Vážené čtenářky, vážení čtenáři,

stále více organizací využívá softwarové appliance, tedy systémy dodávané jako virtuální stroje. Jde o oblíbený způsob, jakým dodavatelé softwaru distribuují své produkty podnikovým zákazníkům, protože obsahují všechny potřebné předkonfigurované sady, které jejich aplikace potřebují, a zároveň je lze snadno nasadit v cloudech či on-premise datových centrech.

Podle nedávno zveřejněné studie společnosti Orca Security jsou však tyto systémy jedním ze zdrojů bezpečnostních hrozeb, a to často už ve chvíli, kdy je jako binární kopii instalujete. Zjistilo se navíc, že řada prodejců včetně těch známých opravuje chyby a aktualizuje softwarové komponenty velmi ledabyle.

Orca naskenovala 2 218 binárních obrazů virtuálních zařízení od 540 dodavatelů, které se distribuovaly na veřejných tržištích běžných cloudových platforem, jako jsou VMware, Amazon Web Services (AWS), Microsoft Azure nebo Google Cloud Platform. Appliance byly jak komerční, tak i volně použitelné.

Společnost vytvořila bodovací systém, který zohledňoval, zda například systémy obsahovaly jednu nebo více ze 17 významných a vysoce rizikových zranitelností, jako jsou Heartbleed, EternalBlue či DirtyCOW, jestli zahrnovaly nějakou kritickou zranitelnost (nad CVSS 9) nebo měly jednu nebo více chyb hodnocených jako CVSS 7-9.

Patnáct procent testovaných appliancí vůbec neprošlo, dalších 16 % obdrželo hodnocení „špatné", 25 % mělo „průměrné" a 12 % „nadprůměrné". Pouze 32 % systémů dostalo vynikající hodnocení. Celkově skenování firmou Orca identifikovalo 401 571 chyb zabezpečení. Následně bylo aktualizovaných 287 produktů a 53 se odstranilo z distribuce.

Téměř polovina appliancí se přitom za poslední rok vůbec neaktualizovala a pouze 2,8 % bylo updatovaných nejdéle měsíc před průzkumem (dalších 14 % pak během předchozích tří měsíců). I když mnozí výrobci projevili snahu o nápravu, 24 prodejců se problémem odmítlo zabývat, a dalších 32 dokonce uvedlo, že jde o záležitost, kterou si mají řešit sami zákazníci.

Je tedy zjevné, že i dobře zavedení prodejci softwaru mohou dodávat problematické aplikace. Také podle výzkumníků není zárukou, že dražší systémy jsou zároveň i bezpečnější nebo lépe udržované.

A co doporučuje sama Orca? Především by vám měl pomoci systém pro asset management, který vám poskytne dostatečné informace o tom, jaké virtuální zařízení máte u sebe i v cloudu nasazené. Zapomenout byste ale neměli i na případné stínové IT.

Pomoci mohou i systémy pro správu zranitelností, které by měly při svém skenování brát v úvahu právě i appliance. Soustředit by se ale měly především na nejzávažnější chyby.

Virtuální zařízení byste tedy měli používat velmi opatrně a raději je sami otestovat, abyste se ujistili, že nemají kritické nedostatky, než je nasadíte do provozu a poskytnete jim přístup k citlivým podnikovým datům. A pokud se staví váš dodavatel k aktualizacím appliancí rezervovaně, měli byste zvážit případnou alternativu.

S přáním příjemně stráveného zimního času i nad stránkami Security Worldu

Pavel Louda
vedoucí projektu

Obsah