7807/18

Kraj Vysočina

121018

KRAJSKÝ ÚŘAD KRAJE Vysočina

Název dokumentu:	Kupní smlouva - Monitoring výkonu aplikací				
Oprávněn/pověřen k podpisu:	MUDr. Jiří Běhounek				
Schváleno:	RK	**Datum:**	14.8.2018	**Č.usnesení:**	1437/22/2018/RK
Dokument uložen u:	OddPKŽÚ				
Počet vyhotovení:	2				
Adresát:	OptoNet Communication, spol. s r.o.				
Smluvní částka: 1)	1942563.04				
Odpovědný odbor: 2)	odbor informatiky				
Podpis zajistit do:	3.10.2018				

		Pracoviště/pracovník	Datum	Podpis
Zpracoval:		OI/T. Mrázková	1.10.2018	
Projednáno s:				
Právní kontrola:		OAPŘ/V. Kotrbová	1.10.2018	
Předkládá:		OI/P. Pavlinec	1.10.2018	
Potvrzení příjmu smlouvy do předběžné evidence 3)		OI/P. Pavlinec	1.10.2018	
Zodpovídá:	**Příkazce operace:**	OI/P. Pavlinec	1.10.2018	
	Správce rozpočtu:	OI/D. Rudiková	1.10.2018	

Poznámka:
Subjekt (IČO: 27750132), se kterým je uzavírána smlouva NENÍ nespolehlivým plátcem dle § 109 od. 3 zákona o DPH; (ověření provedl: mrazkova.t, datum ověření: 26.09.2018 14:50:24):

Kupní smlouva - Monitoring výkonu aplikací

připraveno Projektovou kanceláří

Rozpočtová skladba:
Částka s DPH: 1942563.04, Datum Od: 1.10.2018, Datum do: , Perioda: jednorázově, ODPA: 003636, ORJ: 0000001600, ORG: 0001882000000 POL: 6111 UZ:

1) Použije se, pokud se jedná o písemnost typu smlouvy, jejímž předmětem je peněžité plnění. Pokud je v košilce více smluv, uvede se částka souhrnná. Pokud se jedná o smlouvu, příp. smlouvy, u niž je peněžité plnění stanoveno částkou za čerpanou jednotku (např. hodinovou sazbu), uvede se částka maximálního rozsahu tohoto plnění. V případě smluv na dobu neurčitou uveďte částku jedné platby.

2) Odpovědným odborem se rozumí odbor, příp. sekce nebo samostatné oddělení, které za písemnost, její vyřízení a správu záležitosti (správu smluvního vztahu) odpovídá.

3) Potvrzuje vždy vedoucí odpovědného odboru (nenahrazuje právní kontrolu).

7807/18

SMLOUVA O DODÁVCE PRODUKTŮ

dle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ") a § 131 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZzVZ")

Kraj Vysočina
Sídlo: Žižkova 1882/57, Jihlava, PSČ 587 33
Zastoupený hejtmanem MUDr. Jiřím Běhounkem
IČO: 70890749 DIČ: CZ70890749
Tel: 564 602 111 Fax: 564 602 420
E-mail: posta@kr-vysocina.cz ID datové schránky: ksab3eu
Kontaktní osoba objednatele ve věcech technických dle této Smlouvy je: Ing. Petr Pavlinec, e-mail: pavlinec.p@kr-vysocina.cz, tel.: 564 602 114
(dále jen „**Kupující**")

a

Prodávajícím: **OptoNet Communication, spol. s r.o.**
Sídlo: Červený Kříž 250, Jihlava 586 01
Zapsaná v OR vedeném u Krajského soudu v Brně oddíl C, vložka 56527
Zastoupen: Jiřím Šteflem, jednatelem společnosti
Bankovní spojení: Komerční banka a.s.
č. účtu: 107-1864410247/0100
IČO: 27750132 DIČ: CZ27750132
Tel: 564 040 100 E-mail: info@optonet.cz
ID datové schránky: aamtqr

dále jen „**Prodávající**"; Prodávající nebo jeden z Prodávajících společně s Kupujícím také jen „**Smluvní strany**"

uzavřeli níže uvedeného dne, měsíce a roku tuto Smlouvu o dodávce produktů (dále jen „**Smlouva**")

1. Preambule

1.1. Smluvní strany uzavírají tuto Smlouvu jako výsledek zadávacího řízení veřejné zakázky **„Technologické centrum Kraje Vysočina 2016 – infrastruktura 2"** (dále jen „zadávací řízení"), **část 3 Aplikační monitoring**;

1.2. Předmět plnění této Smlouvy hodlá zadavatel financovat mimo jiné z prostředků dotace z Integrovaného regionálního operačního programu a dalších strukturálních fondů Evropské unie.

1.3. Účelem této Smlouvy je zajištění dodávek dále specifikovaných produktů včetně dopravy a instalace do místa převzetí pro potřeby Kupujícího po dobu trvání Smlouvy.

2. Předmět Smlouvy

2.1. Předmětem této Smlouvy je stanovení podmínek pro dodávky produktů (dále jen „**Věci**“) Prodávajícím Kupujícímu dle přílohy č. 2 Smlouvy.

2.2. Věci budou dodávány za podmínek specifikovaných Smlouvou a jejími přílohami.

2.3. Prodávající odpovídá za to, že odevzdané Věci odpovídají technickým podmínkám, specifikovaným v příloze č. 1 Smlouvy, jsou nové (tzn. nikoliv dříve použité) a jsou vhodné k využití k účelu dle této Smlouvy a obvyklému využití dané Věci.

2.4. Závazek Prodávajícího odevzdat Věci zahrnuje i:

2.4.1 dopravu Věcí na místo jejich odevzdání.

2.4.2 předání dokladů, které jsou nutné k užívání Věcí, zejména návodů k použití a provozní dokumentace v českém nebo anglickém jazyce, které se k Věcem jinak vztahují. Věci budou Prodávajícím odevzdány s veškerou originální dokumentací, příslušenstvím a licenčními dokumenty, pokud takové existují, tedy ve formě standardně poskytované výrobcem. Prodávající je povinen Kupujícímu s Věcmi odevzdat také návod/návody v českém nebo anglickém jazyce, jsou-li nutné pro používání Věcí.

2.4.3 instalační práce a služby v souvislosti s dodáním Věcí sestávající z:

a) kompletace Věcí v místě plnění;
b) instalace Věcí do prostoru připraveného Kupujícím;
c) instalaci veškerých nezbytných programů a aplikací;
d) uvedení Věcí do provozu;
e) provedení akceptačních testů dle přílohy č. 1 Smlouvy;
f) základní zaškolení pracovníků Kupujícího, týkající se Věcí, v místě plnění.

(dále jen „**Instalace**“).

2.4.4 odvoz a ekologická likvidace veškerých obalů, nebude-li Kupujícím stanoveno jinak;

2.4.5 veškeré ostatní činnosti a práce nutné k realizaci plnění dle a v souladu s touto Smlouvou;

2.5. Prodávající potvrzuje, že se při vynaložení veškeré odborné péče seznámil s rozsahem a povahou předmětu plnění dle Smlouvy, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci této Smlouvy, jakož i veškeré další okolnosti a skutečnosti mající vliv na plnění Smlouvy, jakož i na sjednanou výši kupní ceny, a že je považuje za jednoznačné a vyčerpávající a tedy dostatečné k plnění Smlouvy. Současně prohlašuje, že disponuje takovými kapacitami a odbornými znalostmi, které jsou k řádnému a bezvadnému plnění této Smlouvy nezbytné.

3 Čas a místo plnění

3.1. Věci dle této Smlouvy dodá a instaluje do šesti měsíců ode dne účinnosti této Smlouvy. Kupující příjme i dřívější plnění.

3.2. Konkrétní den a hodinu odevzdání Věcí a provedení Instalace je Prodávající povinen avizovat nejméně dva pracovní dny předem e-mailem kontaktní osobě Kupujícího. Nesplní-li Prodávající tuto povinnost, není Kupující povinen neavizovanou dodávku převzít (není v takovém případě v prodlení s převzetím Věcí). Kupující není povinen převzít částečné plnění (pokud Prodávající dodá ze souboru Věcí jen část) a není v takovém případě v prodlení s převzetím Věcí.

3.3. Věci dle Smlouvy budou Prodávajícím odevzdány a Instalovány v sídle či budovách ve vlastnictví Kupujícího nebo budovách Nemocnice Jihlava, příspěvková organizace, Vrchlického 59, 586 33 Jihlava a záložní lokalitě – budově ve vlastnictví Kupujícího nebo jeho příspěvkové organizace.

3.4. Po dodání a Instalaci dle Smlouvy bude před převzetím Věcí provedeno akceptační řízení; lhůta dle článku 3.1 Smlouvy je splněna okamžikem úspěšného akceptačního řízení dle čl. 6.4.3 až 6.4.8 Smlouvy.

4 Dodání a převzetí, akceptační řízení

4.1. Prodávající se zavazuje předat Věci splňující požadavky dle Smlouvy, tj. po dodání a dokončení kompletní Instalace, Kupujícímu nejpozději v termínu dle čl. 3.1. Smlouvy. Konečnému převzetí Věcí Kupujícím bude předcházet akceptační řízení popsané níže v tomto článku.

4.2. Prodávající je povinen vyzvat Kupujícího k zahájení akceptačního řízení, a to s dostatečným předstihem tak, aby Věci Kupujícím dodal, instaloval a akceptační řízení bylo dokončeno v termínu dle čl. 3.1 této Smlouvy.

4.3. Akceptační řízení je proces ověřující, zda Věci dodané Prodávajícím splňuje požadavky Kupujícího dle Smlouvy a jejích součástí, a to prostřednictvím ověření:

4.3.1. zda Věc nebo jeho část odpovídá schváleným funkčním a technickým specifikacím a všem Kupujícím požadovaným parametrům (kvantitativní, kvalitativní, výkonnostní, provozní a bezpečnostní) dle technické specifikace, která tvoří přílohu č. 1 Smlouvy a akceptačním testům dle přílohy č. 1 Smlouvy;

4.3.2. zda byla v požadovaném rozsahu a kvalitě provedena kompletní Instalace, včetně ostatních činností a prací potřebných pro řádné plnění Smlouvy.

4.4. Kupující provede za podpory Prodávajícího ověření funkčnosti jednotlivých vlastností, které jsou požadovány v technické specifikaci, která tvoří přílohu č. 1 Smlouvy.

4.5. V případě prokazatelných nedostatků je Prodávající povinen je odstranit, a to nejpozději do 3 kalendářních dnů ode dne realizace akceptačního řízení, nestanovil-li Kupující Prodávajícímu lhůtu delší.

4.6. Prodávající je povinen účastnit se akceptačního řízení a zavazuje se poskytnout Kupujícímu a jím určeným osobám v průběhu akceptačního řízení veškerou podporu a součinnost pro úspěšné provedení akceptačního řízení.

4.7. Převzetí Věcí Kupujícím je možné pouze na základě akceptačního řízení s výsledkem „Akceptováno" nebo „Akceptováno s výhradou" (uvedeném v předávacím protokolu). Prodávající pro předání Věcí a jeho převzetí Kupujícím zpracuje písemný protokol o předání a převzetí Věcí, který bude detailním výčtem všech položek, které jsou Kupujícímu předávány. Výsledek řízení akceptováno s výhradou je možný v případě, že Věci vykazují vady, které nebrání užívání věci. V případě výsledku akceptačního řízení s výhradou připojí Kupující k protokolu o předání a převzetí Věcí soupis vad s lhůtou jejich odstranění, přičemž Prodávající odstraní vady do 5 pracovních dnů, neurčí-li Kupující v protokolu o předání a převzetí Věcí lhůtu delší.

4.8. Při předání Věcí předá Prodávající Kupujícímu i veškerou dokumentaci, dále potvrzení, osvědčení či jiné doklady a dokumenty, které se k Věci či jeho části vztahují a jež jsou obvyklé, nutné či vhodné k převzetí a k využití takového plnění. Veškeré výše uvedené dokumenty budou v českém jazyce, nedohodnou-li se Smluvní strany jinak, vyjma návodu/návodů, které mohou být v anglickém jazyce, jsou-li nutné pro používání Věcí. Okamžikem jejich předání Kupujícímu se stávají jeho výlučným vlastnictvím.

4.9. Vlastnické právo k Věcem, které jsou předmětem Smlouvy, jakož i nebezpečí vzniku škody na Věci přechází na Kupujícího jejím převzetím na základě akceptačního řízení.

5 Kupní cena

5.1. Kupní cena je jako součet cen za dodání jednotlivých Věcí dle přílohy č. 2 Smlouvy. Prodávající je oprávněn ke kupní ceně připočíst DPH ve výši stanovené v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, (dále jen „ZDPH"), a to ke dni uskutečnění zdanitelného plnění (dále jen „DUZP"). DUZP je den převzetí Věci.

5.2. V případě, že se Prodávající stane plátcem DPH v průběhu trvání Smlouvy, platí, že ceny jím uvedené příloze č. 2 Smlouvy jsou cenami konečnými včetně DPH ve výši stanovené v souladu s ZDPH ke dni uskutečnění zdanitelného plnění.

5.3. Kupní cena je stanovena jako nejvýše přípustná a jsou v ní zahrnuty veškeré náklady Prodávajícího spojené s plněním povinností vyplývajících ze Smlouvy včetně (nikoliv výlučně) dopravy a Instalace.

5.4. Nebude-li Smluvními stranami sjednáno jinak, neodpovídá Kupující za jakékoliv náklady Prodávajícího na plnění předmětu dle Smlouvy přesahující částku dle ustanovení čl. 5.1 Smlouvy. Náklady na plnění předmětu Smlouvy přesahující uvedenou částku nese Prodávající.

5.5. Prodávající na sebe převzal v souladu s ustanovením § 1765 OZ nebezpečí změny okolností, přičemž před uzavřením Smlouvy plně zvážil hospodářskou, ekonomickou i faktickou situaci a je si plně vědom okolností Smlouvy, jakož i okolností, které mohou po uzavření Smlouvy nastat. Smlouvu nelze měnit rozhodnutím soudu v jakékoliv její části.

