

KUPNÍ SMLOUVA

uzavřená níže uvedeného dne, měsíce a roku

dle ustanovení § 2079 a násl, § 2085 a násl. a § 1746 odst. 2 zákona č. 89/2012 Sb., Občanského zákoníku

Čl. 1 Smluvní strany

Kupující: **Nemocnice Slaný**

Sídlo: Politických vězňů 576, 274 01 Slaný
IČ: 00875295
DIČ: CZ00875295
Zastoupený: MUDr. Štěpánem Votočkem, ředitelem
Kontaktní osoba: Ing. Radka Linksfeilerová, vedoucí ICT - Vykazování zdravotní péče, tel. +420 312 575 169, email: radka.linksfeilerova@nemocniceslany.cz
Bankovní spojení: Komerční banka, a.s.
Číslo účtu: 27-6107220297/0100
Zápis v OR: Městský soud v Praze, sp.zn. Pr 1040
jako kupující, na straně jedné
(dále jen kupující)

a

Prodávající: **STORAGE ONE, a.s.**

Sídlo: Pod Habrovkou 338/7, 150 00 Praha 5 - Hlubočepy
IČ: 023 01 245
DIČ: CZ023 01 245
Zastoupený/Jednající: Milan Hlišák, Předseda představenstva
Kontaktní osoba: Vít Umlauf
Bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.
Číslo účtu: 2109680467/2700
Prodávající je plátce DPH: Ano
Zápis v OR: vedeném Městským soudem v Praze, oddíl B, vložka 19458
jako prodávající na straně druhé
(dále jen prodávající)

Čl. 2 Úvodní ustanovení

- 2.1. Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení“, zadávanou kupujícím jakožto zadavatelem.
- 2.2. Technická specifikace kupujícího (zadavatele) k veřejné zakázce a technická specifikace z nabídky prodávajícího tvoří nedílnou součást této smlouvy jako její přílohy.

Čl. 3 Vlastnické vztahy

- 3.1. Prodávající prohlašuje, že je výlučným vlastníkem prvků technologií (licence a zařízení) a jejich příslušenství, které jsou předmětem plnění této smlouvy.
- 3.2. Detailní technická specifikace předmětu plnění této smlouvy a počtu kusů jednotlivých technologií, licencí a jejich příslušenství je obsažena v příloze č. 1 a č. 2 této smlouvy a je její nedílnou součástí. V případě rozporu vzniklého mezi přílohami č. 1 a 2 této smlouvy v podobě technické specifikace platí vždy specifikace kupujícího obsažená v příloze č. 1 této smlouvy.

Čl. 4 Předmět smlouvy

- 4.1. Předmětem této smlouvy je hmotný majetek v podobě zařízení (komponent) a nehmotný majetek v podobě licencí, obojí včetně příslušenství. Vše v tomto odstavci uvedené ve vlastnictví prodávajícího. Předmět smlouvy je detailně specifikován v příloze č. 1 této smlouvy, včetně příslušenství. Prodávající je tímto povinen odevzdat kupujícímu zařízení a licence, která jsou předmětem této smlouvy a umožnit mu nabytí vlastnického práva k nim a současně závazek kupujícího zařízení převzít a zaplatit za ně prodávajícímu kupní cenu.
- 4.2. Součástí předmětu plnění jsou dále služby a práce prodávajícího se zařízeními a licencemi přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu, které jsou blíže specifikovány v příloze č. 1 této smlouvy. Jedná se zejména o montáž, oživení, instalaci, konfiguraci, dodávku dokumentace, dodávku licencí a zaškolení administrátorů.
- 4.3. Prodávající se zavazuje dodat předmět smlouvy kupujícímu s veškerými doklady nutnými k převzetí a zejména k užívání dodaných zařízení a software.
- 4.4. Prodávající touto smlouvou prodává kupujícímu do výlučného vlastnictví předmět kupní smlouvy definovaný v bodě 4.1 a to včetně příslušenství.
- 4.5. Kupující předmět plnění této smlouvy, jímž jsou věci nové a nepoužité, kupuje za dohodnutou kupní cenu a přijímá do svého výlučného vlastnictví.
- 4.6. Prodávající prohlašuje, že neví ke dni podpisu této kupní smlouvy o žádných vadách prodávaných movitých věcí, na které by kupujícího upozornil.

Čl. 5 Licence

- 5.1. Prodávající v rámci plnění předmětu této smlouvy dodává software podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon) a ustanovení § 2358 a následující zákona č. 89/2012, občanského zákoníku, proto poskytuje kupujícímu licenci (tj. oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném rozsahu), a to

formou licenčního ujednání v této kupní smlouvě. Prodávající prohlašuje, že se jedná o licenci:

- a) nevýhradní licenci k veškerým známým způsobům užití takového software, a to v rozsahu minimálně nezbytném pro řádné užívání software kupujícím;
- b) licenci neomezenou územním či množstevním rozsahem (není-li v této smlouvě uvedeno jinak) a rovněž tak neomezenou způsobem nebo rozsahem užití;
- c) licenci udělenou na dobu určitou,
- d) licenci převoditelnou a postupitelnou, tj. která je udělena s právem postoupení licence třetí osobě
- e) licenci, kterou není kupující povinen využít.

5.2. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy.

5.3. Prodávající prohlašuje, že odměna za poskytnutí licence kupujícímu je již zahrnuta v kupní ceně za poskytnuté plnění dle této kupní smlouvy.

Čl. 6 Kupní cena a platební podmínky

6.1. Kupní cena je nabídkovou cenou předloženou prodávajícím v jeho nabídce na veřejnou zakázku uvedenou v článku 2.1 této smlouvy.

6.2. Kupující se zavazuje zaplatit prodávajícímu za předmět spočívající **v dodávce plnění uvedený v Čl. 4 této smlouvy** kupní cenu ve výši

10.970.000,- Kč bez DPH,

tj. 13.273.700,- Kč včetně DPH,

když DPH ve výši 21 % činí 2.303.700,- Kč.

6.3. Kupní cena je stanovena jako cena konečná a úplná, zahrnuje veškeré dodávky a služby s dodávkami související a veškeré jiné náklady nezbytné pro řádnou a úplnou realizaci předmětu plnění této smlouvy včetně všech rizik a vlivů s plněním předmětu této smlouvy souvisejících.

6.4. Prodávající není oprávněn požadovat po kupujícím poskytnutí zálohy.

6.5. Prodávající na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy. V případě, že dojde mezi dnem podpisu kupní smlouvy a dnem uskutečnění zdanitelného plnění ke změně sazby DPH podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, bude daň z přidané hodnoty připočtena ke kupní ceně ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

6.6. Kupní cenu zaplatí kupující prodávajícímu bankovním převodem na bankovní účet prodávajícího uveden v článku 1 této smlouvy na základě daňového dokladu (faktury) vystaveného prodávajícím ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu na předmět plnění dle této smlouvy. Daňový doklad je považován za proplacený okamžikem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.

- 6.7. Na daňovém dokladu (faktuře) bude uveden rozklad fakturované částky na jednotlivá zařízení, tak aby byla zřejmá cena jednotlivých zařízení, a tak aby bylo kupujícímu usnadněno zavedení do majetkové evidence.
- 6.8. Splatnost daňového dokladu je 30 dnů ode dne jeho doručení kupujícímu.
- 6.9. Daňový doklad bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude mít náležitosti obchodní listiny dle § 435 zákona č. 89/2012 Sb., občanského zákoníku. V případě, že daňový doklad takové náležitosti nebude splňovat, bude kupujícím vrácen do dne splatnosti daňového dokladu k opravení bez jeho proplacení. V takovém případě lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nového vyhotovení daňového dokladu.
- 6.10. Všechny faktury dle této kupní smlouvy musí obsahovat odpovídající název a registrační číslo projektu
- Integrovaný regionální operační program Výzva č. 10
 - Název projektu: ZVYŠOVÁNÍ EFEKTIVITY, TRANSPARENTNOSTI A KVALITY SYSTÉMŮ IKT V NEMOCNICI SLANÝ
 - Číslo projektu: CZ.06.3.05/0.0/0.0/15_011/0006951
- 6.11. Pro případ, že prodávající je, nebo se od data uzavření smlouvy do dne uskutečnění zdanitelného plnění stane na základě rozhodnutí správce daně „nespolehlivým plátcem“ ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o DPH, ve znění pozdějších předpisů, souhlasí prodávající s tím, že mu kupující uhradí cenu plnění bez DPH a DPH v příslušné výši odvede za nespolehlivého plátce přímo příslušnému správci daně. V souvislosti s tímto ujednáním nebude prodávající vymáhat od kupujícího část z ceny plnění rovnající se výši odvedeného DPH a souhlasí s tím, že tímto bude uhrazena část jeho pohledávky, kterou má vůči kupujícímu a to ve výši rovnající se výši odvedené DPH.

