Příloha č. 1

Technická specifikace předmětu plnění – položkový rozpočet

Položka	Ks	Specifikace	Nabídková cena v Kč bez DPH za 1 kus zařízení/1 hodinu	Nabídková cena v Kč bez DPH za požadované množství ks
L2_L3 přepínač	8	48 RJ-45 autosensing 10/100/1000 portů, 2 SFP+ 10GbE porty, 2 RJ-45 1/10GBASE-T porty 1x dual-personality (RJ-45 nebo USB micro-B), serial console port, 1x RJ-45 out-of-band management port, 1x USB 2.0 Přepínač bude mít možnost redundantního napájení (možno i externí) Paměť min. 1 GB SDRAM; Packet buffer size: min. 3 MB 1000 Mb Latence max. 5 µs 10 Gbps Latence max. 3 µs Propustnost min. 130 Mpps Routing/Switching capacita min. 176 Gbps Velikost routovací tabulky min. 512 záznamů Podpora SSL, SSHv2, ARP, DHCP Podpora QoS, L2, L3 Podpora zapojení více přepínačů do virtuálního switche s podporou automatického load balancingu a vysoké dostupnosti bez využití Spanning Tree Protocolu Vzdálená konfigurace a management přes zabezpečený web prohlížeč, příkazovou řádku, podpora SNMP, Telnet, HTTPS, FTP Dodávka celkem 2x 10G SFP+/SFP+ 1 m DAC Cable (pro 8 přepínačů: celkem 16x 10G SFP+/SFP + 8x1m DAC Cable) Záruka doživotní s výměnou druhý den od nahlášení závady v servisním středisku	74 500,00 Kč	596 000,00 Kč

L2_L3 přepínač	**1**	48 RJ-45 autosensing 10/100/1000 portů-370 W PoE+, 2 SFP+ 10GbE porty, 2 RJ-45 1/10GBASE-T porty S možností přidání redundantního zdroje s minimálním celkovým výkonem pro PoE 740 W 1x dual-personality (RJ-45 nebo USB micro-B), serial console port, 1x RJ-45 out-of-band management port, 1x USB 2.0 Switch bude mít možnost redundantního napájení (možno i externí) Paměť min. 1 GB SDRAM; Packet buffer size: min. 3 MB 1000 Mb Latence max. 5 µs 10 Gbps Latence max. 3 µs Propustnost min. 130 Mpps Routing/Switching capacita min. 176 Gbps Velikost routovací tabulky min. 512 záznamů Podpora SSL, SSHv2, ARP, DHCP Podpora QoS, L2, L3 Podpora zapojení více přepínačů do virtuálního switche s podporou automatického load balancingu a vysoké dostupnosti bez využití Spanning Tree Protocolu. Dodávka celkem 2x 10G SFP+/SFP+ 3 m DAC Cable Vzdálená konfigurace a management přes zabezpečený web prohlížeč, příkazovou řádku, podpora SNMP, Telnet, HTTPS, FTP Záruka doživotní s výměnou druhý den od nahlášení závady v servisním středisku	89 000,00 Kč	89 000,00 Kč
UTM Firewaly (Cluster)	**2**	Dvojice UTM firewallů ve formě hardwarových appliance ve režimu vysoké dostupnosti (L2 ISO modelu) s možností komunikace Aktivní/ Aktivní i Aktivní / Pasivní Licence minimálně 36 měsíců na HW výměnu zařízení v případě poruchy, včetně licence na upgrade firmware po dobu minimálně 36 měsíců	149 000,00 Kč	298 000,00 Kč

	Integrované funkce Antivir, WebFiltering, Email Filtering, Aplikační kontrola, Intrusion Protection (IPS), DNS Filtering, SSL/SSH inspekce, Load Balancing, VPN IPsec a SSL Firewall Throughput (512 byte UDP packets) 7.3Gbps a více Firewall Throughput (Packets Per Second) 6.5 Mpps a více Concurrent Sessions (TCP) 2 Million a více IPsec VPN Throughput (512 byte packets) 4 Gbps a více SSL-VPN Throughput 250 Mbps a více Application Control Throughput 800 Mbps a více Možnost virtualizace firewallu s licencí na min 10 virtuálních domén minimálně na 36měsíců Wi-Fi Controler s licencí pro minimálně 64 přístupových bodů minimálně na 36 měsíců Vestavěné interní úložiště pro záznam logů minimálně 450 GB Integrovaná funkcionalita ochrany proti Zero Day útokům na reálném/virtualizovaném/cloudovém prostředí. (Ve smyslu technologie Check Point SandBlast, Forti SendBox, PaloAlto WildFire apod.) Licence minimálně na 36 měsíců. Ochrana před nevyžádanou poštou s transparentní kontrolou minimálně SMTP protokolu. Licence minimálně na 36 měsíců Antivirová kontrola provozu, detekce aplikací na L7 vrstvě a její kontrola (aplikační firewall), Kategorizace a filtrace URL, systém pro detekci a prevenci průniku (IPS), neomezené licence těchto funkcí po dobu minimálně 36měsíců Automatická aktualizace databází bezpečnostních signatur u výrobce. Neomezená po dobu minimálně 36 měsíců. (Komerční databáze, nikoliv komunitní nebo otevřenou) Automatická aktualizace databází IP adres botnet C&C center (black listů) u výrobce po dobu minimálně 36 měsíců.		