6 Platební podmínky

6.1. Úhrada kupní ceny bude uskutečněna na základě daňového dokladu vystaveného Prodávajícím nejpozději do 14 dnů po převzetí Věcí Kupujícím. Podmínkou pro vznik oprávnění vystavit daňový doklad za poskytnutí plnění dle Smlouvy je podpis předávacího protokolu, kterému předcházelo ukončení akceptačního řízení s výsledkem „Akceptováno" nebo „Akceptováno s výhradou".

6.2. Daňový doklad vystavený Prodávajícím je splatný do 30 kalendářních dnů od jeho doručení Kupujícímu.

6.3. Bankovní účet uvedený Prodávajícím na jím vystaveném daňovém dokladu za účelem úhrady kupní ceny musí odpovídat bankovnímu účtu zveřejněnému dle ustanovení § 98 ZDPH příslušným správcem daně způsobem umožňujícím dálkový přístup. V opačném případě je Kupující vystavený daňový doklad za podmínek dle ustanovení odst. 5 tohoto článku Kupujícímu vrátit. Pokud se po dobu účinnosti této Smlouvy Prodávající stane nespolehlivým plátcem ve smyslu ustanovení § 106a zákona o DPH, smluvní strany se dohodly, že Kupující uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Kupujícím takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované Prodávajícím.

6.4. Součástí daňového dokladu musí být soupis skutečně dodaných Věcí a jejich detailní specifikace, zejm. rozsah a cena skutečně provedených dodávek v členění dle specifikace s uvedením položky, jednotkové ceny, množství a výsledné ceny za příslušnou položku, uskutečněných Prodávajícím a potvrzených Kupujícím.

6.5. Daňový doklad Prodávajícího musí být vystaven v souladu s požadavky právních předpisů na daňové doklady. Daňový doklad platí jako došlý v den, kdy byl v originále s přílohami prokazatelně doručen Kupujícímu. Kupující je oprávněn vrátit daňový doklad do 14 kalendářních dnů od doručení s písemným odůvodněním, neodpovídá-li Smlouvě či obecně platným právním předpisům, nebo není-li možné jej zkontrolovat. Byl-li daňový doklad takto vrácen, není Kupující v prodlení s placením kupní ceny. Splatnost je určena podle ustanovení odst. 1 tohoto článku, přičemž lhůta splatnosti se počítá ode dne doručení opraveného daňového dokladu Kupujícímu. Není-li daňový doklad ve lhůtě 14 kalendářních dnů vrácen, platí, že s ním Kupující souhlasí.

6.6. Daňový doklad bude obsahovat název a číslo projektu „Služby Technologického centra Kraje Vysočina 2016", reg. č. CZ.06.3.05/0.0/0.0/16_044/0002837.

7 Poddodavatelé

7.1. Poddodavatelem se rozumí každá osoba, jejímž prostřednictvím Prodávající plní určitou část předmětu Smlouvy a je odlišná od Prodávajícího.

7.2. Smluvní strany výslovně sjednávají, že okruh poddodavatelů Prodávajícího, jejichž prostřednictvím prokázali v rámci zadávacího řízení část kvalifikace, a jejichž seznam tvoří přílohu č. 3 Smlouvy, je možné měnit pouze se souhlasem Kupujícího, přičemž Prodávající je povinen před provedením změny takového poddodavatele prokázat splnění kvalifikačních předpokladů v odpovídajícím rozsahu rovněž u osoby nového poddodavatele.

7.3. Plnění poddodavatelů se pro účely Smlouvy, zejména vzhledem k odpovědnosti za vady plnění poskytnutých poddodavateli, považuje za plnění Prodávajícího.

8 Právo užití Věci

8.1. Bude-li součástí předmětu Smlouvy jakýkoliv standardizovaný software zhotovovaný Prodávajícím či třetí osobou, jenž nemá povahu díla vytvořeného na objednávku ve smyslu ustanovení § 61 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, je Prodávající povinen zajistit, aby Zadavatel nabyl veškerá oprávnění z práv duševního vlastnictví, která se týkají takového autorského díla a která jsou nezbytná k jeho užívání Kupujícím při provozování Věci, a k jejímu řádnému užívání a zachování její funkčnosti, a to po celou dobu trvání příslušných práv (například formou nevýhradní licence poskytované třetí stranou, či podlicence) (dále jen „**Licence**").

8.2. Prodávající výslovně prohlašuje, že nositelům práv ke standardizovaným software dle předchozího ustanovení nepřísluší a nebude přísluší vůči Kupujícímu žádné právo na odměnu, či jakékoliv jiné plnění v souvislosti s užitím Věci nebo jeho částí.

8.3. Prodávající je povinen Kupujícímu uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že Kupující nemohl standardizovaný software užívat řádně a nerušeně v důsledku autorskoprávních a/nebo jiných nároků vznesených třetí osobou.

8.4. Prodávající odškodní Kupujícího a právně ho na své náklady ochrání před veškerými nároky, požadavky, škodami, ztrátami a jinými náklady v případě oprávněných požadavků vznesených třetími stranami, které vzniknou z činnosti Prodávajícího při plnění ze Smlouvy, nebo jsou z této činnosti odvoditelné, včetně nároků vyplývajících

z autorského práva a jiného práva duševního vlastnictví. Toto ustanovení se aplikuje rovněž na případy, kdy by byl Kupující vyzván příslušným správcem daně k úhradám z titulu ručení příjemce zdanitelného plnění ve smyslu ustanovení § 109 ZDPH.

9 Vady Věci a záruka za jakost

9.1. Prodávající poskytuje na Věci komplexní záruku za jakost, tj. záruku, že si dodané Věci udrží takové vlastnosti, že budou plně způsobilé pro užívání k účelu dle Smlouvy (zejména technické specifikace), že veškeré dodané Věci, včetně technologie, technického vybavení a materiálu, včetně veškerého software, mají a udrží si vlastnosti (zejména garantované parametry) stanovené Smlouvou, v platných právních předpisech a v příslušných platných normách, a že dodávka a Instalace Věcí byly provedeny v souladu se Smlouvou, platnými právními předpisy, příslušnými platnými normami, a že si tuto jakost udrží.

9.2. Prodávající poskytuje záruku za jakost podle předchozího odstavce v rozsahu záruční doby 60 měsíců.

9.3. Záruční doba začíná běžet okamžikem protokolárního předání a převzetí Věci Kupujícím. V případě částečného předání a převzetí Věci začne běh záruční doby vztahující se k dotčené části dodávaných Věcí okamžikem částečného předání a převzetí dané konkrétní části Věcí, pokud je toto vzhledem k předávané části možné.

9.4. V případě výskytu či vzniku vady Věcí, problému, poruchy či incidentu (dále společně jen „**Incident**") je Kupující povinen ohlásit tento Incident bez zbytečného odkladu na kontaktní telefonní nebo e-mailový kontakt hotline 561 201 555, hotline@optonet.cz a servicedesk, který je umístěn na webových stránkách www.optonet.cz, a nebo kontaktní osobě uvedené ve Smlouvě. Prodávající je povinen přijímat oznámení v pracovní dny od 8:00 do 17:00 hod. Prodávající bezodkladně potvrdí ohlášení Incidentu elektronickou poštou na adresu, ze které oznámení obdrží, nebo kterou mu Kupující telefonicky či e-mailem sdělí.

9.5. Kupujícímu vzniká nárok na odstranění Incidentu okamžikem ohlášení jeho výskytu.

9.6. Reklamovanou vadu resp. Incident je Prodávající povinen odstranit bezodkladně, nejpozději však do 3 pracovních dnů ode dne ohlášení Incidentu. V případě nedodržení této lhůty je Prodávající povinen do následujícího pracovního dne poskytnout Kupujícímu náhradní Věc stejných vlastností. Zapůjčí-li Prodávající náhradní Věc, není v prodlení s odstraněním vad, resp. Incidentu, sankce za prodlení s termínem odstranění vad, resp. Incidentu se neuplatní.

9.7. Prodávající se zavazuje poskytovat Kupujícímu při odstraňování vad veškerou potřebnou součinnost tak, aby byly řádně a včas odstraněny. Nebude-li mezi Prodávajícím a Kupujícím dohodnuto jinak, pak je Prodávající povinen zejména:

9.7.1 Věc, jejíž vada má být odstraněna opravou mimo místo Instalace, převzít k opravě v místě, Instalace, a po provedení opravy opravenou Věc opět v tomto místě Instalovat a předat Kupujícímu, a

9.7.2 v případě odstranění vady dodáním nové Věci dodat a Instalovat novou Věc na totéž místo, kde byla Kupujícímu odevzdána nahrazovaná Věc.

9.8. Prodávající bez zbytečného odkladu informuje Kupujícího o odstranění Incidentu. Zadavatel neprodleně zkontroluje funkčnost zařízení, jehož se odstranění Incidentu týkalo, a potvrdí ji (akceptuje) Prodávajícímu.

9.9. Záruční doba vadného plnění neběží od okamžiku, kdy se konkrétní Incident objevil, až do okamžiku potvrzení (akceptace) odstranění Incidentu Kupujícím Prodávajícímu, jak uvedeno v předchozím odstavci.

9.10. I v případech, kdy Prodávající reklamaci vady Věci neuzná, je povinen vadu Věci, resp. Incident odstranit na náklady kupujícího, na jejichž výši se Prodávající s Kupujícím dohodnou.

9.11. V případě, že Prodávající odmítne Incident vyřešit, je Kupující oprávněn, po předchozím oznámení Prodávajícímu, tento Incident odstranit na své náklady. Náklady vynaložené na odstranění vad Věci, resp. vyřešení Incidentu představují splatnou pohledávku Kupujícího za Prodávajícím. Prodávající je povinen Kupujícímu uhradit náklady vynaložené na odstranění vady Věci, resp. vyřešení Incidentu, a to do 21 kalendářních dnů ode dne jejich písemného uplatnění u Prodávajícího, a to veškeré náklady uplatněné Kupujícím, maximálně však do výše hodnoty 90 % celkové ceny vyplývající ze Smlouvy. V případech, kdy ze záručních podmínek vyplývá, že záruční opravy může provádět pouze autorizovaná osoba a neautorizovaný zásah je spojen se ztrátou práv vyplývajících ze záruky, je Kupující oprávněn postupovat podle předchozí věty pouze v případě, že odstranění vady Věci, resp. vyřešení Incidentu provede autorizovaná osoba. Ustanovení tohoto Odstavce se přiměřeně použijí i na vady provádění a na jiné vady v plnění povinností Prodávajícího podle Smlouvy.

9.12. Bude-li Prodávající v prodlení s odstraněním vady Věci, resp. vyřešením Incidentu ohlášeného Kupujícím dle tohoto článku, je Kupující oprávněn, po předchozím oznámení Prodávajícímu, odstranit vadu, resp. vyřešit Incident sám na náklady Prodávajícího, který je povinen je Kupujícímu na jeho výzvu uhradit.

10 Bezpečnost informací

10.1 Prodávající je povinen dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.

10.2 Prodávající se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv kupujícího uvedené v příloze č. 4 této smlouvy.

10.3 Prodávající je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech poddodavatelů či jiných osob, které mají přístup k informačním aktivům Kraje Vysočina prostřednictvím prodávajícího.

10.4 Prodávající je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi prodávající seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění prodávajícího veřejně přístupnými stanou (dále jen „důvěrné informace"). Prodávající nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch kupujícího. Povinnosti dle tohoto odstavce je prodávající povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění prodávajícího. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je prodávající povinen zveřejnit důvěrnou informaci na základě povinnosti uložené prodávajícímu právním předpisem nebo rozhodnutím orgánu veřejné moci.

11 Sankční ujednání

11.1. Prodávající je povinen na výzvu Kupujícího zaplatit Smluvní pokuty, které jsou sjednány pro případ následujících porušení povinností Prodávajícího sjednaných Smlouvou:

11.1.1. V případě, že Prodávající nepředá Kupujícímu Věci splňující požadavky uvedené ve Smlouvě včetně Instalace a Akceptačního řízení dle čl. 4 ve sjednaném termínu dle ustanovení čl. 3.1 Smlouvy, je Kupující oprávněn uplatnit a Prodávající je povinen zaplatit Smluvní pokutu ve výši 0,05 % z kupní ceny dle ustanovení čl. 5.1 Smlouvy za každý započatý den prodlení;

11.1.2. V případě, že v důsledku porušení této Smlouvy ze strany Prodávajícího dojde k nedodržení dotačních podmínek programu, z něhož bude čerpána dotace na financování předmětu Smlouvy, které bude mít za následek krácení či neproplacení dotace, je Kupující oprávněn uplatnit a Prodávající povinen uhradit Smluvní pokutu ve výši částky, o kterou bude dotace snížena; tato Smluvní pokuta je limitována částkou ve výši 90% kupní ceny dle ustanovení čl. 5.1 Smlouvy. V případě, že se bude jednat o porušení Smlouvy, za které již Prodávající Kupujícímu uhradil Smluvní pokutu dle čl. 11.1.4 Smlouvy, bude Smluvní pokuta dle toho článku Smlouvy snížena o již uhrazené takové Smluvní pokuty;

11.1.3. V případě, že v důsledku porušení této Smlouvy ze strany Prodávajícího bude Kupujícímu uložena sankce za porušení rozpočtové kázně, je Kupující oprávněn uplatnit a Prodávající povinen uhradit Smluvní pokutu ve výši rovnající se částce odvodu za porušení rozpočtové kázně spolu s penále, jež bude Kupující povinen uhradit; tato Smluvní pokuta je limitována částkou ve výši 90% kupní ceny dle ustanovení čl. 5.1 Smlouvy. V případě, že se bude jednat o porušení Smlouvy, za které již Prodávající Kupujícímu uhradil Smluvní pokutu dle čl. 11.1.4 Smlouvy, bude Smluvní pokuta dle toho článku Smlouvy snížena o již uhrazené takové Smluvní pokuty;

11.1.4. V případě, že Prodávající poruší povinnosti stanovené v ustanoveních čl. 4.5, 4.7, 7.2, 9.6, 9.11, 9.12, 14.13.1 Smlouvy, je Kupující oprávněn uplatnit a Prodávající povinen uhradit Smluvní pokutu ve výši 0,05 % z kupní ceny dle ustanovení čl. 5.1 Smlouvy za každý započatý den prodlení, a to ve vztahu ke každému jednotlivému porušení zvlášť;

11.1.5. V případě, že Prodávající opakovaně porušuje kteroukoliv svou Smluvní povinnost (včetně Smluvních povinností, pro které jsou sjednány zvláštní Smluvní pokuty), u níž byl již v průběhu plnění ze Smlouvy na její porušování opakovaně písemně upozorněn, z toho nejméně jednou s výslovným poukazem na možnost uložení Smluvní pokuty podle tohoto ustanovení Smlouvy, je Kupující oprávněn uplatnit a Prodávající povinen zaplatit Smluvní pokutu ve výši až do 5 % z kupní ceny dle ustanovení čl. 5.1 Smlouvy za každý takový případ porušování Smluvní povinnosti, přičemž konkrétní výši příslušné Smluvní pokuty stanoví Kupující v písemném upozornění na možnost uložení Smluvní pokuty podle závažnosti postihovaného porušení Smluvní povinnosti.

