Příloha č. 5 – Technická specifikace

Předmět veřejné zakázky

Předmětem dohody je povinnost poskytovatele zajistit provoz cloudové platformy pro jednotlivé internetové projekty odboru Digitálních služeb Českého rozhlasu dle aktuálních potřeb objednatele (zejména integrační část projektu mujRozhlas – rAPI, web mujRozhlas.cz, web Ježíškova vnoučata, informace o programu, atd.). Cloudová platforma (dále také jako „platforma“) je tvořena infrastrukturní / HW vrstvou (viz bod 1 níže) a SW vrstvou (viz bod 2b níže). Obě tyto vrstvy budou ve správě poskytovatele služeb a budou rozvíjeny na základě požadavků a potřeb objednatele.

Zajištění provozu cloudové platformy znamená:

1) poskytnutí virtualizované HW infrastruktury včetně monitoringu (infrastrukturní cloud)
2) správu, provoz a rozvoj HW a SW prostředí potřebného pro běh internetových aplikací a nástrojů objednatele. Jde zejména o
    a. optimalizace HW infrastruktury a SW prostředí na požadovaný provoz aplikací
    b. správu, monitoring a rozvoj nezbytného SW, tj. OS a middleware.
    c. zajištění bezpečnosti a údržby SW prostředí (aktualizace, zálohování atd..)
3) provozování servisní podpory prostřednictvím online helpdesku a telefonní hotline
4) udržování aktuální dokumentace platformy

Součástí provoz cloudové platformy není:

1) správa aplikační vrstvy projektů, tj. správa samotných aplikací jako např. integrační nástroj RAPI, CMS Drupal 9 a další.
2) správa DNS serverů - spravuje Český rozhlas, úpravy DNS záznamů podléhají schválení.
3) správa SMTP serverů - spravuje Český rozhlas, platforma se k nim pouze připojuje.

Cloudová platforma, která je předmětem této dohody, se nesmí nacházet v datovém centru, kde je umístěn aplikační cloud, viz článek IV. odst. 3. dohody, a to na adrese: Mahlerovy sady 1, 130 00 Praha 3.

1. Technické parametry virtualizované HW infrastruktury

parametr	**hodnota**
specifikace služby	managed server hosting
cloudová technologie (hypervisor)	VMware vCloud Director min. verze 10.2
počet VM / vAPPs	128 / 32
Počet fyzických CPU jader	83 jader (CPU physical cores) o frekvenci alespoň 2,6 GHz (base clock) s možností zapnutí virtuálních jader (HTT, SMT atp.).
vRAM (GB)	520
velikost úložiště (TB)	104
výkon úložiště dle účelu	standardní / vysoký / špičkový
Síť mezi VM	min. 10 Gbit/s
Konektivita	vyhrazená linka 1 GBit/s
veřejné statické IPv4 adresy (počet)	12

veřejné statické IPv6 adresy (počet)	Segment /56
úroveň provozní bezpečnosti datového centra	TIER 3
zálohování	Automatizované zálohování shapshotů (Veeam)

2. Cloudová technologie

Objednatel požaduje cloudovou technologii VMware vCloud Director minimálně ve verzi 10.2. Nižší verze objednavatel nepřipouští z důvodů potencionálních problémů při migraci stávající infrastruktury. Objednatel požaduje konkrétně technologii VMware vCloud s ohledem na skutečnost, že interní zaměstnanci nebo externí smluvní partneři jsou znalí práce s požadovanými technologiemi a jejich změna by znamenala nákladné přebudování a úpravy stávajících postupů.

3. Požadavky na datové centrum

3.1. Provozní bezpečnost

Za účelem garance vysoké dostupnosti služeb datového centra objednatel požaduje, aby datové centrum dosahovalo provozní bezpečnosti minimálně úrovně TIER III ve všech parametrech dle klasifikace Uptime Institute. Naplnění tohoto požadavku musí být prokázáno jedním z níže uvedených způsobů:

a) doložením certifikátu od Uptime Institute alespoň na úrovni návrhu datového centra, tzv. "Certification of Design Documents"
b) čestným prohlášením poskytovatele

Pokud se prokáže, že některý z parametrů datové centra nedosahuje úrovně TIER III dle klasifikace Uptime Institute má objednatel právo uplatnit sankce viz článek XIII. odst. 8 dohody.

