„POŘÍZENÍ ZÁLOHOVACÍHO ŘEŠENÍ“
–
TECHNICKÁ SPECIFIKACE

Popis současného stavu

V současné době zadavatel disponuje dvojicí zálohovacích serverů a SW řešení IBM Spectrum Protect. Z primárního zálohovacího serveru probíhá každý den replikace na sekundární server umístěný v jiné lokalitě. Zároveň probíhá další kopie záloh na pásky prostřednictvím páskové knihovny.

Typy zálohovaných systémů:

- virtuální servery provozované ve virtualizační platformě VMware vSphere
- Microsoft Active Directory servery
- Microsoft Windows souborové servery
- Microsoft SQL servery

Oblasti, ve kterých je prostor pro zvýšení bezpečnosti zálohovaných dat:

- Zabezpečení zálohovaných dat proti napadení hackery, či jiným kybernetickým incidentům.
- Pružnost a rozšiřitelnost zálohovacího řešení.
- Schopnost zajistit rychlou obnovu činnosti zadavatele po kybernetickém incidentu a zabezpečení sekundárních dat před napadením škodlivým kódem.
- Uložení dat s integrovanou ochranou proti ransomware.
- Zajištění neměnnosti záloh.
- Kompletní logování přístupu k datům.
- Zabezpečení přístupu k zálohám.
- Možnost rozšíření o zálohování uživatelských dat v cloudu.
- Vytvoření geolokačně odděleného zálohovacího prostředí pro případ odstavení primární lokality.
- Možnost okamžité obnovy provozu kritických systému po bezpečnostním incidentu jak z primární, tak ze sekundární lokality.
- Vytvoření archivu záloh na již provozovaných páskových knihovnách.

Požadovaný cílový stav

Pořízení nového zálohovacího řešení, které umožní celkově robustnější a efektivnější zálohování dat zadavatele. Záložní a archivní data musí podpořit provozní požadavky na dohledatelnost, obnovitelnost, zabezpečení (security) a privátnost (access management & data privacy) záložních dat, a to jak z pohledu kompletnosti a spolehlivosti obnov, tak i z pohledu minimalizace dopadu na trvání a rozsah degradace kvality a dostupnosti poskytovaných IT služeb.

- Zálohovací infrastruktura s větším výkonem a lepší propustností, což povede k výrazně rychlejšímu obnovení provozu v případě významnějšího kybernetického incidentu.
- Paralelní provoz min. 60 virtuálních serverů přímo ze záložního uložiště (mount záloh k VMware platformě).

- Všechny přístupy k uloženým datům budou kompletně auditovány a vedeny v logu, takže je možné zpětně vyhledat jakékoliv operace – kdo a jaké změny nad daty prováděl.
- Komplexní zabezpečení zálohovaných dat, uložená data je možné obnovit i v případě jejich destrukce.
- Posílení zálohovací infrastruktury pro sekundární zálohovací lokalitu pro replikaci záloh bude mít za následek obnovu provozu i po kompletním výpadku primární lokality.
- Navýšení kapacity zálohovacího prostředí pro uchování stále se navyšujícího objemu zálohovaných dat a možnosti nastavení delších retencí.

Minimální technické požadavky

Zadavatel má v úmyslu prostřednictvím této veřejné zakázky pořídit vysoce dostupný zálohovací cluster včetně SW licencí pro primární i sekundární zálohovací lokalitu. Jako mandatorní požadavek stanovuje nutnost integrovat nové zálohovací řešení na již provozované zálohovací řešení postavené na technologii IBM Spectrum Protect tak, aby bylo možné zálohovaná data ukládat na páskové knihovny spravované tímto stávajícím řešením a byla zachována historie a kontinuita záloh.

Požadované funkcionality a vlastnosti infrastruktury nového zálohovacího clusteru:

Obecný požadavek	Parametr požadavku
Základní parametry	Zabezpečené úložiště dat musí bezpečně uchovávat sekundární data (záložní kopie primárních dat a archivní data) v souladu s doporučeními NÚKIB v oblasti kybernetické bezpečnosti.
	Zálohovací řešení musí splňovat vysoké bezpečnostní požadavky pro zajištění privátnosti dat, řízení přístupu k datům a ochrany proti kybernetickým hrozbám. Musí podporovat personalizaci a audit přístupu k datům, šifrování dat, patch management, zabránění přepisu historických dat, integrovanou antivirovou ochranu, detekci ransomware.
Architektura	Zálohovací řešení musí být postavené na hyper-konvergované architektuře zálohovacího clusteru pro škálovatelnost výkonu.
	Zálohovací řešení musí nabídnout schopnost upgrade SW komponent bez výpadku chodu zálohovacích procesů.
	Zálohovací řešení musí splňovat ochranu dat samotného zálohovacího řešení formou nativní fyzické odolnosti proti napadení, či smazání, kdy jsou jednotlivé komponenty instalovány jako appliance, nejedná se tedy pouze o instalované aplikace v běžném OS (fyzické, virtuální, nebo cloudové).
	Zálohovací řešení musí být možno rozšířit o bezagentové zálohování přímo z bezpečnostního snímku dat pole **IBM FS5200***, které zadavatel již provozuje. Tuto zálohu musí být možné pořizovat jako aplikačně konzistentní zálohu a metodou incremental forever.

Kapacita a fyzická odolnost	Pro primární lokalitu musí být dodáno vysoce dostupné clusterové uložiště typu all-flash pro ukládání záloh o minimální konfiguraci 4 nody na danou lokalitu. Uložiště musí mít zajištěnu vysokou dostupnost, tedy v případě výpadku jednoho nodu clusteru bude zajištěna plná funkčnost řešení, včetně možnosti zálohovat, obnovovat a nakládat s daty. HW platforma musí být certifikovaná pro provoz nabízeného SW řešení. Tato skutečnost musí být ověřitelná na webu výrobce SW.
	Pro sekundární lokalitu musí být dodáno vysoce dostupné clusterové uložiště typu hybrid (kombinace Flash a NL-SAS disků) pro ukládání záloh o minimální konfiguraci 3 nody na danou lokalitu. Uložiště musí mí zajištěnu vysokou dostupnost, tedy v případě výpadku jednoho nodu clusteru bude zajištěna plná funkčnost řešení, včetně možnosti zálohovat, obnovovat a nakládat s daty. HW platforma musí být certifikovaná pro provoz nabízeného SW řešení. Tato skutečnost musí být ověřitelná na webu výrobce SW.
	Konektivita každého nodu clusteru musí být realizována min. 2x 10/25Gbit LAN porty. Možnost rozšíření o FC HBA pro přímý přístup na LUN diskového pole.
	Zabezpečená uložiště musí umožňovat replikaci mezi sebou a být spravovaná z jednoho grafického rozhraní.
	Primární cluster musí umožňovat odsun archivních dat do stávající infrastruktury provozované na **IBM Spectrum Protect*** s páskovou knihovnou **IBM TS4300***. Při odsunu záloh do archivu nesmí dojít k rehydrataci dat do původního stavu (tj. provedení obnovy z původní zálohy) a jejich následného opětovného odzálohování pomocí IBM Spectrum Protect.
	Primární cluster musí mít kapacitu min. 100 TB typu NVME. Sekundární cluster musí mít min. 100 TB hybridní kapacity, kdy kapacita Flash musí tvořit min. 5 % celkové hybridní kapacity. Výše uvedené požadované kapacity jsou kapacity čisté. Čistou kapacitou se rozumí celková kapacita bez deduplikace, ale po zajištění odolnosti proti poruše prostředky redundance (cluster/raid/node).
	Veškerá kapacita musí podporovat deduplikaci a komprimaci napříč celým řešením.
	Zálohovací řešení musí být odolné proti výpadku nodu a proti výpadku jednoho disku u Flash tieru, a dvou disků magnetického tieru.
	Čistá kapacita každého zabezpečeného uložiště musí být rozšiřitelná na min. dvojnásobek dodané kapacity, a to bez nutnosti budoucí výměny dodaného HW.
	Zálohovací řešení musí podporovat možnost odsunu dat ze zabezpečeného uložiště (min. přes NFS/SMB protokol) na externí uložiště typu NAS.

	Zálohovací řešení musí podporovat připojení externí tieru typu Cloud S3 a umožnit do něj ukládání a správu dat.
Bezpečnost	Schopnost asynchronní replikace uložených dat do vzdálené lokality (druhé datové centrum) s přepnutím primárního provozu na repliku v záložní lokalitě při výpadku primární lokality (failover) minimálně pro účely čtení/obnovy.
	Automatická detekce ransomware.
	Integrovaná antivirová kontrola s pravidelnou aktualizací.
	Podpora WORM (Write Once Read Many) funkcionality, která zabraňuje neautorizovanému smazání či úpravě uložených dat. Implementace WORM musí být certifikována bezpečnostní normou SEC Rule 17a-4(f) bez nutnosti instalovat další zařízení nebo řešení třetích stran.
	Pro data obsahující osobní údaje klientů je vyžadováno uchování záznamu o klientech na nepřepisovatelných médiích a v nezměnitelném formátu v souladu s regulací HIPAA.
	Šifrovaná komunikace vyhovující standardu FIPS 140 při replikaci mezi datovými centry.
	Šifrování uložených dat napříč zálohovací infrastrukturou. Zálohovací řešení musí být uzavřené z pohledu odposlechu dat (šifrování), přístupu k datům (multifaktorová autentizace, multiadmin schvalování) a zranitelnosti (uzavřené jádro hypervizoru/OS pro externí přístup, nemodifikovatelnost pořízených záloh).
	Zajištění garance nepřepisovatelnosti záloh s časovým zámkem.
	Systém musí umožnit plnohodnotnou kompletní integraci celého řešení na IBM QRADAR SIEM a log management systémy.
Funkcionalita	Integrovaná funkcionalita zálohování virtuálních serverů **VMWare***: - s podporou kontinuální zálohy (CDP) pro RPO-kritické systémy - s možností okamžitého obnovení, tj. spuštění virtuálního stroje přímo ze zálohy v read/write režimu při současné fyzické obnově datových bloků probíhající v pozadí, pro min. 60 současně (paralelně) obnovovaných virtuálních serverů.
	Integrovaná funkcionalita zálohování souborových systémů fyzických serverů s OS MS Windows 2016 a novější, MacOS, RHEL, Debian, Ubuntu (tj. pro tyto OS musí existovat klienti s plnou podporou práv v souborových systémech, používaných na těchto OS).
	Integrovaná funkcionalita zálohování a obnovy **MS SQL***, **MySQL***, DB2 a PostgreSQL databází
	Integrovaná funkcionalita zálohování a obnovy dat z Microsoft365 cloudu (Mailboxy, Teams, Sharepoint, One Drive).
	Veškerá uložená data musí být v rámci lokality deduplikovaná a komprimovaná.

	Podpora cloudových služeb Microsoft Azure, Amazon S3, Google Cloud Storage pro možnost replikace dat do cloudu a využití cloudu pro účely odsunu dat do archivu (cloud tier), při zachování jednotného managementu.
	Možnost odsunu vybraných dat na externí NAS nebo do cloudu se zachováním referencí na archivovaná data v interním katalogu úložiště.
	Globální vyhledávání v úložišti napříč celým řešením s využitím indexace obsahu souborových systémů včetně obsahu souborových systémů záloh virtuálních serverů **VMWare***.
	Součástí musí být veškeré SW licence potřebné pro využití veškeré požadované funkcionality po celou dobu požadované podpory. A to včetně případného zajištění kapacitních licencí pro zálohy a repliku s kapacitou min. 60 TB.
	Administrace veškeré požadované funkcionality (zálohování, obnova, souborové sdílení, replikace, antivir, ransomware detekce, vyhledávání dat, řízení a logování přístupu, management dat napříč diskovými tiery) musí být dostupná z jediného centrálního grafického management nástroje. Není možné toto realizovat jako portál s URL odkazy na samostatné management nástroje.
	Soubor všech výše uvedených funkcionalit je nutné plnit jedním produktem a všechny funkce musí být jeho integrální součástí.
	Součástí musí být QoS, kdy musí být možné prioritizovat jednotlivé operace do úrovně obnova, záloha.
	Možnost zálohování neomezené množství virtuálních strojů.
Obnova	Možnost obnovy celého virtuálního serveru, virtuálních disků, nebo souborů.
	Možnost obnovy dat z Active Directory, MS Exchange, MS IIS, MSSQL Server, PostgreSQL Server
	Možnost okamžité obnovy min. 100 virtuálních serverů.
Další požadavky	Součástí dodávky musí být také HW a SW podpora výrobce/ů dodaných komponent v režimu NBD (reakce do dalšího pracovního dne) po celou dobu poskytované servisní podpory, tj. 5 let.
	Přístup do online znalostní databáze nabízeného řešení po celou dobu poskytované servisní podpory.
	Přístup do online portálu výrobce řešení, kam budou zasílána telemetrická data ze zálohování a budou zde automaticky vizualizována.
	Přístup do online portálu, kde bude možné korelovat a spravovat bezpečnostní incidenty napříč zálohovacím prostředím, a to minimálně na již zadavatelem provozovaném **IBM FS5200***.
	Možnost přístupu do online portálu výrobce, kde bude možné zálohovací řešení spravovat.
	Přístup k technické podpoře výrobce řešení po celou dobu poskytované servisní podpory.
	Přístup ke stažení aktualizací a patchů opravující chyby v kódu vydané výrobcem řešení po celou dobu poskytování servisní podpory.

	Přístup ke stažení poslední verze SW zálohovacího řešení po celou dobu poskytování servisní podpory.

*Pokud tato technická specifikace obsahuje přímé nebo nepřímé odkazy na určitého výrobce, dodavatele, produkty, případně patenty na vynálezy, užitné či průmyslové vzory, ochranné známky nebo označení původu, umožňuje zadavatel výslovně použití i jiných, kvalitativně a technicky rovnocenných řešení, která naplní zadavatelem požadovanou či odborníkovi zřejmou funkcionalitu, s výjimkou označených prvků v technické specifikaci z důvodů technické a technologické návaznosti na již existující řešení, které není předmětem této veřejné zakázky (označeno **tučným zvýrazněním** a hvězdičkou***).***