



Redakční otázky k tématu

IDS, IPS, Monitoring

odborného on-line magazínu ICT SECURITY – www.ictsecurity.cz

Nadpis článku:

IDS/IPS jako jedna ze součástí bezpečné sítě

Autor odpovědí:

Mgr. Robert Šefr, IT Security Consultant, COMGUARD a.s.

1) Které parametry provozu sítě je z hlediska bezpečnosti smysluplné sledovat – a proč?

Vše, co potřebujeme k efektivnímu monitorování sítě, je obsaženo v Netflow datech. Nejdůležitějším faktorem pro sledování je změna, ta může být legitimní, ale také může ukazovat na bezpečnostní incident. Výrazně složitější je ale tato data analyzovat tak, abychom dostali výsledky a pozorovali změny, ne jen nesmyslnou změť grafů. Od nástrojů na analýzu Netflow dat očekáváme nejen dostatek vlastní inteligence v podobě signatur útoků, ale také velmi přehledné uživatelské rozhraní, které zpřístupní správci vše od globálního pohledu na dění v síti, až po úplné detaily u jednotlivých strojů.

2) Co všechno můžeme z monitorování sítí a provozu z bezpečnostního hlediska vyčíst?

Můžeme odhalit nově běžící služby na stanicích nebo na serverech, které ukazují na infekci těchto strojů. Dále jsou zcela jasně vidět i zdroje spamu v síti, tedy další infikované stroje. Kromě infekce malwarem můžeme identifikovat např. peer-2-peer sítě, jejichž provoz by mohl vrhnout na společnost špatné světlo, pokud by se přes ně šířila nelegálně data.

Pokud nás zajímá dostupnost služeb, tak je dobré sledovat, jestli někde nepřestala protékat data. Mohla přestat fungovat nějaká služba nebo se změnila konfigurace síťových prvků tak, že tok dat znemožnila. Při nasazování monitorovacích nástrojů bývají zpravidla správci velmi překvapeni tím, co se u nich v síti děje.

Výsledky analýz monitorovacího nástroje nemusí zpracovávat pouze správce, ale mohou být automaticky přeposílány na IPS systémy, jako to např. umožňuje Network Threat Behavioral Analysis (NTBA) od společnosti McAfee. Kombinací s IPS systémem přechází zabezpečení sítě od pasivního sledování k aktivní ochraně.

3) Mají dnes ještě nějaký smysl nástroje IDS, nebo již byly překonány IPS a pokročilejšími systémy?

Nepovažuji IPS systémy za další vývojový stupeň IDS. Většinou se jedná o stejné zařízení, rozlišují se pouze podle aktuálního nastavení. Využití reaktivních vlastností IPS je sice velmi lákavé, ale nemusí být žádoucí ve všech prostředích. Dobrým kompromisem je nasadit blokování u IPS systémů pouze pro zcela zřejmé signatury útoku. V případě signatur útoků, které znamenají menší hrozbu a mají vyšší pravděpodobnost na false-positive, můžeme zůstat u pouhé detekce a upozornění odpovědných osob.



U neověřených systémů pak můžeme použít opačný přístup a blokovat jim veškerý provoz, dokud se neautentizují nebo nesplní podmínky stanovené politikou organizace. Pokud podmínky splněny nejsou, je systém vpuštěn pouze do vyčleněné karanténní zóny, ve které může stáhnout aktuální záplaty, nejnovější signatury pro antivir, popř. cokoliv dalšího, co je vyžadováno a můžeme ověřit nějakým z mnoha testů, např. OVAL (Open Vulnerability and Assessment Language) nebo XCCDF (The Extensible Configuration Checklist Description Format).

4) Jakou úspěšnost mají dnešní systémy IPS v případě nových nebo netypických útoků?

Nikdo nemůže zaručit absolutní úspěšnost 0-day útoků, zvýšení důvěry v heuristiku musí zákonitě vést k vyššímu procentu false-positives. Kvalitní IPS spolupracuje se svým okolím, čímž zvyšuje svoji účinnost na základě ověřených informací a ne „pouhé“ heuristiky. Příkladem může být integrace IPS zařízení společnosti McAfee (Network Security Sensor), které umí spolupracovat s více systémy najednou a dohromady tvoří tzv. Network Security Platform.

Kromě výše zmíněného NTBA síťová IPS sonda komunikuje s IPS agenty na stanicích, zpracovává výsledky Vulnerability Manageru (ten aktivně skenuje stanice a servery kvůli zranitelnostem) a na základě těchto výsledků může lépe vyhodnocovat zranitelná místa na síti. Dále lze pomocí Network Security Platform hlídat přístup do sítě a eliminovat připojení cizích nebo nezaplátovaných zařízení. Proti úplně novým typům malwaru pomůže cloud technologie Artemis, která identifikuje nové hrozby výrazně rychleji, než tradiční postup vydávání signatur.

Více o IPS od McAfee se můžete dočíst např. v oficiálním testu NSS

Labs:<http://nsslabs.com/test-reports/NSSLabs-NIPS-McAfee-M8000.pdf>

5) Jak použít monitorování sítě k zajištění bezpečnosti? Jak síť rozdělit, jaké prvky nasadit?

Každá síť je specifická a každá společnost má odlišné požadavky, nelze se tedy vyjádřit konkrétně. Co se týče nasazení, tam lze najít několik spojitostí. Při zavádění nového IPS/IDS systému je vhodné blokovat pouze zcela zřejmé útoky, jinak pouze monitorovat síť kvůli případným false-positives. Rozsah blokování se dá časem navyšovat.

Jak již bylo zmíněno v minulém bodě, IPS může fungovat mnohem lépe, když je doplněno o další zařízení. Monitorovací zařízení může být jedním z příkladů, který pomáhá při efektivním použití IPS a dává nám dostatek podkladů pro vytváření politik a řešení bezpečnostních incidentů.