Zabezpečte si virtualizované prostředí

V současné době dochází ke značné migraci serverů z fyzického prostředí do cloudu, ať už jde o privátní nebo veřejné cloudy, tedy k postupné virtualizaci kritické infrastruktury organizací z důvodu zvýšení efektivity správy IT a snížení samotných nákladů na provoz systémů. S tímto trendem je však nutné dbát i na fakt, že bezpečnostní řešení, která jsou jinak ve fyzickém prostředí efektivní a dostačující, nejsou přizpůsobená provozu v tom virtuálním.

RENÉ POSPÍŠIL

Pokud se bavíme o tzv. ochraně koncových bodů, je využití klasického plného antimalwarového klienta v tomto prostředí neefektivní a vyžaduje v obecném hledisku velké množství výpočetních zdrojů v datecentrech.

Kromě toho dochází k duplicitám skenů a při současném stahování signatur či skenování jednotlivých strojů k „zamrznutí" samotného hypervizoru – vznikají tak „antivirové bouře".

Proto výrobci v oblasti antimalwarové ochrany přicházejí se specializovanými řešeními pro ochranu virtualizovaného prostředí. Většina z předních dodavatelů však používá pouze princip založený na využití rozhraní vShield u virtualizační platformy VMware vCenter.

To je ale bohužel návrat z hlediska bezpečnosti do období 90. let, kdy se využívalo čistě skenování souborů. Paměť, procesy a registry se tímto přístupem nechránily. Navíc vShield omezuje skenování souborů pouze na MS Windows. Další neduh rozhraní vShield spočívá v tom, že má pouze jeden „host driver", a tím pádem s ním nelze docílit vysoké dostupnosti.

Modernějším trendem jsou řešení, která nabízejí multiplatformní přístup s využitím tzv. lehkých agentů, kteří nabízejí plnou ochranu tak, jako tomu je u klasických agentů ve fyzickém prostředí, a navíc dokážou šetřit výpočetní zdroje samotného hypervizoru.

Taková řešení přenášejí samotný proces skenování z lehkého klienta centrálně na speciální bezpečnostní virtuální appliance instalované ve vysoké dostupnosti.

Ty ve své podstatě představují virtuální stroje, které jsou kompaktně upravené k bezpečnostním úlohám a po jednoduché konfiguraci jsou ihned připravené k použití.

Jelikož jsou už předinstalované, jsou také rychle nasaditelné, navíc dokážou deduplikovat skenovací procesy pomocí deduplikační globální cache. Lepší řešení pak používají globální bezpečnostní síť k ochraně v reálném čase, imunizující proti hrozbám známým či neznámým do několika sekund.

Díky sdílené reputaci jednotlivých aplikací se pak vyloučí zbytečné mrhání výpočetním výkonem pro monitorování aplikací nebo procesů, které mají dobrou reputaci. Díky takto vyladěné architektuře se pak dají významně ušetřit provozní náklady.

Velmi důležitá je pak navíc úspora za nepotřebné licence Windows Serveru a SQL databází, jelikož jsou taková řešení postavená na Linuxu „hardended" OS a open source databázích. Odpadá tak zároveň často zdlouhavá instalace softwaru třetích stran a jejich spravování a záplatování.

V neposlední řadě je důležitá přímá integrace s hypervizory, po stránce jednoduché správy bezpečnostních pravidel je pak možné přímo načíst například VCenter nebo třeba XenServer infrastrukturu přímo do webového rozhraní správy.

Ideální je pak, když řešení dovolí míchat více VS/VDI platforem a zároveň i fyzickou infrastrukturu spravovat v rámci jednoho webového rozhraní.

Kompromitace samotného hypervizoru

V drtivé většině všech útoků na datacentra hraje roli buď špionážní, nebo finanční motiv. Zajímavou informací je také fakt, že většina těchto útoků je odhalena až po půl roce jejich působení.

Jde především o útoky, které mají za cíl převzít administrátorská práva nad daným virtuálním strojem a získat z něj informace, sabotovat systémy, ukrást identity. Problémem většiny dosavadních řešení je, že útočník v případě průlomu často získává stejná práva jako administrátor a pak útočí na samotné procesy antiviru, aby ho vyřadil z provozu.

Největší novou hrozbou jsou viry vytvořené za účelem kompromitovat bezpečnost celého hypervizoru, a jelikož se tento kód často spouští na úrovni jádra, je tím pádem těžce odhalitelný a odstranitelný pro drtivou většinu dnešních antivirových řešení.

Moderním postupem ochrany proti takovýmto a dalším hrozbám je nahlížení do paměti, rozpoznání a blokace hrozby na úrovni analýzy paměti samotného hypervizoru – této nové metodě se také říká HVI (Hypervisor Introspection).

Představte si bezpečnostní řešení, které má vyšší práva než samotný útočník na jednotlivých strojích. Dokázali byste tak blokovat cílené útoky z pozice vyšší instance, která by byla navíc kompletně izolovaná od potenciálně infikovatelného prostoru hosta samotným hypervizorem.

To, kam se ochrana virtualizovaných platforem ubírá, je bezagentové řešení s minimálním vlivem na zdroje, které odchytává útoky na úrovni paměti samotného hypervizoru a je schopné kontrolovat z této vrstvy paměť jednotlivých hostů z pohledu prostoru uživatelského a kernelu (jádra).

HVI tedy nahlíží do paměti přímo tam, kde se útočný kód nemůže skrýt, ani bránit, a z bezpečné, pro útočníka neviditelné úrovně pak odstraní známé či neznámé hrozby ve všech variantách, a to dokonce i bez znalosti toho, jakou konkrétní zranitelnost útočník využil.

Je to zcela nová bezpečnostní vrstva, která může koexistovat s libovolným řešením EPP (Endpoint Protection Platform) a chrání proti unesení přístupů do vaší infrastruktury. ■

Autor pracuje jako security strategist pro Bitdefender.cz.