BEZPEČNOST NA ÚROVNI SÍTĚ? ANO, ALE...

JAN ŠVEŇHA

S rozvojem bezpečnostních technologií a zařízení můžeme pozorovat, že stále rostoucím trendem je budování bezpečnosti na úrovni síťové komunikace. Každý, kdo pracuje v této oblasti, si je vědom toho, že budování bezpečnosti na úrovni sítě přináší mnoho výhod, nevýhod a dokonce i zásadních problémů. Sami výrobci těchto zařízení a řešení přiznávají, že jejich ochrana není stoprocentní. Ale obávám se, že výrobci toto přiznávají a připouštějí nikoliv z důvodu, že by chtěli své partnery a zákazníky varovat před problémy implementace bezpečnostních řešení na úrovni sítě, ale spíše z alibismu, kterým se předem vyhýbají zodpovědnosti v případě, že jejich bezpečnostní řešení selže.

Rozhodl jsem se proto v následujícím textu upozornit na výhody, nevýhody a problémy při nasazování bezpečnosti na úrovni sítě s ohledem na současné trendy. Nakonec si dovolím dát malé doporučení, jak k těmto technologiích přistupovat a efektivně je nasazovat. Pojďme si to rozebrat.

Next-generation/UTM firewally

Naprostá většina podnikových sítí dnes již disponuje tzv. next generation nebo Unified Threat Management firewallem. Dalo by se déle polemizovat o tom, jaký je mezi těmito pojmy rozdíl, ale to není cílem článku, tak předpokládejme, že jde o zařízení se shodnou sadou funkcí, kterými jsou například: intrusion prevention system, application control, web filtering, antivirus, antispam, DLP a v dnešní době již mnoho dalších funkcí. Buďme ale upřímní, málokterý zákazník skutečně dokáže využít všechny tyto funkcionality, a to ze dvou různých důvodů:

1) Nasazení těchto funkcí mezi všemi segmenty sítě je výkonově náročné a málokdo si může dovolit zakoupit firewall tak výkonný, aby tak mohl učinit.

2) Mnoho funkcí na těchto firewallech ani zdaleka nedosahuje kvalit, které zákazník většinou požaduje. Proto se tedy musíme omezit na základní skupinu funkcí, které jsou již ověřené a víme o nich, že jsou kvalitní a vhodné pro každodenní používání s ohledem na globální nasazení.

Jaký tedy máme výsledek u firewallů? Zákazník zakoupí zařízení, ze kterého využije jen část funkcionalit. Navíc většina těchto funkcí využívá metodu detekce známých hrozeb a ty funkcionality, které dokáží detekovat v reálném čase hrozby nové, přinášejí značné množství tzv. false positive hlášení.

Dedikovaná bezpečnostní zařízení – Web, Mail, IPS

Dále budu popisovat problematiku tří nejrozšířenější dedikovaných bezpečnostních zařízení založených na detekci na úrovni síťového provozu.

Webová ochrana, ať už z pohledu návštěvy webových stránek, nebo z pohledu ochrany webového serveru, je zajisté velmi efektivní způsob, jak chránit uživatele od návštěvy závadného či škodlivého obsahu nebo jak zabránit útočníkům využít zranitelností v našich webových stránkách či na našich webových serverech. Upřímný linuxář vám řekne, že žádné webové stránky, které běží na webovém serveru Apache, nejsou nikdy v bezpečí. A co si budeme povídat, Microsoft IIS na tom nebude o moc lépe. Proto je webová proxy a web aplikační firewall dobrou volbou, jak tuto bezpečnost zvýšit. K dosažení maximální efektivity je ale zapotřebí vybírat taková řešení, která nejsou založena pouze na detekci známých hrozeb, ale například na systému, kdy se web-aplikační firewall naučí strukturu webových stránek a povolí použití jen dané sady http příkazů. Nebo integrace webové proxy s tzv. sandboxingem. U sandboxingu je zapotřebí zmínit, že jde vždy o post analýzu, kdy je již potencionálně závadný obsah doručen k uživateli. Výjimkou jsou mailové služby, o kterých budu psát v následujícím odstavci.