		Automatická aktualizace databáze URL kategorií pro web filtering s podporou českých stránek u výrobce. Neomezená po dobu minimálně 36 měsíců. (Komerční databáze, nikoliv komunitní nebo otevřenou) Jednotné grafické administrátorské rozhraní výrobce pro všechna řešení. Konfigurace integrované do jednoho celku Licence pro minimálně 300 současně připojených SSL-VPN klientů po dobu minimálně 36 měsíců Licence pro minimálně 50 současně připojených Gateway-to-Gateway IPsec VPN Tunnels po dobu minimálně 36 měsíců Minimálně 20xGE RJ45 portů a minimálně 2xSFP Geolokace IP adres a filtrování na základě geografického umístění (dle IP adresy) Autentizace administrátorů vůči RADIUS, LDAP a lokální databázi Dynamické směrovací protokoly BGP, RIP, OSPF Integrované SNMP v3 Integrované QoS pro řízení šířky pásma Integrovaná funkce WAN Load Balancing		
Server pro sběr, archivaci a reporting logů síťového provozu	**1**	Samostatné řešení pro zpracování logů a reporting (provedení, standalone server, virtuální server/appliance, dedikované hw zařízení). Detailní specicifikace uvedena v listu 2, této přílohy.	695 000,00 Kč	695 000,00 Kč
Server - Fyzické HOST	**2**	Šasi serveru v provedení do racku, rozměr max. 2U, instalační ližiny do racku a sklopné rameno pro uchycení kabeláže musí být součástí dodávky 2x procesor, z toho každý min. dvanáct fyzických jader, 24 vláken, minimální taktovací frekvence 2.20GHz, min. 30 MB Cache	305 000,00 Kč	610 000,00 Kč

	Minimálně 24 slotů pro paměťové moduly; podpora 128 GB modulů LRDIMM 2400MHz 320 GB RAM DDR4/2400Mhz (32 GB moduly), další paměťové sloty volné pro pozdější upgrade pamětí bez výměny modulů a bez snížení frekvence Minimálně 2 x SSD nebo SAS 10k pevný disk o kapacitě min. 300 GB HW SAS 12Gbit/s RAID řadič s podporou RAID 1, 1+0, 5, 5+0,6, 6+0, 2 GB zálohované cache s možností rozšíření až na 4 GB. Řadič musí umožnit připojení všech diskových pozic v maximální konfiguraci šasi Minimálně 8 interních pozic pro pevné disky s možností rozšíření až na celkem 16 HDD. Podpora až 6ks NVME disků. Počet použitelných portů min.: 4x 1Gb LAN; 2x 10Gb SFP+ LAN; 2x FC 16Gb SAN Integrovaný informační panel (LCD nebo LED) Ventilátory redundantní, vyměnitelné za provozu Minimálně 2 za chodu vyměnitelné redundantní napájecí zdroje Integrovaný nezávislý procesor pro vzdálenou správu umožňující: dedikovaný LAN RJ-45 port umožňující zabezpečený přístup přes síť – webovým prohlížečem i SSH, připojení virtuálních médií (FDD, DVD, ISO i jejich image, USB klíče, adresáře pro čtení), plně integrovanou grafickou konzoli s možností sdílení více uživateli současně, integrovaný nástroj pro upgrade firmware s možností automatické aktualizace od výrobce HW, nezávislý procesor musí pracovat i při nenabootovaném operačním systému serveru, musí umožnit průběžné sledování parametrů serveru, hardwarový stav serveru, včetně uložení event. logu, detekci a zasílání SNMP zpráv o chybových stavech hardware, řízení přístupových práv k centrální části SW a k management nástrojům na serverech pomocí účtů Active Directory domény, Podpora zahrnující jak HW, tak SW daného výrobce i výrobců třetích stran; minimálně Microsoft, VMware. Tato SW podpora musí být v ceně řešení. Záruka 36 měsíců, typ NBD		

Primární datové úložiště	**1**	Provedení do RACKu 19“ Diskové pole s redundantními řadiči, pracujícími v režimu active-active podle standartu ALUA. Každý řadič pole musí mít min. 4 GB cache po odečtení paměti pro vlastní OS Pole musí umět virtualizovat vnitřní diskovou kapacitu a tuto kapacitu poskytovat pomocí standardních protokolů Nabízené pole musí být vybaveno min. 4x 16Gb FC rozhraním (vč. originálních SFP modulů) s možností rozšíření o další čtyři iSCSI 1/10Gb nebo FC16 porty Diskové pole musí podporovat poslední generaci SAS disků i diskových polic (12Gb) Cache paměť musí být zálohována (bateriemi, vysokokapacitními kondenzátory nebo podobnou technologií) po dobu min. 5 let Je požadováno, aby byla kapacita minimálně 20 TB 10k SAS, 150TB 7,2k NL SAS Pole musí být vysoce dostupné a podporovat přidávání a náhradu disků za běhu, mít redundantní řadiče, napájení a větráky Požadujeme podporu těchto RAID geometrií: 0, 1, 1+0, 3, 5, 5+0 a 6 Pole by mělo podporovat SFF i LFF disky se SAS a SATA rozhraním včetně SED Všechny typy disků (SSD, SAS a případně SATA) musí být možno kombinovat v jedné diskové polici Pole by mělo být škálovatelné na více než 180 disků Pole musí umět nastavit spare disky dedikované (pro určitou RAID skupinu) i globální pro celé pole Součástí dodávky budou licence pro „Thin provisioning“ a „SSD Cache“ Pole musí být možné spravovat i z vCenter rozhranní (vytváření nových datastore, templates apod) Pole musí podporovat VAAI primitiva pro VMware integraci Záruka 36 měsíců, typ 24x7, garantovaná doba opravy do 6 h na místě.	960 000,00 Kč	960 000,00 Kč