11.2. Smluvní pokuty dle tohoto článku jsou splatné do 15 kalendářních dnů od doručení písemné výzvy Kupujícího Prodávajícímu. Zaplacením Smluvní pokuty nezaniká příslušný nárok Kupujícího na splnění povinnosti Smluvní pokutou zajištěné. Smluvní pokuty se nezapočítávají na nárok na náhradu škody. Kupující je oprávněn

4

jednostranně započíst pohledávku na zaplacení jakékoli Smluvní pokuty dle Smlouvy na jakoukoli pohledávku Prodávajícího vůči Kupujícímu dle této Smlouvy.

11.3. V případě prodlení Kupujícího se zaplacením faktury vystavené Prodávajícím v souladu s článkem 6.2 Smlouvy je Prodávající oprávněn požadovat na Kupujícím Smluvní pokutu ve výši 0,05% z nezaplacené částky, a to za každý i započatý den prodlení.

11.4. Zaplacení Smluvní pokuty nemá vliv na právo Smluvních stran domáhat se náhrady škody vzniklé porušením Smluvní povinnosti nebo povinnosti vyplývající z obecně závazného právního předpisu. Škoda způsobená Kupujícímu poddodavatelem Prodávajícího se považuje za škodu způsobenou přímo Prodávajícím.

11.5. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

11.6. Prodávající se nedostává do prodlení v případě prodlení Kupujícího s poskytnutím nutné součinnosti Prodávajícímu (např. prodlení s umožněním přístupu do prostor Kupujícího).

12 Odstoupení a předčasné ukončení Smlouvy

12.1. Kupující je oprávněn od Smlouvy odstoupit, pokud Prodávající naplní některý z následujících důvodů tím, že:

a) je proti němu zahájeno insolvenční řízení;

b) vstoupí do likvidace;

c) je v prodlení s předáním Věcí Kupujícímu podle Smlouvy, a to o více než 30 kalendářních dnů;

d) oznámil Kupujícímu, že nesplní své povinnosti ze Smlouvy řádně a včas;

e) ve své nabídce podané v rámci zadávacího řízení uvedl nepravdivé, mylné či zkreslené informace;

f)podstatně porušil své povinnosti podle Smlouvy a uvedené nenapravil porušení své povinnosti ani v dodatečné lhůtě stanovené v písemné výzvě zaslané či osobně předané Kupujícím (dodatečná lhůta bude činit nejméně 5 pracovních dnů ode dne doručení/předání výzvy);

g) přes písemnou výzvu k nápravě s poskytnutím dodatečné lhůty, která činí nejméně 5 pracovních dnů, opakovaně neplní nebo porušuje jinou povinnost danou mu Smlouvou.

12.2. Prodávající je oprávněn odstoupit od Smlouvy, pokud Kupující je v prodlení s úhradou některé z plateb dle Smlouvy o více než 60 kalendářních dnů.

12.3. Účinky odstoupení od Smlouvy nastanou okamžikem doručení písemného projevu vůle vyjadřujícího odstoupení od Smlouvy druhé Smluvní straně.

12.4. Do 30 kalendářních dnů od ukončení Smluvního vztahu podle Smlouvy jinak než splněním Kupující určí a potvrdí:

a) na jakou finanční částku případně vznikl Prodávajícímu nárok ke dni ukončení Smluvního vztahu podle Smlouvy;

b) hodnotu nepoužitého nebo částečně použitého materiálu, technického vybavení či Věcí, které Kupující zamýšlí od Prodávajícího odkoupit.

12.5. Poté, co nabude účinnosti právní jednání, jímž dojde k ukončení Smlouvy, Prodávající neprodleně:

a) přestane provádět veškeré činnosti související s plněním Smlouvy kromě těch, k nimž dal Kupující pokyn; stanovuje se, že náklady na takové činnosti uskutečněné na pokyn Kupujícího Smluvní strany ponese Kupující;
b) předá Kupujícímu příslušnou dokumentaci a dosud dodané Věci, nebo jejich část, za něž obdržel nebo má obdržet úhradu příslušné části kupní ceny.

13 Ostatní ustanovení

13.1. Prodávající je povinen archivovat do konce roku 2028 veškerou dokumentaci související s plněním ze Smlouvy včetně účetních dokladů a kdykoli po tuto dobu umožnit Kupujícímu na jeho výzvu přístup k této dokumentaci.
13.2. Prodávající je povinen minimálně do konce roku 2028 poskytovat požadované informace a dokumentaci související s plněním Smlouvy zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
13.3. Prodávající se zavazuje poskytnout Kupujícímu písemně jakékoliv informace související s realizací Smlouvy, a to v rozsahu a termínu stanoveném v písemné žádosti Kupujícího.
13.4. Prodávající je oprávněn převést svoje práva a povinnosti z této Smlouvy na třetí osobu pouze s předchozím písemným souhlasem Kupujícího; § 1879 OZ se nepoužije.

14 Závěrečná ustanovení

14.1. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem uveřejnění v informačním systému veřejné správy - Registru Smluv.
14.2. Vzhledem k veřejnoprávnímu charakteru Kupujícího Prodávající výslovně prohlašují, že jsou s touto skutečností obeznámeni a souhlasí se zveřejněním Smlouvy v registru Smluv, a dále v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ZzVZ.
14.3. Prodávající výslovně souhlasí se zveřejněním celého textu této Smlouvy včetně podpisů v informačním systému veřejné správy - Registru Smluv. Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona o registru Smluv splní Kupující. Současně bere Prodávající na vědomí, že tím není dotčeno ustanovení § 3 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých Smluv, uveřejňování těchto Smluv a o registru Smluv (zákon o registru Smluv). V případě nesplnění zákonné povinnosti je Smlouva do tří měsíců od jejího podpisu bez dalšího zrušena od samého počátku.
14.4. Smlouva může být měněna pouze formou písemných očíslovaných dodatků podepsaných oprávněnými zástupci Smluvních stran.
14.5. Smluvní strany výslovně sjednávají, že e-mail nebo jiná obdobná forma elektronické komunikace se nepovažují za písemný dodatek ke Smlouvě.
14.6. Situace neupravené Smlouvou se řídí OZ a dalšími obecně závaznými právními předpisy České republiky.
14.7. Vůle Smluvních stran je vyjádřena též v dále uvedených dokumentech a podkladech, které tvoří nedílnou součást této Smlouvy:

a) Příloha č. 1 Smlouvy: Technická specifikace ze zadávací dokumentace a akceptační testy
b) Příloha č. 2 Smlouvy: položkový rozpočet z nabídky Prodávajícího
c) Příloha č. 3 Smlouvy: seznam poddodavatelů, jejichž pomocí Prodávající prokázal v nabídkách část kvalifikačních předpokladů
d) Příloha č. 4 Smlouvy: Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv

14.8. Jestliže se některé ustanovení Smlouvy, nebo jeho část ukáže jako zdánlivé, neplatné, neúčinné nebo nevymahatelné, nebude tím dotčena platnost ani účinnost Smlouvy jako celku ani jejích zbývajících ustanovení, nebo jejich částí. V takovém případě Smluvní strany změní nebo přizpůsobí takové zdánlivé, neplatné, neúčinné nebo nevymahatelné ustanovení písemnou formou tak, aby bylo dosaženo úpravy, která odpovídá účelu a úmyslu stran v době uzavření Smlouvy, která je hospodářsky nejbližší zdánlivému, neplatnému, neúčinnému nebo nevymahatelnému ustanovení, popřípadě podniknou jakékoliv další právní kroky vedoucí k realizaci původního účelu takového ustanovení.

14.9. Smluvní strany výslovně vylučují použití ustanovení § 582 odst. 2 občanského zákoníku.

14.10. Uzavření této Smlouvy bylo v souladu s ustanovením § 59 odst. 3 zákona č. 129/2000 Sb., o krajích (krajské zřízení), v platném znění rozhodnuto usnesením č. 1437/22/2018/RK Radou Kraje Vysočina na jednání č. 22/2018 konaném dne 14.8.2018.

14.11. Smluvní strany prohlašují, že Smlouva byla uzavřena podle jejich pravé a svobodné vůle, vážně a srozumitelně, nikoli v tísni a za nápadně nevýhodných podmínek, a že souhlasí s jejím obsahem, což stvrzují svými podpisy.

14.12. Smlouva je zhotovena ve dvou stejnopisech. Každá ze smluvních stran obdrží po jednom řádně podepsaném stejnopise.

V Jihlavě dne 4.10.2018

Kraj Vysočina
MUDr. Jiří Běhounek, hejtman kraje

Kraj Vysočina
Žižkova 57, 587 33 Jihlava
27

V Jihlavě dne 20.9.2018

OptoNet Communication, spol. s r.o.
Jiří Štefl, jednatel společnosti

OptoNet Optical Network
Dipl. Ing. Jiří Štefl
Jednatel/CEO
spol. s r.o.
OptoNet,
Červený Kříž 250, 588 02 JIHLAVA
tel.: +420 564 040 106, fax: +420 564 040 134
www.optonet.cz, optonet@optonet.cz

Příloha č. 2 – Technická specifikace

Obecný úvod

Technologické centrum Kraje Vysočina (dále jen TCK) bude provozováno ve dvou provozních lokalitách v Jihlavě umístěných v budově Krajského úřadu Kraje Vysočina (Žižkova 57) a v Nemocnici Jihlava (Vrchlického 59) a jedné záložní (adresa bude upřesněna před instalací).

Popis stávající (dostupné) vybavenosti a propojení lokalit TCK:

1. Společné pro obě lokality TCK (uvedeno pro jednu lokalitu TCK) :
   - Datové rozvaděče o velikosti 2200x800x800 19" s nosností 800kg
   - Maximální prostor pro instalaci komponent v datových skříních - v každé lokalitě 80U
   - Napájení jednofázové 230V, lišty s napájecími koncovkami C13, UPS
2. Využitelné (k dispozici) optické propojení mezi lokalitami Nemocnice Jihlava a Krajský úřad:
   - Vzdálenost lokalit 3km
   - 8 kusů SM šedých vláken 9/125um (využití pro Fibrechannel i Ethernet – předpokládá se použití technologií xWDM/WDM, dodávka xWDM MUX/DEMUX součástí zakázky
3. Využitelné optické propojení mezi provozními lokalitami TCK a záložní lokalitou:
   - Vzdálenost lokalit 5km
   - 2 kusy SM vláken 9/125um (využití pro Fibrechannel i Ethernet – předpokládá se použití technologií xWDM/WDM, dodávka xWDM MUX/DEMUX součástí zakázky)

Popis stávající (dostupné) vybavenosti záložní lokality:

1) 2 datové rozvaděče o velikosti 2200x800x800 s nosností 800kg
2) Napájení jednofázové 230V, lišty s napájecími koncovkami C13, UPS

Další stávající (dostupné) vybavení TCK:
Zadavatel nyní provozuje datové centrum, ze kterého je možné využít následující licence (nikoliv hardware) pro případný upgrade:

a. 2ks FalconStor NSS server verze 7.0, unlimited storage **(HW nutno dodat v rámci této části části zakázky)** s licencí na neomezenou diskovou kapacitu v této verzi
b. HP IMC Branch Intelligent Management System Software Module with 100-node

Na všechny uvedené produkty je platná smlouva o podpoře (zaplacen maintenance).

Zadavatel dále poskytne pro instalaci následující licence:

a. 18ks Windows server 2016 datacenter 16core
b. 18ks VMWARE vSPHERE ESX Enterprise plus v aktuální verzi
c. 1ks VMWARE vCENTRE Standard (možné použít i stávající instalaci) v aktuální verzi
d. 18ks VMWARE NSX Enterprise edition v aktuální verzi
e. VMWARE LogInside – licence pro 50 zařízení

Požadované rozmístění technologie v rámci dodávky:

1. **Lokalita Nemocnice Jihlava**
   - 7ks serverů pro virtualizaci
   - 2ks FC switchů
   - 4ks Ethernet switchů pro datový provoz
   - 1ks Ethernet switchů pro managementový provoz
   - 1ks diskového pole
   - 1 node diskové virtualizace
   - 1 node Web-aplikačního firewallu (samostatná část vz.)

2. **Lokalita Krajský úřad:**
   - 7ks serverů pro virtualizaci
   - 2ks FC switchů
   - 4ks Ethernet switchů pro datový provoz
   - 1ks Ethernet switchů pro managementový provoz
   - 1ks diskového pole
   - 1 node diskové virtualizace
   - 1 node Web-aplikačního firewallu (samostatná část vz.)