Statistiky, které vypovídají o tom, jakým způsobem dojde nejčastěji v podnikové síti k nákaze, hovoří na prvním místě vždy o mailové komunikaci. Je logické, že pro útočníky je nejsnazší se pokusit zacílit přímo na uživatele a využít tak jeho důvěřivosti. Musíme si ale přiznat, že antispamové databáze většiny bezpečnostních společností jsou kvalitní a k uživatelům nechají projít jen naprosté minimum spamu a hrozeb. A přesto se podívejme na útoky typu ransomware, které většinou projdou k uživateli skrze e-mail. Jedna věc je totiž armáda robotů, která odesílá mnoho spamu, který je pro výrobce relativně dobře identifikovatelný, a druhá věc je, když se skupina útočníků rozhodne vytvořit seznam e-mailových adres, na které z gmailového účtu zašlou novou mutaci ransomwaru využívající maker v Microsoft Excel. Narážíme tedy opět dokola na ten samý problém, že tato ochrana je založena na základě detekce známých hrozeb. Naštěstí s příchodem sandboxingu získáváme možnost e-mail pozdržet otestovat a nakonec na základě výsledku ze sandboxu zahodit, nebo doručit. Toto je velká výhoda, kterou nám možnost pozdržet e-mail o pár minut přináší. Jenže e-mail je jen jednou z možností, jak kyberneticky zaútočit na organizaci. Pokud se útočník rozhodne zaútočit zrovna na vaši společnost, tak rozhodně může zkusit využít cílených útoků, které využívají všelijakých zranitelností a chyb v systémech.

Tím jsme se plynule dostali k další části, kterou je intrusion prevention system. IPS nám tedy pomáhá chránit proti různým zranitelnostem v operačních systémech, aplikacích apod. Nebudeme příliš dlouho zdržovat a rovnou napíšeme, že se opět setkáváme se stejným problémem, kterým je detekce na základě databáze známých hrozeb. Bezespornou výhodou je ale doručení záplaty, kdy administrátorovi (například MS Windows serverů) může trvat týdny i měsíce, než zaktualizuje všechny operační systémy zasažené chybou. V takovém případě nasazení záplaty v podobě IPS signatury zabere pouze pár minut nebo dokonce sekund, a to samozřejmě s možností učinit tak zcela automaticky... tedy... aspoň u některých výrobců.

Zatím dobrý, teď přichází PROBLÉM!

Respektive dva problémy. Začnu tím „menším“ problémem, kterým je segmentace a propustnost sítě.

Pokud chceme zajistit aktivní bezpečnost na úrovni sítě, tak musíme vytvořit takové podmínky, aby přes naše bezpečnostní zařízení procházela veškerá data, což se nám ale nikdy nepovede. Jak jsem již zmiňoval výše, tak většina organizací není schopna vytvořit dostatečně velký rozpočet na rozvoj IT bezpečnosti, aby zajistila nákup firewallu s dostatečným výkonem, který by dovolil zapnutí bezpečnostních funkcionalit mezi všemi segmenty sítě. Stejně je tomu tak i s dalšími bezpečnostními zařízeními. Organizace tedy chápou, že je zapotřebí zakoupit NGFW, IPS, Proxy, zabezpečení mailu apod., ale po vytvoření rozpočtu a nakoupení zařízení se při implementaci začíná tím, že se rozhodne, co nebude monitorováno, protože zařízení nemá dostatečný výkon. To samozřejmě není případ všech společností, ale přesto si musím stát za tím, že se nám nikdy nepovede zajistit, aby přes naše bezpečnostní zařízení procházela veškerá data. Co taková komunikace uvnitř jednoho segmentu sítě? Uživatelský počítač s vedlejším uživatelským počítačem. Princip síťové komunikace je nastaven tak, že takový stroj komunikuje pouze přes nejbližší přepínač a tím to končí. Ještě bych měl zmínit propustnost, která dokáže být v dnešní době na centrálním přepínači v hodnotách desítek gigabitů. V takovém případě už nemusí jít vůbec o peníze, ale o to, že žádné bezpečnostní zařízení nemá dostatečný výkon takový provoz obsloužit.

A ten největší a nejzásadnější problém, který z mnoha síťových bezpečnostních zařízení dělá drahé stroje na výrobu vyšší odezvy sítě, je SSL komunikace. Na webových stránkách Transparency Report, které zpracovává společnost Google, se můžete dočíst, že přes 80 % webových stránek v dnešní době využívá SSL šifrování. Útočníci se rozhodně nenechali zahanbit a ke své síťové komunikaci (dle společnosti Gartner) využívají přes 60 % SSL šifrovaného provozu. To znamená, že zařízení nebo organizace, které nedisponují SSL inspekcí, nejsou schopny zachytit 60 % hrozeb, které na ně útočníci přímo či nepřímo posílají. Toto číslo je samozřejmě jen orientační, ale i tak je to děsivé. Zvlášť, když report výrobce říká, že zachytí 99,8 % hrozeb. Ne, že by lhali, jen berou v potaz nešifrované kanály. Asi si teď spousta lidí řekne: „Jsem v pohodě, mám nasazenou SSL inspekci“. Pojďme se na SSL inspekci podívat zblízka.