Zálohovací datové úložiště 1	Provedení do RACKu 19“		
	Diskové pole s redundantními řadiči, pracujícími v režimu active-active podle standartu ALUA. Každý řadič pole musí mít min. 4 GB cache po odečtení paměti pro vlastní OS		
	Nabízené pole musí být vybaveno min. 4x 16Gb FC rozhraním (vč. originálních SFP modulů) s možností rozšíření o další čtyři iSCSI 1/10Gb nebo FC16 porty		
	Diskové pole musí podporovat poslední generaci SAS disků i diskových polic (12Gb)		
	Cache paměť musí být zálohována (bateriemi, vysokokapacitními kondenzátory nebo podobnou technologií) po dobu min. 5 let		
	Je požadováno, aby byla kapacita minimálně 192TB 7,2k NL SAS		
	Pole musí být vysoce dostupné a podporovat přidávání a náhradu disků za běhu, mít redundantní řadiče, napájení a větráky	765 000,00 Kč	765 000,00 Kč
	Pole by mělo podporovat SFF i LFF disky se SAS a SATA rozhraním včetně SED		
	Požadujeme podporu těchto RAID geometrií: 0, 1, 1+0, 3, 5, 5+0 a 6		
	Všechny typy disků (SSD, SAS a případně SATA) musí být možno kombinovat v jedné diskové polici		
	Pole by mělo být škálovatelné na více než 180 disků		
	Pole musí umět nastavit spare disky dedikované (pro určitou RAID skupinu) i globální pro celé pole		
	Součástí dodávky budou licence pro „Thin provisioning“ a „SSD Cache“		
	Pole musí být možné spravovat i z vCenter rozhranní (vytváření nových datastore, templates apod)		
	Pole musí podporovat VAAI primitiva pro VMware integraci		
	Záruka 36 měsíců, typ 24x7, garantovaná doba odezvy NBD		

Záložní zdroj napájení	**1**	Výkon modulů minimálně 15kW Možnost budoucího kapacitního rozšíření o další rámy Modulární konstrukce umožňující vnitřní redundanci, možnost výměny výkonových modulů za provozu Doba zálohy při zatížení 15kVA minimálně 10 minut Max vyzářené teplo při 15kW maximum 650 W Možnost startu na baterie Účinnost v režimu online > 96 % Vstupní účiník minimálně 99 % Musí obsahovat ovládací LCD panel Harmonické zkreslení vstupního proudu (ITHD) < 3 % Harmonické zkreslení výstupního napětí (UTHD) <1 % (100% lineární zátěž); < 5 % (standardní nelineární zátěž) Musí být vybaven stykačem proti zpětnému napájení Připojení vstupu 3 f + N + PE Připojení výstupu 3 f + N + PE Podpora správy přes webové prostředí Možnost integrace managementu v rámci virtuálního prostředí včetně licence pro minimálně 100 zařízení Bezpečnostní normy IEC 62040-1 Monitoring teploty Monitoring vlhkosti Monitoring sepnutých kontaktů Port pro síťovou komunikaci (RJ45) Management pro vCenter Minimálně 2 přepínače (Automatic Transfer Switch) 16 A pro zajištění redundance napájecích cest.	345 000,00 Kč	345 000,00 Kč

		Instalace jištěného rozvodu a rozvaděče pro distribuci zálohovaného napájení 230 V mezi centrální UPS a PDU v rozvaděčích. V datacentru Mánesova. Zpracování dokumentace zapojení a revizní zprávu.		
Workshop	**20**	workshop pro 5 zaměstnanců v obsluze hardwaru a softwaru a zaškolení v implementačních a konfiguračních provedeních dodaného zboží	560	11 200,00 Kč
Nabídková cena bez DPH				**4 369 200,00 Kč**

Detailní požadavky na server pro sběr, archivaci a reporting logů síťového provozu		
Číslo	**Popis**	**Splňuje**
1	**Obecné parametry**	
2	Zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz seznam podporovaných zařízení)	Ano
3	Možnost dopsání parseru pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery.	Ano
4	Systém standardizuje přijaté logy do jednotného formátu a logy jsou parserovány (rozdělovány) do příslušných políček dle jejich typu.	Ano
5	Nad takto standardizovanými daty systém automaticky vytváří indexy pro rychlejší vyhledávání pro všechna pole standardizovaného logu.	Ano
6	Všechny rozparsované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Ano
7	Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, JSON RFC7159.	Ano
8	Systém nesmí umožnit mazání nebo modifikování již uložených logů.	Ano
9	Konsolidace logů na centrálním místě.	Ano
10	Snadné vyhledávání událostí (ad hoc) bez nutnosti programování.	Ano
11	Grafické znázornění událostí (grafy událostí).	Ano
12	Grafické znázornění TOP událostí nad všemi daty za určité časové období.	Ano
13	Automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě.	Ano
14	Automatické doplňování reverzních DNS záznamů k IP adresám.	Ano
15	V případě přetížení systému jsou události ukládány do vyrovnávací paměti.	Ano
16	Unifikované vyhledávání napříč všemi typy dat a zařízení.	Ano
17	Potvrzení, vystavené autorizovanou osobou, o shodě, že nabízený systém splňuje požadavky normy ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením.	Ano
18	Možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.	Ano
19	Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů.	Ano
20	Předpřipravené pohledy na uložená data.	Ano
21	Aktualizace reportů a pohledů výrobcem.	Ano
22	Konfigurační a Systémové rozhraní a On-line dokumentace v Českém jazyce.	Ano
23	Kapacitní i výkonová škálovatelnost.	Ano

