



NEDEJTE ZÁŠKODNÍKŮM ŠANCI

Co je nového ve světě IDS/IPS

Aby IDS/IPS zařízení udržela krok s neustále se rozvíjícím spektrem hrozeb, jsou výrobci nuceni inovovat své technologie tak, aby zákazníkovi poskytly co nejlepší úroveň zabezpečení jejich sítě. Co nám IDS/IPS systémy vlastně nabízejí a co se v této sféře aktuálně děje, zodpovídají následující řádky.

Marketingová oddělení výrobců se doslova předhánějí v popisu vlastností svých produktů, aby dokázala, že jejich řešení poskytuje maximální ochranu. Nejprve si krátce řekněme pár základních informací, k čemu slouží a co nám přináší IDS/IPS systémy (Intrusion Detection Systems/Intrusion Prevention Systems).

Začlenění do síťové infrastruktury

IDS/IPS systémy sledují datové toky a hledají v nich pokusy o útok na konkrétní aplikace. Prostřednictvím výstrah (alertů) a statistik poskytují obsluze informace o případných útocích, systémy IPS pak nabízejí ještě možnost aktivní reakce – zabránění útoku modifikací datového toku v reálném čase. Některé IDS systémy umějí přerušit datové spojení tím, že spolupracují s firewallem a dynamicky mění jeho politiku. V tomto případě se ale jedná o přerušení již navázaného spojení, a tak v mnohých případech již může být pozdě. Tato funkcionalita tedy nedosahuje účinnosti systému prevence narušení, neboť ten je schopen spojení zastavit ještě před tím, než útok dorazí k aplikaci.

K vlastní analýze paketů se používají tyto 3 základní technologie. Zařízení a aplikace renomovaných výrobců je kombinují pro získání co nejlepších výsledků:

» Signatury (unikátní sekvence znaků) – Technika spočívá v hledání určitých znakových sekvencí v datovém toku.

Vzhledem ke generování vyššího množství falešných poplachů byla technika dále zdokonalena o detekci stavu. Vyhledává se nejen znaková sekvence, ale zároveň se zjišťuje, zda-li se tato sekvence nachází ve správné části datového toku. Sofistikovanější varianta této metody dovoluje rekonstruovat celou výměnu dat. Systém je pak schopen nalézt útoky, které vyžadují datovou výměnu nebo jsou rozděleny do více paketů právě kvůli snížení pravděpodobnosti odhalení.

» Dekódování protokolů – Metoda vychází z definic jednotlivých protokolů daných standardy RFC. Odchyly od norem jsou detekovány a dále analyzovány. V takto dekódovaném provozu jsou vyhledávány obecné zranitelnosti, jako je kupříkladu přetečení vyrovnávací paměti.

» Detekce anomálií v síťovém provozu – Systém na základě statistických metod odhaluje síťový provoz, který se vymyká dosud běžnému provozu.

Z hlediska přesnosti odhalení útoku je nejlepší detekce signatur s detekcí stavu. Ta je ovšem použitelná jen na již známé útoky. Naopak detekce anomálií v síťovém provozu generuje více planých alertů, nicméně dokáže upozornit i na doposud nedefinovaný útok. Pro zajištění efektivního fungování je potřeba automatické doplňování znalostní báze IDS/IPS. Obvykle postačuje aktualizace jednou za hodinu. Důležitý je samozřejmě obsah (rozsah) báze a podstatným faktorem je též reakční doba výrobce na nové incidenty. Doba mezi zveřejněním nového útoku a jeho zařazením do znalostní báze se u renomovaných firem pohybuje v řádu hodin. Důležitou vlastností je i možnost vkládání vlastních pravidel a signatur. Můžete si tak zadávat například vlastní pravidla pro

Pohled z praxe

Oslovily vás poměrně nové technologie IDS/IPS?

Jan Zahrádka, Computer Press
(45 serverů, 200 PC)

Nejenže oslovily, ale zabýval jsem se i myšlenkou na jejich nasazení. Ale jedná se o dosti zásadní věc a je třeba tyto technologie dlouhodoběji zkoumat, než bychom přistoupili k jejich implementaci, aby výstupy byly věrohodné a nezhoršila se stabilita informačního systému.

