

Průměrně 56% spojení na servery je z Ruska

11.10.2023 - | PROTEXT

Nefunguje vzdálená plocha

Scénář je vždy stejný a možná to znáte z vlastní zkušenosti. Chcete se připojit na vzdálenou plochu firemního serveru, ale nějak se nedaří. Přitom třeba kolega vedle připojen je a další služby serveru běží bez problému. Začnete tedy pátrat u sebe. Zkontrolujete počítač, připojení, router, kontaktujete svého ISP. A najednou to zase funguje. Záležitost uzavřete s tím, že šlo o "erupci na slunci" a pokračujete v práci. Ovšem tato "anomalie" se opakuje stále častěji a v okamžiku, kdy se na server nemůže připojit ani účetní firmy, zoufalost nabírá na zcela nových rozměrech.

Za touto anomálií se může skrývat nadměrný počet spojení na port vzdálené plochy serveru (RDS). Služba je přetížena nadměrným počtem spojení a buď přestane odpovídat, nebo se na váš požadavek o připojení se na server jednoduše včas nedostane. A to je typické chování DoS/DDoS útoku.

Datový tok za 1 hodinu

Síťoví technici analyzovali hodinový vzorek datového toku datového centra Coolhousing a výsledek je poměrně alarmující. Na prvním místě v počtu spojení na TCP port 3389 suverénně vedou zdroje provozu pocházející z Ruské federace, a to s 56,4% podílem. Druhé místo obsadily zdroje z Panamy se 8,2% a třetí místo obsadily zdroje z Ukrajiny s 5,4%.

Lze se domnívat, zdali dynamicky vyšší počet spojení z Ruské federace nesouvisí s aktuálně probíhajícím konfliktem na Ukrajině, z pohledu bezpečnosti a dostupnosti síťových služeb je však třeba tuto situaci řešit. Ale jak?

Řešením je VPN nebo VPN Firewall

V rámci síťové bezpečnosti existuje několik možností, jak lze těmto problémům spolehlivě se vyhnout. Obě níže uvedené varianty jsou vysoce funkční i finančně dostupné a vždy záleží, jakou cestou se chcete vydat.

1) Coolhousing SSTP VPN

Nejjednodušší a nejrychlejší řešení je zřízení tzv. VPN, neboli virtuální privátní sítě, díky které je síťová komunikace pomocí vzdálené plochy, SSH, IPMI, iLO či iDRAC, mezi serverem a počítačem/notebookem uživatele zcela skryta veřejnosti. Ze strany uživatele se jedná o řešení bez starostí a jakékoliv správy. Po jednorázovém nastavení je vše funkční a spuštění takové ochrany je otázkou dvou kliknutí.

Služba je plně out of band SSTP VPN a pro fyzické servery je poskytována na fyzicky odděleném síťovém rozhraní, pro virtuální servery prostřednictvím druhé virtuální LAN.

2) Privátní VPN s Firewalllem

Druhou variantou, jak se efektivně bránit, je služba VPN s Firewalllem. Jedná se o komplexní řešení ve formě předkonfigurovaného fyzického boxu, který plní funkci automatizovaného firewallu s blacklistem. Takový box si lze představit jako bodyguarda, který stojí před serverem a kontroluje veškerý provoz k němu. Žádoucí porty či služby mohou postupovat dále k serveru a nežádoucí jsou naopak vykazovány. V případě nestandardního nadužívání povolených portů je útočník umístěn na

zakázanou listinu a jeho spojení jsou automaticky rušena, což zvyšuje bezpečnost a výkon serveru. Ke službě je rovněž zřízena VPN síť na protokolu SSTP nebo L2TP.

Takové zařízení se připravuje na míru daného síťového provozu a buď se o něj následně můžete starat, nebo se o něj postarají ve formě managed varianty zkušení L2 síťoví administrátoři z datového centra Coolhousing, kteří jsou připraveni veškeré incidenty řešit v režimu 24/7.

Řešení existují a jejich hned několik. Stačí si pouze vybrat dle dovedností a možností. Svěřte se do rukou profesionálů, kterým na bezpečnosti vašich serverů i sítě opravdu záleží.

O Coolhousingu

Datové centrum Coolhousing poskytuje od roku 2003 profesionální hostingové a datové služby ve třech moderních, klimatizovaných serverovnách splňující vysoké požadavky na špičkový provoz serverů v režimu 24/7.

Coolhousing je dlouhodobým partnerem, který si zakládá jak na transparentnosti podmínek a smluv včetně SLA dostupnosti, na spolehlivosti dodaných služeb a funkčních řešeních, tak na vstřícnosti a lidskosti v komunikaci.

Kontakt

<https://www.coolhousing.net/>

ČTK ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese <https://www.protext.cz>.

<https://www.ceskenoviny.cz/tiskove/zpravy/prumerne-56-spojeni-na-servery-je-z-ruska/2425074>