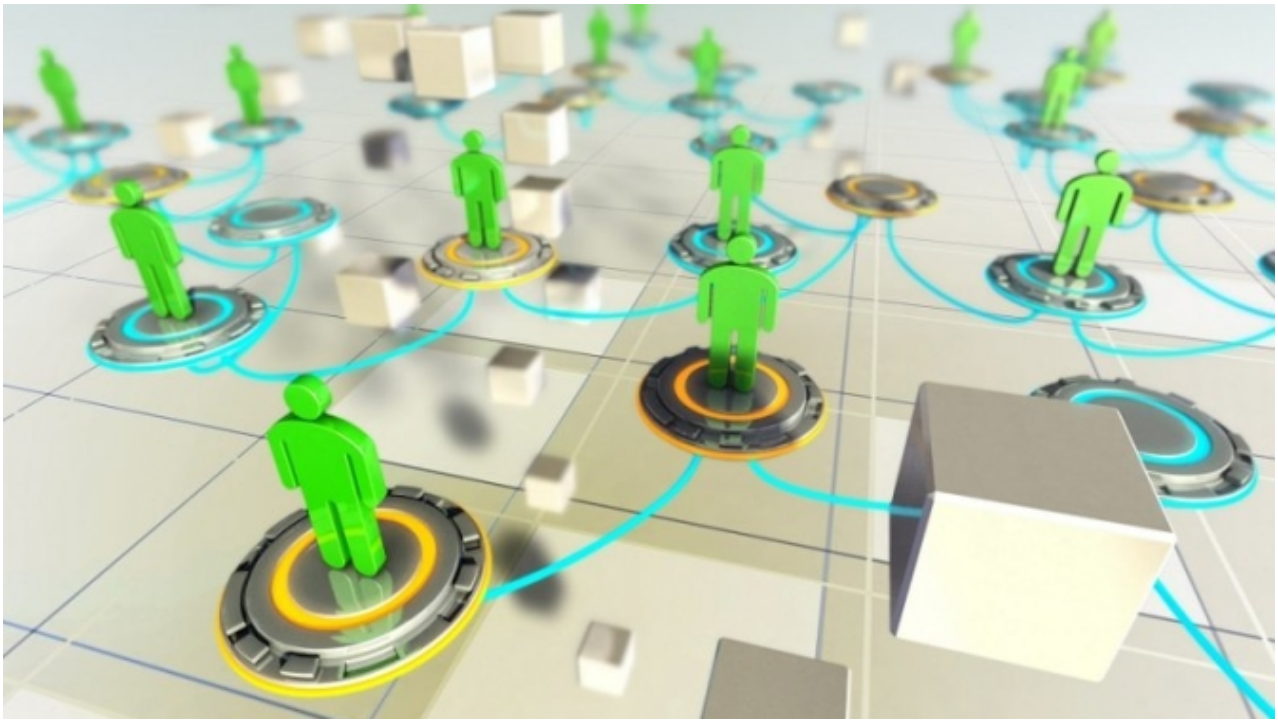
Mikrosegmentace zlepšuje zabezpečení sítě

computerworld.cz/clanky/mikrosegmentace-zlepsuje-zabezpeceni-site



Autor: (c) Fotolia - Andrea Danti

Mikrosegmentace je metoda vytvoření bezpečných zón v datových centrech (DC) a cloudu, které umožní firmám izolovat pracovní zátěže od sebe navzájem a individuálně je zabezpečit. Je zaměřena na zajištění větší granularity sítě.

Segmentace sítě není novinka. Společnosti využívají firewally, virtuální lokální sítě (VLAN) a seznamy řízení přístupu (ACL) pro segmentaci sítě již léta. Při mikrosegmentaci se zásady uplatňují na individuální pracovní zátěže pro zajištění větší odolnosti vůči útokům.

„VLAN umožňují velmi hrubozrnnou segmentaci a mikrosegmentace dovoluje segmentaci jemnější. Kdekoli tedy potřebujete zajistit detailní rozdělení přenosů, najdete ji tam," uvádí analytik Zeus Kerravala, zakladatel společnosti ZK Research.

Vzestup softwarově definovaných sítí a síťové virtualizace připravil cestu pro mikrosegmentaci. „Můžeme dělat věci softwarově na vrstvě, která je oddělená od nosného hardwaru," tvrdí Kerravala. „V důsledku toho se segmentace zavádí mnohem snáze."

