Příloha č. 9 zadávací dokumentace
Shrnutí výsledku předběžné tržní konzultace

Konektivita

Otázka	Respondent č. 1	Respondent č. 2	Respondent č. 3	Vyhodnocení otázky pro veřejnou zakázku
Umožňuje poskytovatel navýšení propustnosti internetové konektivity v režimu tzv. Pay-as-YouGrow? Pokudano, za jakých podmínek?	Do kapacity 5 Gbps je to pouze otázka konfigurace a dohody mezi stranami na nových podmínkách. Pro kapacitu vyšší než 5Gbps je nutné změnit technologii a navýšení si vyžádá určitý čas.	Jelikož bude služba předávána na 10 Gbps portech, je možné navýšit rychlost linek až na 10 Gbps bez potřeby výměny nebo úpravy technologie.	Služba Internet 95%, kde jsou definovány Nominální rychlost a Maximální rychlost, kdy zákazník platí pevnou sazbu za Nominální a pokud je překročena, účtuje se dle překročené rychlosti. Zde např. Nominální rychlost 2,5 Gb, Maximální 10 Gb, tzn platí za 2,5 Gb, mají možnost vylézt až na 10 Gb a platí navíc podle max. dosažené rychlosti.	Poskytovatelé internetové konektivity nabízejí přijatelné varianty rozšíření kapacty internetové konektivity. Otázka převedena jako požadavek do zadávací dokumentace veřejné soutěže.
Dokáže poskytoval zajistit ochranu proti tzv. Single Point of Failure pomocí redundantních HW prvků přívodu internetové konektivity?	Ano, poskytovatel bude mít linky připojené na různé HW prvky.	Každá z lokalit by byla připojena pomocí dvou geograficky redundantních linek (primární a záložní), které by byly zakončeny na straně Zadavatele každá na samostatném CPE. Na straně dodavatele by linky byly zakončeny každá na jiném PE.	Ano, musí být technicky navrženo na dvou nezávislých technologiích a ukončeno dvěma routery, de facto se musí udělat dvě linky.	Poskytovatelé internetové konektivity nabízejí přijatelné varianty řešení problematiky SPoF internetové konektivity. Otázka převedena jako požadavek do zadávací dokumentace veřejné soutěže.
Dokáže poskytoval zajistit ochranu proti tzv. Single Point of Failure pomocí využití tzv. linkové agregace?	ANO	Každá z lokalit by byla připojena pomocí dvou geograficky redundantních linek (primární a záložní), které by byly zakončeny na straně Zadavatele každá na samostatném CPE. Na straně dodavatele by linky byly zakončeny každá na jiném PE. Standardně je primární a záložní linka v režimu active/pasive, je ale možné dodat i v režimu active/active.	Ano, umíme udělat na LACP protokolu	Poskytovatelé internetové konektivity nabízejí přijatelné varianty řešení problematiky SPoF internetové konektivity. Otázka převedena jako požadavek do zadávací dokumentace veřejné zakázky.
Je poskytovatel schopen zajistit konektivitu do datových center v lokalitách Praha na adrese ČD Telematika, a.s., Pod Táborem 369/8a, Praha 9 a Plzeň na adrese Purkyňova 22, Plzeň.	ANO	ANO	ANO - PHA - CRA fiber – přes ulici – dokop; CETIN fiber – na místě	Otázka na lokality převedena jako požadavek do zadávací dokumentace.
Je schopen dodavatel zajistit přestěhování konektivity z lokality Plzeň do lokality Přerov na adrese SŽ -CDP Přerov, Tovární 3137, Přerov.	Poskytovatel má v současné době vlastní infrastrukturu na adrese Přerov, Tovární 12C, která by měla být v majetku Zadavatele. Pokud Zadavatel poskytne Dodavateli místní optický propoj mezi budovou 12C a 12, potom je možné konektivitu z Plzně bez problémů přestěhovat do Přerova.	Ano (realizace linek cca 10 měsíců) Doporučujeme specifikovat, jak dlouho bude linka v Plzni provozována, než bude přestěhována do Přerova (rozdělení 60měsíčního závazku).	ANO - Přerov – CETIN – fiber – před objektem. Nutný dokop do objektu, nebo dle technického šetření	Otázka na stěhování z lokality Plzeň do lokality Přerov převedena jako požadavek do zadávací dokumentace.
V případě, že by zadavatel disponoval vlastním IPv4 a IPv6 rozsahem veřejných adres. Umožňuje poskytovatel propagaci adres (autonomní režim) pomocí BGP protokolu?	ANO	Ano, případně je možné i blok veřejných adres pro tento účel zapůjčit	ANO	Zadavatel se na základě odpovědí rozhodl využít standardního přidělení IP adres.
Umožňuje zadavatel koexistenci sdíleného rozsahu veřejných adres v obou lokalitách?	ANO	ANO		Na základě odpovědí byla ujasněna architektura vysoké dostupnosti a otázka byla převedena jako požadavenk do zadávací dokumentace.