24	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data musí být minimálně 40TB.	Ano
25	Požadujeme, aby ze systému bylo možné vytáhnout 2 libovolné disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	Ano
26	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	Ano
27	Možnost dotazování externím monitorovacím systémem pro další zpracování alertů a prahových hodnot (Zabbix, Nagios, MRTG a další).	Ano
28	Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 316 / 2014 ze dne 15. prosince 2014 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)" k Zákonu 181 / 2014 „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) bezpečnosti" ze dne 23. července 2014.	Ano
29	Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému.	Ano
30	Uživatelské role definující přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému.	Ano
31	Možnost ověřovat uživatele systému na externím LDAP serveru.	Ano
32	**HW parametry**	Ano
33	Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	Ano
34	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.	Ano
35	1 procesory (min. 10 jader), podpora HyperThreadingu.	Ano
36	Min. 64GB DDR-4.	Ano
37	HW 12Gb SAS RAID řadič s podporou RAIDu 0/1/5/6/10/50/60 s cache min. 2GB, která je zálohována baterií nebo flash pamětí.	Ano
38	Z výkonových důvodů požadujeme, aby v systému bylo minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček.	Ano
39	Minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.	Ano
40	Větráky v serveru musí být vyměnitelné za provozu a redundatní.	Ano
41	2x napájecí zdroje s redundancí napájení 1+1.	Ano
42	Virtuální KVM (tj. převzetí textové i grafické konsole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	Ano
43	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).	Ano
44	Požadovaná min. 3 letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.	Ano

45	**SW parametry**	Ano
46	Zařízení funguje formou appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli - viz bod 29, není nutné editovat žádné konfigurační soubory včetně IP adresace systému).	Ano
47	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli (viz bod 29).	Ano
48	Průměrný příjem min. 6 tis událostí / s.	Ano
49	Špičkový příjem 30 tis událostí / s, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později.	Ano
50	Licenčně neomezený počet zařízení pro příjem zasílaných událostí.	Ano
51	Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli (viz bod 29). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	Ano
52	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	Ano
53	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat.	Ano
54	V centrální správcovské konzoli (viz bod 29) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.	Ano
55	V centrální správcovské konzoli (viz bod 29) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	Ano
56	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	Ano
57	Podpora zrcadlení a clusteru – 2 a více zařízení v režimu active / active.	Ano
58	Vícenodový systém se chová jako 1 celek.	Ano
59	V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.	Ano
60	Rozšiřování kapacity i navyšování výkonu pomocí přidávání dalších zařízení do clusteru.	Ano
61	V případě rozšíření na cluster (přidání dalšího node) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody.	Ano
62	**Alerty**	Ano
63	Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert.	Ano

64	Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozpársované události.	Ano
65	Předpřipravené sety/vzory alertů výrobcem.	Ano
66	Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	Ano
67	V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha).	Ano
68	**Sběr událostí z Microsoft prostředí**	Ano
69	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring souborových logů.	Ano
70	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	Ano
71	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole z bodu 29.	Ano
72	Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole z bodu 29. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	Ano
73	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému (viz bod 29). Správa a aktualizace Windows agenta se neprovádí z Group Policy.	Ano
74	Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).	Ano
75	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	Ano
76	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	Ano
77	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 29) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb.	Ano
78	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	Ano
79	Počet instalací Windows agenta nesmí být licenčně omezen.	Ano
80	**Sběr událostí z poboček**	Ano
81	Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.	Ano
82	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	Ano

83	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	Ano
84	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	Ano
85	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí /s. a to i v trvalé zátěži.	Ano
86	Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.	Ano
87	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi.	Ano
88	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	Ano
89	**Seznam požadovaných podporovaných zařízení a systémů**	Ano
90	Apache httpd	Ano
91	Apache Tomcat	Ano
92	Antivir AVG	Ano
93	Antivir Avast	Ano
94	Antivir Eset	Ano
95	Antivir Eset Remote administrator	Ano
96	Brocade FC switches	Ano
97	ArcSight CEF format all sources	Ano
98	Cisco ASA	Ano
99	Cisco Firepower	Ano
100	Cisco IOS	Ano
101	Cisco IronPort	Ano
102	Cisco SMB	Ano
102	Cisco WLC	Ano
102	Dell Force10	Ano
102	Dell iDrac (Server OoB management)	Ano
102	Dell PowerConnect	Ano
102	Dell SonicWALL	Ano
102	Dell W-series WiFi	Ano
102	Discard (Special distard rule)	Ano
102	Dropbear SSH (mostly Embedded Linux)	Ano
102	Extreme Networks XOS	Ano
102	FlowMon	Ano
102	FortiAuthenticator	Ano
102	FortiDDoS	Ano
102	FortiGate (FOS 5.2)	Ano
102	FortiMail	Ano

102	FreeRADIUS	Ano
102	Qradar LEEF format all sources	Ano
102	HPE Aruba Networks WLAN	Ano
102	HPE iLo 4 (Server OoB management)	Ano
102	HPE IMC	Ano
102	HPE routers	Ano
102	HPE switches Procurve OS	Ano
102	HPE switches Comware OS	Ano
102	HPE Comware WLAN	Ano
102	CheckPoint	Ano
102	ISC BIND	Ano
102	ISC DHCP	Ano
102	ISC DHCPD	Ano
102	JSON (format)	Ano
102	Juniper SRX	Ano
102	Kaspersky Endpoint Security	Ano
102	Kaspersky Security Center	Ano
102	Kerio Connect	Ano
102	Kerio Control	Ano
102	Kernun Clear Web	Ano
102	Kernun web filter	Ano
102	Linux Cron	Ano
102	Linux Freeradius	Ano
102	Linux Iptables	Ano
102	Linux postfix	Ano
102	LOGmanager	Ano
102	Mikrotik	Ano
102	Microsoft SharePoint	Ano
102	Microsoft SQL	Ano
102	Microsoft Windows DHCP log	Ano
102	Microsoft Windows firewall	Ano
102	Microsoft Windows IIS	Ano
102	MySQL	Ano
102	Nginx	Ano
102	Novell eDirectory	Ano
102	OpenSSH server	Ano
102	Oracle DB	Ano
102	Palo Alto Networks NGFW	Ano
102	SAP	Ano
102	Shorewall	Ano