Čl. 7 Předání a převzetí věci a vlastnické právo, doby poskytování služby

- 7.1. **Prodávající předá kupujícímu** předmět plnění této smlouvy **do dvaceti (20) týdnů** od uzavření této smlouvy jako celek, když však pro jednotlivé části dodávky dle této kupní smlouvy stanoví příloha č. 1 této smlouvy - Technická dokumentace dílčí harmonogram plnění, který musí být ze strany prodávajícího dodržen.
- 7.2. Místem dodání a předání předmětu plnění této smlouvy je adresa sídla kupujícího Politických vězňů 576, 274 01 Slaný, která může být pro dílčí zařízení blíže specifikována v příloze č. 1 této smlouvy.
- 7.3. V souvislosti s dodávkou předmětu koupě zejména v její části týkající se nasazení nové pasivní infrastruktury a nasazení síťových prvků bude docházet k nasazování těchto technologií za plného provozu organizace kupujícího, tedy za plného provozu zdravotnického zařízení - nemocnice. Z tohoto důvodu bude nezbytné ze strany prodávajícího dodržet níže uvedené a to za účelem minimalizace dopadů v souvislosti s dodávkou na výkon činností kupujícího, zejména s ohledem na potřebu neomezení provozu a zachování klidového režimu pro pacienty, zejména na lůžkových odděleních. Jedná se o následující omezení:

- v pracovních dnech budou moci práce na pasivní infrastruktuře probíhat výhradně v časech od 15 do 20 hodin
- o víkendech a dalších dnech pracovního klidu budou moci práce na pasivní infrastruktuře probíhat výhradně v časech od 12 do 20 hodin
- v případě potřeby provedení prací na specializovaných pracovištích nemocnice bude termín realizace práce podléhat odsouhlasení ze strany kontaktní osoby objednatele nejpozději 5 pracovních dnů před zahájením prací na předmětném specializovaném pracovišti
- pro všechny ostatní práce mimo specializovaná pracoviště a dále pro možnost vyžádání si součinnosti pracovníků IT objednatele bude mít dodavatel povinnost veškeré práce v oblasti dodávky pasivní infrastruktury hlásit kontaktní osobě objednatele vždy nejpozději 2 pracovní dny předem
- pro naplnění výše uvedených bodů prodávající kupujícímu před zahájením prací na nasazování aktivních prvků předloží harmonogram ve vztahu k nasazování technologií

- 7.4. Vlastnické právo k předmětu plnění přechází na kupujícího v okamžiku jeho předání prodávajícím a převzetí kupujícím potvrzeného na předávacím protokolu.
- 7.5. Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností předmětu plnění včetně užítka přechází na kupujícího současně s nabytím vlastnictví.
- 7.6. Náklady spojené s předáním předmětu plnění, zejména dopravu, nese prodávající a náklady spojené s převzetím nese kupující.
- 7.7. O předání a převzetí předmětu plnění a souvisejících dokladů bude sepsán předávací protokol podepsaný zástupci obou smluvních stran. Za kupujícího je předávací protokol oprávněn podepsat a předmět plnění převzít Jakub Boček, specialista ICT, Nemocnice Slaný.
- 7.8. Pokud prodávající předmět plnění nedoručí vlastními prostředky, ale využije k tomu dopravce, považuje se za odevzdání věci kupujícímu až okamžik doručení takovým dopravcem. Ustanovení § 2090 a § 2091 zákona č. 89/2012 Sb., občanského zákoníku, se nepoužijí.

Čl. 8 Další práva a povinnosti smluvních stran

- 8.1. Prodávající se zavazuje realizovat předmět plnění této kupní smlouvy v části dodávky a instalace zařízení a licencí prostřednictvím projektového týmu, kterým prokázal kvalifikaci ve veřejné zakázce, na jejímž základě byla uzavřena tato kupní smlouva.
- 8.2. Prodávající se zavazuje zaslat seznam sériových čísel dodaných zařízení a MAC adres síťových karet, a to v elektronické podobě na e-mail kontaktní osoby kupujícího nejpozději do 1 týdne od realizace dodávky.
- 8.3. Prodávající se dále zavazuje předat kupujícímu listinné potvrzení dodaných licencí, které jsou předmětem plnění této kupní smlouvy.
- 8.4. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu (předmětu plnění této smlouvy) včetně účetních dokladů minimálně do konce roku 2029.

- 8.5. Prodávající je povinen minimálně do konce roku 2029 poskytovat požadované informace a dokumentaci související s realizací projektu (předmětu plnění této 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 (předmětu plnění této smlouvy) a poskytnout jim při provádění kontroly součinnost.

Čl. 9 Práva z vadného plnění a smluvní záruka

- 9.1. Kupující požaduje a prodávající se zavazuje držet záruku (včetně záručního servisu) na předmět plnění této smlouvy v rozsahu definovaném v příloze č. 1 smlouvy – Technické specifikaci, kdy je pro každý typ zařízení definován odlišný typ a rozsah požadované záruky.
- 9.2. Záruka na jednotlivá zařízení, která jsou předmětem plnění této smlouvy, počíná svůj běh dnem jejich předání kupujícímu na základě řádně oběma smluvními stranami podepsaného předávacího protokolu.
- 9.3. Prodávajícím poskytnutá záruka v délce uvedené ve specifikaci jednotlivých zařízení obsažených v příloze č. 1 této smlouvy se vztahuje na funkčnost dodaného plnění, jakož i na jeho vlastnosti požadované kupujícím.
- 9.4. Na příslušenství bude prodávajícím poskytována záruka v délce dvou (2) let, nestanoví-li příloha č. 1 této smlouvy u konkrétního příslušenství jinak. V případě vad takového příslušenství se prodávající zavazuje provést opravu nebo věc nahradit novou do 30 kalendářních dnů ode dne nahlášení vady kupujícím v sídle kupujícího, nestanoví-li příloha č. 1 u konkrétního příslušenství jinak.
- 9.5. Po celou záruční dobu na samotná zařízení podle této smlouvy prodávající garantuje kupujícímu přijmout od něj nahlášení poruchy a dle parametrů záruky pro jednotlivé zařízení dle specifikace uvedené v příloze č. 1 této smlouvy garantuje realizaci opravy technikem v místě dodávky.
- 9.6. Prodávající odpovídá kupujícímu za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, stanovené v minimální konfiguraci v technické specifikaci kupujícího a v konečné konfiguraci ve specifikaci obsažené v nabídce prodávajícího.
- 9.7. Prodávající odpovídá kupujícímu dále za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání a že je bez právních a faktických vad. Dále prodávající zaručuje, že na dodaném předmětu smlouvy neváznou práva třetích osob.
- 9.8. Prodávající se zavazuje zajistit, že veškerá komunikace na základě této kupní smlouvy bude z jeho strany vedena v českém jazyce a to včetně uplatňování a řešení závad a reklamací jednotlivých zařízení a licencí na základě této smlouvy.
- 9.9. Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.
- 9.10. Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.

Čl. 10 Smluvní pokuty

- 10.1. Pro případ prodlení se zaplacením kupní ceny se kupující zavazuje uhradit prodávajícímu smluvní pokutu ve výši 0,01 % z fakturované ceny za každý den prodlení.
- 10.2. Pro případ prodlení prodávajícího s dodávkou předmětu plnění této smlouvy v rozsahu a termínech uvedených v této smlouvě se stanovuje smluvní pokuta ve výši 0,1 % z hodnoty dodávky za každý den prodlení.
- 10.3. V případě nedodržení pravidel pro práce související s nasazením nových technologií a pasivní infrastruktury dle čl. 7.3. této smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 2.000,- Kč za nedodržení jakéhokoliv z bodů tohoto článku, a to i opakovaně, včetně například souběžných porušení.
- 10.4. V případě prodlení prodávajícího s odstraněním nahlášené závady ve lhůtě uvedené v čl. 9.5. smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 500,- Kč za každou, i započatou, hodinu prodlení prodávajícího s odstraněním nahlášené závady, max. však do výše 100 % pořizovací ceny daného zařízení.
- 10.5. V případě prodlení prodávajícího s odstraněním nahlášené závady na příslušenství se stanovuje smluvní pokuta ve výši 200,- za každý celý kalendářní den prodlení.
- 10.6. V případě nedodržení složení projektového týmu, kterým je realizován předmět plnění této kupní smlouvy spočívající v dodávce a instalaci zařízení a licencí je oprávněn kupující vyúčtovat smluvní pokutu ve výši 20.000,- Kč za každý případ.
- 10.7. V případě nedodržení komunikace v českém jazyce na základě této smlouvy podle článku 9.8. smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 1.000,- Kč za každý případ.
- 10.8. V případě nedodržení jednotlivých termínů harmonogramu dodávky předmětu koupě stanoveného v příloze č. 1 této smlouvy - Technické dokumentaci, bez ohledu na smluvní pokutu za nedodržení celkového termínu plnění, je kupující oprávněn vyúčtovat prodávajícímu smluvní pokutu ve výši 5.000,- Kč za každý případ.
- 10.9. Zaplacením smluvní pokuty nezaniká povinnost druhé strany závazek splnit a není tím dotčeno právo poškozené strany na náhradu škody, které nesplněním povinnosti vznikla.
- 10.10. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30-ti dnů od doručení jejího vyúčtování.

Čl. 11 Odstoupení od smlouvy

- 11.1. Odstoupení od smlouvy se řídí ustanoveními § 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a dále § 2001 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
- 11.2. Nebude-li uhrazena kupní cena do 60 dnů ode dne splatnosti daňového dokladu prodávajícímu v důsledku zavinění kupujícího a ani do dalších 15 dnů po opakovaném vyzvání prodávajícím k takové úhradě, sjednává si prodávající právo odstoupit od této kupní smlouvy.
- 11.3. Právo odstoupit od této kupní smlouvy má kupující tehdy, jestliže jej prodávající ujistil, že předmět plnění této smlouvy má určité vlastnosti, zejména vlastnosti kupujícím

vymíněné, anebo prodávající kupujícího ujistil, že předmět plnění této smlouvy nemá žádné vady, a toto ujištění se ukáže být nepravdivým.