Aleš Kotmel, Annex Net
(2 servery, 10 PC)

IPS systém používáme jako součást komplexního bezpečnostního řešení již více jak rok a jsme s ním maximálně spokojeni. V dnešní době, kdy hlavním bezpečným jsou útoky na aplikační úrovni, je IPS systém nutností. Máme tak plně pod kontrolou nejenom bezpečnostní útoky na aplikační vrstvě, ale také korektní používání některých nových typů komunikačních služeb jako jsou P2P sítě, přenos souborů přes instant messaging nebo telefonování přes skype.

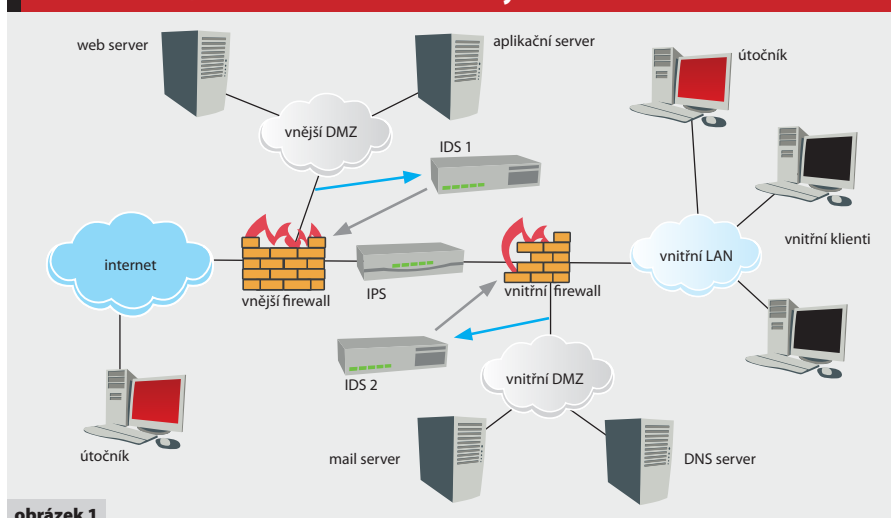
rozpoznávání scanů. Konečně ještě důležitější může být možnost si prohlédnout existující pravidla a signatury – pomůže to nejen pochopit fungování daného útoku, ale také, a to hlavně, odladit nastavení sond tak, aby se co nejvíce omezily falešné popluchy.

Pojďme se tedy společně podívat na některé produkty výrobců, kteří nejsou v tomto oboru žádnými nováčky, a jejich novinky.

IDP – Juniper Networks

Produkty Intrusion Detection and Prevention (IDP) integrují aplikační a síťovou přehlednost s funkcemi pro prozkoumání a nápravu incidentů, což umožňuje rychle a spolehlivě implementovat in-line prevenci útoků. Rovněž porovnávají signatury a vyhodnocují protokolové anomálie, takže efektiv-

Začlenění IDS/IPS do síťové infrastruktury



obrázek 1

ně identifikují hrozby. Za předpokladu, že jsou produkty IDP implementovány in-line, dokáží efektivně zastavit útoky na úrovni sítě i útoky na úrovni aplikací, a to daleko předtím, než mohou způsobit škodu. Produkty IDP nejen účinně chrání síť proti útokům, ale také poskytují informace o škodlivých serverech a aplikacích, které mohly být do sítě instalovány bez vědomí administrátora. Pomocí nástroje Enterprise Security Profiler (ESP) získávají přehled o komunikaci ve sledovaných segmentech sítě, na jehož základě vyhodnocují odchylky od „běžného“ provozu. Prevenční vlastnosti systémů napomáhají detekovat hrozby, které mohou v konečném důsledku dosahovat enormních rozměrů.