3. ***Záložní lokalita:***
   - Archivační úložiště – ODA
   - 1ks ethernet switch pro mgmt provoz
   - 1ks FC switch

Následující seznam požadavků zadavatele přesně vymezuje technické a množstevní parametry pro plnění jednotlivých komodit veřejné zakázky z pohledu jejich minimálních parametrů.

U položek s předpokládaným dodáním více kusů se jejich popis týká parametrů pro jeden kus.

Požadované minimální technické parametry musí nabízené řešení závazně splňovat v rámci nabídky nebo formou softwarového upgradu a to nejpozději do okamžiku plnění kupní smlouvy.

Součástí dodávky je u všech částí zakázky:

- zpracování prováděcího projektu, včetně detailní analýzy celého řešení a vypracování detailního harmonogramu nasazení
- návrh a nasazení funkcí a procesů vhodných pro použití pro datové centrum o velikosti 400+ virtuálních serverů
- doprava a dodávka na místo instalace včetně nezbytného příslušenství (např. kabeláže, zářiče apod.) pro propojení všech komponent (s výjimkou SM vláken mezi lokalitami)
- instalace a konfigurace všech potřebných komponent do stavu, ve kterém bude možné provést akceptační testy
- instalace produktů VMWARE vSPHERE ESX, VMWARE NSX (licence poskytne zadavatel) včetně konfigurace (cluster, sítě, storage apod.)
- úspěšné provedení akceptačních testů
- zpracování dokumentace finálního vyhotovení, která musí minimálně obsahovat oblasti uvedené v příloze č. 3 zadávací dokumentace. Pro část č. 1 minimálně v rozsahu kapitol 2, 5, 6, 7, 8, 10, 12, 13 a 15 a pro část č. 2 a 3 v rozsahu všech kapitol.
- provedení školení pro uživatele systému a základního školení pro administrátory systému (ukázka přístupů, řízení a základní mgmt k dodaným technologiím) v rozsahu 2 pracovních dnů
- migrace konfigurací a datových struktur (RAW disky a VMDK soubory)

stávajícího TCK u všech relevantních prvků (LAN, přepojení interface fyzického firewallu, SAN, disková i serverová virtualizace) v rozsahu uvedeném v akceptačních testech. Kompletní migrace stávajícího TCK není požadována.

- Při využití licenčního modelu formou cross-update je požadováno zajištění souběžného provozu stávající a nové infrastruktury po dobu 6 měsíců od akceptace díla

Technické požadavky části č. 1 - Serverová a síťová infrastruktura

1. ESX HW (Servery)

1.1. Servery pro virtualizaci aplikací v počtu 12ks

a) Provedení: rack 19", výška max. 2U, plnovýsuvné ližiny včetně ramena pro vedení kabeláže
b) CPU architektura x86 s 12 plnohodnotnými jádry, taktovací frekvence min. 2,6 GHz, FSB min. 2666 MHz, min. 19 MB L cache celkem nebo architektura, která v testu http://spec.org/cpu2006/results/cint2006.html pro daný typ serveru dosahuje "Results Base" min. 71 (v tomto případě je maximální počet jader omezen na 16 z důvodu licenční politiky produktu MS Windows Server 2016 datacenter, FSB min. 2666MHz)
c) 1CPU osazeno a jeden volný slot na dodatečnou instalaci dalšího CPU
d) RAM 384 GB, DDR4-2666, ECC
e) Min. 2x LAN 10/100/1000 1000BASE-T
f) Min. 2x 10Gbps SFP+ porty včetně 2ks MM zářičů
g) Min. 4x 25Gbps SFP28 porty včetně 4ks MM zářičů, podpora RDMA
h) Diskový řadič s podporou HBA (pass-throught), RAID-1, RAID-5 zálohovaný, vytvoření 3 RAID skupin, velikost cache min. 2GB, rychlost 12Gbit/s
i) Diskový prostor pro instalaci VMWARE ESX, v režimu vysoké dostupnosti o min. velikosti 16GB (technologie SD nebo SSD)
j) Express Flash NVMe PCIe SSD, velikost 1.6TB, latency do 100us, nasazení jako vFlash read cache
k) Server musí být osaditelný min. 14x 2,5-palcovými disky v libovolné kombinaci disků (rotační i SSD) SAS, Near Line SAS, SATA zároveň – veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již nyní osazeny tak, aby server bylo možné funkčně osadit plným počtem min. 14 HDD pouhým dodatečným vložením disků
l) 1 ks karet Fibre Channel adapter (dual port), min. 16Gbps
m) 2 ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, účinnost min. 94%
n) IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
o) Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
p) Kompatibilita všech komponent s VMWARE ESX 6.5 a vyšší dle https://www.vmware.com/resources/compatibility/search.php

1.2. Servery pro virtualizaci databází v počtu 2ks

a) Provedení: rack 19", výška max. 2U, plnovýsuvné ližiny včetně ramena pro vedení kabeláže
b) CPU architektura x86 s 6 plnohodnotnými jádry, taktovací frekvence min. 3,4 GHz, FSB min. 2666 MHz, min. 19 MB L cache celkem nebo architektura která v testu http://spec.org/cpu2006/results/cint2006.html pro daný typ serveru dosahuje hodnoty "Results Base" min. 71 (v tomto případě je maximální počet

jader omezen na 8 z důvodu licenční politiky produktu MS SQL Server, FSB min. 2666MHz)

c) 1CPU osazeno a jeden volný slot na dodatečnou instalaci dalšího CPU
d) RAM 384 GB, DDR4-2666, ECC
e) Min. 2x LAN 10/100/1000 1000BASE-T
f) Min. 2x 10Gbps SFP+ porty včetně 2ks MM zářičů
g) Min. 4x 25Gbps SFP28 porty včetně 4ks MM zářičů HW akcelarace
h) Diskový řadič s podporou HBA (pass-throught), RAID-1, RAID-5 zálohovaný, vytvoření 3 RAID skupin, velikost cache min. 2GB, rychlost 12Gbit/s
i) Diskový prostor pro instalaci VMWARE ESX, v režimu vysoké dostupnosti o min. velikosti 16GB (technologie SD nebo SSD)
j) Express Flash NVMe PCIe SSD, velikost 1.6TB, latency do 100us, nasazení jako vFlash read cache
k) Server musí být osaditelný min. 14x 2,5-palcovými disky v libovolné kombinaci disků (rotační i SSD) SAS, Near Line SAS, SATA zároveň – veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již nyní osazeny tak, aby server bylo možné funkčně osadit plným počtem min. 14 HDD pouhým dodatečným vložením disků
l) 1 ks karet Fibre Channel adapter (dual port), min. 16Gbps
m) 2 ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, účinnost min. 94%
n) IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
o) Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
p) Kompatibilita všech komponent s VMWARE ESX 6.5 a vyšší dle https://www.vmware.com/resources/compatibility/search.php

Procesory nabídnuté v bodech 1.1 a 1.2 budou od stejného výrobce a kompatibilní pro funkci VMWARE vMOTION.

2. SSD diskové pole (kapacita 70TB) v počtu 2ks, specifikace pro 1ks:

a) Box o velikosti max. 6U se dvěma hot-swap redundantními aktivními řadiči (při výpadku musí být zachován minimálně 75 % výkon pole), plně odolný proti výpadku klíčových komponent (no single point of failure), cache, paměti, ventilátorů, napájecích zdrojů.
b) Čistá kapacita úložiště bez deduplikace a komprese prezentována VMWARE ESX 70TB SSD se zabezpečením proti výpadku jednoho disku. Pro každý opotřebený či vadný disk (flash médium) je požadována jeho bezplatná záruční výměna (viz kupní smlouva).
c) Výměna vyjímatelných komponent a přidávání (výměna) disků za chodu, on-line firmware upgrade na řadičích i discích, on-line přidávání dalších diskových polic, odolnost proti výpadku jedné police (kruhování)
d) Možnost rozšíření kapacity o 70TB SSD se zabezpečením proti výpadku jednoho disku (formou doplnění police nebo instalací dalších disků do stávajícího chassis)
e) Každý řadič bude obsahovat nejméně 4 porty Fibre Channel 16Gbps pro připojení k SAN infrastruktuře a minimálně 64GB CACHE. Nedojde ke ztrátě žádných dat (včetně dat v cache) při výpadku el. napájení (min. po dobu 48 hodin).
f) Pole bude plně virtualizováno s možností určení redundance uložených dat
g) Správa prostřednictvím grafického rozhraní (GUI), i příkazové řádky (CLI). Podpora SNMP v2c pro vzdálený monitoring.
h) Management plugin do prostředí VMWARE vSPHERE, dodávka včetně instalace a licence.

i) Dodávka řešení pro získání informací o aktuálním zatížení (počet IO) a latencí na jednotlivých skupinách disků a LUNs s historií 1 rok, vyčítání do externího systému přes standardizované rozhraní (možno řešit přes SNMP).
j) Mód přístupu klientů VMWARE ESX na storage LUNs asymetrický ACTIVE – ACTIVE (ALUA) a to i pro Thin Provisioning.
k) Pole vnitřně virtualizováno pro celkové usnadnění administrace a efektivní zacházení s výkonovými a kapacitními rezervami tj. na stejných fyzických discích musí být možné vytvářet logické disky s různými RAID geometriemi.
l) Podpora Thin Provisioning s automatickou reklamací uvolněného prostoru do poolu přístupného všem serverům pro celou nabízenou kapacitu.
m) Prostředky pro vytváření plných klonů a ReadOnly a ReadWrite snapshotů z logických disků.
n) Deduplikace dat na blokové části diskového pole.
o) Funkcionalitu QoS (omezení výkonu na úrovni pole v IOPs nebo MB/s) pro jednotlivé LUNy nebo skupiny LUNů.
p) Funkcionalita vVOL pro VMWARE vSphere
q) Kompatibilita s VMware vSphere 6.5 dle kompatibility listu https://www.vmware.com/resources/compatibility/search.php?deviceCategory=san
r) Kompatibilita providerů pole s VMware vSphere 6.5 API – dle kompatibility listů https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vasa a https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vvols
s) Plná podpora VMware VAAI - při připojení k prostředí VMware vSphere 6.5 bude diskové pole podporovat všechny aktuálně dostupná VAAI primitiva pro bloková zařízení včetně „thin provisioning primitives".
t) Obsažené licence v rámci dodávky (na plnou dodanou diskovou kapacitu):
    a. licence pro Migraci LUN a konverze typu RAID apod.
    b. licence pro multi-path v módu active-active
    c. potřebné licence pro integraci s VMware a to včetně managementu
    d. potřebné licence vyplývající z požadavku na funkcionalitu uvedenou výše

Požadované funkcionality musí být nabídnuty pro neomezený počet připojených serverů a plně pokrývat dodávanou kapacitu.

Pole budou dodána a nakonfigurována tak, aby umožňovala vzájemnou synchronní replikaci určených svazků a v případě výpadku jednoho z polí, druhé automaticky převezme veškerý datový provoz s výpadkem komunikace ke klientům maximálně 20s. Dále musí pole podporovat rollback scénáře (uvedení do stavu před poruchou) bez výpadku komunikace ke klientům (režim metrocluster).

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

3. ARCHIVAČNÍ ULOŽIŠTĚ (1KS) – ODA

Z důvodu kompatibility se stávajícím řešením pro dlouhodobou archivaci dat (aktuálně realizováno na HW SONY ODA, jednotka ODS-D77U, média ODC1500R) je poptáváno řešení podporující tuto technologii uložení dat. Konkrétně knihovna podporující již používaná média s možností souběžné práce dvou a více R/W jednotek, zásobníku min 30ti médií s robotickou obsluhou a možností pořízení expanze až na 90 médií a 6ti jednotek (typově 1ks ODS-L30M).

Součástí dodávky bude i zapojení celého řešení do FC infrastruktury (min 1 interface) a vzorová konfigurace zálohovacího serveru (HW zapojený do FC infrastruktury dodá zadavatel).

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

4. **Veeam (ZÁLOHOVACÍ SOFTWARE) –Veeam Backup and Replication Enterprise for VMWare - 3 ks licencí (3xCPU)**

Dodávka licencí zálohovací software – bez dalších požadavků (včetně dokumentace)

5. **VIRTUALIZACE DISKOVÁ - HW cluster (HW+SW)**

Virtualizace diskových systémů bude provozována ve dvou datových centrech. Požadavkem je design řešení funkční i v případě výpadku jedné lokality.

a) Předmětem poptávky je řešení diskové virtualizace v hardware provedení, rozdělené mezi dvě lokality vzájemně propojené na bázi FC se synchronním zrcadlením dat mezi oběma lokalitami v režimu vysoké dostupnosti (možno i active-pasive konfigurace)
b) latence při provozu nižší než 0,4ms při 50% vytížení deklarované max. kapacity dle výrobce (v IOPs), vhodné pro nasazení pro virtualizaci datového prostoru SSD polí
c) V případě výpadku jednoho z uzlů řešení nebo jedné datové kopie musí být zachování provozu pro provozované servery a aplikace plně transparentní, tj. provozované servery a aplikace nesmí zaznamenat výpadek (bez zásahu obsluhy).
d) Celkové řešení musí poskytnout min. 4x Fibre Channel 16 Gb/s a 8x iSCSI 10 Gb/s porty dedikované pro připojení diskových svazků serverům
e) Celkové řešení musí poskytnout min. 4x Fibre Channel 16 Gb/s porty dedikované pro připojení diskových polí.
f) Řešení musí umožnit snadné rozšíření počtu FC portů prostřednictvím instalace dodatečných FC HBA.
g) Řešení musí umožnit snadné rozšíření iSCSI konektivity prostřednictvím instalace dodatečných 25 Gb/s Ethernet adaptérů do existujícího řešení.
h) Součástí diskové virtualizace bude dodávka a implementace veškerého HW související s během tohoto řešení (HW appliance, FC komponenty apod.)
i) Jednotná administrátorská konzola pro konfiguraci všech instancí řešení, virtuálních LUNů a operací nad nimi s možností definice různých administrátorských oprávnění a rolí pro tyto virtuální LUNy.
j) Součástí jednotné administrátorské konzole musí být nástroje pro plánování frekvence vytváření snapshotů nad jednotlivými virtuálními svazky.
k) Jako externí diskové systémy mohou být použity obvyklé diskové systémy s jedním nebo dvěma RAID řadiči s Fibre Channel nebo iSCSI rozhraním.
l) Řešení musí umožnit virtualizace diskových polí s konektivitou Fibre Channel.
m) Řešení musí umožnit virtualizaci diskových polí s konektivitou iSCSI bez nutnosti implementace dodatečného hardware.
n) Požadavky na služby nad jednotlivými virtuálními svazky:
    - Možnost vytváření až 255 snapshotů nad jedním svazkem.
    - Podpora vytváření konzistentních snapshotů
    - Možnost vytváření klonů.
    - Možnost zpřístupnění vytvořených snapshotů serverům prostřednictvím FC a iSCSI.
    - Možnost rollbacku dat diskového svazku z existujícího snapshotu
    - Synchronní zrcadlení svazků prezentovaných serverům na primárním úložišti v úložišti sekundárním s podporou rozdílové resynchronizace po výpadky jedné instance.
    - Asynchronní replikace svazků prostřednictvím TCP/IP do vzdálených lokalit
        - Podpora komprimace a šifrování dat při asynchronní replikaci.