Čl. 12 Registr smluv - doložka

- 12.1. Prodávající tímto uděluje souhlas kupujícímu k uveřejnění všech podkladů, údajů a informací uvedených v této smlouvě, k jejichž uveřejnění vyplývá pro kupujícího povinnost dle právních předpisů.
- 12.2. Prodávající je současně srozuměn s tím, že kupující je oprávněn zveřejnit obraz smlouvy a jejich případných změn (dodatků) a dalších dokumentů od této smlouvy odvozených včetně metadata požadovaných k uveřejnění dle zákona č. 340/2015 Sb., o registru smluv.
- 12.3. Zveřejnění smlouvy a metadata v registru smluv zajistí kupující.

Čl. 13 Závěrečná ustanovení

- 13.1. Tato smlouva je vyhotovena ve čtyřech (4) výtiscích, každý s platností originálu. Smluvní strany obdrží po dvou vyhotoveních.
- 13.2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv.
- 13.3. Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku.
- 13.4. Přílohami této smlouvy jsou:
- Příloha č. 1 – Technická specifikace zadavatele (kupujícího)
 - Příloha č. 2 – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky, včetně jednotkových cen zařízení
- 13.5. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy na smlouvě.

Za kupujícího

Ve Slaném dne

Za prodávajícího

V Praze dne

.....
MUDr. Štěpán Votoček

ředitel

.....
Milan Hlíňák

předseda představenstva

Příloha č. 1 smlouvy – Technická specifikace zadavatele (kupujícího)

Příloha č. 1 Zadávací dokumentace - Technická dokumentace zadavatele
Příloha č. 1 Kupní smlouvy - Technická dokumentace kupujícího

Technická dokumentace veřejné zakázky a kupní smlouvy s názvem
**„Dodávka technologií za účelem zvýšení kybernetické bezpečnosti -
druhé vyhlášení“**

1 Technická specifikace zadavatele/kupujícího

1	TECHNICKÁ SPECIFIKACE ZADAVATELE/KUPUJÍCÍHO	2
1.1	OBECNÉ POŽADAVKY NA PLNĚNÍ	2
1.2	VAZBA PŘEDMĚTU PLNĚNÍ NA KYBERBEZPEČNOST V PROSTŘEDÍ KUPUJÍCÍHO	5
1.3	POPIS STÁVAJÍCÍHO PROSTŘEDÍ VE VAZBĚ NA REALIZOVANÉ PLNĚNÍ	5
1.4	SPOLEČNÉ MINIMÁLNÍ POŽADAVKY NA DODÁVANÉ ŘEŠENÍ	9
2	SPECIFIKACE JEDNOTLIVÝCH DODÁVEK	10
2.1	FIREWALL 2 KS (CLUSTEROVÉ ŘEŠENÍ K ZAJIŠTĚNÍ VYSOKÉ DOSTUPNOSTI)	10
2.2	AKTIVNÍ PRVKY A JEJICH PŘÍSLUŠENSTVÍ	12
2.2.1	Centrální (hlavní) přepínače - 2 ks	13
2.2.2	Přepínače přístupové - 24 ks	14
2.2.3	Příslušenství přepínačů – optické moduly a kabely	14
2.2.4	Příslušenství přepínačů – softwarová funkcionality – systém pro centrální správu aktivních prvků a ověřování uživatelů (systém zabezpečení síťových portů)	15
2.2.5	Access pointy WiFi - 40 ks	16
2.3	SBĚR A VYHODNOCOVÁNÍ KYBERNETICKÝCH UDÁLOSTÍ - SIEM (SYSTÉM PRO CENTRALIZOVANOU SPRÁVU EVENTŮ A LOGŮ)	17
2.3.1	Server pro SIEM a posílení systémových prostředků	21
2.4	ZABEZPEČENÍ FYZICKÉHO VSTUPU DO SERVEROVNY	21
2.5	MODERNIZACE SPRÁVY ELEKTRONICKÉ POŠTY	22
3	HARMONOGRAM DODÁVKY	25
4	PROJEKTOVÉ ŘÍZENÍ	26
5	ŠKOLENÍ	27

1.1 Obecné požadavky na plnění

Kupující požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky jednotlivých technologií je i návrh způsobu jejich nasazení a konfigurace, úpravy konfigurace dle potřeb kupujícího, doporučení výrobců i tzv. nejlepších praktik.

Součástí služeb implementace bude dále představení nového prostředí uvedeného do provozu s možností ověření jeho funkčnosti kupujícím a to v oblastech provedené konfigurace jednotlivých dodaných technologií. Cena implementačních služeb musí být součástí ceny dodávaných technologií.

Prodávající je povinen zahrnout do nabídky veškeré činnosti a prostředky, které jsou nezbytné pro realizaci předmětu plnění v rozsahu doporučeném výrobcem a dle tzv. nejlepších praktik, i v případě, že nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Pro prokázání naplnění požadavků prodávajícího navrhne prodávající způsob a provedení akceptačních testů. Součástí akceptačních testů musí být pro každou část minimálně:

- Prokázání kompletnosti dodávky a splnění povinných požadavků.
- Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

- Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

Pro každou část dále prodávající navrhne vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Kupující si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Propojení zařízení – SFP moduly a kabely

Všechny dodané technologie musejí být v rámci dodávky propojeny odpovídajícím způsobem a technologií, tedy zejména pro všechny síťové karty jednotlivých zařízení musejí být dodány i SFP a obdobné moduly a kabely do serverovny kupujícího, které takové propojení v kvalitě požadované u každého ze zařízení umožní. V případě 10Gbit karet musí být dodány SFP prvky a kabely umožňující využití této maximální rychlosti karty, v případě jiných rychlostí toto pravidlo musí být dodrženo stejně.

Využití stávajících systémových prostředků - instalace softwarových komponent do prostředí kupujícího - pro poštovní server a SIEM

Instalace řešení a jeho nastavení dle kupujícím odsouhlasené Dokumentace skutečného provedení bude provedena na hardware a software kupujícího. Pro potřebu nasazení a provozu dodávaného řešení budou prodávajícímu poskytnuty systémové prostředky ze strany kupujícího.

Veškeré softwarové komponenty a databáze poběží ve virtualizovaném prostředí kupujícího. Licence serverové virtualizace poskytne kupující. Jedná se o jednotnou platformu virtualizace provozovanou objednatelem v jeho serverovém prostředí (VMware). Proávající musí v rámci své dodávky dodat i odpovídající licence operačního systému potřebných k provozu nabízeného software nad virtualizovanou platformou kupujícího. Veškeré další potřebné licence software potřebného pro běh předmětu plnění musí v rámci své dodávky zajistit a dodat prodávající.

Pro provoz dodávaného řešení tedy všech částí plnění a software na základě této technické dokumentace budou v prostředí kupujícího vyčleněny tyto systémové prostředky, které budou alokovány po dobu min. 5 let a které musí prodávající garantovat, že budou po celou uvedenou dobu naprosto dostatečné, tedy, že za účelem optimálního běhu řešení nebude minimálně po tuto dobu prodávající po kupujícím požadovat navýšení takových systémových prostředků:

- 6 procesorová jádra,
- 128 GiB RAM,
- 1 TiB diskového prostoru (VMware datastore)
- 1 TiB diskového prostoru na úložišti WORM (write one read many) – garantovaném úložišti
- Neomezený počet virtuálních síťových karet do celkové rychlosti 5 Gbit.

Ze strany kupujícího bude dále nasazeno zálohování na úrovni virtuálních strojů, ve kterých dodávané řešení poběží. Nastavení systémových záloh dodávaného řešení bude součástí plnění prodávajícího, když kupující umožní přístup na separátní úložiště pro odkládání takových záloh.

Výše uvedené systémové prostředky jsou prostředky maximálními společnými pro řešení poštovního serveru a SIEM, které kupující ve stávajícím prostředí vyčlenil. Tyto prostředky bude možné dle návrhu prodávajícího v dokumentaci skutečného provedení rozdělit na dva samostatné virtuální servery.

Dokumentace

Součástí předmětu plnění bude i dodávka dokumentace skutečného provedení, která bude před realizací dodávky předána k odsouhlasení kontaktní osobě kupujícího dle kupní smlouvy, na jejímž základě dojde k tomuto plnění. Součástí takové dokumentace musí být uvedení termínů a způsobů provádění jednotlivých dodávek. Po provedení dodávky bude tato dokumentace aktualizována na skutečné provedení, včetně grafické vizualizace nové síťové topologie a jejího řádného popisu co do konkrétních konfigurací jednotlivých zařízení, jejich typu, jejich funkce v rámci vybudovaného síťového prostředí a způsobu jejich správy.

Součástí dokumentace bude zároveň i konkrétní návod na správu sítě včetně postupů obměny/záměny aktivních prvků sítě (přepínačů) a dále postupů na připojování a odpojování jednotlivých koncových zařízení. Pro návrh nové konfigurace sítě musí být respektována, převzata nebo jiným způsobem předpracována pravidla již konfigurovaná v prostředí sítě kupujícího.

Součástí dodávky bude návrh a provedení nastavení odpovídajících politik zejména ve formě VLAN sítí a dále konfigurace FireWallu pro potřebu organizace kupujícího.

Veškerá dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

Předání dokumentace v úplném a řádném rozsahu bude jednou z podmínek akceptace plnění ze strany kupujícího.