Anti-DDoS

Otázka	Respondent č. 1	Respondent č. 2	Respondent č. 3	Vyhodnocení otázky pro veřejnou zakázku
Umožňuje poskytovatel navýšení objemu DDoS útoku, proti kterému je poskytována ochrana v režimu tzv. Pay-as-You-Grow? Pokud ano, za jakých podmínek?	Standardně se při sjednávání ochrany při DDoS útoku definuje tzv. legitimní kapacita, tj. kapacita provozu, který má být vpuštěn do sítě zákazníka. Poskytovatel může s růstem kapacity internetové konektivity současně navyšovat i kapacitu ochrany proti DDoSm útokům.	Nabízená služba je operátorským řešením, kde jsou definované chráněné cíle (IP adresa, ASN, síťový port, ...). Pro tyto cíle bývá stanovena šířka chráněného pásma (kolik legitimního provozu garantujeme doručit). Tzn služba není určována velikostí útoku, ale šířkou chráněného pásma.•Vkapitole „4.1 Vyplněná Příloha 1 ZD –Parametry internetové konektivity a Anti-DDoS řešení“ je uvedena „Cena za poskytování služby po dobu 60 měsíc“ pro šířku chráněného pásma 2x 100Mbps. Kdykoliv vprůběhu poskytování služby je však možné tuto hodnotu měnit, tak aby odpovídala aktuálním potřebám zákazníka. O2 používá pro službu AntiDDoS platformu společnosti Arbor Networks –Peakflow SP. Ta je rozdělena na 3 části:-CP část, která zahrnuje analytickou část systému -TMS část obsahuje mitigační část-PI část –portálové rozhraní pro zákazníkyVšechny změny konfigurace TMS jsou prováděny v CP zařízení. CP zařízení vytvářejí BGP peering s dotčenými směrovači (ISP hraniční routery) jako BGP host (RRC route reflector client), a přijímá všechny BGP oznámení obdržené nebo předané ISP routery. CP zařízení je také spojeno s hraničními routery pro příjem NetFlow dat, která jsou využívána jako hlavní zdroj pro analýzu chování a provozu. Jakmile CP zařízení označí daný provoz jako podezřelý, může požádat TMS o BGP přesměrování provozu přes TMS k dalšímu zkoumání. Pokud TMS vyhodnotí provoz jako DoS/DDoS útok, zahodí nežádoucí provoz, jinak jej pošle zpět původní cestou a ten je následně doručen do cíle.	Model PaYG nenabízíme, nabízíme ochranu na základě kapacity internetového připojení zákazníka. Velikost našeho Scrubbing centra je 40GB, tzn dokážeme odvrátit útok do této velikosti, poté dochází k Blackholingu	Na základě odpovědí byly pro zadávací dokumentaci definovány dvě možné varianty způsobu Anti-DDoS ochrany: - Kapacita ochrany (50 Gbps) - Chráněné pásmo (2,5 Gbps a 254 IP adres)
Jaká technologie zajišťuje trvalou ochranu proti DDoS útokům?	Radware	Pro antiDDoS řešení používáme primárně technologii Radware + další technologie, např Arbor		Odpovědi ujistili zadavatele, že dodavatelé využívají kvalitních a moderních technologií. Otázka nebyla převedena na požadavek.
Umožňuje poskytovatel přístup do uživatelského rozhraní, kde může zadavatel sledovat právě probíhající útoky, historii útoků a obecnou statistiku o toku dat	V současné době technologie nemá uživatelské rozhraní pro zákazníky. To bude dostupné v roce 2023. V současnosti je automaticky reportován každý začátek útoku a automaticky jsou zasílány reporty po jeho skončení.	Ke službě aktuálně nenabízíme žádný online monitoring. V případě útoků zákazníka informujeme Zákazníkovi můžeme zasílat každý měsíc přehledový report – tj. informace za předešlý měsíc, jako průběhy a detaily provozu pro hlavní protokoly, nejčastější typy útoků apod.	Ano. Přesně k tomu slouží v předchozí odpovědi uvedené portálové rozhraní pro zákazníky	Možnost sledování průběhu útoku byla vyhodnocena jako důležitý požadavek, a proto byla otázka převedena na požadavek v rámci zadávací dokumentace.