- Podpora kontinuální (continuous) a periodické delta (pouze změny) replikace.
- Asynchronní replikace dat mezi dvěma systémy v režimu M:N, tzn. jeden virtualizační celek musí umožnit replikaci na více jiných celků a stejně tak musí být připraven přijímat data z více jiných celků.
- Periodická replikace musí umožnit přenos dat garantovaně aplikačně konzistentních dat mezi dvěma systémy v časových periodách, které se dají volitelně nastavit.
- Na vzdálené straně replikace musí systém udržovat replikované garantované aplikačně konzistentní snapshoty.

o) Požadovaný systém musí jednoduchým způsobem umožnit integraci se systémy zálohování dat pro provádění záloh z konzistentních snapshotů bez účasti aplikačních serverů a to bez nutnosti dodatečného skriptování – součástí dodávky musí být aplikace včetně GUI umožňující snadnou konfiguraci zálohování ze snapshotů.
p) Jednoduchá migrace LUNů prezentovaných serverům z úložiště na úložiště bez odstávky běžící aplikace
q) Licence pro neomezenou virtualizovanou diskovou kapacitu a všechny storage funkce, resp. pro celkovou kapacitu 300TB v případě, že neomezená kapacitní licence není k dispozici.
r) Licence pro neomezený počet modulů pro zajištění konzistentních snapshotů. V případě, že jsou moduly licencovány na kapacitu, pak licence na neomezenou kapacitu.
s) Licence na veškeré výše popsané služby nad virtuálními svazky na neomezenou kapacitu, resp. kapacitu 300TB bez omezení počtu klientských serverů
t) Podpora Thin Provisioning
u) Podpora akcelerace operací čtení/zápis – automatizovaný přesun nejčastěji využívaných diskových bloků na vyšší Tier, zpravidla Tier 0, bez nutnosti zásahu administrátora.
v) Certifikace pro serverovou virtualizaci - https://www.vmware.com/resources/compatibility/search.php?deviceCategory=san
w) Kompatibilita s polem IBM DS 5100, HUAWEI OceanStor 5500v3
x) Dodávka SW na měření IOPs a latencí per LUN (požadovány pro všechny nakonfigurované LUNy) včetně historizace po dobu 1 roku s vizualizací výstupů a s definicí prahových hodnot pro alertizaci per LUN

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

6. SAN infrastruktura (FC přepínače)

6.1. Vyžadován je plně redundantní design SAN v obou provozních lokalitách datového centra. Požadavky na SAN:

a) 4x FC switch (2ks do každé lokality), každý min. 24 aktivních portů (zalicencovány)
b) Rychlost FC portů 16Gb/s včetně připojení zařízení o rychlosti 4 a 8Gb/s
c) Licence Full fabric a ISL trunking (sdružování portů)
d) Součástí dodávky budou SFP moduly do FC switchů:
   - moduly na propojení mezi lokalitami technologického centra s využitím ISL trunking včetně potřebných optických propojovacích kabelů, celková kapacita spoje pro jeden fabric 32Gb/s (předpokládá se xWDM)
   - moduly na propojení mezi lokalitami technologického centra a záložní lokality, celková kapacita spoje 16Gb/s (předpokládá se xWDM)
   - moduly na připojení zařízení včetně propojovacích kabelů (MM)
   - zbylé porty osazeny MM zářiči bez dodávky propojovacích kabelů

6.2. Požadavky na SAN switch v záložní lokalitě:

a) 1x FC switch, min. 8 aktivních portů (zalicencovány)
b) Rychlost FC portů 16Gb/s včetně připojení zařízení o rychlosti 8Gb/s
c) Licence Full fabric a ISL trunking (sdružování portů)
d) Součástí dodávky budou SFP moduly do FC switchů:
   - moduly na propojení mezi lokalitami technologického centra a záložní lokality (SM), celková kapacita spoje 16Gb/s (předpokládá se xWDM)
   - moduly na připojení zařízení včetně propojovacích kabelů (MM)
   - zbylé zalicencované porty osazeny MM zářiči bez dodávky propojovacích kabelů

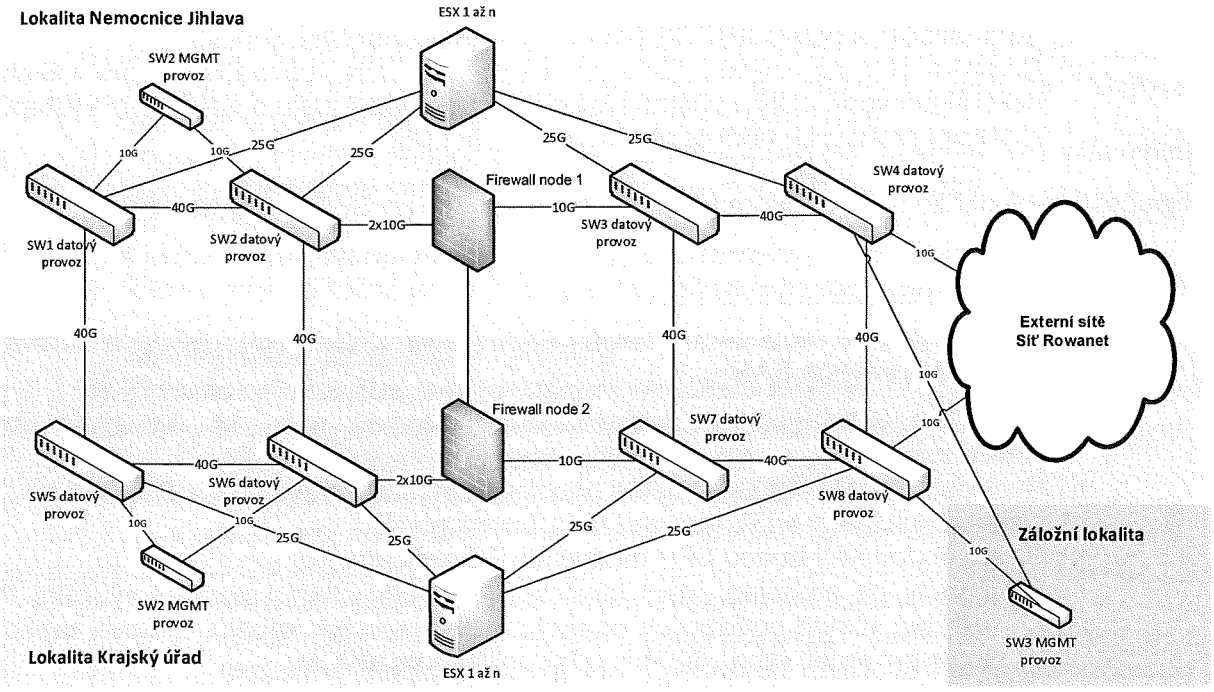
V případě nedostatku vláken, viz.kapitola „Popis stávající vybavenosti a propojení lokalit" je nutné pro realizaci spojů zajistit další vlákna, popř. xWDM řešení na straně dodavatele (musí být součástí nabídky).

7. Ethernet infrastruktura

Vyžadován je redundantní design sítě:

- pro připojení serverů
- pro propojení lokalit technologického centra
- pro směrování packetů (routingu)
- připojení k síti ROWANet (www.rowanet.cz)
- Zachování dostupnosti provozovaných služeb při upgrade firmware
- V případě nedostatku vláken, viz.kapitola „Popis stávající vybavenosti a propojení lokalit" je nutné pro realizaci spojů zajistit další vlákna, popř. xWDM řešení na straně dodavatele (musí být součástí nabídky)

Návrh topologie:



Navrhovanou topologii sítě je možné upravit, avšak musí být splněny všechny požadavky uvedené v zadávací dokumentaci, tj. rychlosti spojení, dostupnost.

Všechna propojení budou v režimu active, tj. nebudou uzavřeny pro komunikaci protokolem řešícím zálohování infrastruktury (např. spanning tree).
Splnění požadavků na kapacitu propojení může být řešeno i logickým sdružením linek (např. LACP protokol). Připojení každého ze serverů pro provoz serverové virtualizace bude realizováno na rychlostech 4x25Gbit/s.

Ethernetové switche musí být plnohodnotně začlenitelné do managementu a monitoringu. Optické zářiče budou poskytovat údaje o výkonových úrovních optické linky (DMI monitoring).

7.1. Přepínače pro datový provoz

Síťová infrastruktura musí být aplikačně propojena s řízením serverové virtualizace a konfigurována z něj přes API (pro aplikační propojení může být použit SW na správu síťové infrastruktury, který bude API obsahovat), tj. synchronizace VLAN mezi řízením hypervizorů a síťovou infrastrukturou, tj. vytvoření VLANy se provede jednou ve VMware vCENTRE pomocí port group v distribuovaném switchi a síťové prvky tuto VLAN automaticky převezmou (VLAN-ID a jméno podle port group).

Dále požadujeme budoucí možnost splnění požadavků na chování jako softwarově definovaná síť s nasazením overlay vrstvy (provoz přes VXLAN) pro zajištění L2 propojení technologického centra s externími datovými a výpočetními zdroji, tj. doplnění těchto funkcí pouze nákupem licence v rámci budoucího rozvoje.

Požadujeme dodávku celkem 8ks switchů, minimální konfigurace jednoho boxu:

a) Výška max 2U, rackmount 19"
b) AC redundantní napájecí zdroje, hotswap
c) Redundantní ventilátory, hotswap, určení směru proudění vzduchu (bude upřesněno při plánu instalace)
d) Interfaces potřebné pro propojení poptávaných komponent. Po osazení poptávaných komponent zůstane pro budoucí využití volných 10 portů o rychlosti 10/25Gb SFP+/SFP28
e) Data Center Bridging - DCBx Data Center Bridging Exchange Protocol, Priority Flow Control (PFC), Enhanced Transmission Selection (ETS)
f) 4096 VLAN
g) Velikost Mac adress tabulky 96 000 záznamů
h) Velikost routovací tabulky 96 000 záznamů IPv4
i) Dual stack IPv4 a IPv6
j) Statické směrování, dynamické směrování (BGP, OSPF) protokolu IPv4 a IPv6
k) IPv4 ALCs, IPv6 ACLs
l) Policy routing na základě ACL, IP prefix, as path
m) VRF s minimálně 16 instancemi při zapnutém dynamickém routingu
n) Směrování multicast provozu, IGMP
o) Protokol VRRP, použití v rámci VRF instancí
p) Protokol ECMP
q) 12MB packet buffer per box
r) Všechna dodávaná zařízení propojena přes optické zářiče, potřebné optické zářiče pro zapojení součástí dodávky
s) Možnost použití OEM, SFP+ a SFP28 modulů (budoucím využití ze strany zadavatele)
t) jumbo rámce min. 9216B
u) MLAG – sdružení 8 linek přes 2 switche
v) LACP (802.3ad) při použití MLAG i přes více boxů
w) Radius klient – možnost přihlašování na mgmt s ověřením na Radius server včetně definice úrovně přístupu (user, administrator)
x) Management – konzolový port, ssh, snmpv3

y) download/upload konfigurace v textovém tvaru
z) SNMPv3 trap, SYSLOG, SNTP klient, RMON
aa) Funkcionalita na sběr informací o tocích např. sFLOW

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

7.2. Ethernet přepínače pro managementový provoz

Dodávaná technologie obsahuje ethernetová řídící rozhraní, která nelze připojit na linky o rychlosti vyšší než 1Gb/s. Z tohoto důvodu požadujeme dodávku 3ks switchů s následující specifikací:

a) Rackmount 19"
b) 24 portů RJ45 10/100/1000
c) 4 porty SFP+ / SFP
d) Switching capacity 100 Gbps
e) Troughput 90 Mpps
f) Packet buffer min. 0,5 Mb/port nebo 1,5 MB/box
g) Velikost MAC address table min. 16000 záznamů
h) Plná podpora IPv4/IPv6 (adresace pro MGMT switche IPv4 i IPv6,...)
i) Jumbo frames větší než 9000 B
j) Management – serial konzole, SSH, SNMPv1,2,3
k) SNMPv3 trap, SYSLOG, RMON
l) NTP klient
m) IGMP, IGMP snooping
n) Plná implementace 802.1q – 4096 VLAN, určení nativní a management VLAN
o) Implementace LACP podle 802.3ad –minimálně 4 nezávislé skupiny po 4 fyzických portech
p) Implementace QoS – minimálně 8 HW fronty
q) RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator)
r) MSTP, RSTP, STP root guard, ST BPDU guard
s) omezení počtu broadcastů na koncových portech – broadcast Storm control
t) download/upload konfigurace v textovém tvaru
u) archivování min. dvou verzí konfigurací a firmware přímo v zařízení
v) DHCP snooping, IPv6 MLD snooping
w) ARP inspection nebo obdobná funkcionalita dle výrobce
x) DoS prevention nebo obdobná funkcionalita dle výrobce
y) IP ACL na mgmt user interface

8. MANAGEMENT A MONITORING

Zadavatel požaduje implementovat systémy pro management a monitoring SSD pole, serverové virtualizace, diskové virtualizace, ethernetové sítě.