Uvedení konkrétních označení a názvů

Pokud tyto zadávací podmínky obsahují požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užité vzory, průmyslové vzory, ochranné známky nebo označení původu, pak je to z důvodů, že se jedná o stávající zařízení v majetku kupujícího a systémy, se kterými musí být nabízené vybavení kompatibilní. V ostatních případech, pokud by se v některé části ZP takové požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užité vzory, průmyslové vzory, ochranné známky nebo označení původu vyskytly, pak je to z důvodů, že stanovení technických podmínek jiným způsobem nemůže být dostatečně přesné a srozumitelné. V

každém takovém případě je v souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, možné nabídnout i jiné, rovnocenné řešení.

1.2 Vazba předmětu plnění na kyberbezpečnost v prostředí kupujícího

Předmět plnění této technické dokumentace je součástí realizovaného projektu kupujícího v oblasti zvýšení kyberbezpečnosti na IT technické úrovni v prostředí kupujícího.

V rámci realizovaného předmětu plnění kupující sleduje naplnění dílčích cílů v následujících oblastech jako jednotlivých opatření pro potřebu naplnění zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, a jeho prováděcích předpisů. Jedná se o následující oblasti

- zajištění fyzické bezpečnosti datových center a technologických místností,
- ochrana integrity komunikačních sítí,
- řízení přístupových oprávnění,
- sběr a vyhodnocení kybernetických události,
- a aplikační bezpečnost.

Prodávající musí předmět plnění realizovat při dodržování výše uvedené legislativy a v takové kvalitě a podobě tak, aby kupujícímu umožnil a zajistil naplnění dílčích opatření v oblasti kyberbezpečnosti minimálně v části dodávek a plnění, které je obsahem této technické dokumentace.

1.3 Popis stávajícího prostředí ve vazbě na realizované plnění

Kupující dále uvádí parametry a technologie v rámci svého IT infrastrukturního prostředí, které je potřeba pro realizované plnění zohlednit a dále které musí být na nové technologie v odpovídající podobě provázáno. Dané provázání je dále u jednotlivých technologií uvedeno v minimální požadované míře (např. vazba na SIEM ze stávajícího serverového vybavení).

Základní přehled

Serverové ICT technologie jsou rozmístěny ve 2 technologických místnostech – serverovnách – umístěných v rámci areálu a propojených optickými vlákny typu single mode. Zařízení jsou umístěna v datovém rozvaděči – racku.

Servery

Současná serverová infrastruktura je postavena na serverech DELL PowerEdge FC630 ve společném šasi Dell PowerEdge FX2 osazeném dvěma síťovými přepínači 10 Gb (každý se 4 externími porty), serverovou virtualizací VMware vSphere 6.

Operační systémy

Většina stávajících virtuálních serverů využívá operační systém Windows 2016 Standard a kupující disponuje klientskými licencemi CAL pro tuto verzi operačního systému.

Identity

Kupující nemá zavedenu centrální databázi identit (adresářovou službu) pro ověřování uživatelů, zařízení a centrální správu.

Antivirová ochrana

Pro ochranu počítačů a serverů kupující využívá antivirový systém ESET Secure s centrální správou.

Diskové úložiště

Pro potřeby ukládání dat je využíváno diskové pole NetApp FAS2650 redundantně připojené k serverům technologií 10 Gb FCoE. Část kapacity diskového pole je konfigurována a využívána jako standardní datastore pro virtuální servery Vmware a část kapacity tvoří tzv. garantované úložiště typu WORM.

LAN

LAN je realizována strukturovanou kabeláží na úrovni CAT5/6. Síťová infrastruktura je aktuálně plochá bez core vrstvy, rychlost je na úrovni 100 Mb, na vybraných místech 1 Gb. LAN není centrálně spravovaná a zahrnuje i starší prvky, které není možné centrálně spravovat.

Firewall

Ochrana sítě je řešena na úrovni zařízení Router Mikrotik CCR1009-8G-1S-1S+ (Rack 20), tzn. že pro novou dodávku FW bude prodávající čerpat aktuální politiky zabezpečení z tohoto zařízení.

Přepínače

V prostředí nemocnice se používají aktivní prvky několika výrobců a od každého v několika modelových řadách:

- **Budova A**
 - přízemí - ARO, RTG, Interna ambulance
 - SW-11 TP-Link TL-SG5426
 - SW-12 TP-Link TL-SG5426
 - Wifi Mikrotik RB951G-2HnD (RTG)
 - Wifi Mikrotik cAP (ARO lůžka)
 - Wifi Mikrotik RB750 (ARO ambulance)
 - 1. patro - interna „A“, Interna JIP
 - SW-15 TP-Link TL-SL2218
 - Wifi Mikrotik RB951G-2HnD (Interna A)
 - Wifi Mikrotik RB2011UiAS-2HnD (Interna A)
 - Wifi Mikrotik RB951G-2HnD (Interna JIP)
 - 2. patro – pokoje doktorů
 - Mikrotik CRS212-1G-10S-1S+
 - SW-3 HP 2530-48G
 - Wifi Mikrotik RB2011UiAS-2HnD (pokoje doktorů)
 - Wifi Mikrotik cAP (interna pokoje doktorů – zasedací místnost)
- **Budova B**
 - suterén – rehabilitace
 - SW-6 TP-Link TL-SG5426
 - přízemí – chirurgie, ortopedie, chirurgie JIP
 - SW-13 TP-Link TL-SL2218
 - Wifi Mikrotik RB2011UiAS-2HnD (ortopedie)
 - Wifi Mikrotik RB2011UiAS-2HnD (ortopedie)
 - Wifi Mikrotik RB2011UiAS-2HnD (kardio ambulance)
 - 1. patro – chirurgie
 - SW-19 TP-Link TL-SL2218 (chirurgie 1)
 - SW-16 TP-Link TL-SL2218 (chirurgie 2)
 - Wifi Mikrotik cAP (chirurgie 1)
 - 2. patro – interna
 - SW-17 TP-Link TL-SL2218 (interna b muži)
 - Wifi Mikrotik RB2011UiAS-2HnD (interna b muži - chodba)
 - Wifi Mikrotik RB750GL (interna b ženy)
 - 3. patro – pokoje doktorů
 - SW-5 TP-Link TL-SG5426

- Wifi Mikrotik RB951Ui-2HnD (chirurgie)
- Wifi Mikrotik cAP (ortopedie)
- Wifi Mikrotik cAP (interna)
- **Budova C**
 - suterén – servery „DC1“
 - SW-1 Aruba 2530-48G (Rack 1)
 - SW-20 HP 2530-24G (Rack 20)
 - SW-21 HP 2530-24G (Rack 20)
 - Router Mikrotik CCR1009-8G-1S-1S+ (Rack 20)
 - SW-Sklep Planet GSW-2404SF (IT kancelář)
 - Wifi Mikrotik RB951Ui-2HnD (IT kancelář)
 - přízemí – laboratoř
 - Wifi Mikrotik cAP (ředitelství)
 - Wifi Mikrotik cAP (laboratoř)
 - Wifi Mikrotik RB941-2nD (diabetologická ambulance)
 - Wifi Mikrotik SXT Lite2 (vysílač do školky Budova G)
- **Budova D**
 - suterén – gynekologie ambulance
 - SW-8 TP-Link TL-SG5426
 - 1. patro – gynekologie, dětské ambulance
 - SW-10 TP-Link TL-SG5426
 - Wifi Mikrotik RB2011UiAS-2HnD (gynekologie chodba u sálů)
 - Wifi Mikrotik RB2011UiAS-2HnD (gynekologie chodba u výtahu)
 - 2. patro – porodnice, dětské odd.
 - SW-14 HP 2530-48G
 - Wifi Mikrotik RB2011UiAS-2HnD (chodba u sálů)
 - Wifi Mikrotik RB2011UiAS-2HnD (chodba u vyšetřovny)
 - Wifi Mikrotik RB2011UiAS-2HnD (chodba u výtahu)
- **Budova E**
 - přízemí – soukromé ambulance
 - SW-24 TP-Link TL-SL2218
 - Wifi Mikrotik cAP (chodba)
- **Budova F**
 - sklad, parní vyvíječ, spol. místnost
 - Wifi Mikrotik RB941-2nD (sklady)
 - Wifi Mikrotik RB951Ui-2HnD (parní vyvíječ)
 - Wifi Mikrotik cAP (společenská místnost)
 - 1. patro – stravovací provoz, pojišťovna
 - SW-18 TP-Link TL-SL2218
 - Wifi Mikrotik RB2011UiAS-2HnD (pojišťovna chodba)
 - 2. patro – mzdy, fakturace
 - SW-9 TP-Link TL-SG5426
 - Wifi Mikrotik RB941-2nD (klient pro tiskárny mzdy)
- **Budova G**
 - suterén – dětská školka
 - SW-22 TP-Link TL-SL2218
 - Wifi Mikrotik cAP
 - přízemí – ubytovna

- Mikrotik RB450G
- Wifi Mikrotik SXT Lite2 (přijímač z budovy C)
- Wifi Mikrotik cAP (chodba ubytovna 1)
- Wifi Mikrotik cAP (chodba ubytovna 2)
- **Budova H**
 - přízemí – vrátnice, doprava
 - SW-7 TP-Link TL-SL2218
 - Wifi Mikrotik RB951G-2HnD
- **Budova J**
 - přízemí – lékárna
 - SW-23 TP-Link TL-SG5426
 - Wifi Mikrotik RB951Ui-2HnD (přízemí)
 - Wifi Mikrotik RB951Ui-2HnD (1. patro)
- **Budova L + Komín**
 - přízemí – „mazut“
 - Mikrotik RB750GL (switch pro zadní závoru a kameru)
 - komín
 - Mikrotik RB260GS (opticko-metalický převodník)



Přepínače jsou v mnoha případech za hranicí své morální životnosti. Stávající stav neumožňuje nastavit a bezpečně spravovat ověřování uživatelů přistupujících do sítě (technologie 802.1x).