3.2. Dostupnost služeb datového centra musí dosahovat alespoň 99,95% ročně.

3.3. Připojení serverů na alespoň dvě nezávislé větve napájení kdy výpadek jedné libovolné větve nijak neomezí provoz serverů.

3.4. V případě HA clusteru virtuálních serverů, musí být každý virtuální server na vlastním HW, tak aby případná HW porucha neovlivnila celý cluster

4. Úložiště

Cloudové úložiště bude poskytovat 3 výkonové úrovně dle účelu jeho využití.

Úroveň výkonu	rychlost čtení / zápisu	Účel úložiště
standardní	rychlost čtení / zápisu není prioritou	zálohování a archivace dat
vysoká	vysoká rychlost čtení / zápisu	běžné aplikace a databáze
špičková	špičková rychlost čtení a zápisu dat	databáze s min. dobou odezvy (business critical)

5. Zálohování

Poskytovatel bude automaticky vytvářet snapshoty běžících VM pomocí technologie Veeam a zálohovat je tak, aby mohl tyto zálohy použít i objednavatel pro obnovu VM mimo infrastrukturu poskytovatele, především pak na prostředcích objednatele. Vzhledem k tomu, že objednatel již disponuje zálohovací technologií společnosti Veeam a virtualizační infrastrukturou VMware vSphere, počítají jeho havarijní plány a plány obnovy s případnou možností přemístění VM na tuto infrastrukturu. Retence zálohování je minimálně 4 týdny.

6. Konektivita

- Minimálně 2 nezávislé optické trasy konektivity
- Přímá konektivita do NIX
- Neomezený datový přenos v rámci ČR i mimo ČR.
- Konektivita minimálně 1 Gbps.

7. Administrační rozhraní virtualizace

Služba musí poskytnout zabezpečený přístup do administračního rozhraní pomocí webového prohlížeče (bez nutnosti využívat FLASH technologii) a umožňovat následující administraci - vytváření virtuálních strojů, konfigurace jejich parametrů, nastavování sítě, poskytovat přehled o přidělování systémových prostředků, zálohování.

8. API virtualizace

Služba musí umožňovat plnohodnotnou správu, konfiguraci a vytváření VM skrze vCloud Director API nebo kompatibilní.

9. Bezpečnost

9.1. DDoS ochrana

9.1.1. Ochrana proti DDoS útoku je nepřetržitá, v reálném čase. Funguje automaticky s možností ručních zásahů. Použité technologie jsou přímo určeny k ochraně proti DDoS na IPv4 a IPv6.

9.1.2. Ochrana je určena primárně na volumetrické útoky, TCP State-Exhaustion útoky a útoky na aplikační vrstvě. Ochrana funguje proti více současným útokům v jeden okamžik.

9.1.3. Ochrana na ISO/OSI vrstvě 3 a 4 (ochrana sítě) je implementována minimálně na úrovni celého datacentra nebo (lépe) u poskytovatelů připojení datacentra.

9.1.4. Ochrana na ISO/OSI vrstvě 7 (ochrana serveru) chrání minimálně protokol HTTP.

9.1.5. Ochrana eliminuje útoky až do 1 Gbps příchozího (ingress) provozu s možností rozšířit kapacitu minimálně na 5 Gbps ingress provozu po jednotkách Gbps. Při výpočtech se uvažuje celkový provoz (tedy legitimní i škodlivý dohromady).

9.1.6. Ochrana umožňuje výrazné omezení nebo úplného odříznutí mezinárodního provozu (požadavků přicházejících mimo ČR)

9.1.7. Možnost úprav a nastavení vlastních pravidel a limitů pro detekci a prevenci útoků na základě žádosti objednatele včetně explicitního whitelistingu/blacklistingu.

