

Systemy detekce a prevence narušení

Rychle chránit, rychle rozhodovat

Aleš Nosek

Hledáte-li IDS/IPS řešení, které bude růst s potřebami organizace a patří mezi dostatečně výkonné a kvalitní, nebylo by správné opominout jedno z předních řešení dlouhodobě umístěné v Leader kvadrantu společnosti Gartner. McAfee Network Security Platform IDS/IPS systémy dobře cílí na kratší životní cyklus hrozeb, neustále se objevující nové typy útoků, a tedy i rostoucí možnosti kompromitace systémů organizace i formou útoků vedených zevnitř, z napadených osobních počítačů uživatelů. A to je právě problém, zde, byť kvalitně nastavený, firewall na perimetru nepomůže. Autoři propracovaného malwaru stále častěji provádějí útoky šité na míru konkrétní zemi, jazyku, společnosti nebo softwarové platformě a ladí své akce vzhledem ke kulturním odlišnostem a patřičným způsobem upravují postupy sociálního inženýrství, tak aby napadly síť přes nejslabší článek, přes uživatele. Tvůrci malwaru po celém světě zneužívají náchylnosti k malware nákazám aplikací Web 2.0 a P2P sítí. Z toho pro nás vyplývá otázka, jak přizpůsobit naši firemní strategii právě těmto novým trendům a jakým způsobem můžeme ochránit své kritické aplikace, databáze, groupware?

Firemní infrastruktura se stále rozšiřuje, což znamená ztíženou schopnost pokrýt všechny zranitelnosti systémů okamžitě.



IDS/IPS zařízení jsou určena ke zvýšení úrovně bezpečnosti lokální sítě či jejího vybraného segmentu na maximální možnou úroveň, kdy systém umožní eliminovat nově vzniklou hrozbu dříve, než na ni příslušný výrobce vydá bezpečnostní záplatu, nebo umí rozpoznat či eliminovat i nové formy neznámých a cílených forem útoků.

Tyto systémy se implementují tak, aby monitorovaly a blokovaly závadný provoz na citlivých místech v síti, nejčastěji ve vnitřních segmentech sítě s vysokými nároky na dostupnost, ale i propustnost, kde by implementace firewallů způsobovala komplikace. Systémy, například pomocí databáze signatur, heuristické analýzy nebo detekce anomálií provozu, jsou schopny odhalit útoky i ve zdánlivě nesouvisejících pokusech o spojení, například skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod. Výhodou těchto systémů je vysoká úroveň bezpečnosti kontroly procházejících protokolů při zachování relativně snadné konfigurace.

Kvalitní IPS zajišťuje podrobný monitoring provozu v reálném čase s možností okamžitého blokování provozu při identifikaci útoku. Způsob reakce probíhá dle administrátorem předem definovaných bezpečnostních politik.

Systémy dále poskytují a ukládají podrobné informace o událostech z datového provozu. Z těchto záznamů je možné dohledat chyby v konfiguracích, chyby v aplikacích,

pokusy o nekorektní provoz pro odchozí či příchozí komunikaci z vnitřní sítě, odhalování výskytu škodlivých kódů sledováním jejich aktivit v čase apod.

IPS/IDS systémy můžeme rozdělit dle platformy na host intrusion prevention systémy, které jsou instalovány na servery a koncové počítačové stanice (zejména ty mobilní) ve formě softwaru, a network based intrusion prevention systémy, které sledují a kontrolují síťový provoz ve formě samostatné sondy (hardwarové jednotky). U nich je klíčové zajištění vysoké propustnosti (McAfee sondy jsou například certifikovány až na plných 10Gbps propustnosti), minimálního zanesení zpoždění (latency). Zde nejlepších výsledků dosahují všechny IPS systémy postavené na specializovaném hardwaru bez točivých komponent se specializovanými čipy pro sken a dekryptaci. Výhodou také je, že na rozdíl od klasických, na procesorech Intel založených IPS, zde není skenovací jádro nainstalováno na jiném „bezpečném“ operačním systému. Určitě bychom zároveň neměli při IPS režimu opomenout možnost přechodu do fail open (či fail close) dle bezpečnostních požadavků nebo požadavků na dostupnost.

Network based intrusion prevention systémy

Při výběru a návrhu vhodného IDS/IPS systému požadujeme údaje s certifikovanou propustností v IPS režimu, počet skenovacích portů a možnosti konfigurace virtuálních IPS. Počet skenovacích portů umožní samostatně sledovat daný počet fyzických rozhraní (segmentů), případně v polovičním počtu zajistit in-line zapojení v preventivním režimu. McAfee sondy mají přitom k dispozici až dvacet detekčních portů (zapojení in-line mód, span mód, TAP mód a port clustering) a umožňují tak jednoznačně ušetřit náklady jindy potřebné na nákup i několika samostatných systémů a jejich správu. Virtuální IPS přispívají k minimalizaci false positives při možnosti maximalizace úrovně bezpečnosti.

Například tisíc virtuálních IPS v rámci jedné sondy dokáže pokrýt potřeby už opravdu velkého datového centra a velmi granulárně definovat pravidla pro stovky různých webových aplikací, databází, informačních systémů apod.