1.4 Společné minimální požadavky na dodávané řešení

V této části jsou uvedeny povinné parametry prvků nabízeného řešení.

Účastník ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek.

Účastník uvede konkrétní technické parametry nabízeného zboží, včetně uvedení výrobce a obchodního / typového označení jednotlivých komponentů – ke každé nabízené komponentě (s výjimkou příslušenství) budou uvedeny údaje o výrobcí a obchodním (nebo typovém) označení.

Konkrétní parametry jednotlivých komponent účastník buď vypíše nebo je doloží např. formou katalogových listů – v takovém případě ale musí být uveden jasný a přehledný odkaz na část nabídky, ve které je možné splnění parametrů ověřit.

Popis způsobu naplnění každého povinného parametru musí být konkrétní, úplný a musí jasně prokazovat, že nabízené řešení jednoznačně naplňuje požadované parametry.

V případě, že by zadávací podmínky obsahovaly požadavky nebo odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užité vzory, průmyslové vzory, ochranné známky nebo označení původu, které by vedlo ke zvýhodnění určitých dodavatelů nebo určitých výrobků, zadavatel v takových případech výslovně umožňuje pro plnění VZ použití i jiných, kvalitativně a technicky rovnocenných řešení. Zadavatel v některých částech Technické specifikace označuje konkrétními názvy přístroje, software a technologie, které v současné době využívá, a pro které požaduje s nově pořizovanými přístroji plnou kompatibilitu, a to z důvodu ochrany předchozích investic zadavatele a využitelnosti těchto přístrojů. Jedná se tedy o konkrétní označení stávajících zadavatelem využívaných přístrojů, se kterými požaduje kompatibilitu (nikoliv o označení výrobků, které mají být předmětem dodávky).

Požadavky na dodávky konkrétních typů a verzí operačních systémů vycházejí z důvodu potřeby organizace na udržení logické koherence její stávající infrastruktury, kompatibility se stávajícími programy a z důvodu nezvyšování nákladů na přeškolení uživatelů při případném přechodu na jiný software. Zaměstnanci organizace jsou na tento software již vyškoleni a použití jiného SW by jí a jejím zaměstnancům způsobilo mimořádné obtíže z důvodu znesnadnění obsluhy, ztráty času dodatečným zaškolováním na jiný SW, nekompatibility s ostatním zařízením v organizaci, a tím i zvýšené náklady.

2 Specifikace jednotlivých dodávek

2.1 Firewall 2 ks (clusterové řešení k zajištění vysoké dostupnosti)

Prodávajícím bude dodáno nové řešení FireWallu pro zajištění ochrany komunikačního systému v podobě LAN. To musí být implementováno v podobě pokročilého, tzv. Next generation firewallu, který je oproti běžnému síťovému firewallu vybaven sadou bezpečnostních funkcionalit, které jsou obvykle sdruženy pod pojmem UTM (Unified threat management). Kupující požaduje dodávku firewallů minimálně s následujícími parametry (pro 1 kus):

Parametr	Popis povinného parametru
Provedení	pro montáž do 19" racku, výška max. 1U
Porty	min 20x 1GbE, z toho min. 2x WAN, 2x heartbeat pro cluster (HA - high availability), 2x 1Gb SFP, USB pro ext. modem (záložní konektivita)
Agregace portů	podpora slučování portů (linková agregace) včetně virtuálních portů (VLAN) a portů pro heartbeat clusteru, podpora LACP
Propustnost	min. 4 Gbps pro libovolnou velikost paketu
Počet současných spojení	min. 2 milióny
Interní úložiště	Interní úložiště typu SSD pro ukládání logů a akceleraci výkonu (cache), kapacita min. 400 GB
Propustnost SSL VPN	min. 200 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 50 klientů
Propustnost IPS	min. 500 Mbps pro reálný podnikový provoz (údaje označované výrobcí např. jako Realworld, Enterprise mix apod.) s aktivním logováním
Propustnost antivir	min. 250 Mbps pro reálný podnikový provoz (údaje označované výrobcí např. jako Realworld, Enterprise mix apod.) s aktivním logováním
Propustnost NGFW	min. 350 Mbps min. 500 Mbps pro reálný podnikový provoz (údaje označované výrobcí např. jako Realworld, Enterprise mix apod.) s aktivním logováním. NGFW - aktivní firewall, IPS, aplikační kontrola
Propustnost SSL inspekce	min. 120 Mbps při běžném HTTPS provozu a obsahu
Virtualizace	min. 8 virtuálních kontextů (virtuálních firewallů)
Vysoká dostupnost	režimy Active/Passive i Active/Active se společnou konfigurací (cluster)
Dualstack	podpora současného běhu IPv4 a IPv6
Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,...)
Antivir	antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd)
Kategorizace a blokáce provozu	založená na kategorizaci webového obsahu aktualizované výrobcem a uživatelsky upravitelné, možnost monitorování a blokování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určité době během dne
Antispam	antispamová a antivirová inspekce elektronické pošty
Bezpečnost	automatická aktualizace UTM funkcí poskytovaná výrobcem zařízení
SSL akcelerace	Integrovaná hardwarová akcelerace SSL, HTTPS publikovaného obsahu
DLP	integrovaná ochrana dat DLP (data lost prevention), automatické i ruční značkování souborů (kontrolní součet nebo jiný unikátní identifikátor, použití značek v bezpečnostních pravidlech/politikách)
Ověřování uživatelů	interní databáze, LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, TACACS+, Ověřování na základě certifikátu, podpora skupin
Management a monitoring	HTTP/S, SSH, SNMP, syslog,
Sledování toků	export síťových toků (Netflow nebo ekvivalent)
Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů
Rozšířená bezpečnost	integrovaný Sandbox - kontrola podezřelého kódu spuštěním v reálných operačních systémech přímo ve firewallu nebo v externím systému poskytovaném výrobcem
SD-WAN	integrovaná podpora softwarově definovaných WAN (SD-WAN) - https://en.wikipedia.org/wiki/SD-WAN
VPN portál	Možnost sestavení uživatelské VPN prostřednictvím integrovaného konfigurovatelného portálu. Portálové aplikace pro bezpečný přístup k interním zdrojům bez nutnosti sestavení VPN min. pro aplikace/protokoly http/s, RDP, SMB, SSH, VNC
Záruční servis a podpora	min. 60 měsíců v režimu 24x7. Odeslání náhradního zařízení max. následující den po nahlášení závady, včetně nároku na aktualizace firmware, bezpečnostní signatury UTM (URL filtrace, IPS, antimalware, antispam, aplikační kontrola) a Sandboxu

Dodávané řešení musí zajistit trvalou ochranu sítě firewallem a musí proto být implementováno jako vysoce dostupné řešení v podobě clusteru dvou firewallů umístěných v různých lokalitách (technologických místnostech). S automatickým převzetím služeb vadného (či jinak nedostupného) firewallu záložním firewallem.

Součástí funkčního vybavy firewallu dále musí být schopnost exportu detailních informací o průchozím provozu, jeho charakteru, aplikovaných komunikačních a bezpečnostních pravidlech i o stavu samotného systému a také schopnost exportu síťových toků v podobě tzv. netflow. Uvedené schopnosti musí umožnit úzkou integraci s nástrojem pro sběr, detekci a vyhodnocení kybernetických bezpečnostních událostí, který je další částí předmětu plnění této technické dokumentace, a tato integrace bude jako součást plnění tohoto předmětu plnění provedena v maximální možné míře.

Firewall dále musí být vybaven rozhraním příkazové řádky dostupné zabezpečeným protokolem SSH, které umožní dávkové změny konfigurace pomocí skriptů (a to např. i z nadřazených systémů).

Jako součást dodávky technologie provede prodávající minimálně následující služby a práce, které s dodávkou technologie bezprostředně souvisí:

- analýza stávajícího řízení internetového provozu, návrh jeho optimalizace a uplatnění nových funkcionalit dodávaného firewallu,
- implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) dle návrhu,
- vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu,
- respektování min. 3 různých skupin uživatelů (uživatelé, správci, hosté) v návrzích a implementaci bezpečnostních a ostatních politik,
- konfigurace blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele/skupinu
- zavedení DNSSEC pro interní DNS služby i zabezpečení domén kupujícího
- autentizace uživatelů vůči Active Directory
- zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách,
- zavedení IPv6 pro publikované služby z interních či externích prostředků. Včetně zajištění jednání a řízení změn u externích poskytovatelů služeb. Jde zejména o služby hostování domén, DNS, e-mail, web,
- zabezpečení publikovaných služeb – SSL, HTTPS, e-mail apod. za využití možností dodávaného firewallu
- na nové firewally budou migrovány veškeré podporované funkcionality a konfigurace stávajících firewallů a budou zprovozněny příslušné next-generation služby,
- provedení akceptačních testů včetně výkonových testů.