Produkt IDP je dostupný buď jako samostatná appliance (hardware + software), nebo jako integrovaný systém řady ISG. Všechny tyto systémy mají plnou funkcionalitu IDP a liší se pouze výkonem a počtem monitorovacích portů.

Zmíníme několik nejdůležitějších vlastností: ochrana a prevence vůči wormům, trojanům, spywaru, keyloggerům a jinému malwaru, celkem 8 detekčních metod včetně porovnávání signatur a protokolových anomálií, 5 operačních módů (sniffer, inline bridge, inline Proxy ARP, inline router, transparent L2) nebo policy editor ke stanovení bezpečnostních restrikcí a pravidel.

Aktuální verze 3.2r2 umožňuje implementaci IDP systému do management platformy NetScreen Central Management určené pro široké spektrum produktů Juniper Network. Novinkou je také nástroj IDP Scheduler, který zprostředkovává automatické úkony související s aktualizací signatur a politik a vytvářením periodických reportů.

Velmi zajímavou novou funkcí je možnost vzájemné kooperace zařízení Secure Access SSL VPN a IDP. Senzor detekuje podezřelou činnost uživatele přihlášeného do domácí sítě přes SSL tunel, který zprostředkovává právě SA SSL VPN brána. Senzor uvědo-

mí SA bránu a ta na základě poskytnutých informací zablokuje uživateli dané spojení, umístí jej do karantény a o daných skutečnostech uvědomí administrátora.

Dragon – Enterasys

Dragon Intrusion Defense je integrované řešení zajišťující komplexní ochranu sítě. Je navrženo tak, aby splňovalo požadavky korporátního prostředí a nabízí funkce, které minimalizují zranitelnosti sítě. Dragon dokonce umí kombinovat analýzu událostí na síti s událostmi z jiných zařízení (firewally, směrovače, prepínače, popř. další bezpečnostní platformy a aplikace). Díky komplexní analýze a schopnostem monitorování v reálném čase poskytuje systém Dragon vyšší stupeň ochrany infrastruktury zákazníka. Řešení Dragon Intrusion Defense obsahuje zejména:

» Dragon Network Sensor – Ochrana proti napadení sítě s až gigabitovou rychlostí prostřednictvím analýzy provozu TCP/IP a srovnávání vzorů založených na charakteristických znacích, analýze protokolů a technik pro zjišťování anomálií. Dragon Network Sensor je dostupný buď jako software (pro běžně používané OS včetně XOS společnosti CrossBeam Systems), nebo jako appliance. Funkce Active Response (aktivní reakce) může ukončit relaci a dynamicky rekonfigurovat firewally, prepínače a směrovače založené na konkrétních varováních, a tak minimalizovat škody nebo jim zcela zabránit. Od verze 7.1 je senzor dostupný i jako IPS systém.

» Dragon Host Sensor – Ochrana proti napadení, která je aplikována na hostiteli a je poskytována prostřednictvím modulární a pružné architektury nejběžnějším operačním systémům dnešní doby. Funguje na základě monitorování operačního systému a kritických aplikací pomocí řady různých technik.

» Dragon Web Server Intrusion Prevention – Technologie Dragon Web Server Intrusion Prevention je určena k ochraně



BlueCoat ProxySG

řešení pro ochranu a monitoring web komunikací

Komunikace se zákazníky, obchodními partnery i zaměstnanci stále více závisí na Internetu.

Webový prohlížeč je univerzálním oknem do kritických komunikací a informací.

Moderní aplikace pro web browsing, instant messaging, webový e-mail nebo sdílení souborů typu P2P sice pomáhají uživatelům komunikovat mnohem efektivněji, ale zároveň pro podnik znamenají mnohá rizika.

Ošetření těchto rizik zajišťují specializovaná zařízení typu www proxy navržená speciálně pro správu a kontrolu uživatelské komunikace přes Internet.

