MIKROSEGMENTACE ZOHLEDŇUJÍCÍ KONTEXT S VYUŽITÍM ŘEŠENÍ VMWARE NSX DATA CENTER

Ochrana sítě před laterálním šířením hrozeb

Moderní aplikace jsou komplexní, distribuované a dynamické

Všechny organizace se snaží přijít na to, jak provozovat své podnikání v extrémně propojeném světě, ve kterém jsou hnacím motorem aplikace a data. Moderní aplikace jsou distribuovány ve více datových centrech a cloudech a sahají až na samotné hranice prostředí.

Virtualizace spolu s nástupem koncepce DevOps, kontejnerizace a mikroslužeb umožňuje vytvářet a měnit aplikace rychleji než kdy dříve. V důsledku distribuované povahy moderních aplikací a rychlosti, s jakou se mění, představuje udržování zabezpečení velkou výzvu.

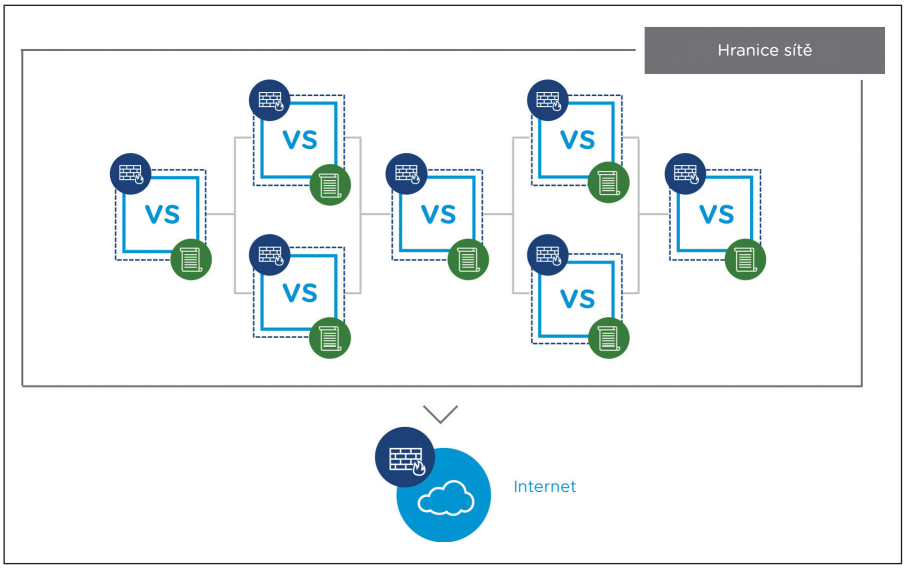
Starší strategie zabezpečení již nejsou efektivní

S tím, jak šíření aplikací stále pokračuje, se ukazuje, že dřívější přístupy k zabezpečení zaměřené na ochranu vnějších hranic jsou již na ochranu aplikací a dat nedostatečné. Opakovaně jsme se přesvědčili o tom, že útočníci dokážou vnější ochranou proniknout nebo bezpečnostní opatření na hranicích sítě obejít. Jakmile se dostanou dovnitř, mohou se nerušeně pohybovat laterálně – z jednoho serveru na druhý – a hledat informace, které by mohli odcizit nebo za které by mohli žádat výkupné.

Týmy, které mají na starost zabezpečení IT a sítě, stojí v moderním světě distribuovaných aplikací často před náročným úkolem udržovat nesourodé zásady zabezpečení v různých částech svých prostředí, což vytváří nedostatky v celkové bezpečnostní situaci.

Konzistentní zabezpečení od datového centra přes cloud až po hraniční zařízení

Při používání řešení VMware NSX® Data Center je možné zásady zabezpečení definovat konzistentně v celém prostředí bez ohledu na to, jakého typu aplikace je nebo kde je nasazena. Zásady jsou vymáhány na úrovni jednotlivých pracovních zatížení, což umožňuje segmentaci pracovních zatížení provozovaných na stejném fyzickém hostiteli bez potřeby směrovat přenosy oklikou přes externí fyzickou nebo virtuální bránu firewall. Tato podrobná úroveň zabezpečení se nazývá mikrosegmentace.



Obrázek 1: Mikrosegmentace znamená vymáhání zásad zabezpečení sítě na úrovni jednotlivých pracovních zatížení.

„Vzhledem k rostoucímu počtu zařízení IoT je vhodné, aby naše síť byla co nejvíce segmentovaná. Hrozby se pak nemohou šířit laterálně do celého datového centra.“