9.1.8. V případě detekovaného útoku je objednatel o této skutečnosti neprodleně notifikován včetně podrobností o útoku a přijatých opatřeních. Během probíhajícího útoku je pak pravidelně informován o aktuálním stavu.
9.1.9. Součástí měsíčních reportů jsou detailní informace o zachycených útocích.
9.1.10. Součástí služby je podrobná dokumentace, jak ochrana funguje, jakým způsobem útoky řeší a jaké jsou výhody/nevýhody jednotlivých opatření. Jaké jsou možnosti nastavení ochrany nad rámec výše uvedených minimálních požadavků.

9.2. Ochrana IPS/IDS pro detekci a prevenci dalších typů útoků
9.2.1. databáze pravidel se automaticky aktualizuje
9.2.2. systém vidí do kompletního síťového provozu
9.2.3. jednotlivá pravidla lze dynamicky vypínat / zapínat
9.2.4. pro jednotlivé pravidla lze nastavit zda se mají aplikovat v režimu IDS (pouhá detekce) nebo IPS (blokování)
9.2.5. poskytovatel nacení řešení pro minimálně 1 Gbps ingress provozu
9.2.6. objednatel zváží nasazení IPS/ IDS dle evaluace přínosů vs. nákladů (viz vyhrazená změna závazku), tj. nacenění výše se nezapočítává do nabídkové ceny

9.3. L4 Firewall
9.3.1. Možnost blokace definovaných cílových portů (TCP i UDP)
9.3.2. Možnost blokace ICMP
9.3.3. Možnost blokace na základě sítě či IP adresy zdroje či cíle

9.4. Webový Aplikační firewall
9.4.1. Automaticky aktualizovaná pravidla, minimálně OWASP core a pravidla specifická pro Drupal.
9.4.2. Možnost vlastních pravidel a deaktivace / konfigurace všech pravidel
9.4.3. Detekce robotů (legitimních i nelegitimních)
9.4.4. Různé možnosti reakce, minimálně:
- Blokace
- Omezení rychlosti (rate-limiting)
- Logování

9.4.5. poskytovatel nacení řešení jako cenu za milion prozkoumaných HTTP(S) požadavků
9.4.6. objednatel zváží nasazení WAF dle evaluace přínosů vs. nákladů (viz vyhrazená změna závazku), tj. nacenění výše se nezapočítává do nabídkové ceny

9.5. Všechny způsoby ochrany jsou v maximální možné míře transparentní z hlediska provozu a logování atp. pro další prvky, které chrání. V případě, že libovolná ochrana pro svoje fungování musí měnit IP adresu původního (legitimního) klienta, je zajištěno její předání dalším systémům HTTP hlavičkou nebo PROXY protokolem.

10. Dokumentace

10.1. Veškerá zmíněná dokumentace je v češtině nebo angličtině.
10.2. Správnost a úplnost dokumentace je kontrolována a aktualizována každé 3 měsíce.
10.3. Kompletní uživatelská i správcovská dokumentace všech komponent, které jsou součástí řešení
10.4. Dokumentace k zabezpečení a procesům (např. VPN, ukládání hesel, TLS atd.) zejména pro účely auditů a kontrol třetích stran.

11. Podpora a údržba

11.1. Poskytovatel provozuje online Helpdesk - elektronickou evidenci všech Požadavků, reakcí na ně a jejich způsobů vyřešení. Všechna data z Helpdesku jsou k dispozici po celou dobu trvání Smlouvy. V evidenci jsou vedeny informace o tom, kdy byl vznesen Požadavek, kdo jej vznesl, jaký byl jeho obsah, kdo jej vyřizoval, kdy bylo na Požadavek reagováno a kdy, jak byl Požadavek vyřešen a jak dlouho trvalo jeho řešení. Provoz Helpdesku zajištěn v režimu 24/7, uchovávání historie požadavků po celou dobu trvání Smlouvy.