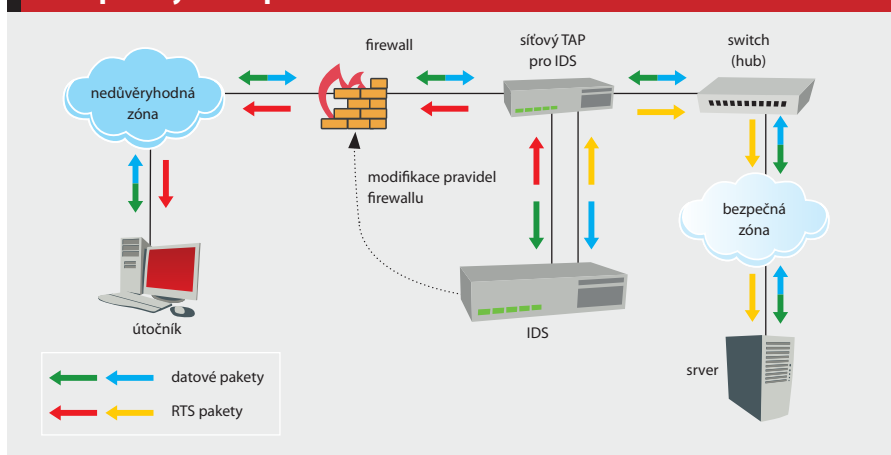
Zařízení Proxy SG společnosti BlueCoat poskytují organizacím schopnost kontrolovat a řídit komunikaci takovými metodami, které firewally a jiná externě zaměřená zařízení nemějí.

BlueCoat



Global Systems a.s.
Vlastislavova 4
140 00 Prague, CZ
Phone: +420 2 6718 4911
www.globsys.cz

Princip zachytávání provozu na síti TAPem



podnikových webových serverů. Dragon Web Server Intrusion Prevention provádí ochranu na úrovni aplikací. Jedná se v podstatě o add-on modul do Dragon Host Sensoru. Podporovány jsou web servery Apache a IIS.

S použitím Virtual Sensor Technology (VST) lze na jednom zařízení nakonfigurovat více virtuálních senzorů, které se navenek tváří jako samostatné funkční jednotky s vlastní politikou. Unikátní vlastností zastřešujícího Management Serveru je, že dokáže zpracovávat data z produktů třetích stran (CheckPoint, Juniper, Cisco, TippingPoint, Nokia, Snort a jiné další). Prováděná analýza a korelace všech posbíraných informací snižuje možnost generování falešných alarmů.

Horkou novinkou je začlenění Dragona do konceptu Secure Networks Architecture. Jedná se o vytvoření zcela nového úhlu pohledu na problematiku zabezpečení síťové infrastruktury za pomoci nástrojů společnosti Enterasys a produktů třetích stran (i když s jistými omezeními).

Význam Snortu roste

Představitel Open Source komunity, jehož obliba s postupujícím časem narůstá. Pozice systému Snort bude s největší pravděpodobností dále posilovat v podnikovém sektoru vzhledem k jeho komerční verzi dodávané společností SourceFire. O významu Snortu svědčí i nedávný odpor FBI a Pentagonu k akvizici SourceFiru společností CheckPoint, která se nakonec díky tomu neuskutečnila.

Je pravdou, že implementace Snortu vyžaduje opravdu zkušeného administrátora, navíc pohodlné ovládní, na jaké jsme zvyklí u komerčních produktů, je spíše utopií než realitou. Problém v tomto případě netkví v tom, že by neexistovaly vhodné nadstavby usnadňující administraci a použití, takových doplňků je k dispozici celá řada, ale většinou se jedná o projekty, které velmi často zanikají, a jejich další použití, například s novými verzemi, je

velmi komplikované až nemožné. Je tedy potřeba pečlivě vybrat nástroje, kterými chceme sondy spravovat, konfigurovat politiky, popř. vytvářet bezpečnostní reporty. Výhodou celého řešení je pak to, že vynaložené finanční náklady se rovnají pouze ceně za použitý hardware.

Ale vraťme se ke Snortu samotnému. V současné době je aktuální verze 2.4.4 (vydaná 17. 4. 2006), stejně tak verze určená pro in-line nasazení, která byla vydána o něco málo později (23. 4. 2006). Navíc je k dispozici (zatím stále jen pro testovací účely) i nová verze 2.6.0 a její uvolnění jako produkční se očekává již brzy.