Zadavatel nyní využívá pro monitoring stávající infrastruktury software Mikrotik DUDE verze 3.6 (https://mikrotik.com/thedude) a software ZABBIX verze 3.2.7 (www.zabbix.com). Součástí dodávky řešení je zakreslení dodaných komponent do zvoleného monitorovacího SW včetně nastavení alertingu dostupnosti, stavových hodnot a prahových výkonových hodnot jednotlivých zařízení a logických celků.

SW pro vzdálený MGMT a automatizaci ethernetové sítě

Součástí dodávky bude SW pro vzdálený management dodaných ethernetových switchů, který bude splňovat min. tyto požadavky:

a) centralizování informací z jednotlivých zařízení
b) Nastavení minimálně těchto parametrů prvků:
    a. VLAN (vytvoření, přiřazení portů...)
    b. Fyzický interface (up/down, rychlost, duplex...)
    c. NTP server
    d. Spanning tree
    e. Link aggregation
c) Správa úloh pro konfiguraci:
    a. Periodické zálohy konfigurací
d) Hromadný upgrade FW
e) Přímý přístup ke vzdálenému managementu zařízení z jedné konzole
f) Použití minimálně těchto nástrojů:
    a. Ping
    b. Ping IPv6
    c. Tracert
g) Monitoring výkonu a zátěže jednotlivých zařízení.
h) Statistiky a alerting:
    a. Stav fyzických portů včetně chybovosti a zatížení, Stav vytížení CPU a operační paměti, stav fyzického HW
    b. statistiky, reporting s retencí minimálně 90 dní, automatické odesílání definovaných reportů e-mailem
    c. alerting administrátora (zaslání informace o změně stavu systému emailem – stavové alerty)
i) Integrace přes API s VMWARE vCENTRE:
    a. Poskytnout informaci o jménu VM, operačním systému VM, IP adrese, MAC, aktuálním portu a prvku pro účely dohledu a viditelnosti
    b. Poskytnout informaci o historické lokaci pro každou VM (port a prvek daná VM komunikovala v čase)
    c. Ve VMware vCENTRE poskytnout informaci o aktuálním portu a aktivním prvku, kde daný provoz vstupuje do fyzické sítě (zapsání např. do pole „notes" u dané VM)
j) Vytvoření rolí pro přístup do systému minimálně Administrátor/Operátor, ověření na základě členství ve skupině v Active Directory
k) RADIUS server pro ověřování přístupu oproti účtům z Active Directory na prvky (možno řešit i jako službu OS)
l) Rozkreslení topologie sítě – mapa zařízení a spojů včetně přidání vlastních zařízení
m) dodávka jako virtuální appliance pro VMWare ESX
n) architektura klient-server
o) Licenční pokrytí na 100 koncových zařízení a 500VM

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

Akceptační testy:

Následující testy budou provedeny v rámci akceptace konečného stavu implementace díla na prvcích náhodně učených zadavatelem. Součástí akceptace je i kontrola zobrazení chybových stavů a hlášení v řídících a monitorovacích softwarech včetně alertingu.

Ethernet switche a SW pro vzdálený MGMT a automatizaci ethernetové sítě:

a) Ukázka mapy sítě v MGMT nástroji, ukázka historie vytížení linek
b) Test redundance zapojení – odpojení redundantních linek, vypnutí boxů – kontrola dostupnosti MGMT switchů, zobrazení v MGMT nástroji, kontrola dostupnosti routovacích interfaces

C

c) Nastavení a ukázka ověřování přístupu pro management prostřednictvím RADIUS serveru pro 2 úrovně přístupu přes protokol SSH
d) Zasílání syslog informací (IP syslog serveru poskytne zadavatel)
e) Nastavení IP ACL na management interface
f) Testovací scénář SDN (portgroup v vCENTRE je v distribuovaném switchi), probíhá na jednom ESX a přes jedno síťové rozhraní:
    a. Vytvoření portgroup1, portgroup2 ve vCENTRE – ukázka převzetí informace přes API do MGMT nástroje
    b. Zapojení VM1,VM2 do portgroup1 ve vCENTRE – ukázka zobrazení informace o VM1 v MGMT
    c. Zapojení VM3,VM4 do portgroup2 ve vCENTRE – ukázka zobrazení informace o VM3 v MGMT
    d. Vytvoření 4x IP interface v infrastruktuře (interní router), ukázka vytvoření komunikační cesty mezi VMs a IP interfaces
    e. Ukázka ARP, MAC, VLAN ,konfigurace přes CLI uvnitř infrastruktury
g) Migrace VM1,VM2,VM3,VM4 mezi ESX hosty zobrazení informace o historické lokaci VM v síti, kontrola dostupnosti
h) Vyhledání VM dle MAC, IP, Názvu, OS.
i) Přesun VM4 z portgroup1 do portgroup2 - kontrola zobrazení informace o VM
j) Ukázka vysoké dostupnosti = výpadek kterékoliv komponenty neomezí provoz mezi VM, neomezí funkčnost migrace VM ze serveru na server
k) Dostupnost IP konektivity při vypnutí hlavního routeru – ukázka převzetí routování záložním routerem s výpadkem max. 3s, kontrola dostupnosti ze strany VM

Servery a VMWARE vSPHERE:

a) ukázka přístupu ke správě serveru bez instalace host OS
b) nastavení SNMP pro management serveru bez instalace host OS a ukázka akce pro špatný/odpojený zdroj, špatný/odpojený ventilátor
c) ukázka konfigurace HA clusteru
d) test VMOTION (storage i VM)
e) test vysoké dostupnosti clusteru
    a. vypnutí jednoho ESX (host failure)
    b. síťová nedostupnost (host network isolation)
    c. odpojení storage (datastore under PDL a APD)
f) test redundance zapojení hostů FC a ethernetu (fyzické odpojení redundantních linek)
g) ukázka Hardware health monitoring (např. CIM)
h) ukázka nakonfigurované vFLASH read cache a její přiřazení VM
i) ukázka funkce NSX mikrosegmentace – definice pravidel a jejich logování v syslogu
j) nastavení zasílání NETFLOW z distribuovaného switche na kolektor

Diskové pole (testováno z pohledu VM):

a) Při charakteru provozu 70% random read / 30% random write IOPs pro osazenou diskovou kapacitu musí diskové pole poskytovat výkon minimálně 80 000 IOPs s response time maximálně 1ms pro 32KB bloky.
b) Test chování v případě odpojení datových linek do jednoho kontroleru pole
c) Výpadek serveru witness (pokud je součástí konfigurace)
d) Sestavení LUNu v konfiguraci synchronní replikace
    a. snížení výkonosti svazku maximálně o 20% oproti konfiguraci bez synchronní replikace
    b. publikace serveru ESX, kontrola dostupnosti
    c. simulace poruchy jednoho pole bez přerušení konektivity a snížení výkonosti systému
    d. synchronizace svazku po navázání konektivity
    e. změna primárního pole pro svazek

f. Odstavení jednoho kontroleru na obou polích současně formou restartu a kontrola dostupnosti svazku na VMWARE ESX
g. Zvýšení velikosti svazku

e) Ukázka funkčnosti vVOL s VMWARE ESX
f) Ukázka SPACE RECLAMATION funkce
g) Ukázka výkonového monitoringu pole
h) Ukázka funkčnosti plugin ve VMWARE vCENTRE
i) Vytvoření snaphootu na LUNu, clon snaphootu, přiřazení snapshootu serveru
j) Ukázka deduplikace na LUN presentovaného jako VMWARE VMFS datastore

Disková virtualizace:

a) Ukázka MGMT rozhranní
b) Vytvoření datového svazku, přiřazení ESX, kontrola dostupných cest ze strany ESX
c) Test redundance zapojení:
   a. Odpojení FC interface pro publikaci svazků
   b. Odpojení FC interface pro připojení diskových polí
   c. Kontrola dostupnosti publikovaného svazku ve VMWARE ESX
d) Ukázka synchronního mirroru svazku rozprostřeného mezi 2 diskovými poli
e) Odpojení diskového pole s primárním svazkem
f) Ukázka převzetí funkce druhým nodem clusteru
g) Ukázka replikace svazku a přiřazení ESX serveru
h) Ukázka snapshootu svazku a přiřazení ESX serveru
i) Ukázka SW pro monitoring (IOPs)

Ukázka migračních procedur:

Migrace VM ze stávajícího prostředí TCK do nového datacentra se stávajícími parametry:

- migrace datových a konfiguračních souborů náležejících jedné VM ze stávajícího VMFS datastore do nového prostředí a spuštění VM
- zachování IP adresy, ostatní VM ve stejném IP subnetu zůstávají v původní infrastruktuře, migrovaná VM je síťově dostupný
- bloková migrace RAW disku umístěného ve stávajícím systému diskové virtualizace (FalconStor NSS server verze 7.0) do nového prostředí (disk zůstává jako RAW po migraci), přidělení RAW disku VM v novém prostředí, RAW disk dostupný ve virtuálním OS jako konzistentní čitelný diskový svazek

Technické požadavky části č. 2 - Bezpečnostní infrastruktura

Předmětem veřejné zakázky je analýza a nasazení systému na monitorování, ukládání, správu a vyhodnocování událostí informačních systémům v prostředí Krajského úřadu Kraje Vysočina nebo další rozvoj stávajícího řešení. Systém bude sloužit k centrálnímu sběru logů a flow dat z různých systémů, jejich shromažďování, vyhodnocování, analyzování, korelaci a archivování. Musí zaručit neměnnost a zabezpečení sebraných údajů pro případné pozdější forenzní analýzy. Rovněž bude sloužit k detekci, vyhodnocování a hlášení bezpečnostních hrozeb, událostí a incidentů.
Řešení musí být dodáno jako appliance/appliances do virtuálního prostředí VMware.

Výstupy realizace zakázky jsou vedle obecných požadavků:

- nastavení přenosu auditních záznamů a dalších potřebných informací ke zpracování a archivaci
- nastavení centrálního vyhodnocování, alertingu a korelace

Požadavky na systém:

1. Typy a způsoby sbíraných událostí a dat – systém musí umět zpracovat data a logy minimálně z následujících technologií:
   a. MS Windows event log
   b. MS Exchange

c. MS IIS
d. MS DHCP a DNS
e. Zprávy protokolu syslog
f. Zprávy protokolou syslog over TLS
g. Apache / Tomcat
h. VMWare
i. Logy z DB platforem:
    i. MS SQL
    ii. MySQL
j. UNIX-like OS log
k. Packet Filter
l. SNMP Trap
m. W3C logy
n. JSON
o. možnost zpracování logů jiných systémů (zpracování TXT, CSV, XML, záznamů v relační DB, atd.)
p. NetFlow v5,7,9, sFlow
q. datové toky s vidítelností do aplikační vrstvy (flow obohacené o tzv. payload) nebo kopie síťového provozu

2. Kapacita a výkon systému:
    a. průměrná zátěž 2000 událostí za sekundu (EPS)
    b. špičková zátěž 5000 událostí za sekundu (EPS)
    c. možnost dolicencování až na 10000 událostí za sekundu (EPS)
    d. průměrná zátěž 500 flow za sekundu (FPS)
    e. špičková zátěž 750 flow za sekundu (FPS)
    f. možnost dolicencování až na 2000 flow za sekundu (FPS)
    g. minimálně 300 monitorovaných zařízení
    h. ad-hoc filtrace logů zpětně za 3 měsíce
    i. archivace logů za minimálně 1 uplynulý rok s možností selektivního obnovení pro účely dodatečné filtrace
    j. možnost současné práce 3 analytiků
    k. Rychlost odezvy systému, je definována jako časová prodleva mezi dokončením zadání funkčního požadavku z uživatelského rozhraní a zobrazením požadované informace na zobrazovacím rozhraní příslušného technického zařízení. Tato prodleva nesmí být delší než 2 sekundy při rychlosti připojení uživatele 0,5 Mb/s. Tato podmínka neplatí v případě logování do systému nebo prvního načítání rozsáhlých číselníků.
3. Bezpečnost systému – systém musí umožnit následující bezpečnostní opatření týkající se logovaných událostí:
    a. hlídání a reporting operace smazání logu na hlídaném zařízení
    b. hlídání a reporting zastavení operace sběru a vyhodnocování logů
    c. zabezpečený přístup k datům a zachování jejich integrity
        i. šifrování přenášených dat
        ii. autentizace klienta i serveru
        iii. logování operací uživatelů a správců
    d. ochrana před změnou logů a dalších sbíraných dat ze strany administrátora
    e. používání zabezpečených (šifrovaných) protokolů (HTTPS, TLS, apod.)
    f. správa uživatelů a uživatelských oprávnění na bázi typizovaných rolí (např. administrátor, operátor, apod.)
    g. autentizace uživatelů vůči LDAP (MS AD)
4. Provozní požadavky na systém:
    a. sběr, vyhodnocování a korelace událostí probíhá v reálném čase
    b. možnost korelací více typů zdrojů a typů událostí
    c. preferována možnost tzv. bezagentního sběru událostí.

d. vytváření a generování reportů a plánování jejich tvorby v čase bez nutnosti sestavování SQL dotazů
e. zobrazení dat pomocí tzv. dashboardů
f. možnost vyvolání akcí na základě vyhodnocení událostí (například SMTP e-mail, odeslání SMS zprávy, SNMP zprávy, spuštění scriptu, vygenerování reportu, apod.)
g. automatická aktualizace agentů
h. synchronizace systémového času vůči NTP
i. GUI systému je na bázi webové aplikace, která je optimalizovaná pro všechny běžné webové prohlížeče (IE, Firefox, Chrome, ...) na všech běžných platformách (MS Windows, GNU/Linux, MacOS)
j. systém umožňuje self-monitoring a logování vlastních událostí
k. Aktualizace systému probíhá ve formě vzdálené aktualizace celého řešení bez nutnosti instalace komponent na koncových stanicích a bez nutnosti instalace na místě (on-site) v datovém centru kromě předem definovaných specifických situací.
l. Systému umožňuje integraci s jinými informačními systémy pomocí (REST) API.