Záruka a podpora:

- Záruční servis min. 5 let v režimu 24x7. Odeslání náhradního zařízení max. následující den po nahlášení závady,
- Nárok na aktualizace firmware, bezpečnostní signatury UTM (URL filtrace, IPS, antimalware, antispam, aplikační kontrola) a Sandboxu

Záruka a podpora budou hrazeny jednorázově společně s dodávkou zařízení na výše uvedenou dobu.

2.2 Aktivní prvky a jejich příslušenství

V rámci stávající síťové topologie dojde k nasazení nových hlavních i přístupových přepínačů, které zajistí komplexní a plošné nasazení technologie 802.1x v síťovém prostředí kupujícího s následujícím minimálním počtem zařízení

- 200 ks koncových stanic,
- 100 ks síťových koncových zařízení (tiskárny, modality apod.)
- 6 ks fyzických serverů.

Celé výše uvedené licencování musí umožnit užití minimálně 350 uživateli, což je předpokládaný počet uživatelů kupujícího.

Do celé LAN kupujícího bude jako součást plnění naimplementováno řízení přístupu k médiu (síti) na základě rolí a členství v uživatelské skupině adresářové struktury Active Directory za využití technologie 802.1x nad dodanými aktivními prvky.

Prodávající provede nad dodanými aktivními prvky dodávku a implementaci systému centrální správy, který poskytne celkový pohled na stav a konfiguraci LAN jako celku a současně umožní centrálně provádět změny konfigurace prvků LAN (stávajících i nově dodaných ve finální podobě a konfiguraci LAN na základě realizace plnění této technické dokumentace) a vytvořením jednotně spravovaných VLAN zavést segmentaci sítě. Součástí dané centrální správy bude i systém řízení přístupu zařízení a uživatelů do LAN (jako komunikačního systému kupujícího) založený na standardu IEEE 802.1x.

Prodávající jako součást dodávky provede konfiguraci ověřování přístupu do LAN prostřednictvím protokolu 802.1x vůči adresářové službě za využití protokolů RADIUS a P/EAP. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet); konečné určení omezení přístupu bude rozhodnuto kupujícím v době přípravy konfigurace řešení před jeho nasazením.

Pro koncová zařízení bez podpory standardu 802.1x musí být ze strany prodávajícího dodáno a implementováno jiné řešení způsobu jejich ověřování založeného na kombinaci více identifikátorů zařízení (např. MAC adresa, typ zařízení, výrobce, operační systém, hostname apod.)

Součástí dodávky je dále i vzorová konfigurace 802.1x na všech typech standardních koncových zařízení kupujícího a dále detailní dokumentace jak dané standardní typy koncových zařízení v souladu s 802.1x nasazeným na úrovni aktivních prvků konfigurovat.

Ze stávajícího síťového vybavení prodávající převezme nasazenou konfiguraci, tuto konfiguraci vlastními silami analyzuje, za možnosti podávání doplňujících dotazů kupujícímu ve vztahu, proč jsou vybrané konfigurace provedeny ve stávající infrastruktuře daným konkrétním způsobem, a dále nad provedenou analýzou prodávající navrhne a kupujícímu předloží k odsouhlasení nasazení upravené topologie sítě a nasazení nových technologií konfigurace, správy a řízení sítě. Kupující požaduje, aby toho bylo dosaženo primárně nasazením VLAN (802.1Q), segmentací sítě s přepínáním provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Dále musí dojít k nasazení řízení provozu na úrovni kvality služeb za využití technologie QoS (Quality of Services). Dále pro zajištění vysoké dostupnosti služeb musí být klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy. Kupující dále upozorňuje prodávajícího, že jednotlivé prvky jsou a budou umístěny v různých lokalitách areálu kupujícího a v těchto lokalitách bude nezbytné nasadit nové technologie a služby LAN dle potřeb v jednotlivých koncových lokalitách areálu kupující na adrese sídla kupujícího, a to nejen např. co do počtu ethernetových portů zařízení, ale i služeb LAN v dané lokalitě v areálu a dále i dispozic pro umístění jednotlivých technologií (zdroj el. energie a dispozice v podobě umístění v místnosti a velikosti určeného prostoru).

Jako součást dodávky technologie provede prodávající minimálně následující služby a práce, které s dodávkou technologie bezprostředně souvisejí:

- analýza stávajícího síťového prostředí a návrh nové architektury LAN,

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

- implementace dodávaných technologií,
- provedení segmentace LAN – VLAN, adresování, routování,
- návrh a implementace 802.1X pro LAN včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů – PC, notebooky, chytré telefony, tablety, tiskárny – Windows, Linux, MacOS, Android, IOS, embedded systémy síťových tiskáren. Systém 802.1x musí být integrován s adresářovou službou Active Directory,
- zavedení systému centrálního dohledu a správy dodávané infrastruktury včetně jednotného managementu,
- provedení akceptačních testů včetně výkonových testů.

2.2.1 Centrální (hlavní) přepínače - 2 ks

Prodávajícím budou dodány a implementovány síťové přepínače ve vysoce dostupné konfiguraci (stohu) rozloženém do různých lokalit (technologických místností), který bude tvořit logické jádro (core) lokální sítě. Core bude sloužit současně pro přenos běžných síťových dat (propojení serverů a klientů) i jako SAN (storage area network) pro přenos blokových dat mezi servery a diskovými úložišti. Core bude také zajišťovat rychlé směrování mezi VLAN.

Kupující požaduje dodávku přepínačů minimálně s následujícími parametry (pro 1 kus):

Parametr	Popis povinného parametru
Provedení	Velikost zařízení 1RU
Určení	výkonný L2/L3 přepínač, včetně routování IPv4 a IPv6, plně spravovatelný,
Porty	Počet portů min. 48x 10 Gb SFP+, 6x 40 Gb QSFP+, samostatný port pro out-of-band management
Porty 100 Gb	Podpora 100 Gb QSFP28 portů – min. 2 QSFP+ porty lze osazením QSFP28 modulů provozovat na rychlosti 100 Gb. Při použití takové konfigurace nemusí být ostatní QSFP+ porty využitelné.
Propustnost	Neblokovaná architektura, přepínací a směrovací kapacita min. 1440 Gbps
Redundance	Interní redundantní napájecí zdroje a ventilátory vyměnitelné za provozu (součást dodávky)
Paměť	Dostatečná kapacita RAM pro využití jako CORE přepínač – vyrovnávací paměť paketů min 10 MB, minimální počet záznamů tabulek: ARP – 60 000, MAC 200 000, IPv4 routování 8 000, IPv6 routování 8 000
VLAN	Min. 1024 současných VLAN včetně směrovaných rozhraní, podpora VXLAN
Správa front	Podpora standardu 802.1ad Q-in-Q včetně Selective Q-in-Q
Velké pakety	Podpora „jumbo“ rámců min. 10000 Bytes
Řízení provozu	Podpora QoS – zařazování dle MAC, IP, VLAN, typu protokolu, portu, aplikace a DSCP
Ověřování uživatelů a zařízení	Podpora 802.1x včetně dynamického přiřazování do VLAN a RADIUS
Automatizace	Podpora SDN (Software defined networking) – standard OpenFlow nebo obdobný
Dualstack	Podpora IPv4 a IPv6 – dual stack, IPv6 over IPv4, 6to4, ISATAP Tunnel. Včetně směrování a QoS.
Stohování	Podpora rozšířeného stohování po 40 a 100 Gb portech min. 4 přepínačů (technologie ekvivalentní s technologiemi VSS, IRF nebo VirtualChassis) - stoh se chová jako jeden přepínač/router z pohledu správy i připojených zařízení
Linková agregace	Agregace portů napříč stohem, podpora LACP
IGMP	Podpora IGMP včetně řízení – IGMP, IPv4 a IPv6 PIM a MLD snooping
Ochrana DHCP	DHCP snooping
Modulární upgrade	Podpora In-Service Software Upgrades (ISSU) pro upgrade firmware stohu
Blokové přenosy	podpora protokolů standardu Data Center Bridging (DCB) – min. Priority-based Flow Control (PFC), Data Center Bridging Exchange (DCBX)
Správa	Plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní.
Interoperabilita	Podpora protokolu OVSDB (Open vSwitch Database)
Zrcadlení portů	Podpora zrcadlení portů do vzdáleného přepínače přes L2 i L3 (tzv. RSPAN and ERSPAN)

Záruka a podpora:

- Záruční servis min. 5 let. Oprava do 2 pracovních dnů v místě instalace.
- Nárok na aktualizace firmware a podporu výrobce

Záruka a podpora budou hrazeny jednorázově společně s dodávkou zařízení na výše uvedenou dobu.