11.2. Objednatel má k dispozici telefonní hotline v režimu 24 hodin / 7 dnů v týdnu.

11.3. Servisní doba Poskytovatele je 365 dní v roce, 7 dní v týdnu, 24 hodin denně.

11.4. Pro servisní práce a údržbu platformy může Poskytovatel využít plánované odstávky (tzv. Servisní okno) v maximálním rozsahu 2 hodiny v součtu za kalendářní měsíc. Ve výjimečných případech (např. jednorázová migrace apod.) lze domluvit se souhlasem Objednatele i servisní okno delší.

11.5. Poskytovatel je povinen písemně informovat Objednatele o plánované odstávce v dostatečném předstihu, minimálně 14 kalendářních dní.

11.6. Minimální dostupnost platformy je 99.95 % v každém kalendářním měsíci.

11.7. Nedostupnost je zjištěna monitorovacím nástrojem Poskytovatele, nebo též může být nahlášena při jejím zjištění Objednatelem.

11.8. Dostupnost platformy v procentech se vypočítá za každý kalendářní měsíc tak, že celkový počet celých minut, po který byla platforma dostupná nebo probíhala plánovaná údržba v servisním okně, se vydělí celkovým počtem minut v měsíci a vynásobí 100. Pokud je mezi samostatnými nedostupnostmi období kratší než 10 minut, považuje se toto celé období za nedostupnost.

11.9. Je dodržována reakční lhůta (fyzickým člověkem, ne automatem) a lhůta pro odstranění vady od nahlášení závady dle následující tabulky:

Stupeň priority závady	*Popis závady*	*Reakční lhůta od oznámení požadavku*	*Lhůta pro odstranění vady od oznámení požadavku*
1- Kritický incident*	Jeden nebo více serverů platformy nejsou dostupné nebo způsobilé pro provoz aplikací Objednatele z následujících důvodů: Nefunguje / není dostupná infrastrukturní vrstva platformy. Mimo jiné může způsobit například: • výpadek konektivity • výpadek HW (porucha diskového pole apod.) • porucha v datacentru Nefunguje / není dostupná vrstva OS a middleware.	1 hodina	4 hodiny

	Mimo jiné může způsobit například: • expirované SSL certifikáty • zaplněné místo na disku		
2 - Vážný incident*	Jeden nebo více serverů platformy jsou dostupné, ale vyskytují se vážné výkonnostní problémy a omezení pro jejich způsobilost k provozu aplikací Objednatele	4 hodiny	24 hodin
3 - Běžný incident*	Vyskytuje se problém, který ale významně nesnižuje výkon ani dostupnost platformy	1 pracovní den	3 pracovní dny
4 - Běžný požadavek	např. úprava konfigurace nebo drobná chyba, která neovlivňuje činnost	2 pracovní dny	5 pracovních dnů

*Pokud se během řešení incidentu ukáže, že se jedná o aplikační nebo konfigurační chybu způsobenou objednatelem, nebude tato situace považována za incident.

11.10. Do 5. dne každého měsíce je Objednateli zaslán report, který obsahuje:
- 11.10.1. Dostupnost platformy
- 11.10.2. Přehled využitých servisních oken
- 11.10.3. Přehled řešených Incidentů s výsledným stavem
- 11.10.4. Využití kapacity

11.11. V případě, že nějaká v platformě použitá součást obsahuje bezpečnostní chybu, je součást aktualizována nejpozději do 30 kalendářních dnů, pokud je splněno že má chyba přidělený CVE identifikátor a současně existuje opravná verze či workaround od Poskytovatele či autora této součásti.

11.12. Je veden záznam o servisních zásazích na platformě s přesnými záznamy času, pracovníků podílejících se na zásahu a popis provedené operace.

11.13. Neexistují společné přístupové účty, každý pracovník Poskytovatele má samostatný přístup vedený na jeho jméno.

11.14. Součástí ceny Podpory a Údržby je **měsíčních 10 hodin určených na správu a konfiguraci platformy**.

11.15. V případě ukončení poskytování služby poskytne poskytovatel objednateli součinnost při migraci na jinou infrastrukturu.

