

NIKOLI VIRTUÁLNÍ BEZPEČNOST

Jak virtualizovat bezpečně

Pravděpodobně jste již zaznamenali informace hovořící o slabinách hypervizoru i o možném malwaru, který by jej napadal. Se zabezpečením virtualizace je tedy nutné se vypořádat stejně jako s dalšími problémy bezpečnosti ICT. Zjednodušeně řečeno, je třeba na ni myslet hned od počátku.

Výběru bezpečnostní brány zcela určitě musí předcházet znalost jednotlivých technologií a pro jejich pochopení je vhodné znát i historii.

Vraťme se tedy do minulosti, do doby, kdy poprvé člověk stanul na Měsíci, tedy do roku 1969, kdy vznikl ARPANET, předchůdce internetu. Cílem tohoto projektu bylo propojit 4 lokality po USA a řešil se pouze způsob přenosu dat, nikoli jejich bezpečnost. Tehdy k tomu byl použit NCP předchůdce dnešního TCP/IP protokolu, který vznikl až v roce 1983. Z původních 4 uzlů se ARPANET v roce 1973 rozrostl na 40 uzlů a překročil hranice Spojených států. S rozšířením ARPANETu docházelo i k hlášení prvních významných bezpečnostních problémů. I přesto trvalo dalších 5 let, než se zrodil první nástroj, který se zaobírá bezpečností, a dalších deset let, než vznikl první firewall.

Z výše uvedeného vyplývá, že z počátku internetu (resp. ARPANETu) byla bezpečnost až na posledním místě a dnes dohání to, co v minulosti bylo zanedbáno. Nicméně jsme se stále nepoučili z minulosti a máme tendenci bezpečnost řešit až nakonec. Je třeba se jí zabývat hned od samého začátku, při implementaci jakéhokoli prvku nebo jakéhokoliv nového přístupu, například nyní při hromadně realizované virtualizaci.

Firewall, jak se vlastně zrodil?

Z počátku se bezpečnost řešila na velmi nízké úrovni, hlavně rozšířením funkcí switchů a routrů. Cílem bylo oddělit svou vlastní síť od internetu. Reálné bezpečnostní prvky vznikly až v 90. letech. Průkopníkem v této oblasti byl projekt SEAL, na jehož vedení se podíleli Marcus Ranum

a Fred Avolio a z něhož vznikl první firewall FWTK (Firewall ToolKit).

Ve šlépějích FWTK pokračoval i první komerční firewall Gauntlet, který přišel na svět v roce 1993. Vývoj Gauntletu pokračoval ve spojení s Firewallem Sidewinder G2, kde označení G značí Gauntlet. Dnes tento firewall nese název McAfee Enterprise Firewall (Sidewinder) a dospěl i do virtuálního světa a jeho zabezpečení.

Jak zvolit správný firewall?

Při výběru firewallu je třeba vzít v potaz následující citát: „Ten, kdo se ve jménu bezpečnosti vzdává svobody, nezaslouží si ani svobodu, ani bezpečnost.“ Je třeba dbát na to, aby zvolená bezpečnost nenarušovala zbytečně chod společnosti a bezhlavě neomezovala uživatele. Musíme si uvědomit, že zavádění nových technologií jde ruku v ruce s jejich zabezpečením, tj. již při výběru řešení je zapotřebí myslet na bezpečnost. Do komplexního již fungujícího prostředí vizualizovaných služeb se bezpečnost integruje mnohem obtížněji, než když je součástí prvotního návrhu.

Kriteria pro výběr firewallu mohou být různá, ale rozhodně je třeba se vyvarovat klíše typu, že jen firewall se stavovou paketovou filtrací zajistí společnosti tolik potřebnou propustnost, a nezajímat se o pokročilé ochrany aplikačními proxy firewally. Dnešní aplikační proxy firewally s hybridní technologií poskytnou uživateli srovnatelnou propustnost a na aplikační úrovni mnohdy výrazně vyšší, protože jsou pro tento provoz navrhovány, a navíc přinesou daleko větší bezpečnost než stavový paketový firewall.

Při zamyšlení nad otázkou, ze kterých kritérií vycházet při výběru firewallu, by se také mělo čerpat z jednoduché definice Stevna M. Bellovina, jednoho z průkopníků v oblasti firewallu, který ho definoval, jako zařízení schopné oddělit „nás“ od „nich“

(pod slovem „nich“ si lze představit vše nedůvěryhodné). Samozřejmě k zajištění této funkcionality dochází díky definici politik, kdy politika představuje pravidlo, které je třeba vynutit, aby byla zaručena bezpečnost. Tuto funkcionalitu dnes splňují více či méně každý firewall. Rozdíl však naleznete ve schopnosti účinně a efektivně vymoci dodržení tohoto pravidla.