102	SonicWall	Ano
102	Sophos	Ano
102	SpamAssasin	Ano
102	TrendMicro DeepDiscovery	Ano
102	TrendMicro TippingPoint NG-IPS	Ano
102	UBNT Rocket	Ano
102	UBNT UniFI	Ano
102	VMware	Ano
102	Windows - any logs from Event Viewer	Ano
102	Windows - any text log from file	Ano

Ústav zemědělské ekonomiky a informací

Rámcový popis stávajícího stavu technické infrastruktury

Obsah

1 MANAŽERSKÝ SOUHRN

Účelem tohoto dokumentu je rámcový popis prostředí ÚZEI v návaznosti na již vypracovanou a schválenou IT Architekturu.

V dokumentu je zohledněn jak současný, tak i budoucí předpokládaný stav s výhledem na požadavky na rozšíření výpočetních a datových kapacit. Nejedná se pouze o rozšíření, ale také o návrh nových funkcionalit dle moderních trendů v daných IT oblastech.

2 STÁVAJÍCÍ ICT ARCHITEKTURA

Současný stav IT architektury je zobrazen na následujícím obrázku.

Obrázek 1 Celková IT architektura

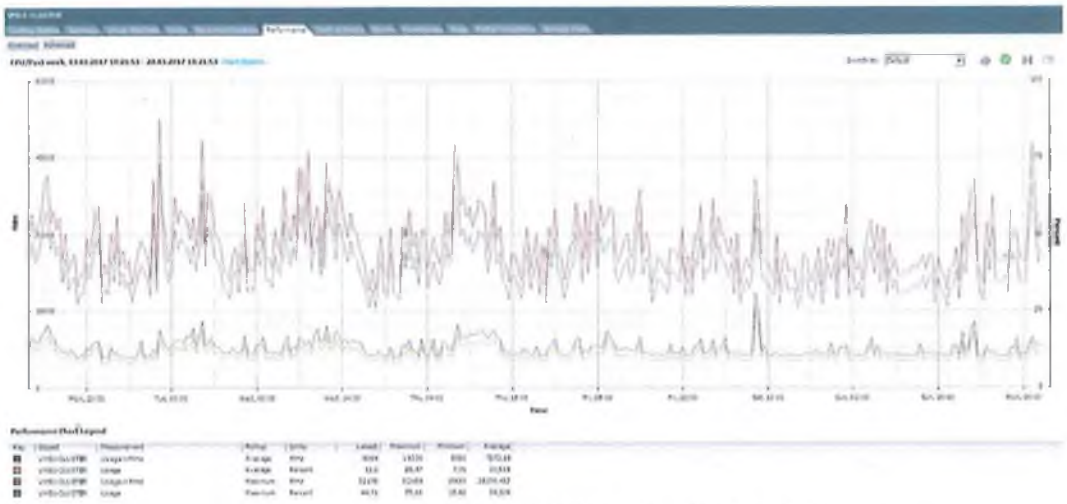
Jedním z hlavních vstupů pro celkový budoucí návrh IT architektury je také budoucí výhled ÚZEI při plánování nasazení nových aplikací případně nárůstu požadované úložné kapacity pro digitální dokumenty. Tyto budoucí požadavky mají přímý dopad na dimenzování HW zdrojů. Navržená architektura by měla být plně flexibilní a rozšiřitelná do budoucna. Budoucí požadavky z pohledu zdrojů se budou týkat zejména těchto oblastí:

- Požadavky na úložiště dat – kapacita, výkonnost, návaznost na zálohování a archivaci
- Požadavky na výpočetní výkon – CPU, RAM, návaznost na režim vysoké dostupnosti
- Požadavky na přenosovou kapacitu – odezva aplikací, návaznost zejména na přenosovou kapacitu směrem do sítě internet anebo na další lokality ÚZEI

Na následujících obrázcích jsou zobrazeny grafy využití CPU a RAM v clusteru (3 servery). Statistiky zobrazují využití zdrojů v jednotlivé dny v týdnu. Monitoring se prováděl týden.

Základní parametry serverů v clusteru jsou následující:

- 3 x 12 CPU x 1,99GHz
- 3 x 128 GB RAM



Obrázek 2 Využití CPU v clusteru ÚZEI

Obrázek 3 Využití RAM v clusteru ÚZEI

V následující tabulce jsou uvedeny informace o maximálním využití CPU a RAM na jednotlivých server v clusteru v období týdenního sledování.

	Max CPU usage:	Max RAM usage:
Host 1	38.05 %	53 %
	9 132 MHz	
Host 2	57.77 %	61 %
	13 864 MHz	
Host 2	86.55 %	66 %
	20 772 MHz	

Tabulka 1 Maximální využití zdroje jednotlivých serverů

V současnosti nelze zcela jednoznačně určit všechny předpokládané budoucí požadavky na výpočetní výkon v ÚZEI. Při dimenzování celé IT architektury na dvojnásobnou aktuální kapacitu bude i tato kapacity dostačující pro budoucí požadavky.