2.2.2 Přepínače přístupové - 24 ks

Přístupové stohovatelné Ethernet přepínače s neblokující architekturou o velikosti max. 1 RU, kompatibilní s nabízenými centrálními přepínači. Maximální přípustná hloubka zařízení je 35 cm, z důvodu stávajícího rackového vybavení a jeho dispozice v areálu nemocnice kupujícího. Je požadována podpora pro trvalou provozní teplotu 45°C nebo vyšší. Kupující požaduje dodávku přepínačů minimálně s následujícími parametry (pro 1 kus):

Parametr	Popis povinného parametru
Provedení	Velikost zařízení 1RU
Určení	výkonný L2/L3 přepínač, včetně směrování IPv4 a IPv6, plně spravovatelný,
Porty	Počet portů min. 24x 1 GbE PoE+, 4x 10 Gb SFP+
Propustnost	Neblokovaná architektura, přepínací a směrovací kapacita min. 128 Gbps
Redundance	Možnost doplnění redundantního napájecí zdroje (není součástí dodávky)
Paměť	Dostatečná kapacita RAM – vyrovnávací paměť paketů min 1,5 MB, minimální počet záznamů tabulek: MAC 16 000, IPv4 směrování 250, IPv6 směrování 250
VLAN	Min. 1024 současných VLAN včetně směrovaných rozhraní
Správa front	Podpora standardu 802.1ad Q-in-Q včetně Selective Q-in-Q
Velké pakety	Podpora „jumbo“ rámců min. 9000 Bytes
Řízení provozu	Podpora QoS – zařazování min. dle MAC, VLAN, IP, VLAN, typu protokolu, portu, aplikace a DSCP
Ověřování uživatelů a zařízení	Podpora 802.1x včetně dynamického přiřazování ACL a do VLAN, podpora RADIUS
Automatizace	Podpora SDN (Software defined networking) – standard OpenFlow nebo obdobný
Dual stack	Podpora IPv4 a IPv6, včetně směrování a ACL
Stohování	Podpora rozšířeného stohování po 10 Gb SFP+ portech min. 7 přepínačů (technologie ekvivalentní s technologiemi VSS, IRF nebo VirtualChassis) - stoh se chová jako jeden přepínač/router z pohledu správy i připojených zařízení
Linková agregace	Agregace portů napříč stohem, podpora LACP
IGMP	Podpora IGMP včetně řízení – IGMP, MLD snooping
PoE	Podpora PoE+ standardu IEEE 802.3at na metalických portech, min. 30W/port, celkový výkon PoE min. 370W
Alokace výkonu	Konfigurovatelná alokace výkonu PoE - automaticky, dle třídy IEEE 802.3af, dle LLDP-MED či manuálně
Hlasové VLAN	Automatické přiřazení IP telefonů do "hlasové" VLAN
Efektivita	Podpora standard IEEE 802.3az pro snížení energetické náročnosti
Správa	Plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní.
Zrcadlení portů	Podpora zrcadlení portů do vzdáleného přepínače (tzv. RSPAN)

Záruka a podpora:

- Záruční servis min. 5 let. Oprava do 2 pracovních dnů v místě instalace.
- Nárok na aktualizace firmware a podporu výrobce

Záruka a podpora budou hrazeny jednorázově společně s dodávkou zařízení na výše uvedenou dobu.

2.2.3 Příslušenství přepínačů – optické moduly a kabely

Následující tabulka specifikuje minimální požadovanou sadu optických prvků pro realizaci předmětu. Vyžaduje-li řešení nabízené prodávajícím pro plně redundantní propojení všech klíčových prvků (servery, diskové úložiště, přepínače) další optické prvky, zahrnuje je prodávající do své nabídky.

Cena jednotlivého příslušenství musí být zanesena do ceny nově dodávaných zařízení v rámci tohoto předmětu plnění, s jehož souvislostí bude příslušenství dodáno, spolu s ním bude na základě realizovaného plnění i fakturováno.

Kupující požaduje dodávku příslušenství přepínačů minimálně s následujícími parametry:

Parametr	Popis povinného parametru
SFP+ moduly	58 ks modulů SFP+ 10 Gb, SM, min. 10 km, včetně DMI diagnostiky pro nabízené centrální přepínače 48 ks modulů SFP+ 10 Gb, SM, min. 10 km, včetně DMI diagnostiky pro nabízené přístupové přepínače 4 ks modulů SFP+ 10 Gb, SM, min. 10 km, včetně DMI diagnostiky pro Dell FN410S přepínač 4 ks modulů SFP+ 10 Gb, SM, min. 10 km, včetně DMI diagnostiky pro NetApp FAS2650, 4 ks modulů SFP+ 10 Gb, SM, min. 10 km, včetně DMI diagnostiky pro nabízený server
SFP moduly	2 ks modulů SFP 1 Gb, SM, min. 10 km, včetně DMI diagnostiky pro nabízené centrální přepínače
QFSP+ moduly	4 ks modulů QSFP+ 40 Gb, SM, min. 10 km, včetně DMI diagnostiky pro nabízené přístupové přepínače

Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení

Patch kabely	Ke každému modulu optický patch kabel 2 m, konektory SC – dle nabízených modulů
--------------	---

Záruka a podpora:

- Záruční servis min. 3 roky.

Záruka bude hrazena jednorázově společně s dodávkou zařízení na výše uvedenou dobu.

2.2.4 Příslušenství přepínačů – softwarová funkcionalita – systém pro centrální správu aktivních prvků a ověřování uživatelů (systém zabezpečení síťových portů)

Pro zajištění jednotné evidence a správy identit navrhne a vybuduje prodávající vysoce dostupnou (min. 2 řadiče) adresářovou službu Active Directory a zajistí její naplnění uživatelskými účty. Systém pro centrální správu aktivních prvků a ověřování uživatelů bude s vybudovanou adresářovou službou propojen a bude ji využívat pro autentizaci i autorizaci zaměstnanců a jejich koncových zařízení zařazených do Active Directory.

Pro vybudování adresářové služby není možné poskytnout stávající licenci OS stávajícího majoritního serverového operačního systému Windows kupujícího. Potřebnou licenci OS proto musí prodávající v potřebném rozsahu zahrnout do ceny své dodávky.

Kupující požaduje dodávku řešení (uceleného systému) minimálně s následujícími parametry (pro 1 kus):

Parametr	Popis povinného parametru
Centrální správa aktivních prvků	
Provedení	Management nástroj pro správu sítě s plnou podporou správy nabízených přepínačů
Virtuální prostředí	Správa virtuálních sítí vytvářených na úrovni hypervizorů (podpora VMware), přehled o spojení virtuální a fyzické vrstvy
Rozpoznání sítě	Ruční i automatická detekce a inventarizace zařízení, mapování topologie (L2, L3, VLAN, spanning tree apod.), včetně vyhledávání
Vizualizace	Logické pohledy (L2, L3, VLAN, virtuální šasi, stohy apod.), vizualizace topologie, vizualizace datového centra (racky, přepínače, servery apod.), tvorba vlastních hierarchických pohledů
Audit zařízení	Typ zařízení včetně jednotlivých komponent, verze operačního systému, sériová čísla, informace o jednotlivých portech, historický audit jednotlivých zařízení (např. přesuny), vyhledávání a historie zařízení na základě MAC, IP nebo názvu
Správa ACL	Správa access listů, pravidel a šablon, jejich zálohování a nasazení. Podpora optimalizace, tj. snižování náročnosti zpracování pravidel na výkon prvků.
Automatizace	Možnost tvorby SNMP, TELNET a SSH šablon pro hromadný přístup k zařízením
Správa konfigurací	Zálohy a obnova konfigurace, ukládání historie, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel, centrální aktualizace firmware zařízení. Alerting při změně konfigurace prvku.
Správa výkonu	Nástroje pro diagnostiku a plánování – sumární a okamžité pohledy na provoz, trendy, sledování zátěže, dostupnost zařízení i linek, vytížení procesoru, využití operační paměti, vytížení linek. Tvorba SNMP statistik-dlouhodobých a historických i real-time grafy. Importování vlastních MIB databází a kompilátor
Správa VLAN	Globální změna nastavení, přidávání, přiřazení portů
API	Otevřené rozhraní pro integraci s dalšími systémy
Logy	Bezpečnostní systém analýzy logů
Bezpečnost	Správa přístupových oprávnění a rolí (administrator, operátor) na úrovni jednotlivých zařízení a jejich funkcí. Možnost přizpůsobení ovládacího prostředí pro každého uživatele systémem widgetů nebo obdobným.
Alerty	Alarmy, práce se syslog a SNMP trapy včetně vytváření vlastních reakcí na události nebo notifikace ve formě emailu
Monitorování	Vestavěné monitorování funkčnosti služeb – min. DNS, FTP, HTTP, TCP/UDP, VoIP, SMTP, DHCP, ICMP, Radius, TACACS+
Kompatibilita	plná podpora nabízených přepínačů, alespoň základní podpora výrobců třetích stran (roznání, ověření funkce, vzdálená správa)
Licence	Min 50 spravovaných aktivních prvků
Ověřování uživatelů	
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
Autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, podpora TACACS+ autentizace správců síťových zařízení
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC
Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google, Facebook, Twitter, LinkedIn
Autorizace	Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v Active Directory

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

Parametr	Popis povinného parametru
Single-sign-on	Podpora Single Sign-On - min SAML 2, Oauth
Komplexní autorizace	Autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období
Dynamická autorizace	Podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení.
Izolace klientů	Zpracovávání syslog zpráv z externích zdrojů, vyhledávání definovaných událostí a automatizovaná reakce na ně. Minimálně v rozsahu příjmu zpráva z nabízeného firewallu a izolace konkrétního klienta na základě těchto zpráv.
Zpracování syslog	Vestavěná podpora tvorby a úprav vlastních parserů syslog zpráv pro napojení na další systémy třetích stran
Rozšířené informace	Podpora sběru rozšířených informací o připojovaných zařízeních (např. DHCP parametry, HTTP agent, IP parametry, typ zařízení apod.) a jejich využití v autorizačních politikách
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení
Portál	Captive portál pro pacienty a návštěvy a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně.
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (např. jen potvrzení uvítací/informační stránky.
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem apod.
Vysoká dostupnost	Podpora rozšíření o druhý nod pro sestavení vysoce dostupného clusteru (druhý nod není součástí dodávky)
API	Otevřené API pro integraci s dalšími systémy
Provedení	Virtuální appliance pro stávající virtualizační platformu
Licence	Licencování pro min. 500 současně ověřených zařízení bez omezení počtu uživatelů

Záruka a podpora:

- Nárok na aktualizace software a podporu výrobce po dobu 60 měsíců

Záruka a podpora bude hrazena jednorázově společně s dodávkou systému na výše uvedenou dobu.