5. Další požadované vlastnosti systému:
   a. Systém musí ve výchozí instalaci (tzv. out-of-the-box) obsahovat předdefinovaná pravidla pro identifikaci základních typů hrozeb, útoků a incidentů. Minimálně pro tyto oblasti:
      i. Získávání informací (různé typy skenování)
      ii. Činnosti botnetů
      iii. DoS, DDoS útoky
      iv. Autentizace
      v. Exploit, Malware
      vi. Podezřelé aktivity a anomálie (např. připojení na adresy na blacklistu, nestandardní připojení, nestandardní nárůst počtu událostí, ...) + tzv. Network Behaviour Anomaly Detection funkcionalita.
   b. Systém musí obsahovat aktivní modul pro sdílení informací o aktuálních bezpečnostních hrozbách, tzv. cyber threat intelligence feed, automatické aktualizace tohoto modulu musí být zahrnuty v ceně licence za systém.
   c. Systém musí umožňovat automatické upravování a doplňování pravidel na základě informací ze cyber threat intelligence poskytované výrobcem systému
   d. Systém musí umožňovat integraci s lokálním cyber threat intelligence systémem (např. systém WARDEN, apod.).
   e. Systém musí obsahovat formulář pro hlášení kybernetického bezpečnostního incidentu dle zákona o kybernetické bezpečnosti přímo jako součástí webového rozhraní produktu.
   f. Systém musí obsahovat aktivní modul pro skenování zranitelností (tzv. modul pro vulnerability assessment) a umožňovat integraci a korelaci událostí s nalezenými zranitelnostmi. Skener zranitelností musí mít níže uvedené vlastnosti. Pokud by systém neobsahoval vestavěný vulnerability assessment modul, nebo by nenaplňoval požadované vlastnosti, musí systém umožňovat integraci s externími skenery zranitelností. V tomto případě musí být součástí dodávky a pořizovací ceny i licence pro skener zranitelností třetí strany, který naplňuje požadované vlastnosti. Licence pro skener zranitelností nesmí omezovat celkové počty skenů ani celkové počty skenovaných zařízení/systémů. Licence pro skener zranitelností může omezit počet skenovaných zařízení/systémů v jeden čas, kdy minimální počet skenovaných zařízení v jednom časové okně musí být minimálně 200 IP adres.
   i. Požadované vlastnosti skeneru zranitelností:
      1. Skener musí nabízet minimálně tyto typy scanů: discovery scan, vulnerability scan, patch scan, autentizovaný i

neautentizovaný scan (scan pomocí autentizovaného i neautentizovaného uživatele)
2. Skener musí umožnit jak sken z Internetu pro test DMZ zón, tak sken vnitřní sítě se zachováním bezpečnosti architektury sítí
3. Skener musí obsahovat pravidelně (denně) aktualizovanou databázi zranitelností, jejíž součástí jsou i návrhy na opravu zranitelností
4. Skener musí podporovat skenování těchto zařízení a systémů:
    - síťová zařízení (firewally, aktivní síťové prvky)
    - virtualizační platformy (VMware ESX, vSphere, vCenter, ...)
    - operační systémy (MS Windows, Unix)
    - databázové systémy (MSSQL, MySQL)

g. Systém musí obsahovat tzv. asset discovery modul, který slouží pro automatické zjišťování, detekci a evidenci prvků/zařízení/aktiv na síti. Evidence aktiv musí obsahovat minimálně tyto parametry: IP adresa, MAC adresa, název aktiva a verze operačního systému, otevřené porty a na nich běžící služby. Tento modul musí umožňovat korelaci a spolupráci s modulem pro skenování zranitelností.
h. Systém musí umožňovat sběr datových toků obohacených o data z aplikační vrstvy prostřednictvím virtuálních sond nasaditelných do virtuálního prostředí VMWare. Součástí dodávky a pořizovací ceny systému musí být licence pro použití minimálně 2 virtuálních sond.

Požadavky na údržbu systému – v rámci údržby a podpory k systému jsou požadovány tyto činnosti:

1. Pravidelná aktualizace systému, která zahrnuje bezpečnostní a funkční aktualizace
2. Tvorba a implementace nových pravidel dle zadání
3. Pravidelná automatická aktualizace bezpečnostních pravidel z tzv. cyber threat intelligence modulu

Akceptační testy

1. Provoz
    a. Konfigurace systému pro autentizaci uživatelů vůči Active Directory.
    b. Zavedení skupiny uživatelů v Active Directory jako uživatelů systému.
    c. Přiřazení třem různým uživatelům tři různé role s různou úrovní přístupových oprávnění.
    d. Konfigurace synchronizace systémového času systému s NTP serverem.
2. Asset Discovery
    a. Vytvoření úvodní databáze aktiv v síti s požadovanými parametry.
    b. Nastavení automatického zjišťování nových aktiv v síti.
3. SIEM – logování, sbírání, vyhodnocování, korelace a reporting událostí
    a. Přenos a zpracování dat
        i. Nastavení zdrojů dat, přenosu dat a zpracování dat pro účely out-of-the-box vyhodnocování hrozeb, útoků a incidentů. (Pozn. typy potřebných zdrojů a typy událostí/dat určí dodavatel podle best-practise implementace systému tak, aby byly pokryty minimálně požadované oblasti out-of-the-box vyhodnocování).
        ii. Nastavení zdrojů dat, přenosu a zpracování dat v níže uvedeném rozsahu. Toto zpracování dat bude sloužit pro účely vyhodnocování dat pomocí pravidel dále uvedených v těchto akceptačních testech.
            1. MS Active Directory – 3 servery
            2. MS Windows servery – 5 serverů
                a. Pro účely logování událostí operačního systému
            3. Unix (GNU/Linux, FreeBSD) servery – bezagentový sběr, 5 serverů

a. Pro účely logování událostí operačního systému
4. VPN servery - SonicWall 1 server, MS RAS 1 servery
5. DNS servery –1x FreeBSD, 1x MS Windows
6. DHCP MS Windows – 1 server
7. FW (FreeBSD, packet filter) – bezagentový sběr, 1 server
8. Web servery – 1x IIS, 1x Apache
9. DB servery – 1x MSSQL
10. MS Windows File server – 1 server
11. VMware vSphere – 1 server
12. SAN IPStor - 1 management server
13. Veeam Backup & Replication, 1 server
14. SMTP FreeBSD/Postfix – bezagentový sběr, 1 server
15. MS Exchange – 2 servery
16. Síťové prvky pro sběr Netflow – 1 prvek

iii. Konfigurace virtuálních sond pro sběr datových toků obohacených o informace z aplikační vrstvy tak, aby byla data posílána a zpracovávána pomocí systému.

b. Vyhodnocování a korelace

i. Out-of-the-box vyhodnocování událostí bude ověřeno následujícími testy, které provede objednatel, kdy bude posuzováno vyhodnocení události systémem:
1. Horizontální sken 5 IP adres v LAN a 5 adres v DMZ na 1 konkrétní port pomocí specializovaného nástroje (např. NMAP)
2. Vertikální sken 1 IP adresy v LAN a 1 IP adresy v DMZ na standardních 1024 portů pomocí specializovaného nástroje (např. NMAP)
3. Vulnerability scan 1 IP adresy v LAN a 1 IP adresy v DMZ pomocí specializovaného nástroje (např. OpenVas)
4. Provedení DDoS útoku na 1 web server vygenerováním velkého množství GET požadavků.
5. Spuštění brute-force útoku vůči službě SSH na 1 serveru pomocí specializovaného nástroje.
6. Zastavení logování/sběr dat ze 3 různých zdrojů (logy i flow).
7. Smazání logu na 3 různých zdrojích.

ii. Vyhodnocování událostí dle uživatelsky specifikovaných pravidel – v rámci akceptačních testů je nutné nastavit tato vyhodnocovací pravidla:
1. MS Windows
a. Přidání uživatele do konkrétní AD skupiny – log, alert
b. Přidání uživatele do určité built-in local skupiny na Windows server – alert
c. Instalace software na Windows serveru – log
d. Spuštění konkrétního příkazu na Windows serveru – log, alert
e. Chybějící bezpečnostní aktualizace na Windows serveru – log, agregace
2. Unix (Linux, FreeBSD)
a. Neúspěšná autentizace pomocí su příkazu 5x za sebou – alert
b. Editace konkrétního souboru – alert
c. Přístup ke konkrétnímu souboru (R/W, cp, mv) – log, alert, v případě operace write logovat kdo a jako změnu provedl
d. Úspěné SSH připojení bez předchozího VPN spojení v určený čas – alert
e. Spuštění konkrétního příkazu – log

f. chybějící aktualizace + jak dlouho chybí - sbírat, agregace, prioritizace (řazení)

3. Autentizace obecně z více zdrojů
   a. Autentizace účtu z konkrétní skupiny od jinud, než z LAN – alert
   b. Připojení účtu z konkrétní skupiny na konkrétní servery – alert
   c. Úspěšná autentizace účtu z konkrétní skupiny v určenou dobu bez předchozího VPN připojení – alert
   d. Horizontální přihlašování (přihlášení jednoho účtu na více serverů) v definovaném čase –log
   e. Zablokování účtu x krát za sebou v daném časovém rozmezí - alert
4. VPN
   a. Souhrnné info o přidělených IP adresách uživatelům – log
   b. Pokusy o připojení uživatelů z konkrétní skupiny – log, agregace
   c. Nepovedené pokusy o připojení Yx/Xs – log
5. Networking
   a. monitoring zařízení připojujících se na konkrétní port, kde destination IP není X.X.X.X – alert
   b. souhrnné info o přidělených IP adresách z DCHP serverů (minimálně IP, hostname, MAC) – log, agregace
   c. na DHCP serveru v konkrétním scope (IP) se objeví jiné než definované zařízení – log
   d. připojení server>>any host na definovaných portech - sbírat, agregace
   e. počet připojení na 1 konkrétní host je větší než stanovený počet za stanovený čas - alert
6. WEB server
   a. V logu web serveru se objeví klíčová slova – alert
   b. Více jak X požadavků z jedné IP adresy v definovaném časovém úseku – alert
   c. Trend počtu připojení na webserver se změní X násobně za stanovený čas – alert
7. DBMS MSSQL
   a. Přidání uživateli definované role – alert
   b. Pokus o přístup (povolení/spuštění) konkrétní uložené procedury – alert
   c. Uživatel se nepřihlásil déle jak X hodin – log
   d. Kontinuálně neúspěšné přihlášení jednoho uživatele X za sebou – log
   e. Úspěšné přihlášení z konkrétních IP rozsahů – alert
   f. Záloha DB provedené jiným než definovaným uživatelem – log
8. File server
   a. Zápisy souborů na konkrétní fileservery – log
   b. Zápis souboru jehož koncovka neodpovídá vydefinovaným typům
   c. Chybějící konkrétní event, který se vyskytuje v pravidelných intervalech
9. SMTP/Exchange
   a. Úspěšný přístup k mailboxu z IP adresy mimo ČR – log
   b. Přidělení access rights na mailbox – log

c. Přidělení full access na cizí účet - log
d. Více jak X odchozích e-mailů na cílovou IP za definovaný čas – alert, agregace

10. Backup
    a. X neúspěšně ukončených vydefinovaných jobů za sebou – alert, agregace
11. Disková virtualizace
    a. Úspěšné přihlášení konkrétního uživatele z jiných, než povolených IP rozsahů – log, alert
12. VMWare
    a. Přidání oprávnění uživatelskému účtu – log
    b. Přidání nového virtuálního zařízení – log
    c. Smazání virtuálního zařízení – log, alert
    d. Kopie logu vCentra - log

iii. Reporting a provádění akcí – v rámci výše zpracovaných vyhodnocovacích pravidel je třeba nastavit tyto metody reportingu a provádění akcí

1. Report
    a. Nastavení automatického pravidelného generování vybraného reportu
    b. Nastavení jednoho vybraného reportu a jeho vygenerování tzv. „na kliknutí"
    c. Automatické odesílání vybraného reportu e-mailem na vybranou skupinu uživatelů
2. Dashboard – konfigurace jednoduchého dashboardu, který bude umožňovat zobrazení jednotlivých monitorovaných oblastí (např. AD, DBMS, Aplikace, SMTP/EXCHANGE, apod) s odkazem na pravidla, která způsobila tento stav alertu.
3. Vyvolání akce
    a. Odeslání vybraného alertu e-mailem na definovanou skupinu uživatelů, e-mail musí obsahovat kromě základních informací o události rovněž odkaz, který vede do uživatelského rozhraní systému a zobrazí danou událost.
    b. Spuštění skriptu na základě vybrané události
        i. Skript musí být spuštěn na serveru, kterého se událost týká pod definovanými oprávněními

4. Vulnerability assessment
    a. Konfigurace skeneru zranitelností, případně nastavení integrace se systémem.
    b. Úvodní oskenování vybraných aktiv – 5 IP adres z DMZ, 5 IP adres z LAN

Ty akceptační testy, u kterých nebude objednatel schopen dodat relevantní data potřebná pro vyhodnocení pravidel, nebudou objednatelem vyžadovány.