11.16. Součinností při migraci na jinou infrastrukturu je myšleno poskytnutí odborného školení zaměstnancům Objednatele, na provoz v rozsahu 3 (tří) pracovních dnů v budově Objednatele. Cena tohoto školení byla Poskytovatelem zahrnuta v ceně úvodní migrace (viz. Příloha – Cenová nabídka poskytovatele). Na školení Poskytovatel Objednateli zejména:

A. popíše obsah veškeré písemné dokumentace, vzniklé v souvislosti s plněním Smlouvy, která byla nebo má být předána Objednateli, a vysvětlí, k čemu dokumentace slouží a jak s ní dále pracovat;

B. předá přístupy k Infrastruktuře, včetně všech přístupových údajů, hesel a bezpečnostních kódů a přístup do všech administrátorských rozhraní a vysvětlí, k čemu slouží a jaké mají funkce;

12. Milníky

1. dodání virtualizované HW infrastruktury připravené pro migraci stávající infrastruktury, migraci dat a testování – **nejpozději do 2 týdnů od účinnosti 1. dílčí smlouvy**;

2. dokončení migrace stávající infrastruktury včetně middleware a aplikační vrstvy a uvedení cloudu do plného provozu – **4 týdny od účinnosti 1. dílčí smlouvy**.

13. Migrace

Objednatel požaduje provedení migrace stávající infrastruktury bez dopadu na služby objednatele provozované v současné infrastruktuře. Za tímto účelem je poskytovatel povinen koncipovat migraci jako bezvýpadkovou. Migrace může probíhat po jednotlivých službách.
Pokud nebude možné z technických důvodů dosáhnout úplné bezvýpadkovosti, je povinnen poskytovatel zajistit minimalizaci výpadků, tak aby v celkovém součtu nepřesáhly 2 hodiny v časovém okně definovaném objednatelem (např. mezi půlnocí a 4 hodinou ranní). Dle potřeb objednatele může být migrace rozdělena na více takových oken (každé s výpadky v součtu pod 2 hodiny). Celkový čas výpadků přes všechna migrační okna nesmí překročit 4 hodiny. Objednatel pro tento účel poskytne nezbytně nutnou součinnost.

Dodavatel předloží objednateli harmonogram migrace a s objednatelem určí datum, kdy bude k dispozici kopie produkčního prostředí. Za účelem sestavení harmonogramu Objednavatel dodá seznam všech služeb a jejich provázanost. Součástí bude i vazba konkrétních aplikací na konkrétní jednotlivé databáze (kvůli přenosu dumpů). Dodavatel zajistí všechny další potřebné kroky migrace kromě přepnutí DNS.

14. Současný technický stav

Platforma je tvořena několika desítkami (více než šedesát) virtuálních strojů (dále len VM) seskupených do několika logicky uspořádaných skupin (dále jen vApp).

Jako OS je použit Debian ve verzích 7-11, případně Ubuntu 18.

Použitý middleware zahrnuje širokou škálu běžně používaných technologií. V naprosté většině se jedná o otevřený software, například:

- HAproxy
- Varnish
- Nginx
- MariaDB / Galera
- Elastic Stack
- Redis
- RabbitMQ
- Zabbix
- Cassandra
- Minio
- Flask
- Zabbix

- Kong

Jediným zástupcem komerčního software je několik instancí Wowza Streaming Engine.

Architektura jednotlivých vApps se obecně snaží poskytovat vysokou dostupnost a horizontální rozkládání zátěže (HA/LB řešení), vždy v rámci možností použitých technologií. Pokud je to vhodné, je použitý clustering (Galera, Elasticsearch, Kong, Cassandra).

Monitoring všech VM zajišťuje nástroj Zabbix s vhodně nastaveným alertingem.

Na aplikační úrovni se opět jedná o běžné technologie, například:
- PHP / Symfony
- Drupal
- Python / Celery
- Bash