Jaké jsou nejnovější hrozby a výzvy moderní ochrany hybridní IT infrastruktury?

Zeptali jsme se v rozhovoru s René Pospíšilem, country managerem za Bitdefender CZ/SK.

Jak byste popsal nejzásadnější výzvy existujících řešení ochrany hybridní IT infrastruktury?
Jednoznačně největší výzvou je to, že už není možné bez umělé inteligence docílit akceptovatelných výsledků ochrany. Jednoduše proto, že dnes se musíme rozhodovat řádově v sekundách, a ne v jednotkách hodin. Bylo to vidět například při nedávném útoku WannaCry, kdy z více než 40 výrobců detekovalo v prvních hodinách jen pět.

Dále pozorujeme také čím dál tím více cílené útoky na konkrétní instituce, což vede k tomu, že se firmy snaží bránit vrstvením více řešení, aby zvýšily úroveň ochrany, což s sebou často nese ztrátu výkonu a následné konflikty několika nekompatibilních řešení, a ty pak vedou k tomu, že administrátoři vypnou některé zásadní funkce, a tím sníží zase ochranu. A proto doporučuje Gartner použít vícevrstvou ochranu, ale od jednoho výrobce, který musí zaručit, že budou všechny vrstvy mezi sebou odladěny, a zákazník tak získá maximální ochranu bez ztráty výkonu. Je třeba zároveň volit řešení s ucelenou jednotnou správou přes všechna fyzická, virtualizovaná i cloudová prostředí, a zamezit tak duplikaci pravidel a konfliktů ve správě.

Kam se ubírá dnešní moderní ochrana proti pokročilým hrozbám (APT) či cíleným útokům?
Největší výzvou ochrany jsou rychlost a přesnost rozhodování, především ve fázi před spuštěním samotné aplikace či služby v produkčním prostředí. Ta nejmodernější řešení musejí mít postavenou detekci proti pokročilým hrozbám a útokům nultého dne na efektivních samoučících se algoritmech strojového učení. Přičemž záleží především také na kvalitě a přesnosti těchto algoritmů, tak aby měly co nejnižší chybovost po stránce falešných poplachů. Proto moderní řešení umožňují individuální nastavení „agresivity“ algoritmů a jejich módů od reportování až po následnou blokaci kódu před jeho spuštěním. Nejmodernější řešení

dovedou pak zamezit i pokročilým novým útokům, které jsou vedeny bez nutnosti spuštění souboru (fileless) na cílové kompromitované stanici.

Jaké zásadní nové funkcionality musejí obsahovat bezpečnostní řešení nejnovější generace?
Ta nejmodernější řešení jako například Bitdefender Gravity Zone HD Elite používají až šestivrstvou ochranu s důrazem na detekci před spuštěním pomocí umělé inteligence, dotazování se globální bezpečnostní sítě a spouštění podezřelých aplikací v síti výrobce za účelem hloubkové analýzy v zabezpečeném sandboxovém prostředí u výrobce na výkonné, za tímto účelem vytvořené infrastruktuře. Zároveň se musejí umět tato řešení přizpůsobit potřebám a schopnostem zákazníka. Musejí umožňovat například kombinované nasazení jak v cloudu, tak on premise i běžet na jakékoliv virtualizované platformě.

Jaká úskalí skýtá ochrana virtualizovaného prostředí?
Největším úskalím je zbytečné mrhání zdroji, protože většina řešení používá klasické klienty, které byly vytvořeny za účelem ochrany fyzických strojů, a tím pádem duplikují virové databáze na každém VS.

Dalším nevhodným přístupem je například použití rozhraní vShield, které umožňuje pouze skeny souborů, a v takovém případě nelze chránit paměť, služby ani registry.

Moderní řešení proto musejí kombinovat to nejlepší z fyzické a virtuální ochrany dohromady, tzn. použít lehké klienty, které fungují jako brány zasílající jen části neznámých podezřelých souborů na centrální security appliance ve vysoké dostupnosti s globální deduplikací skenů, tak aby bylo docíleno co nejmenší utilizace IT zdrojů a zároveň bylo možné chránit všechny potřebné části VS.

Podle jakých kritérií by měli zákazníci vybírat vhodné řešení?
Nejlepším měřítkem kvality je pozorovat nezávislé laboratoře jako av-test.org anebo av-comparatives.com a zprůměrovat výsledky detekce v reálných testech za posledních pět let.

Pro většinu zákazníků postačí čtyřvrstvá ochrana s klasickými signaturami, lokálním sandboxem, pokročilou ochranou procesů v reálném čase a dotazováním do bezpečnostní sítě s SLA několika sekund. Ovšem pokud máte vysoké nároky na bezpečnost a obáváte se cílených útoků, doporučujeme další dvě vrstvy navíc, konkrétně pokročilou ochranu pomocí umělé inteligence (hyper detekci) se speciálními algoritmy pro ochranu proti cíleným útokům a dále pokročilou analýzu v sandboxovém prostředí výrobce v cloudu, kde mohou probíhat bezpečně intenzivnější inspekce. Pro ty zákazníky, kteří disponují bezpečnostními analytiky, je vhodné rozšířit funkcionalitu o EDR (Endpoint Detection Response) řešení obsahující pokročilou detekci, vizualizaci útoku s pokročilým reportováním a hloubkovou analýzou útočného kódu, vše ideálně od jediného výrobce.

V neposlední řadě je potřeba prověřit, jestli dovede výrobce věrohodně potvrdit soulad s GDPR a absenci zadních vrátek ve správě vybraného řešení.