Řízení přenosů v DC

Tradiční firewally, systémy IPS (prevence proti vniknutí) a další bezpečnostní systémy jsou navržené tak, aby kontrolovaly a zabezpečovaly provoz přicházející do datového centra ze severojižního směru.

Mikrosegmentace poskytuje firmám větší kontrolu nad rostoucím množstvím komunikace mezi východem a západem (tj. laterální, boční), která probíhá mezi servery a obchází bezpečnostní nástroje zaměřené na hranici.

Když dojde k průlomu, omezuje mikrosegmentace hackerům možnosti potenciálního bočního průzkumu.

„Většina firem umístí všechny své vysoce hodnotné nástroje zabezpečení do jádra datového centra: firewally a systémy IPS. Provoz severojižního směru tedy musí přes tyto firewally projít.

Provoz mezi východem a západem tyto bezpečnostní nástroje obchází," upozorňuje Kerravala. „Mohli byste použít firewall pro každé propojení, ale bylo by to příliš nákladné. Také to není moc agilní."

Kdo řídí mikrosegmentaci?

Mikrosegmentace získává hybnost, ale stále existují otázky, kdo by za ni měl být odpovědný. Ve velkém podniku by mohl vést takové aktivity inženýr zajišťující zabezpečení sítě. V menších společnostech by se o nasazení mikrosegmentace mohl starat tým, který zajišťuje provoz zabezpečení a sítě.

„Nevím, zda lze skutečně určit jednu skupinu, která by to měla mít na starost. Myslím, že záleží na účelu použití," tvrdí Kerravala. Vidí zájem síťových i bezpečnostních profesionálů.

„Myslím, že protože funguje jako vrstva sítě, ve většině případů je snadné ji v rámci provozu zabezpečení nasadit a provozovat nad sítí. Vidím však také personál síťového provozu, který ji například využívá jako způsob zabezpečení zařízení IoT. Máme zde tedy reálně dvě primární publika."

Přínosy mikrosegmentace

Díky mikrosegmentaci mohou IT profesionálové přizpůsobit nastavení zabezpečení různým typům provozu a vytvářet zásady, které omezují síťové i aplikační toky mezi pracovními zátěžemi na ty, jež jsou výslovně povoleny.

V modelu zabezpečení typu Zero Trust (více viz Computerworld 3/2018) může společnost nastavit zásady, které například určí, že zdravotní přístroje mohou komunikovat jen s dalšími zdravotními přístroji. Když se zařízení nebo zátěž přesune, přesunou se s ním bezpečnostní zásady a atributy.

Cílem je snížit prostor pro síťové útoky: Použitím pravidel segmentace pro pracovní zátěž či aplikaci lze snížit riziko, že by se útočník dostal z jedné zkompromitované zátěže či aplikace na jinou.

Další podporou je provozní účinnost. Seznamy řízení přístupu, směrovací pravidla a zásady firewallu se mohou stát těžko zvládnutelné a přinést velkou režii pro správu, takže je potom v rychle se měnících prostředích škálování zásad obtížné.

Mikrosegmentace se obvykle vykonává v softwaru, což usnadňuje definování jemnozrnných segmentů. Díky mikrosegmentaci může personál IT pracovat na centralizaci zásad segmentace sítě a na snížení počtu potřebných pravidel brány firewall.

Rozhodně to není malý úkol – nebude snadné konsolidovat seznamy řízení přístupu a pravidla firewallu vzniklá v průběhu let a převést je na zásady, které lze vynucovat v dnešních složitých a distribuovaných podnikových prostředích.

Pro začátek – mapování spojení mezi pracovními zátěžemi, aplikacemi a prostředími vyžaduje viditelnost, kterou mnoho podniků nemá.

Jedním z velkých problémů se segmentací je, že musíte vědět, co segmentovat. Některé výzkumy ukazují, že 50 % firem má malou nebo žádnou jistotu, že vědí, jaká IT zařízení mají v síti.

„Pokud ani nevíte, jaká zařízení jsou v síti, jak byste mohli vědět, jaký druh jakých segmentů chcete vytvořit? V oblasti toků datových center je nedostatečná viditelnost," dodává Kerravala.

Tento příspěvek vyšel v Security Worldu 1/2018. Časopis (starší čísla i předplatné těch nadcházejících) si můžete objednat na adrese našeho vydavatelství.

Našli jste v článku chybu?