NetFlow Security

Nové české technologie, které Vám pomohou detekovat dosud neznámé (nedetekovatelné) útoky a nové druhy malwaru! Už znáte NBA?

O co se jedná?

- Nová a velmi efektivní pasivní technologie.
- Řeší bezpečnost na úrovni netflow* protokolu, doplněk IDS/IPS a firewallu.
- Z určitého pohledu ji lze považovat za levnější náhradu IDS s efektivnější detekcí neznámých druhů malwaru a napadení.

NetFlow* - protokol, který vytvořila společnost CISCO, jedná se pouze o data ke statistickému popisu komunikace. Protokol říká kdo, kdy, s kým, jak mnoho a čím komunikoval. Protokol neobsahuje vlastní přenášená data!

Charakteristika produktů NetFlow Security

- Cílem je detekce anomálii a nestandardního chování v síti na základě zpracování netflow dat z celé sítě.
- Zařízení je pasivní, zpravidla napojeno na centrální router/switch.
- dokáže identifikovat změny v síti, slovníkové a brute-force útoky, p2p sítě, DoS útoky, malware atp.

Doporučení společnosti Gartner

- Neexistuje bezpečnost bez monitoringu. Mnoho lidí bylo dlouho přesvědčeno, že bezpečnost stačí budovat na perimetru a monitoring je zbytečná práce navíc. Opak je pravdou.
- Monitoring síťových komunikací a Network Behavior Analysis byly zařazeny do TOP10 nejdůležitějších technologií roku 2010.
- Bezpečná organizace = firewall + IPS + NBA/NBAD/ADS.

Hlavní výhody NBA

- Dokáže detekovat nové druhy škodlivého softwaru a neznámé útoky.
- Jedná se o pasivní nástroj, který nezasahuje do komunikace ani nezpracovává přenášená data.
- Doplňuje ostatní systémy o schopnost odhalit závažné a těžko postižitelné bezpečnostní události v síti, zejména organizované sofistikované útoky, „zero-day“ útoky či útoky polymorfního malwaru.

Co vám NBA přinese?

- Přehled o dění v síti (protokoly, komunikace)
- Detekci vnitřních i vnějších útoků
- Snížení nákladů na provoz sítě
- Monitorování služeb i uživatelů
- Nástroj pro řešení incidentů na síti

NetFlow Security - NBA

NBA (Network Behavior Analysis) je systém, který provádí inteligentní analýzu nad NetFlow* síťovými daty, a dokáže tak identifikovat veškeré i velmi drobné anomálie provozu. NBA tak doplňuje běžné bezpečnostní systémy (IDS, IPS, firewall, aplikační proxy) o behaviorální analýzu nad NetFlow daty, určenou k odhalení nových, neznámých a pokročilých útoků v síti.

- Velmi sofistikovaný nástroj využívající prvky umělé inteligence (teorie her + neuronové sítě atp.), dokáže identifikovat také velmi drobné odchylky – zapouzdřená komunikace trojského koně.
- Informace ze systému jsou vhodné pro bezpečnostního správce, IRM, znalého administrátora sítě apod.
- Cílovou skupinou jsou organizace, které řeší bezpečnost nebo mají bezpečnostního správce (finanční instituce, zabezpečené státní úřady, společnosti s vysokým „know-how“ a další).

Proč bezpečnost s NetFlow?

Detekce nových útoků a škodlivého softwaru je problematická. Veškeré současné detekční techniky jsou buď velmi málo efektivní (heuristika), nebo využívají detekční vzorky (profily, signatury malwaru). Vytvoření detekčních vzorů je časově náročné - a ne každý malware je odhalen, resp. jsou k němu vytvořeny detekční profily. Jedinou možností, jak detekovat neznámé útoky, nový neznámý malware, je využití NBA.

- Sledování a dlouhodobý monitoring sítě přináší nejen bezpečnostní přínosy, ale i řešení provozních problémů, optimalizaci toků, dohled nad uživateli, snížení nákladů na provoz (nežádoucí odchozí komunikace apod.).
- Ztráty plynoucí z bezpečnostních incidentů dosahují jen v České republice desítek až stovek milionů korun ročně. NBA dokáže těmto ztrátám efektivně předejít.
- NBA muže být využita i jako levná náhrada IDS.
- Výstupy z NBA lze samozřejmě velmi snadno integrovat do SIEM.

www.aec.cz

Nekupujte zajíce v pytli

- Využijte možnost nezávazného vyzkoušení této nové technologie ve vlastním prostředí vnitřní sítě či DMZ!
- Instalace je velmi jednoduchá a vyžaduje minimální nebo žádné změny v současné konfiguraci.

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY