



Technická specifikace

na realizaci

„Nákup serverové infrastruktury, včetně instalace“

Pro:

Městská část Praha 5

zpracovala společnost

JECOM IT Consulting s.r.o.





Úvod – předmět plnění VZ

Zadavatel požaduje rozšíření/obnovu infrastruktury z důvodů potřeb rozšíření a obnovy částí infrastruktury, ale i zkušeností s RANSOMWARE útokem. Jedním z faktorů je dosažení maximální ochrany proti výpadku a dostupnosti všech systémů on-line.

Zadavatel rozdělí infrastrukturu do odlišných lokalit, čímž zajistí, dostupnost všech systémů v případě, že jedna z lokalit bude jakkoli poškozena – přírodní katastrofa, výpadek na přívodu elektrické energie, vytopení Datového centra ICT a jiné.

Hlavní požadavek zadavatele na funkci nových systémů je automatizace pro případ výpadku jedné či druhé lokality. Bezobslužné automatické přepnutí/spuštění systémů s aktuálními daty v druhé lokalitě. Funkce automatického přepnutí musí splňovat jak SW, tak HW část navrhovaného řešení.

Navrhované řešení musí být kompatibilní s používaným SW a HW zadavatele, které je specifikováno v příloze č. 2 Zadávací dokumentace.

Důležitá část navrhovaného řešení je aktivní obrana proti RANSOMWARE a jiným útokům. Systém, který zadavateli pomůže detekovat hrozby, pak jednotlivé hrozby analyzovat a následně je řešit. Ochrana v reálném čase před kybernetickým útokem, tak aby nedošlo k poškození dat.

Finální řešení bude obsahovat **2ks storage a 4ks serverů** na obou lokalitách. Přičemž na jedné lokalitě budou použity již stávající 4ks serverů.

Technická část Storage:

Specifikace Business Continuity/Disaster recovery

Navržený systém musí poskytovat dostupnost služby na úrovni definovaných SLA parametrů. Návrh řešení předpokládá eliminaci chyb, které by způsobily nedostupnost služby (SPOF) v celé infrastruktuře poskytující provozní platformu pro klíčové aplikace a další podpůrné systémy.

Diskové kapacity poskytované zejména pro produkční systémy a databáze musí být navrženy tak, aby byly schopny odolat výpadku jednoho diskového pole bez afektování host systémů, které mají na takovém poli data. Zadavatel očekává technologii diskového pole, která zajistí transparentní fail-over bez okamžité asistence obsluhy.

Rekonfigurace systémů jsou vyžadovány na úrovni transparentní a dynamické operace, která nebude mít dopad na provoz hostovaných aplikací. Tím se myslí například rekonfigurace virtuálních serverů, jejich migrace mezi servery nebo rozšiřování diskové kapacity.

Navržené řešení musí disponovat odolností proti výpadku jedné z lokalit. Zadavatel očekává návrh výkonnosti celého řešení tak, aby byl zajištěn kontinuální provoz z jedné lokality.



Požadavky na bezpečnost

Navržené diskové systémy musí být připraveny pro budoucí integraci pod jednotný systém kybernetické ochrany eliminující zneužití zranitelnosti ICT systémů. V tomto ohledu je nezbytné, aby návrh eliminoval takové komponenty, které jsou v rozporu s doporučeními NÚKIBu a také ty, které mají neúměrně vysoké množství evidovaných zranitelností viz Mitre.org katalog.

Zadavatel očekává zpracování návrhu řešení a aktivní bezpečnostní profylaxi použitých komponent. Výrobce jednotlivých zařízení nesmí být také pod sankčními nebo legislativními omezeními EU.

Uvažované komponenty pro návrh systému musí být schopny udržovat konfiguraci dle bezpečnostního souladu tak, aby bylo možné v budoucnu vynutit požadovanou úroveň zabezpečení.

Zadavatel vyžaduje aktivní přístup na úrovni odepření přístupu a také proaktivní ochraně dat pořízením nesmazatelných kopií s omezeným přístupem pod více faktorovou autentizací (MFA) a také na úrovni rozdílných rolí včetně možnosti kombinace autorizovaného přístupu s asistencí výrobce.

Privilegované přístupy k systémům musí být vždy pod mutli-factor autentizací. Aktivita privilegovaných uživatelů musí být logovaná a ukládaná do log management nástroje.

Predikce Ransomware

Zadavatel očekává aktivní přístup při kontrole datové integrity ukládaných dat. Profylaxe, která bude probíhat pravidelně, bude spočívat v aktivní analýze nesmazatelných kopií pro kritická data. V rámci zjednodušení správy je nutné zajistit celkovou orchestraci vytváření aplikačně konzistentních kopií a jejich automatické obnovy v případě například kybernetického útoku formou ransomware, který zakrytuje operační systém kritické aplikace a tím ji vyřadí z provozu.

Zmiňovaná orchestrační vrstva by měla být integrovatelná se systémy typu SIEM a reagovat na jeho podněty a incidenty, které vznikají při ohrožení cílových systémů. Zadavatel očekává zcela automatický response proces pro incidenty ze systému SIEM v podobě vyhledání a validování poslední nenakažené zálohy, její obnovu na produkční aplikační server a ověření aktuálního stavu a dostupnosti aplikačního serveru po obnově zálohy.

Pokud není orchestrační nástroj součástí řešení a jedná se o samostatný nástroj pro orchestraci, automatizaci a odezvu, tak zadavatel vyžaduje, aby tento nástroj byl od stejného výrobce s úzkou kompatibilitou a integrací na nabízené řešení.



číslo:	Požadavek	Popis funkcionality	Povinnost plnění	Způsob plnění požadavku
oddíl	Kybernetická odolnost			
1	User management	Rozdělení privilegií k přístupu a řízení datových a zabezpečených diskových svazků. Aktivace a deaktivace účtů s asistencí podpory výrobce	ANO	<i>Je-li relevantní, účastník přesně vyspecifikuje způsob splnění požadavku (tj. Přesná hodnota funkcionality nabízeného produktu)¹</i>
2	Zabezpečené kopie dat	Vytváření zabezpečených kopií dat na úrovni nesmazatelné a nepřístupné pro host systémy	ANO	
3	Automatizace obnovení kopií	Na základě rozpoznání hrozby (např. Ransomware), tedy šifrování souborů na koncovém zařízení nebo serveru, řešení automaticky obnoví poslední nešifrovanou kopii	ANO	
4	Ověření stavu po obnově kopie	Řešení musí být schopné ověřit stav koncového zařízení nebo aplikačního serveru po obnově zabezpečené kopie (např. funkčnost webového serveru přes port 443)	ANO	
5	Editace automatizačního procesu	Řešení musí nabízet úpravu automatizačního procesu pomocí grafického rozhraní bez hlubší znalosti programování	ANO	
6	Editace automatizačního procesu	Automatizovaný proces obnovy musí jít v editoru logicky větvit pomocí logických spojek a procesních konstrukcí if, else, start, end, atd. pro přesnou definici procesu a podchycení okrajových	ANO	

¹ Platí pro všechny buňky sloupce „Způsob plnění požadavku“



		případů, kdy např. po obnově kopie není webový server dostupný		
7	Email notifikace	Řešení musí upozornit konkrétního uživatele ve specifické skupině a se specifickou rolí emailem o tom, že došlo k detekci Ransomware a byl spuštěn automatizovaný proces pro obnovu zabezpečené kopie	ANO	
8	Licencování	Řešení musí licenčně pokrýt minimálně 8 kritických aplikačních serverů, které budou mít zabezpečené kopie k obnově v případě potřeby	ANO	
9	Licencování	Řešení nesmí být omezené na počet akcí (tedy např. počet obnovených kopií), které může provést za den/týden/měsíc	ANO	
10	Licencování	Řešení nebude licenčně omezeno počtem používaných korelačních pravidel.	ANO	
11	Licencování	Řešení nebude licenčně omezeno počtem generovaných reportů	ANO	
12	Detekce pomocí pravidel	Řešení musí poskytovat analytické a korelační funkce bez dalších zásahů a činností (out-of-the-box)	ANO	
13	Alerting	Řešení musí poskytnout alerting vycházející z detekovaných bezpečnostních hrozeb od monitorovaných zařízení	ANO	
14	Detekce pomocí pravidel	Korelační modul musí poskytovat již po instalaci (out-of-the-box) metody korelačních pravidel, která automatizují zjišťování incidentů a související workflow procesy	ANO	



15	Historie incidentu	Řešení musí podporovat schopnost monitorovat historii útoků (typů událostí) na kritické komponenty	ANO	
16	Sběr logů	Řešení musí umožňovat bez-agentový sběr logů (sběr bez nutnosti instalovat agenta na cílový systém)	ANO	
17	Identifikace zdrojů logů	Řešení musí podporovat automatickou identifikaci systémů – zdrojů logů	ANO	
oddíl	Hardware požadavky			
18	Předmět plnění	Jsou požadována dvě totožná disková pole do každé lokality jedno, níže jsou uvedené minimální parametry pro jedno nabízené diskové pole, pokud není specifikováno jinak.	ANO	
20	Architektura	modulární, minimálně dvou řadičové all flash nebo hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce	ANO	
21	Výkonnost	škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do osmi řadičové konfigurace a škálování kapacit pomocí expanzních jednotek. Škálování řadičů ani expanzních jednotek není povoleno řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů	ANO	
22	Velikost a rozšiřitelnost cache	celková velikost cache/RAM v jednom řadiči je minimálně X 128 GB	ANO	



23	Rozšiřitelnost počtu disků / modulů	celková nativní rozšiřitelnost je minimálně 700 disků, v případě nasazení více řadičů až čtyřikrát tolik disků. Jak je popsáno výše na řádku výkonnost, nelze toto řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů	ANO	
24	Podpora osazených disků, SSD a flash modulů	podpora 2,5" nebo 3,5" disků technologie SSD/flash včetně rotačních disků a to současně: - podpora SCM (Storage Class Memory) - SSD enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 2 a vyšší - všechny požadované typy SSD a flash modulů musí být NVMe typu - možnost mixování minimálně dvou různých disků / modulů (SCM a SSD) v rámci jednoho řadiče i expanzního boxu - rotační disky minimálně na SAS 3.0 architektuře	ANO	
25	Redukce dat	řešení musí umožňovat nasazení redukce dat v reálném čase tak, aby nedošlo k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je požadována separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat	ANO	



26	Minimální požadovaná hrubá kapacita	<ul style="list-style-type: none"> - Tier 0: minimálně 96 TB na SSD / Flash ve variantě enterprise (DWPD 2 a vyšší), velikost jednoho disku nebo modulu je maximálně 10TB - Tier 1: minimálně 260 TB na SSD / Flash / SAS nebo NL-SAS ve variantě enterprise, velikost jednoho disku nebo modulu je maximálně 12 TB. 	ANO	
27	Konektivita k hostitelským serverům (front-end)	diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC a 10Gbit iSCSI s možností rozšíření pomocí rozšiřujících karet do řadičů diskového pole o další přenosové protokoly (např. min. 25Gbit Ethernet RoCE v2 nebo iWARP)	ANO	
28	Minimální počet a typy hostitelských portů (front-end)	jsou požadovány min. 2 porty 32Gb FC a 2 porty 10Gb iSCSI na řadič, tzn. minimálně 4x 32Gbit FC portů a 4x 10Gbit iSCSI portů na jedno dvou řadičové diskové pole	ANO	
29	Velikost nabízeného řešení do racku	Maximálně 5U		
oddíl	Software požadavky			
30	Vytváření LUNů	vytváření virtuálních logických disků	ANO	
31	Technologie pro redukci datového prostoru	thin provisioning (včetně detekce a reklamace prázdného prostoru)	ANO	
32	Technologie pro redukci datového prostoru	komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou	ANO	



		nabízenou kapacitu včetně patřičného HW akcelérátoru nebo na jednotlivých modulech		
33	Technologie pro redukci datového prostoru	deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence	ANO	
34	Šifrování dat	šifrování dat pro celou nabízenou kapacitu včetně příslušné licence. Pro tier 0 je požadována certifikace ve standardu FIPS 140-2. Pokud nabízené řešení neumožňuje šifrování dat nad / na úrovni disků, jsou požadovány SED disky pro celou nabízenou kapacitu	ANO	
35	Tiering	inteligentní správa výkonnostních charakteristik (pro minimálně 3 tiery a to včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM)	ANO	
36	Monitoring	Podpora nástrojů pro sledování historických dat o využití datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok (možnost řešit i externím SW nástrojem v rámci dodávky)	ANO	
37	Kopie dat	Microsoft VSS podpora	ANO	
38	Podpora virtualizačních platforem	VMware VAAI, VASA a VVOL podpora, je požadován VASA provider	ANO	



		přímo ve FW nabízeného diskového pole		
39	Kopírovací funkce	zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole)	ANO	
40	Snapshoty	možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: <ul style="list-style-type: none"> - snapshot se po určité době může automaticky stát klonem - inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu - reverzní snapshoty - lze provést zpětné přesunutí dat z klonu do původního originálního Volume - lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) 	ANO	
41	Migrace dat	transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možností rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit	ANO	
42	Migrace dat	bezvýpadková migrace - řešení musí umožňovat migraci dat bez jakéhokoliv přerušení, tzn. aplikace a jejich OS nezaznamenají žádnou nedostupnost dat (LUNů)	ANO	



43	Počet připojených host serverů a licence	řešení obsahuje licence na neomezený počet připojení hostitelských serverů	ANO	
44	Management	SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru)	ANO	
45	Vzdálený dohled	Remote Service (call home) v ceně řešení	ANO	
46	Řízení proběhlých operací	Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd.	ANO	
47	Potvrzení výrobce	Je požadováno potvrzení od lokálního zastoupení výrobce, že nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce	ANO	
48	Příslušenství	Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.	ANO	
49	HW a SW podpora	Lokalita 1: minimálně 5 let; v online režimu 24x7 s garantovanou dobou opravy do 24 hodin včetně SW podpory, která umožňuje např. přístup k novým verzím FW, opravným patchům atd. Lokalita 2: minimálně 5 let; v online režimu 5x9	ANO	



		s odezvou následující pracovní den včetně SW podpory, která umožňuje např. přístup k novým verzím FW, opravným patchům atd.		
50	Podpora operačních systémů a cluster nadstavby	IBM AIX 7.1, 7.2 a vyšší IBM VIOS 2.2 a vyšší RHEL 6.x a vyšší VMware 7 a vyšší včetně VAAI a VASA integrací Windows server 2016 a vyšší SQL Supermicro? Co ještě používám? Cisco?	ANO	
51	Podpora virtualizace	podpora externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný.	ANO	
oddíl	Datová odolnost			
52	Odolnost proti výpadku disku / modulu	podpora minimálně následujících režimů RAID - 1, 5, 6, 10 nebo minimálně DRAID 1 a 6	ANO	
53	Podpora clusteringu	jednotlivá disková musí být možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod.	ANO	
54	Replikace	podpora replikace do třetí lokality včetně případných licencí	ANO	
55	Odolnost datových cest	SW pro redundantní datové cesty v ceně řešení	ANO	
56	Kompatibilita s HA řešením virtualizačních platforem	Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí	ANO	



		být dohledatelné v matici kompatibility na stránkách VMware		
57	Odolnost proti výpadku celé RAID skupiny	vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na běžných OS nebo virtualizační platformě včetně příslušných licencí	ANO	
58	Odolnost proti nedostupnosti lokality	Nabízené diskové pole musí umožňovat replikaci dat na synchronní a asynchronní úrovni po FC i IP	ANO	
59	Bezvýpadkový upgrade řadičů	upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datům	ANO	



Technická část servery:

Předmět plnění

Jsou požadovány 4 ks totožných serverů, níže jsou uvedené minimální parametry pro každý nabízený server

číslo	Požadavek	Popis funkcionality	Povinnost plnění	způsob plnění požadavku*
	Provedení	velikost 1U	ANO	
	CPU	1x CPU 16 jader (32 vláken), min 2.8 GHz a výkon v Passmark min 32500 bodů	ANO	
	RAM	768GB RAM s možností rozšíření na dvojnásobek se zachováním stávajících RAM modulů	ANO	
	HDD sloty	8 hotplug pozic na disk	ANO	
	HDD	2x 240GB SSD disky HW RAIDu 1	ANO	
	Network	2x 10/25Gb LAN SFP+ porty	ANO	
	FC	2x 32Gb FC porty	ANO	
	TPM	Trusted Platform Module 2.	ANO	
	Management	dedikovaný management port, management umožňuje kompletní vzdálenou správu serveru	ANO	
	Management Cloud	možnost napojení na cloudový dohledový a analytický nástroj engine pro proaktivní správu	ANO	
	Power	Redundantní napájecí zdroje min 500W	ANO	
	maintenance	Support na 3 roky s odezvou technika v místě instalace do následujícího pracovního dne	ANO	

*** Je-li relevantní, účastník přesně vyspecifikuje způsob splnění požadavku (tj. Přesná hodnota funkcionality nabízeného produktu). Platí pro všechny buňky sloupce „Způsob plnění požadavku“.**



Technická část Switch 48 port 1 GB

1 ks zařízení Switch 48 portový 1 GB			
Požadavek	Popis funkcionality	Povinnost plnění	Způsob plnění požadavku *
Počet přepínaných ethernetových portů RJ-45	48	ANO	
Typy přepínaných ethernetových portů RJ-45	Gigabit Ethernet (10/100/1000)	ANO	
Počet slotů SFP modulu	4	ANO	
Konzolový port	RJ-45/Mini-USB	ANO	
Počet portů USB 2.0	1	ANO	
Síťové standardy	IEEE 802.1AX, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ab, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3ae, IEEE 802.3af, IEEE 802.3ah, IEEE 802.3at, IEEE 802.3az, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z	ANO	
Podpora 10G	Ne	ANO	
Plně duplexní režim	Ano	ANO	
Agregace spojení	Ano	ANO	
Broadcast storm control	Ano	ANO	
Přenosová rychlost sítě Ethernet	10,100,1000 Mbit/s	ANO	
Auto MDI/MDI-X	Ano	ANO	
Protokol větvícího se stromu (STP)	Ano	ANO	
Automatické vyjednávání	Ano	ANO	
Podpora VLAN	Ano	ANO	
Počet VLANs	256	ANO	
Kapacita přepínání	104 Gbit/s	ANO	
Rychlost přetáčení	77,38 Mpps	ANO	
Tabulka MAC adres	16000 pol.	ANO	
Statické směrování	Ano	ANO	
Počet statických cest	16	ANO	
Podpora pro Jumbo Frames	Ano	ANO	
Rámy jumbo	10240	ANO	

*** Je-li relevantní, účastník přesně specifikuje způsob splnění požadavku (tj. Přesná hodnota funkcionality nabízeného produktu). Platí pro všechny buňky sloupce „Způsob plnění požadavku“.**