Z pohledu rozvoje ÚZEI očekává zajištění těchto klíčových služeb:

- DMS
- Spisovou službu
- Skenování knih v knihovně s metadaty
- digitální knihovna Kramerius

Kritickým místem je zejména predikování požadavků na diskovou kapacitu:

- Současné nároky jsou 50 TB, včetně alokace 200 GB na centrálním úložišti pro každého ze 170 uživatelů
- Roční přírůstek dat je cca 16 TB
- FADN infrastruktura disponuje kapacitou cca 5 TB

2.1 Východiska pro funkční celky

Následující kapitoly se věnují detailněji jednotlivým funkčním celkům architektury ICT. Vychází z předchozího dokumentu *Návrh architektury ICT prostředí UZEI* verze 2.0 ze dne 12.12.2016. Tyto kapitoly shrnují nejdůležitější body, které je nutné zohlednit v detailním technické návrhu.

2.1.1 Síťová infrastruktura

- Zajištění vysoké dostupnosti HA na L3 prvcích v Datacentru Mánesova. Nahradit nevyhovující 1Gbit propojení těchto prvků na přístupové switche a použít technologii 10Gbit Ethernet.

- Nahrazení stávajícího L2 stacku přístupových switchů za switche s podporou stacku na 10Gbit. Podpora PoE, IPv6, 802.1Q minimálně 4x10Gbit a 48x1Gbit o celkové kapacitě L2 minimálně 384 1Gbit portů a 32 10Gbit portů.

- Integrace infrastrukturních technologií sítě FADN na přístupové switche UZEI. Vyřazení nevyužitých IBM přístupových switchů a zajištění vysoké dostupnosti HA.

- Zřízení zabezpečené bezdrátové sítě s centrálním controllerem pro řízení a plánování celé bezdrátové sítě z jednoho místa, jedním nástrojem. Technologie 2,4GHz a 5GHz 802.11AC. Autentifikace přístupu do produkční sítě přes jednotnou správu identit (RADIUS nebo LDAP/AD). Použití captive portal pro Hostovskou síť oddělenou od produkční sítě. Zajištění monitorování a logování provozu bezdrátové sítě. Aplikace bezpečnostních technologií proti standartním útokům na bezdrátové sítě. (Rogue access point, man in the middle apod.)

- Uskutečnění optického spoje mezi lokalitou Mánesova a Slezská na technologiích T-Mobile a ponechání si záložní bezdrátové propojení na technologii SIKLU. Vyřadit bezdrátový spoj PLUTO.

- Vytvoření plánu na implementaci IPv6 a možnost budoucí realizace nasazení IPv6.

2.1.2 Perimetr s bezpečnost

- Nahrazení stávajících DMZ switchů s technologií Fast Ethernet za Gigabitové switche

- Nutná výměna stávajících nedostačujících UTM Fortigate 100D za výkonnější zařízení. Nasazení bezpečnostních pravidel zejména SSL inspekce.

- Revize firewallových pravidel, přístupů a VPN účtů. Implementace jednotné správy identit (RADIUS Server nebo LDAP) a propojení SSL-VPN a přístupových účtů s Active Directory.

- Revize a nasazení bezpečnostních funkcí a aplikace na firewallová pravidla (antivir, webfiltering, aplikační kontrola, intrusion prevention systém, DoS). Zřízení proxy a SSL inspekce pro šifrovaný provoz HTTPS, FTPS, SMTPS. Nasazení SSL certifikátu pro inspekci šifrovaného provozu.

- Revize zabezpečení emailové komunikace pomocí zařízení (emailové brány) pro zajištění účinné antispamové a antivirové kontroly příchozí a odchozí pošty.

- Realizace řešení proti Zero-Day útokům, Ransomware a dalšího škodlivého mallware v reálném čase na hardwarové platformě.

- Zajištění dlouhodobějšího ukládání logů síťového provozu s možností následné analýzy a výstupního reportingu. Zřízení Vulnerability managementu pro detekci zranitelnosti systému a předcházení bezpečnostním incidentům.

- Zajištění komunikace na protokolu IPv6 současně s IPv4. Nasazení současně pro WAN i pro vnitřní sítě.

2.1.3 Serverová infrastruktura a datové uložiště

- Konsolidace serverové infrastruktury UZEI a FADN na jednu platformu, při zachování požadavku na logické oddělení a nezávislost obou systémů s možností jednoduché migrace na samostatnou platformu v případě vzniku tohoto požadavku. Fyzické oddělení obou systémů je značně neefektivní a neúměrně zvyšuje nároky na záložní zdroje UPS, síťovou a SAN infrastrukturu a administraci.

- Pořízení serverů v zapojení ve vysoké dostupnosti HA jako Hypervizory pro virtualizační platformu (Hyper-V nebo VM-ware). Nahrazující současné 3 vmware hypervisory pro UZEI a 2 vmware hypervizory pro FADN.

- Možné vyřazení 3 VM-ware hostů z infrastruktury UZEI, jednoho standalone serveru FJS siemens spisová služba, 2 vmware hostů z infrastruktury FADN.

- Produkční datové úložiště Storwize V7000 je po 4letém provozu na konci své morální životnosti a prodloužení HW podpory je neefektivní. Datové úložiště je navíc značně poddimenzované a slouží primárně pouze pro serverový provoz a jejich aplikace. Nemá dostatečnou kapacitu na ukládání produkčních uživatelských dat. Ty jsou nechráněná a nezálohovaná na lokálních počítačích uživatelů, popřípadě nevyhovujících NAS zařízeních.