Pokud uvažujeme o zapojení v režimu IPS (in-line) velmi často využijeme i možnosti řídit přidělování šířky pásma (QoS) a monitoring aplikací, což přináší další možnosti úspor, kdy díky takto komplexnímu IPS není nutné pořizovat specializovaná QoS zařízení.

Host intrusion prevention systémy

Host IPS pro desktopy a servery je systém, který kombinuje funkce desktop firewallu a několik stupňů detekce narušení, od rozpoznání známých útoků na základě aktualizovaných signatur až po pravidla chování pro detekci neznámých útoků včetně DoS útoků, anomálií provozu a zero day attack ochran s možnostmi sledování jak síťového provozu v rámci network stacku, tak i systémových volání na úrovni kernelu operačního systému. Jestliže IPS identifikuje přicházející nebo odcházející útoky, může zablokovat průnik, umožnit výstrahu a provést záznam do logu událostí a reportovat událost na serveru nebo koncové stanici a zajistit i návazné akce IPS sondy na síťovém segmentu.

Snadné nasazení a správa v každé síti

Častým místem v topologii, na kterém je potřeba IDS/IPS nasadit, jsou vnitřní perimetry, tedy rozhraní mezi sítěmi s různou důvěryhodností a s různou úrovní zabezpečení či bezpečnostní politiky. Další často chráněná oblast, která by neměla být opomíjena, je ochrana konkrétního serveru,

popřípadě farmy serverů, či konkrétní aplikace ve vnitřní síti jako ochrana před útokem z řad vlastních uživatelů/zaměstnanců.

U McAfee sond je pro nasazení k dispozici vestavěný průvodce, který zajistí, že nepomenete podstatné aspekty konfigurace. Jednoduchá správa vlastní sondy i bezpečnostních politik je dostupná prostřednictvím webového prohlížeče a zahrnuje předdefinované, okamžitě použitelné bezpečnostní politiky, integrovanou podporu pro autentizaci uživatelů do externí databáze, automatizovaný „failover“ a „fail-back“ a systém obnovy kritických konfiguračních dat. Pro rozsáhlejší implementace sond je k dispozici nástroj poskytující hierarchizovanou správu s centrální kontrolou. Nastavení pro vysokou dostupnost umožňuje transparentní, Stateful, L7 Fail-over, L2 Fail-open a hardware Fail-open pro odstranění rizika představujícího nefunkčnost prvku v síti.



Proč integrovat IPS a Vulnerability Manager?

Například McAfee Vulnerability Manager umožňuje administrátorům na základě provedeného skenování sítě určit zranitelnost systémů, aktivních prvků, stanic, databází nebo operačního systému serverů. Zároveň umožňuje určit, která ohrožení jsou kritická

a uplatnitelná v konkrétní situaci dané sítě, respektive která jsou méně relevantní. Network IPS pak dokáže tyto informace využívat (automaticky importovat reporty Vulnerability Manageru) a preventivně tak chránit potenciálně ohrožené systémy na základě znalosti využití dané zranitelnosti. Těmto ochranám se říká virtuální záplatování, tj. zajištění ochrany zranitelného systému bez nutnosti aplikovat patch.

Propojení sond s monitoringem sítě

U McAfee je využit nástroj centrální správy a monitoringu společný pro všechna McAfee řešení nazývaný ePolicy Orchestrator (ePO), navíc podporuje i SIEM řešení, jako je LogRhythm nebo ArcSight. ePO ve spolupráci s McAfee IPS urychluje čas potřebný k výkonu ochranných činností díky jednotnému pohledu na bezpečnost celé IT infrastruktury. Poskytuje podrobné informace o „hostech“, jejich IP adresách (nebo i identitě z účtů v doméně), útocích na ně a jiných událostech.

Propojení IPS s NAC

McAfee opět nabízí spolupráci IPS sondy se sondami Network Access Control a dokáže na základě předem daných pravidel automaticky přeměrovat neshodné či nelegitimní přistupující systémy do karantény, která je součástí McAfee IPS. Tím je vytvořen systém dynamické kontroly přístupu do sítě. ■

Autor pracuje ve společnosti Comguard.

Inzerce

Full Spectrum Security

WWW.ASKON.CZ

 <p>Bezpečná autentizace</p> <ul style="list-style-type: none"> - USB tokeny iKey - čipové karty SC330 a JCOP - podpora biometrie, PKI, CA - Smart Card Management - HSM moduly pro PKI - zabezpečení XML - zabezpečení databází - přístupové systémy 	 <p>Šifrování dat</p> <ul style="list-style-type: none"> - šifrování dat na discích a partitions - šifrování souborů a složek - šifrování databází - ethernetové šifratory - HW autentizace 	 <p>Bezpečná komunikace</p> <ul style="list-style-type: none"> - SPAM firewall - WEB filter - IM firewall - Load Balancer - VPN Gateways
---	--	---



tel.: +420 222 742 475, fax: +420 222 742 471, e-mail: info@askon.cz