Pro lepší pochopení si představme, že firewall je celník, jehož cílem je splnit jasně definované pravidlo, které určuje, co má pustit a co ne. Otázkou je, do jaké míry bude účinný? Do jaké míry dokáže odhalit narušitele, aniž by příliš omezoval legitimní provoz. V dnešním světě, kdy nelze takřka ničemu věřit, se tato funkcionalita ukazuje jako nejdůležitější. Jelikož dnes se běžně škodlivý provoz vydává za žádoucí, a proto je nutné vše do hloubky ověřit. Vraťme se k našemu příkladu celníka. Dnes náš celník nemůže věřit tomu, co vidí na první pohled, ale zároveň nesmí příliš omezovat provoz či odbavení. Mohl by celý náklad „kostečku po kostečku“ zkontrolovat a přeskládat na vlastní prověřený vůz, a ten teprve pustit za hranice. To ale při rychlosti běžného provozu není možné, a tak prověří jen běžné symptomy. Aplikační proxy firewally to již umí, a to jsou jeho hlavní přednosti, rychlost a úplnost kontroly – dovnitř sítě jde jen provoz z důvěryhodných proxy (naš vlastní nákladní vůz převážející prověřené zboží). Při sestavování kritérií je třeba považovat propustnost za samozřejmost, ale bezpečnost za nutnost!

Hlavní rozdíl mezi dnes nabízenými firewally je právě v jejich schopnosti rozlišit povolený od nepovoleného provozu s minimální odchylkou. Tato funkcionalita se ukázala jako kritická. Například již v roce 1991, kdy Marcus J. Ranum předvedl světu, jak je snadné zneužít otevření SMTP port k poslání TELNET provozu a oklamat tím tehdy běžně používané firewally.

V případě, že budeme vycházet z výše uvedeného požadavku a z definice pana Bellovina, je nutné, aby firewall plnil funkci jakéhosi prostředníka mezi dvěma sítěmi. A je třeba, aby tuto funkcionalitu byl schopen plnit za všech okolností. Dnes ji plní zcela určitě aplikační proxy firewally s hybridní technologií, které přinášejí ochra-

ny na principu proxy, jejichž cílem je zajistit maximální bezpečnost, za jakýchkoli okolností, právě oním rozkladem provozu a jeho důkladnou kontrolou. Protože podobných řešení na současném trhu, byť tolik potřebných, není mnoho, dovolím si ještě jednou zmínit bránu McAfee Enterprise Firewall (Sidewinder), která má k dispozici IPS integrované do 47 proxy bran, včetně dnes tolik vyžadované VoIP SIP brány, a zároveň nabízí možnost tvorby generických proxy bran pro proprietární služby a dokáže unikátním způsobem chránit kritické služby,

Pro lepší pochopení dopadů virtualizace na bezpečnost uvedme naprosto běžný a reálný případ. V typických architekturách pro aplikace založené na webu jsou web, samotná aplikace i databázový server instalovány na odděleném hardwaru a každý z nich má svůj operační systém, zabezpečený podle individuálních pravidel a také odpovídajícím způsobem patchovaný. Obvykle mezi webovým serverem a backendovým databázovým serverem neexistuje žádný vztah, protože sám aplikační server se chová jako jakýsi proxy server mezi

Musíme znát minulost a poučit se z ní, abychom uspěli v budoucnosti

jako SMTP nebo DNS v DMZ, vnitřní síti nebo ve virtualizovaném prostředí. K ochraně těchto služeb využívá Sidewinder servery (přímo na sobě), které mohou běžet ve split módu (různé pro externí a interní segment), a jsou chráněny proti útokům patentovanou technologií Type Enforcement pracující na principu Mandatory Access Control.

Při výběru bezpečnostní brány je vhodné myslet i na kontrolu šifrovaného provozu. Bohužel již dávno neplatí, že co je šifrované, je bezpečné! Jak asi sami víte, protokol HTTPS není používán jen důvěryhodnými zdroji, jakými jsou například banky, ale též pornografickým průmyslem, či dokonce heckery na různých warez stránkách nebo při pokusech o phishing. Proto je velmi důležité, aby vámi zvolenou bezpečnostní politikou na Firewallu bylo možné aplikovat i na šifrovaný provoz typu https, ssh, sftp a tím zaručit, že ji nebude možné obejít použitím šifrovaného provozu.