- Zálohovací datové úložiště FiberCAT je již řadu let out of sale i out of support a je osazeno nepodporovanými disky. Samotné pole vykazuje chyby jednoho controlleru a jeho další používání v infrastruktuře je nemyslitelné. Vzhledem k plnění funkce zálohování, doporučujeme nahradit stávající datové úložiště za úložiště s nižšími výkonnostními nároky bez SSD cash a rychlých SAS nebo SSD disky, naopak s vysokou hrubou kapacitou 150TB na levnějších NLSAS nebo SATA discích.

2.1.4 SAN

- Architektura SAN sítě pro zajištění vysoké spolehlivosti používá koncept dvou naprosto nezávislých SAN infrastruktur (SAN fabric A, SAN fabric B). Jednotlivé servery a systémy pro ukládání dat jsou pak připojeny na obě SAN infrastruktury. Každá SAN infrastruktura je tvořena jedním fiber channel přepínačem, který obsahuje min. 48 FC portů s volitelnou rychlostí v rozmezí 4G – 16G a s podporou virtualizačních technologií, které umožňují členit jednu fyzickou SAN infrastrukturu na několik logických – např. technologie VSAN (Virtual SAN) a s podporou technologií NPIV (N-Port Interface Virtualization) umožňujících snadnou a škálovatelnou integraci fyzických a virtualizovaných serverů do SAN infrastruktury

- Konsolidace serverové infrastruktury UZEI a FADN na jednu platformu s sebou přinese i konsolidaci SAN infrastruktury. Ze současných dvou HA řešení na jedno.

- Stávající SAN infrastruktura UZEI, má již nyní dostatečný počet portů a licencí na provoz obou systémů současně. V případě zvolení levnějšího řešení nové SAN infrastruktury na 8Gbit platformě by mohlo být současné řešení, při zajištění HW podpory výrobce, zachováno. V případě upgrade SAN infrastruktury na platformu 16Gbps je nutné pořídit dva SAN switche s podporou 16Gbps.

2.1.5 Záložní zdroje a systém napájení

- Stávající záložní zdroje napájení jsou v havarijním stavu a hrozí bezprostřední nebezpečí ztráty dat, poškození HW. Baterie v záložních zdrojích neprochází pravidelnou údržbou a nejsou ani jinak kontrolovány. Všechny baterie v záložních zdrojích v Datacentra Mánesova jsou bez několikaleté údržby a hrozí tak riziko poruchy záložního zdroje.

- Záložní zdroje nejsou vybaveny síťovým managementem a jsou schopny zajistit napájení infrastruktury, pouze při krátkodobých výpadcích v řádu několika minut. Po vyčerpání kapacity záložních zdrojů, přeruší dodávku elektrické energie do infrastruktury bez ukončení rozpracovaných transakcí, či uložení dat. Nekorektní ukončení běžících systémů může způsobit jejich nevratné poškození, nebo dokonce poškození HW.

- Rozdělení kapacit záložních zdrojů do několika samostatných UPS je neefektivní a ztěžuje tak management řízeného vypínání dle priority systému a velikosti zátěže.

- Absence monitoringu (managementu) těchto zařízení znemožňuje administrátorům rozpoznat, když dojde k výpadku elektrické energie a nemůžou tak ani reagovat na vzniklou situaci případným vzdáleným zásahem neautomatického řízeného vypnutí systémů.

- Běžné managementy záložních napájecích zdrojů zajišťují kromě napájení a automatického řízeného vypínání a zapínání, také monitorování teploty v Datacentru a v závislosti na ni reagovat. Upozorněním administrátora zasláním emailu, nebo opět řízeného vypnutí vybraných technologií, aby nedošlo k jejich poškození. Tato funkce může varovat administrátory před poruchou klimatizace, opomenutí opětovného zapnutí klimatizace při profylaxi a předejít tak poškození HW.

- Doporučujeme pořízení třífázové UPS s management modulem. Instalaci management serveru pro obsluhu. Zařazení všech zařízení pod jednotnou správu do skupin dle priorit a zátěže. Určení identit pro systém včasného varování a správce. Provázání na stávající PRTG monitoring.

- V závislosti na změny v infrastruktuře a vyřazení, nebo naopak pořízení nových aktivních prvků a serverů, doporučeno provést revizi elektrické instalace, PDU a kabeláže.

2.1.6 Systém zálohování

- Současný systém [redacted] je zaměřen na virtuální prostředí s podporou souborové zálohy na pásková média. Pro současný i plánovaný systém je vhodnou volbou z důvodu nízkých provozních nákladů a snadnou administrací. Stejně jako servery UZEI, tak i servery FADN jsou na virtuální platformě je možné tento systém použít i pro zálohování FADN. Není nutné udržovat dva zálohovací systémy a lze tak opustit nákladný IBM Tivoli Storage Manager.

- Plánovaný rozvoj produkčního prostředí a navýšení kapacity produkčního datového úložiště na 100TB z důvodu převedení uživatelských dat na File-Server, vzniknou ekvivalentní nároky na zálohovací systém. Primární zálohovací datové úložiště s kapacitou 150TB na levnějších NLSAS nebo SATA discích a konektivita HBA 2x8Gbps na každý controller je plně vyhovující.

- Naopak další využití datové úložiště FiberCAT je nemyslitelné z důvodu absence podpory, použití nepodporovaných disků, nízkou kapacitou, 4Gbps HBA a častými chyby jednoho controlleru.

- Sekundární datové úložiště pro ukládání kopie záloh a měsíčních záloh je vhodné vytvořit na levnějších zařízeních typu NAS nicméně s dostatečnou hrubou kapacitou 150 TB a 8Gbit FC HBA nebo 10Gbit Ethernet konektivitou. Tato zařízení jsou cenově mnohem dostupnější a vzhledem k využití jako sekundární datové úložiště zcela vyhovující.

