Unikátní Bitdefender HVI

ONDŘEJ DESENSKÝ

Většina dnešních datacenter je chráněna agentovým způsobem, kde v každém chráněném virtualizovaném stroji běží buď klasický, nebo lehký agent. Existuje ovšem ještě novější, zcela bezagentový přístup, nedávno uvedený na trh průkopníkem v oblasti ochrany virtualizačních platforem, firmou Bitdefender. Tento přístup se nazývá Bitdefender Hypervisor Introspection (HVI). Asi se teď ptáte, co tento přístup umožňuje, a v čem je tedy unikátní?

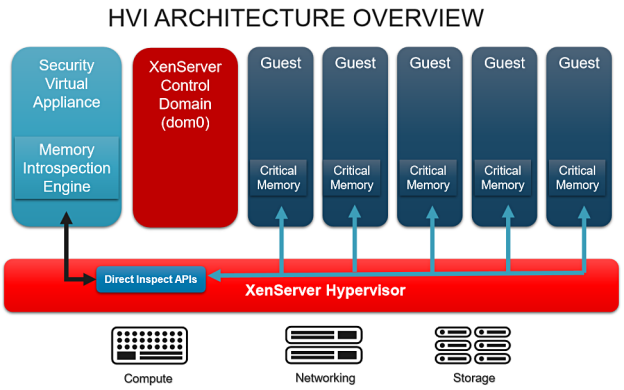
Pojďme si nejprve připomenout a uvědomit si základní problém ochrany IT, a tím je skutečnost, jaká práva má dnešní správce bezpečnosti ve srovnání s útočníkem? Protože běží-li agent na stejném OS, kde se pohybuje také útočník, pak v případě, když se podaří útočníkovi získat práva administrátora, či roota, má stejná práva jako vy, může proto jednoduše útočit na vámi postavené bezpečnostní řešení a může shodit samotné služby ochrany. Všimněte si, že je útočník proto velmi často o krok před vámi.

Existuje na tento problém řešení? Představte si, jaké by to bylo, kdyby veškeré bezpečnostní ochranné funkce byly umístěny o úroveň výše na hypervizoru mimo samotné virtualizované stroje a jejich operační systémy. Co kdybyste mohli přímo nahlížet do pamětí těchto strojů na úrovni hypervizoru a skenovat nezpracované paměťové bloky a pomocí speciálního patentovaného principu analyzovat veškeré útoky přímo na úrovni paměti? Takto byste mohli rozpoznat podezřelé chování a zablokovat známé i neznámé útoky ještě před tím, než se pro ně vytvoří klasické signatury. Co kdybyste dovedli na úrovni paměti pozorovat nebezpečné aktivity a blokovat je, aniž by mohl útočník jakkoliv zasáhnout proti vaší obraně? Dobrá zpráva je, že přesně toho se Bitdefenderu podařilo docílit. Pojďme se tedy detailněji podívat na to, co Bitdefender HVI umí a jak to dělá.

HVI jako ucelená ochrana hypervizoru

Bitdefender HVI je bezpečnostní vrstvou, která posiluje existující infrastrukturu XenApp a XenDesktop proti cíleným útokům pomocí kontroly přístupu do paměti v reálném čase na úrovni hypervizoru.

Bitdefender společně s firmou Citrix přináší tento nový radikální přístup ochrany koncových bodů. Citrix XenServer obsahuje API pro přímou inspekci, a je tedy zatím jediným hypervizorem, který je schopný přinést introspekci paměti virtuálních strojů. Tento přístup eliminuje slepá místa v architektuře, zatímco chrání existující vrstvy proti sofistikovaným škodlivým aktivitám založeným na napadení kernelu jako například některé techniky 0-day útoků. To vše bez jakéhokoliv instalovaného softwaru na virtuálních strojích. Takovýto přístup těží z mnoha možností, které úroveň hypervizoru poskytuje. Umožňuje izolovanou ochranu mimo dosah útočníka a nezanechává stopy na chráněných virtuálních strojích.



Klíčové funkce

- HVI je naprosto bezagentové zabezpečení na úrovni hypervizoru.
- Implementuje se jako zabezpečená virtuální appliance, HVI řídí přístup k řízení hardwaru, aby bylo možné ochránit virtuální stroje s právy nadřazenými škodlivé aktivitě.
- Je kompletně hardwarově izolované od škodlivé aktivity, nemůže být kompromitováno.
- Umožňuje introspekci paměti v reálném čase, která identifikuje hrozby již z raw dat paměti virtuálních strojů.
- Bezprecedentní vhled do technik 0-day a kernel-level útoků.
- GravityZone je plně integrovaná s XenServery pro vynikající správu politik.
- Poskytuje lepší než fyzické zabezpečení díky API pro přímou inspekci XenServeru.
- Je plně kompatibilní se všemi vrstvami Citrix Ready.
- Efektivní skenování bez aktualizací signatur

Namísto skenování skrze miliony signatur nebo metriky závadného chování detekuje introspekce paměti asociované techniky útoku, které jsou viditelné pouze na úrovni hypervizoru. Identifikuje 0-day útoky stejně lehce jako známé exploity. Bitdefender HVI nepotřebuje aktualizace signatur, dokud se techniky útoků nezmění.

Bitdefender HVI pomohl zastavit WannaCry

Útoky jako WannaCry mohou způsobit dočasnou nebo trvalou ztrátu citlivých dat a narušují běžný provoz stejně jako finanční ztráty spojené s obnovou systémů a souborů nebo zničující dopad na reputaci organizace. Čím více je útok zacílen na konkrétní infrastrukturu, tím větší je také poškození, které může způsobit.

Jakožto řešení mimo operační systémy má HVI bezkonkurenční vhled do celé paměti, kde také zastaví WannaCry přímo ve fázi exploitu. Nezaručuje pouze, že ransomware nezačne šifrovat, ale také že se žádný škodlivý kód, který byl kdy vytvořen, do zařízení nedostane.

WannaCry je pouze příkladem, co se může stát, když se rozšířená zranitelnost spojí s rafinovaným exploit kitem a škodlivým ransomwarem.

Exploit EternalBlue, který WannaCry využíval k tomu, aby se tak rychle šířil, byl znám o týdny dříve, než jej objevila skupina The Shadow Breakers. Nedlouho poté publikoval Bitdefender na svém blogu článek zobrazující, jak Bitdefender HVI detekuje a blokuje EternalBlue dlouho před tím, než se WannaCry někde objevil.

HVI je navrženo tak, aby zvládalo pokročilé exploity, jako je EternalBlue, nebo dokonce 0-day (dosud neznámý exploit daleko těžší na detekování a často používaný k cíleným útokům). HVI skenuje na úrovni hypervizoru nezpracované paměťové bloky, což bylo dříve považováno za nemožné.

Znamená to tedy, že Bitdefender HVI může chránit proti široce rozšířeným zranitelnostem systému Windows (MS17-010), a to již dlouho předtím, než na ně Microsoft přijde a vydá aktualizaci.

Bitdefender HVI chrání velmi účinně proti novým neznámým hrozbám, a protože pracuje na úplně oddělené úrovni, lze ho kombinovat s jakoukoliv existující vrstvou ochrany. Více informací naleznete na stránkách bitdef.cz. Produkty Bitdefender jsou lokalizovány do českého jazyka a mají přímou podporu výrobce v ČR a SR.

Autor pracuje jako security solution architect ve společnosti IS4 security