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

Webový aplikační firewall (WAF)

Pro realizaci možno využít stávající řešení - F5 – BIG-IP 3600, aktuální software ASM (Application Security Manager) ve verzi 13.0.0

Nasazení WAF HW appliance (nikoliv virtuální) v cluster designu (možno i active-pasive) s následujícími parametry na jeden box:

a) Porty 8x SFP, 2x SFP+, všechny porty osazeny MM zářiči, redundantní napájení,

b) Průchodnost 75 000 L7 spojení za sekundu přes WAF modul bez zapnuté kontroly provozu
c) High Availability (HA) se synchronizací konfigurace mezi jednotlivými nody
d) Management
   - Lokální management
   - Vzdálený management – dedikovaný management interface (GUI, příkazová řádka)
e) Řízení oprávnění – možnost nastavit různá oprávnění ve WAF pro různé účty (uživatelské role)
f) Aplikační firewall
   - Ochrana proti následujícím typům útoků a událostí:
     - OWASP TOP 10
     - Layer 7 (D(r))DoS a BruteForce
     - Web Scraping
     - Cross Site Scripting
     - Injection typů SQLi, XML, LDAP, OS, XPath, XQuery, PHP Code injection
     - CSRF
     - Session Hijacking
     - Local a Remote File Inclusion (LFI a RFI)
     - Remote Code Execution
     - Detekce skenování
   - Malware detekce (včetně zero-day malware)
   - IP Geolocation, IP Reputation + možnost blokování IP adres na základě těchto kritérií
   - Možnost zajištění čistoty protokolů HTTP(s), FTP, XML, JSON, SOAP
   - Podpora prevence úniku citlivých dat (např. kreditní karty, rodná čísla,...).
   - Možnost provozu v aktivním (blokovacím) i pasivním (transparentním) módu.
   - Možnost automatické konfigurace za využití učícího se módu (self-configuration).
   - Možnost auditovat bezpečnostní politiku v režimu „offline" (export stávající politiky do XML formátu a statická analýza) případně úprava politiky na základě scanu zranitelností externím nástrojem.
   - Poskytuje sadu předdefinovaných vzorů pro nastavení bezpečnostní politiky pro publikované aplikace (Sharepoint 2016, OWA Exchange 2016) a umožňuje vlastní uživatelské sady zohledňující např. typ serverového operačního systému (Windows Server, Unix/Linux), webový/aplikační server (Apache, IIS, Tomcat, JBoss), databázový server (MSSQL, MySQL), případně programovací jazyk (ASP.NET, PHP, XML, JAVA).
   - Schopnost testovat nová bezpečnostní pravidla v non-blokovacím režimu, při zachování funkčnosti stávající bezpečnostní politiky WAF.
   - Schopnost monitoringu URI.
   - Reporting událostí (např. podle nastavených pravidel, podle typu útoků, podle závažnosti, podle IP Geolokace).
   - Možnost logovat na externí Syslog server a SNMP
   - Možnost směrování requestů na základě jejich obsahu (dle typu browseru, URL apod.)
   - Možnost změny requestů (modifikace hlavičky nebo obsahu)
   - Odstranění nežádoucích informací z requestu
   - Možnost filtrování provozu.

   - Proxy reverzní včetně HTTPS (nejedná se o uživatelskou proxy, ale základní proxy funkcionalitu WAF, podpora IPv6 (komunikace klient-WAF po IPv6 dovnitř infrastruktury po IPv4)
g) Autentizace - možnost autentizace uživatelů přes LDAP(AD)/RADIUS pro MGMT přístup

h) Autorizace – možnost autorizace přes skupiny LDAP(AD) pro MGMT přístup
i) Nativní podpora HTTP/2
j) Existence možnosti integrovat výstupy ze skeneru webových zranitelností. Musí umožnit automaticky upravit konfiguraci bezpečnostní politiky na základě nalezených konkrétních zranitelností.
k) Možnost cachování HTTP provozu
l) Plná podpora IPv6
m) Je vyžadováno zpracování SSL komunikace na HW úrovni (šifrovací karta).
n) Možnost napojení na dohledové/řídící systémy třetích stran prostřednictvím dokumentovaného API (čtení a změna konfigurace, čtení statistik). Podpora SNMP (v1/v2c/v3). Možnost odeslání elektronické zprávy (e-mail) určené osobě při vzniku sledované události. Možnost odesílání logu na externí logovací systém.

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW a datové updaty (definice) na dobu 2 let

Akceptační testy

1. Otestování HA (ruční přehození, výpadek nodu, ztráta vzájemné viditelnosti, synchronizace konfigurace mezi zařízeními)

2. Autentizace dvou AD uživatelů do WAF + autorizace dle členství v AD skupině. Dvě různé uživatelské role (dvěma skupinám v AD budou ve WAF odpovídat 2 rozdílné konfigurace uživatelských rolí)

3. IP Geolocation – zablokování uživatele z dané země nebo IP

4. Kontrola HTTP protokolu (např. content length, kontrola počtu hlaviček – obecně ochrana před útoky typu buffer-overflow, null-byte injection, DoS, atp.)

5. Konfigurace 5 webových aplikací (virtuálních serverů) pro blokovací (aktivní) a 5 webových aplikací pro transparentní (pasivní) režim, nastavení bezpečnostních politik viz:

   - netriviální aplikace s různými moduly, uživatelskými filtry a bohatým uživatelským vstupem (rozsáhlé formuláře, dynamické parametry, multi-upload, AJAX)
   - aplikace používá URL rewrite
   - Kontrola XML obsahu – XML firewall
   - publikace webové služby (SOAP)
   - 4 aplikace v blokovacím režimu - jednoduché zabezpečení - blokují se pouze útoky dle známých signatur a obecných pravidel HTTP protokolu. Výběrově se kontrolují konkrétní (tj. ručně zadané) parametry nebo URL
   - 1 aplikace v blokovacím režimu - podrobné zabezpečení (naučení parametrů, URL, typů souborů), určení datových typů (jak na celou aplikaci, tak pro jednotlivé URL různě). Nastavit vhodné (neblokující) chování pro neznámé parametry v blokovacím režimu

6. Prokázání detekce vulnerability scanu jedné vybrané webové aplikace

7. Prokázání detekce DoS útoku na jednu webovou aplikaci vygenerováním velkého množství GET požadavků z jedné IP adresy

8. Prokázání detekce a zablokování pokusu o SQL injection pomocí specializovaného automatického nástroje pro hledání SQLi zranitelností

9. Prokázání detekce a zablokování pokusu o Cross-Site-Scripting útok (na bázi XSS v URL)

10. Provést aktualizaci signatur a jejich nasazení do stávající aplikace v neblokovacím režimu

11. Nastavení SNMP monitoringu (CPU, stav nodů, sledování zatížení)

12. Konfigurace reportingu událostí do SIEM systému, který bude vystupovat jako syslog server

13. Změna obsahu (hlavičky) odchozí komunikace (nastavení secured příznaku pro cookies)

14. Emailová notifikace – odeslaní agregované zprávy o zablokovaných připojeních

15. kontrola průchodnosti na L7 generátorem packetů (parametr dle požadavků ve specifikaci bod b) přes WAF modul bez zapnuté kontroly provozu

16. Kontrola dokumentace - popis a schéma nasazení, výchozí konfigurace

Technické požadavky části č. 3 - Aplikační monitoring

Na síťové úrovni (ethernet) požadujeme implementaci řešení, které monitoruje skutečný aplikační provoz, probíhající mezi uživateli a aplikační infrastrukturou (pasivně, bez instalace agentů na koncové servery). Z kopie tohoto provozu (mirror provozu zajišťuje síťová vrstva) zachytává jednotlivé pakety, rekonstruuje jednotlivé požadavky, přiděluje jim časové známky, dekóduje a analyzuje jejich obsah. Požadujeme použití pro následující aplikace:

- Na bázi HTTP/HTTPS
- Databázové (minimálně MSSQL)

Požadujeme zjištění následujících skutečností:

- Počet transakcí
- Doba odezvy monitorované aplikace (maximální, průměrná, medián, percentil).
- Počet uživatelů souběžně pracujících s aplikací.
- Doba přenosu dat na transportní vrstvě a jejich velikost.
- Přehled transakcí v jednotlivých úrovních SLA a jejich rozložení v čase.
- Počet výskytu chybových kódů a jejich rozložení v čase.
- Detaily jednotlivých transakcí ve formě plného SQL dotazu včetně parametrů a informací z hlavičky HTTP/HTTPS (URL, parametry, UserAgent, Cookie), součástí detailu je i chybový kód, pokud transakce skončila chybou
- Detail pro jednotlivé koncové stanice nebo uživatele

Další požadavky:

- Administrátorské rozhraní přístupné přes HTTPS protokol
- Definice SLA pro každou aplikaci, případně část aplikace a sledování celkového výkonu aplikace na základě splnění SLA
- Párování transakcí na základě definice podřízených aplikací (např. pro daný http požadavek zobrazení transakcí, které proběhly na databázové vrstvě v době řešení http požadavku)
- Nastavení alertů při překročení nadefinovaných hodnoty odezvy pro aplikaci
- SNMP / rest API pro začlenění do monitoringu (https://www.paessler.com/prtg) a provedení vzorové integrace s PRTG
- Forma OVF appliance do prostředí VMWARE vSPHERE
- Možnost vizualizace výkonnostních metrik http aplikace v prostředí webového prohlížeče přímo při zobrazení dané aplikace ve webovém prohlížeči
- Licenční pokrytí pro monitorování komunikace 4 virtuálních strojů (4 datové linky), uchování záznamů po dobu 3 měsíců, 10tis. transakcí za minutu

Součástí ceny pořízení je i podpora výrobce včetně nároku na SW updaty na dobu 2 let.

Akceptační testy na aplikaci vybrané zadavatelem

- Zobrazení naměřených hodnot v monitorovacím SW PRTG (https://www.paessler.com/prtg) – získání hodnot přes SNMP/REST API
- Zobrazení HTTPS komunikace mezi serverem a klientem v detailu URL včetně hodnot
- Zobrazení SQL komunikace v detailu transakce mezi serverem a klientem

Příloha č. 2 Položkový rozpočet
Veřejná zakázka: Technologické centrum Kraje Vysočina 2016 – infrastruktura 2

Dodavatel: OptoNet Communication, spol. s r.o.
Část 3 Monitoring výkonu aplikací

Položka (komodita)	Popis[1]	Počet kusů	Cena Kč bez DPH za jeden kus (jednotková - JC)	Nabídková cena celkem Kč bez DPH (počet ks x JC)	Sazba DPH % / DPH 21	Cena celkem Kč s DPH	Název nabízeného výrobku a označení výrobce
1.	Monitoring výkonu aplikací - AA-NPM	1	45 448,00 Kč	45 448,00 Kč	9 544,08 Kč	54 992,08 Kč	FlowMon Probe 4000 VA – IFP-4000-VA
2.	Monitoring výkonu aplikací - AA-NPM	1	259 988,00 Kč	259 988,00 Kč	54 597,48 Kč	314 585,48 Kč	FlowMon Collector 6000 VA – IFC-6000-VA
3.	Monitoring výkonu aplikací - AA-NPM	1	1 299 988,00 Kč	1 299 988,00 Kč	272 997,48 Kč	1 572 985,48 Kč	FlowMon APM Corporate – FP-APM-C
Nabídková cena celkem - dodávka (kupní smlouva)				**1 605 424,00 Kč**	**337 139,04 Kč**	**1 942 563,04 Kč**	

1 technická specifikace viz příloha ZD

Podmínky a pokyny pro vyplnění:

Dodavatel vyplní zeleně podbarvená pole, tj.:

Dodavatel vyplní u každé položky cenu za jednotku bez DPH (jednotková cena, max. dvě desetinná místa)
Dodavatel vyplní sazbu DPH v % (např. 21-předvyplněno orientačně). Dodavatel neplátce vyplní sazbu "0". Jednotkové ceny jsou v takovém případě konečnými (viz podrobně v ZD)
Dodavatel vyplní u každé označené položky název nabízeného výrobku a označení výrobce
Za správnost výpočtů odpovídá dodavatel (nastavené vzorce nejsou závazné). Ceny budou stanoveny s přesností na dvě desetinná místa.

Seznam poddodavatelů
Technologické centrum kraje Vysočina 2016 – infrastruktura 2
Část 3: Aplikační monitoring

VUMS DataCom, spol. s r.o.
se sídlem: Praha 6 - Vokovice, Lužná 591/4, PSČ 16000
IČO: 485 85 611, DIČ: CZ48585611
společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze,
oddíl C, vložka 17811
bankovní spojení: FIO Banka, a.s.,
číslo účtu: 2100378878 / 2010
zastoupená: **Františkem Pěčem**, jednatelem

Poddodavatel bude využitý pro dodávku aplikačního monitoringu.

Příloha č. 4 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Kraje Vysočina

- Bezpečnost přístupových oprávnění
    - Zhotovitel je povinen chránit veškeré přístupové údaje k informačním aktivům Kraje Vysočina včetně přístupů k informačním aktivům zhotovitele, které umožňují přístup k informačním aktivům Kraje Vysočina či umožnují jejich správu.
    - Zhotovitel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
        - min. délka hesla 10 znaků
        - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
            - malá písmena
            - velká písmena
            - číslice
            - speciální znaky
        - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
        - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
        - platnost hesla musí být maximálně 1 rok.
    - Zhotovitel je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
    - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
    - Pokud by zhotovitel zřizoval přístupová oprávnění třetí straně, je zhotovitel povinen o této skutečnosti informovat Kraj Vysočina. Kraj Vysočina má v tomto případě právo zřízení přístupu zamítnout.
- Řízení kybernetických bezpečnostních incidentů:
    - Zhotovitel je povinen Kraji Vysočina hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv Kraje Vysočina nebo informačních aktiv zhotovitele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv Kraje Vysočina.
    - Zhotovitel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kraje Vysočina.
- Bezpečnost kryptografických prostředků:
    - Pokud zhotovitel používá kryptografické prostředky v souvislosti s informačními aktivy Kraje Vysočina, je nezbytné, aby použité kryptografické algoritmy byly minimálně v souladu s aktuálním zněním vyhlášky č. 316/2014 Sb.