Virtualizovat ano, leč bezpečně!

Virtualizace není žádnou novinkou. Dnes se již virtualizují serverová prostředí téměř pro každou aplikaci, která se ve společnosti zavádí, a navíc spousta již aktuálně užívaných aplikací se do takových prostředí převádí. Se zabezpečením virtualizace je nutné se vypořádat stejně jako s dalšími problémy bezpečnosti ICT. Zjednodušeně řečeno je třeba na ni myslet opět hned od počátku. Pravděpodobně jste již zaznamenali informace hovořící o slabínách hypervizoru i o možném malwaru, který by jej napadal. Dle zveřejněných informací je možné, aby se hacker dostal z operačního systému virtuálního stroje až do OS hostujícího serveru, a tam nasadil rootkity a další druhy škodlivého kódu. Z minulosti víme, že v bezpečnosti ICT je cesta od teoretických hrozeb k reálným velmi krátká a nevyplácí se je ignorovat.

oběma zmíněnými servery. Tím je zajištěno, že pokud se někdo dostal na webový server, nemůže přímo zaútočit proti databázovému serveru.

Ve virtuálním prostředí je to samozřejmě jiné. Webový server, aplikační server i databázový server jsou všechny nainstalovány na jednom hardwaru. Lze tím dosáhnout úspory na nákladech, a dokonce i navýšit výkon. Ovšem pokud nemáte nástroje na potřebné oddělení funkčnosti a vazeb ve virtuálním prostředí, můžete se dostat do velkých potíží. Již zmíněný aplikační proxy firewall od McAfee, tentokrát v podobě software kontejneru pro virtuální servery, dokáže pomoci i zde, a to na potřebné aplikační úrovni. Aplikační proxy vystupují jako server, převezmou požadavek, na aplikační úrovni jej překontrolují a zahájí komunikaci se skutečným serverem. To umožňuje jemnější řízení datového provozu, zadáváním specifických pravidel, a zajistit tak maximální ochranu virtuální farmy. Pro segmentaci zdrojů zde existují také virtuální sítě, jež jsou nakonfigurovány tak, aby bylo zajištěno, že vztahy mezi webovým serverem, i aplikačním a databázovým serverem jsou nastaveny podle opravdových potřeb a že zde nedochází ke zbytečnému navýšení práv. Dobrou zprávou pro všechny je již existující možnost kompletní integrace nových proxy firewallů do stávajícího virtuálního prostředí a schopnost zabezpečit tak vynaložené prostředky na komplexní řešení.

Virtualizované prostředí přináší nejen podstatné úspory, ale již tradičně nové možnosti hrozeb a napadení formou útoků šířených mezi aplikacemi a systémy v rámci virtuální serverové farmy. Naštěstí řešení již existují a nemělo by se tedy na ně zapomínat. □

inzerce ▼

McAfee®

Spojte svoji BEZPEČNOST s leaderem IT SECURITY

Webwasher®

Web Gateway Security

- » Leader Gartner Magic kvadrantu. «
- » Secure Web 2.0 proxy. «
- » Secure Cache. «
- » AntiMalware – vítěz testů od 10/2006. «
- » URL Filtrace SmartFilter. «
- » SSL scanner pro kontrolu https. «

IronMail®

Messaging Gateway Security

- » Leader Gartner Magic kvadrantu. «
- » Přesná a efektivní detekce spamů. «
- » Ochrana proti úniku dat (DLP). «
- » Mail IPS a web mail proxy (OWA, LNWA). «
- » Provázání s LDAP/AD, uživatelské karantény. «

Sidewinder®

Network Gateway Security

- » Nejvyšší možná úroveň zabezpečení. «
- » Model ochrany pomocí aplikačních proxy. «
- » Integrovaný IPS modul s hw akcelerací. «
- » Systém globálních reputací TrustedSource. «
- » Dekryptace SSL pro hloubkovou kontrolu https. «

IntruShield®

Network IPS

- » Leader Gartner Magic kvadrantu IPS sond. «
- » Modely s certifikovanou propustností 10 Gbps. «
- » Až 1000 virtuálních IPS sond per appliance. «
- » Provázanost s Vulnerability Scannerem Foundstone. «
- » Provázanost s McAfee NAC appliance. «

Veškerá řešení formou appliance
PROFESIONÁLNÍ BEZPEČNOST
PROFESIONÁLNÍ SLUŽBY

Distributor pro ČR, SR a Ukrajinu.

COMGUARD
www.comguard.cz; info@comguard.cz