější využívání síťové komunikace v situacích, kde nikdo ještě před pár lety konektivitu nevyžadoval a ani nepředpokládal. S ohledem na ohromný objem přenášených dat je NBA navíc mnohdy jedinou cestou, jak vůbec nějaký smysluplný pohled na bezpečnost síťové infrastruktury získat.

Společnost Dimension Data poskytuje svým zákazníkům v oblasti NBA širokou škálu služeb – od vstupních analýz použitelnosti přes poskytnutí ad-hoc služeb až po dodávku uceleného řešení. Součástí analýz může být samozřejmě i analýza trendů, která v případě potřeby využívá informace z hraničních prvků a ovlivňuje vhodnost jednotlivých způsobů nasazení NBA. Nesporným přínosem je i možnost provozu Network Behavior Analysis v cloudovém prostředí.

Ing. Jiří VOLEK, Senior System Engineer / Network Integration & Security Leader

Dimension Data

Ve společnosti Dimension Data působí od roku 2006. Ve své profesi zodpovídá za technický a personální rozvoj Network Integration & Security oddělení. Z pozice hlavního architekta se podílí na nejvýznamnějších projektech síťové integrace a síťové bezpečnosti.

Dimension Data

Založena v roce 1983, společnost Dimension Data je poskytovatelem ICT služeb a řešení, který využívá své technologické odbornosti, schopnosti poskytovat služby v globálním měřítku a svého podnikatelského ducha k akceleraci obchodních ambicí svých klientů. Dimension Data je součástí NTT Group. www.dimensiondata.com