SSL inspekce, pokud ji nasazujeme, přináší tři základní problémy:

- Musíme zajistit ochranu soukromí uživatelů, tak jak nám to nařizuje zákon.
- Musíme zajistit integritu dat – což znamená, že data, která dešifrujeme, nesmí být žádným způsobem upravena předtím, než jsou doručena k uživateli.
- Zachování úrovně bezpečnosti.

Už první bod nám bude dělat vrásky na čele. Seznam výjimek, jako jsou banky, nemocnice, školy apod., je tak velký a dynamický, že nám ani předdefinované seznamy od výrobce

zcela nepomůžou. To může být ale maličkost proti tomu, kdy velká spousta zařízení zasahuje do integrity dat a částečně (ačkoliv pro uživatele neznatelně) mění jejich strukturu. No a poslední bod nesplňuje naprostá většina výrobců, kdy nám tento požadavek říká, že šifrovací sada, která je použita od našeho dešifrovacího zařízení směrem k uživateli, musí být na stejné úrovni nebo vyšší, jako byla použita na serveru. Ještě si mohu přisadit jeden problém, kdy dešifrovací zařízení nejsou schopna detekovat SSL provoz na jiném portu, než jsou porty standardní (443, 22, 993). Není to zas tak velká práce pro útočníka zvolit si port jiný.

U SSL inspekce ještě chvíli zůstaneme. Všechny majoritní webové prohlížeče a nejnavštěvovanější webové servery (např. Facebook) nasadily funkcionalitu s názvem HTTP script transport security. Nebudu se rozepisovat o tom, jak zmíněné funguje, ale rovnou napíšu, že to znamená, že váš kořenový certifikát na dešifrujícím zařízení musí být důvěryhodný pro všechna koncová zařízení. Tedy například i pro návštěvy, speciální zařízení apod. Z toho nám vychází vytváření dalších výjimek z bezpečnosti. To ale není vše, tato bezpečnostní funkce zároveň dokáže vynutit určité dané parametry důvěryhodného certifikátu. V tuto chvíli s SSL inspekcí selháváme zcela. Bohužel je jen otázkou času, kdy na tento systém přejde naprostá většina poskytovatelů webových služeb. Co se tedy nabízí jako způsob šíření malwaru? Facebook, Google plus, Skype apod.

To ale není vše. Společnost Google přichází s myšlenkou veřejného seznamu důvěryhodných certifikátů, kdy se prohlížeč bude moci do tohoto seznamu podívat a ověřit si, že certifikát není podvržený. Mohli bychom tedy říct, že ani budování bezpečnosti na síťové úrovni není hudbou budoucnosti?

Naštěstí nic není tak hrozné, jak to na první pohled vypadá, ale to, o čem píši v předchozím odstavci, je rozhodně velmi závažné.

Doporučení

V předchozích odstavcích jste se dočetli, že síťová bezpečnost není ani zdaleka tak efektivní, jak nám mohou výrobci prezentovat. Přesto ale musím potvrdit, že například next-generation nebo UTM firewally jsou základními stavební kameny každé podnikové sítě a je rozhodně nutné takové zařízení ve své síti mít. Organizace ale nesmí na tato zařízení spoléhat jako na univerzální řešení svých problémů. Jsem si vědom toho, že mnoha lidem se bude následující doporučení zdát nereálně nákladné, ale dle mého názoru je jen otázkou času, kdy rozpočet na IT bezpečnost bude z donucení natolik vysoký, že navrhované nebude takový problém.

Pokud chceme opravdu efektivně ochránit naší podnikovou síť, tak musíme začít na našich koncových stanicích. Všechny funkce, které jsem zmiňoval v průběhu článku, je možné nasadit i na koncových zařízeních. Navíc ve velmi dobré kvalitě a za rozumnou cenu. A to včetně funkcí, jako je sandboxing, IPS, antispam, web filtering apod. Nevýhodou tohoto řešení je jeho složitější implementace a komplexnější správa, kdy musíme zajistit ochranu každého koncového bodu zvlášť. Navíc bez síťové bezpečnosti by ochrana koncových bodů byla naprosto přetížena, takže by byl přetížen koncový bod jako takový. Je tedy zapotřebí budovat vícevrstvou bezpečnostní architekturu založenou na jednom nebo i více prvcích, kdy síťová bezpečnost filtruje majoritní množství hrozeb (ať už na základě jednoduché IP reputační databáze, nebo na základě aplikačních signatur) a ochrana koncových bodů zajišťuje jemnější ochranu proti neznámým hrozbám (vulnerability scan, strojové učení, sandboxing) nebo proti známým hrozbám přicházejícím z kanálů, které síťové řešení nemůže ochránit (SSL, USB, interVLAN apod.).

Autor pracuje jako pre-sale consultant ve společnosti Veracomp