- Při konsolidaci infrastruktury FADN a UZEI na jednu platformu, nebude již potřeba druhé páskové knihovny původně ukládající data pro FADN. Pásková knihovna, která je součástí zálohování pro UZEI, slouží pro ukládání dlouhodobých záloh a archivu. Tuto činnost převezme sekundární datové úložiště a obě páskové knihovny bude možné dočasně využít pro offside zálohy. Hrubá kapacita jedné knihovny je 53 TB při použití LTO6 médií, je tudíž nutné použít obě knihovny pro zálohu 100 TB (hrubé kapacity) produkčního prostředí. V případě budoucího dalšího navýšení produkčního datového úložiště doporučujeme již pořídit jednu páskovou knihovnu s dostatečnou kapacitou dle velikosti produkčních dat.

- Doporučujeme zřídit postupy a proškolení odpovědné osoby pro systém zálohování a nakládání s archivními médii a jejich případnou obnovu.

- Doporučujeme zavést systém automatického upozornění do systému dohledu a správy, nejen na samotné HW komponenty systému, ale také na události zálohovacího systému, jako jsou chybová a varovná hlášení systému na různé incidenty (nedokončené zálohovací úlohy, nefunkční úlohy, odebrání médií k archivaci apod.)

- V současné době probíhá zálohování veškeré infrastruktury na datové úložiště FiberCAT, které je z důvodu absence podpory, použití nepodporovaných disků, nízkou kapacitou, 4Gbps HBA a častými chyby jednoho controlleru, velmi rizikovým úložištěm. Proto se pořizují archivní zálohy na pásková média jako sekundární zálohy s RPO 1 měsíc. Převážná většina uživatelských dat je uložena na lokálních discích uživatelů a jsou tudíž úplně bez ochrany. Hrozí tak bezprostřední nebezpečí ztráty dat!

2.1.7 Systémy dohledu a správy

- Systém dohledu a správy je provozován na výrobcem nepodporovaném serveru FJS Primergy RX100 S5. Tento server je již dlouhodobě nevyhovující, a i přes nedávno provedenou profylaxi, kdy byli odstraněny závažné chyby a upgrade operační paměti, je nutné tento server nahradit novým.

- Stávající server je provozovaný na operačním systému Microsoft Windows Server 2008R2 a slouží mimo jiné také jako svědek pro Exchange Cluster. Také míchání rolí je zcela nepřijatelné.

- V současnosti provozovaný monitorovací software PRTG má zakoupenou doživotní licenci Network Monitor 1000. Ta obsahuje 1000 sond, která je pro současnou i budoucí infrastrukturu dostačující. Limitující je absence podpory a nemožnost využívat nejnovější verze a funkcionality.

- Po upgrade software doporučujeme nastavit SNMP trap a sběr syslog zpráv, který v současné verzi není plně podporován.

- V současné době je monitorovací systém funkční a používán na detekci incidentů v síti a infrastruktuře. Výhodou je vzdálený monitoring a reporting na mobilní zařízení, spolehlivost, dobrá uživatelská přístupnost a ovládání. Doporučujeme zachovat stávající software a dokoupit podpory výrobce.

Příloha č. 3

Předávací – akceptační protokol – vzor

ÚZEI | ÚSTAV ZEMĚDĚLSKÉ EKONOMIKY A INFORMACÍ

Číslo úkolu ÚZEI

PŘEDÁVACÍ – AKCEPTAČNÍ PROTOKOL

PRODÁVAJÍCÍ:	**KUPUJÍCÍ:**
XANADU a.s. sídlo: Žirovnická 2389, 106 00 Praha 10 IČO: 14498138 zástupce prodávajícího pověřený k předání:	**Ústav zemědělské ekonomiky a informací** sídlo: Mánesova 1453/75, 120 00 Praha 2 IČO: 00027251 zástupce kupujícího pověřený k převzetí:

Číslo smlouvy kupujícího	**Datum uzavření smlouvy**
/2017	

Předmětem akceptačního řízení je ověření plnění Smlouvy

Datum předání:

Závěr akceptačního řízení: (variantu závěru označte křížkem):

☐ ***akceptováno bez výhrad***

☐ ***akceptováno částečně, s výhradami***

☐ ***neakceptováno, k přepracování***

☐ ***neakceptováno s následným odstoupením od smlouvy***

Seznam nedostatků/vad:

Pořadové číslo	Popis nedostatku/vady	Poznámka
1		
2		
3		

Termín pro odstranění nedostatků/vad, v případě akceptace se závěrem „akceptováno částečně s výhradami" či „neakceptováno k přepracování": do .

Tento protokol byl vyhotoven ve třech stejnopisech, z nichž kupující obdrží dva a prodávající jeden.

Akceptační řízení skončeno dne .

podpis zástupce prodávajícího

podpis zástupce kupujícího

Příloha č. 4:

Seznam poddodavatelů

Seznam poddodavatelů

Veřejná zakázka

„Obnova serverovny UZEI"

Plnění veřejné zakázky uvedené výše bude plněno prostřednictvím poddodavatelů ~~**ANO**~~ – **NE**
(nehodící se škrtněte)

Pokud bude plněno prostřednictvím poddodavatelů uveďte seznam poddodavatelů do následující tabulky:

Název subjektu, sídlo, IČO	Definice části plnění, kterou dodavatel bude plnit prostřednictvím poddodavatele	% podíl na plnění	Uvedení, zda tímto poddodavatelem je prokazována kvalifikace