CHRISTOPHER FRENZ
ŘEDITEL PRO INFRASTRUKTURU
INTERFAITH MEDICAL CENTER

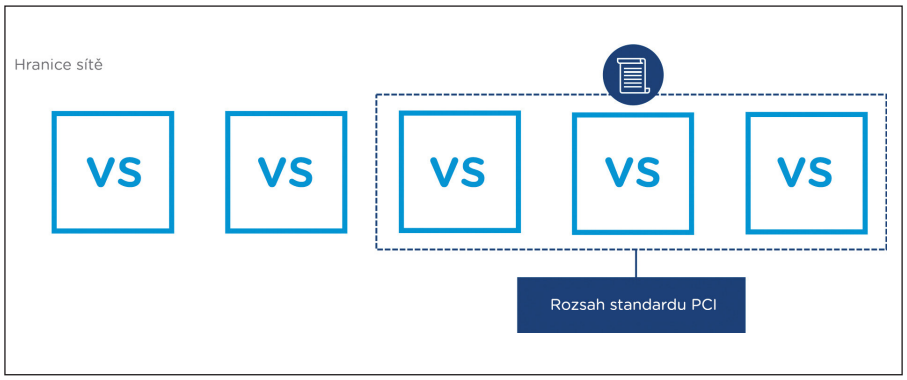
HLAVNÍ BODY

- Moderní aplikace jsou distribuované a dynamické, a proto v minulosti používaný přístup k zabezpečení zaměřený na ochranu vnějších hranic již nestačí.
- Řešení VMware NSX Data Center umožňuje mikrosegmentaci na ochranu aplikací před laterálním šířením hrozeb.
- Zásady zabezpečení jsou definovány v kontextu aplikací a vymáhány v jednotlivých pracovních zatíženích.
- Zabezpečení je poskytováno konzistentně všude od datového centra přes cloud až po hraniční zařízení.

Mikrosegmenty vytvořené pomocí řešení NSX Data Center jsou definovány a spravovány v softwaru, a proto jsou pružné a je možné je automatizovat. Nová pracovní zatížení při nasazení automaticky přebírají zásady zabezpečení, které s nimi zůstávají po celý jejich životní cyklus bez ohledu na to, kde byla vytvořena nebo kam mohou být případně přesunuta.

Mikrosegmentace zohledňující kontext a zabezpečení podle potřeb aplikací a dat

Schopnost definovat zásady zabezpečení podle toho, na čem nejvíce záleží, je stejně důležitá jako konzistentní poskytování zásad. Řešení NSX Data Center odděluje zásady zabezpečení od statických atributů sítě, jako je adresa IP, port nebo protokol, a umožňuje definovat zásady na základě kontextových znalostí aplikace a infrastruktury. Mezi tyto kontextové informace patří atributy uživatele a identity, atributy pracovního zatížení (například operační systém) nebo dokonce i rozsah zajištění shody s legislativou.



Obrázek 2: Mikrosegmenty v řešení NSX Data Center je možné definovat na základě celé řady různých kontextů, včetně rozsahů zajištění shody s legislativou.

Vytváření mikrosegmentace zohledňující kontext s využitím řešení VMware NSX Data Center poskytuje týmům, které mají na starost zabezpečení sítí, pružnost, jakou potřebují pro zabezpečení svých aplikací a dat na základě těch nejdůležitějších faktorů. Pomocí řešení NSX Data Center je například možné zabezpečit nasazení infrastruktury virtuálních desktopů (VDI) vymáháním zásad sítě na základě kontextu uživatele, a to až na úrovni jednotlivých relací vzdáleného desktopu (RDSH). Dalším příkladem je použití zásad zabezpečení pro všechna pracovní zatížení, na která se vztahují standardy PCI (Payment Card Industry), bez ohledu na to, kde se v prostředí fyzicky nacházejí.

Pokročilé služby zabezpečení, kdykoli a kdekoli jsou zapotřebí

Řešení NSX Data Center umožňuje vkládat do příslušných mikrosegmentů pokročilé služby zabezpečení od třetích stran. Přenosy v síti není nutné směrovat přes fyzické nebo virtuální zařízení, jako je brána firewall nové generace (NGFW) a systém detekce průniků (IDS) nebo systém předcházení průnikům (IPS). Řešení NSX Data Center namísto toho může konkrétní typ přenosů dynamicky směrovat do těchto služeb na vrstvě virtuální sítě. Díky tomu je možné pokročilé služby zabezpečení vkládat na správné místo a ve správnou dobu a dosáhnout tak maximální efektivity síťových přenosů a současně zvýšit efektivnost samotných služeb zabezpečení.

Přehled o přenosech v síti v celém prostředí

Prvním krokem k mikrosegmentaci je pochopení současných toků dat v síti. Řešení VMware Network Insight™ poskytuje ucelený pohled na veškeré přenosy v síti v rámci datového centra, včetně přenosů ve fyzické i virtuální síti. Řešení VMware Network Insight po provedení analýzy přenosů v síti automaticky doporučí zásady mikrosegmentace, které je možné implementovat jejich použitím v řešení NSX Data Center.

Začněte ještě dnes bezplatným vyhodnocením virtuální sítě, které vám umožní analyzovat aktuální přenosy v síti a pustit se do plánování vašeho projektu mikrosegmentace. Další informace naleznete na webu na adrese www.vmware.com/cz/products/nsx/security.

VMware, Inc., 3401 Hillview Avenue, Palo Alto CA 94304, USA, tel.: 877-486-9273, fax: 650-427-5001, www.vmware.com
VMware International Limited, Anděl Park Smíchov – Scott&Weber Office, Karla Engliše 3201/6, 150 00 Praha 5, Česká republika, tel.: +420 255 725 410, fax: +420 255 725 401, www.vmware.com/cz