Snort 2.6 Release Candidate 2 je verze určená pro testování a její případné nasazení do produkčního prostředí je třeba pečlivě uvážit. Nová verze přináší podporu pro dynamické plugíny – preprocesory, detekční moduly a podobně. V současné době se změna týká SMTP preprocesoru (nástupce xlink2state) a FTP/Telnet, který nahradí telnet_decode.

Networks Taps

Nezbytnou součástí řešení monitoringu sítě pomocí systémů IDS jsou síťové tapy (pokud není možné využít techniky zrcadlení portů na přepínačích, tzv. SPAN nebo MIRRORING portů). Tapy se v zásadě dají rozdělit do dvou skupin podle typu rozhraní na metalické a optické.

Metalické tapy se na trhu vyskytují v různých verzích podle rychlosti – 10/100M nebo 10/100/1G nebo 10/100/1G/10G. Vzhledem k vysokým cenám gigabitových senzorů jsou zatím stále nejpoužívanější modely 10/100M. V této oblasti je díky jeho vlastnostem velmi oblíbený ShadowTap od firmy Finisar – má dvojité napájení, provoz monitorované linky nevypadne ani při výpadku napájení tapu, podporuje Power Over Ethernet, provoz je monitorován pomocí elektro-optických relé, které poskytují 10× rychlejší reakční dobu než relé elektro-mechanické.

Novinkou jsou konverzní tapy, které mají dvojici TAP portů, takže na monitorování je možno použít současně dvě zařízení, například analyzátor a IDS. Tyto tapy mají dvě vestavěné dvojice 1 000 BaseTx portů (jedna dvojice je pro zapojení na linku a druhá pro monitoring) a dva SFP sloty (do kterých si uživatel může pořídit typ rozhraní dle své potřeby), které jsou určeny pro zapojení druhého monitorovacího zařízení.

Optické tapy se dělí jednak podle použité technologie laseru na SM (Single-Mod) a MM (Multi-Mod) a dále se dělí dle poměru odbočení optického signálu (uvnitř jsou splitter). Díky tomu nedochází k žádným prodlevám mezi porty a navíc není potřeba externího napájení. Někteří výrobci odbočení signálů z obou linek posílají fyzicky do jednoho konektoru (dvou portů) – takže pak na full duplex monitoring stačí pouze 3 konektory (k serveru – k přepínači – k sondě). Díky této technologii se dá ušetřit drahocenný prostor v racku a nedojde ke snížení hustoty portů. Je pochopitelné, že v případě optických tapů nelze ze sondy posílat do monitorované linky žádný provoz, tedy ani RTS pakety používané k přerušení spojení.

Jedním z nejnovějších způsobů monitorování linek je využití přepínačů pracujících na fyzické vrstvě, které umožňují např. kopírovat monitorovanou linku až 1 do N. Dále je možné vzdáleně přepínat, které porty chceme monitorovat – výhodné je to např. tam, kde je jeden analyzátor a více monitorovacích bodů. Výhodou těchto systémů je jejich velká flexibilita – porty lze překonfigurovat přesně dle aktuálních požadavků. Tato technologie se velmi dobře hodí k monitoringu serverových firem, výpočetních středisek, hosting center a podobně.

Samotné IDS/IPS nás nespasí

V každém případě mějme vždy na paměti to, že systémy pro detekci (a prevenci) neoprávněného průniku jsou doporučeným doplňkem k firewallové ochraně sítě, používání šifrovaných spojení (VPN), silné autentizaci a dodržování pravidel stanovených bezpečnostní politikou organizace. Jen kombinací všech těchto produktů a postupů lze docílit vysokého stupně ochrany před neoprávněnými aktivitami v naší síti. □

Odkazy

www.juniper.net/products/intrusion
www.snort.org
www.enterasys.com/products/ids
www.sourcefire.com
www.finisar.com
www.networkinstruments.com/products/ntaps
www.apcon.com