2.2.5 Access pointy WiFi - 40 ks

Kupující požaduje dodávku dvoupásmových bezdrátových WiFi Access Pointů (AP). Současný provoz v pásmech 2,4 GHz a 5 GHz dle Wi-Fi standardů 802.11n a 802.11ac Wave2, připojení pomocí 1x GLAN port s napájením pomocí PoE. Odběr proudu musí být v rámci možností dodávaných LAN přepínačů.

Zařízení musí zajistit:

- Současný provoz více SSID
- Možnost rozdílné implementace 802.1x autentizace pro různá SSID
- Jednotný management
- Vestavěné bezpečnostní a monitorovací funkce
- Centrální správa všech AP jako jednoho uceleného řešení, automatická konfigurace nově přidaných APOD.

Služby WiFi sítě musí být autonomní bez závislosti na službách provozovaných uvnitř LAN. Síť LAN bude použita pouze pro přenos dat a napájení AP.

Kupující požaduje dodávku AP minimálně s následujícími parametry:

Parametr	Popis povinného parametru
Základní funkce	Přístupový bod (AP) WiFi včetně montážního materiálu na stěnu nebo strop
Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly
Anténní systém	25 kusů s interním systémem min. MIMO 3x3 (5 GHz) a min, MIMO 2x2 (2,4 GHz) optimalizovaným pro montáž na strop 15 kusů s externím systémem min. MIMO 3x3 (5 GHz) a min, MIMO 2x2 (2,4 GHz) optimalizovaným pro montáž na stěnu
Standardy	Podpora IEEE 802.3at, 802.11n, 802.11ac Wave 2, 802.1x včetně přiřazování do VLAN
Řízení klientů	Automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)
Rušení	Průběžná detekce non-WiFi rušení a spektrální analýza
Multi SSID	Podpora vysílání min. 6 SSID (WiFi sítí) současně (každé radio), podpora přiřazení každého SSID samostatné VLAN

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

Parametr	Popis povinného parametru
Zatížení	Min. 250 přiřazených (asociovaných) klientů na radiový modul
Porty	Min. 1x 1Gb, PoE s podporou standardů IEEE 802.3at a 802.3af
Úsporné napájení	Podpora standardu 802.3az - Energy-Efficient Ethernet (EEE)
Řízení provozu	Klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu
Řízení kvality služeb	Automatické řízení kvality služeb (QoS) pro hlas a video
Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output
Přenosové rychlosti	SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO min. 850 Mb
Bezpečnost	Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu a schopnost jejich potlačení
Zabezpečení	Podpora WPA2 a WPA3 (Wi-Fi Protected Access)
Virtuální kontroler	Virtuální, vysoce dostupný kontroler součástí firmware všech AP. Umožňuje kompletní a centrální správu WiFi infrastruktury a řízení jejího provozu.
Monitoring a správa	Plná podpora CLI, SSH, SNMP 3, syslog, web rozhraní
Správa frekvenčního pásma	Automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference
Roaming	Spolehlivý rychlý roaming (přepínání mezi AP) klientských zařízení na L2 (2. vrstvě OSI). Podpora standardů IEEE 802.11r, 802.11v, 802.11k
Optimalizace	automatická předávání klientských zařízení mezi AP pro maximalizaci propustnosti a rozložení zátěže

Záruka a podpora:

- Záruční servis min. 5 let. Oprava do 2 pracovních dnů v místě instalace.
- Nárok na aktualizace firmware a podporu výrobce po dobu záručního servisu

Záruka bude hrazena jednorázově společně s dodávkou systému na výše uvedenou dobu.

2.3 Sběr a vyhodnocování kybernetických událostí - SIEM (systém pro centralizovanou správu eventů a logů)

Prodávající dodá a naimplementuje nástroj pro sběr a vyhodnocování kybernetických událostí, který bude automaticky sbírat, normalizovat, analyzovat a archivovat logy a data síťových toků bezpečnostní povahy napříč celou infrastrukturou kupujícího od síťových prvků přes různé operační systémy až po aplikace (minimální výčet zařízení a prvků, které prodávající v rámci dodávky na dodaný SIEM (Security and Incident Event management) prováděje je obsažen v této technické dokumentaci). SIEM bude nasazen nad všemi zařízeními uvedenými v této technické dokumentaci, tedy součástí plnění je i konfigurace těchto zařízení spočívající v předávání předmětných logů do SIEMu a to v části dodávky nových zařízení i zařízení stávajících, která jsou v konkrétní podobě v této technické dokumentaci obsažena rovněž (za účelem konfigurace předávání logů do SIEM bude kupujícím prodávajícímu umožněn přístup a zásah do stávajících technologií, které mají být na SIEM navázány). Nad těmito daty pak bude dodané řešení provádět pokročilou analýzu, korelace a notifikace vyhodnocených bezpečnostních událostí, fenoménů a incidentů. SIEM bude dodán a nakonfigurován tak, aby automaticky analyzoval logy, vyhledával bezpečnostní události a nad těmito událostmi dále prováděl korelace. Zpracování dat bude SIEMem prováděno a konfigurováno v následujícím minimálním rozsahu a způsobu:

- Online sledování – filtrování pohledů na události podle zařízení, uživatele nebo dalších atributů, vyhledávání,
- Korelace událostí – normalizace, klasifikace a korelace událostí v čase z jednoho nebo více zdrojů,
- Upozornění (alerty) – na základě definovaných pravidel budou generována upozornění, která mohou být odeslána emailem nebo zobrazena interaktivně v grafickém rozhraní systému,

- Akce – za vygenerovaným alertem může následovat automatická akce pro aktivní nápravu nalezeného stavu (např. restart služby).

Řešení musí poskytovat aktuální přehled o potencionálních i skutečných anomáliích, hrozbách a bezpečnostních incidentech sledovaného prostředí. SIEM k nim poskytne zdrojová data pro daný kontext a optimálně také (v běžných/známých) případech i návrh řešení. SIEM bude řízen sadou pravidel vzniklých z předem popsanych modelových situací, která budou pro standardní situace dodány a aktualizovány výrobcem a pro specifické situace a systémy organizace vytvořeny prodávajícím a vlastními specialisty. SIEM bude pravidelně informovat o stavu systémů automaticky i ručně generovanými reporty. Ty budou předdefinované podle obvyklých standardů, jako jsou PCI DSS, HIPAA, ISO 27000 nebo uživatelsky definované. Konkrétní návrh dané konfigurace navrhne prodávající kupujícímu, když kupující bude moci přispět návrhy na další reporty dle vlastních potřeb a zkušenosti s informačními systémy provozovanými v jeho prostředí. Návrh ze strany prodávajícího bude předcházet implementaci software do prostředí kupujícího.

Jako součást dodávky technologie provede prodávající minimálně následující služby a práce, které s dodávkou technologie bezprostředně souvisejí:

- detailní analýza a identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné popř. vhodné sbírat, korelovat a analyzovat
- analýza bude obsahovat následující oblasti specifické pro řešení:
 - specifikace profilu pro každý napojovaný zdroj dat, včetně určení vhodné úrovně detailu logování, odpovídající jeho roli v infrastruktuře,
 - klasifikaci zdrojů informací pro stanovení priority události (stejná událost z různých zdrojů může mít různou prioritu) a z hlediska poskytovaných logů (obsažené informace, struktura logu),
 - doporučení nastavení logování pro jednotlivé zdroje,
 - výběr událostí a parametry jejich záznamů a metody sběru z jednotlivých zdrojů,
 - návrh parserů pro zdroje, které nebudou systéme přímo podporovány,
 - návrh doplňování logovaných informací z dalších zdrojů pro zlepšení jejich relevantnosti či srozumitelnosti,
 - metody a pravidla identifikace, zpracování a vyhodnocování událostí, návrhy korelací,
 - pravidla pro vznik varování, upozornění, incidentů včetně priority,
 - doporučenou strukturu oprávnění a řízení přístupových práv
 - proaktivní a reaktivní procesy (aktivity, role, výstupy, doba odezvy) v případě výskytu varování, upozornění, incidentu a apod.
 - popis zajištění autentičnosti logů,
 - definice pohledů na události v konzoli uživatelů (např. setřídění událostí podle zdroje, typu, priority, stupně důležitosti, času vzniku apod.),
 - návrh zálohování konfigurace a dat,
 - návrh průběhu Zkušebního provozu pro ověření funkčnosti systému v reálném provozu,
 - návrh retence logů a archivů s využitím stávajícího WORM úložiště včetně související rekonfigurace úložiště
 - popis monitorovaných aktivit přispívajících k naplnění požadavků dle zákona č.101/2000 Sb. v aktuálním znění a k naplnění požadavků dle Nařízení evropského parlamentu a rady EU 2016/679 o Zabezpečení zpracování osobních údajů (GDPR),
- návrh a provedení konfigurací dotčených a souvisejících systémů
- návrh a provedení akceptačních testů, musí zahrnovat výkonové testy, testy archivace a obnovy logů a ověření detekce jejich neoprávněné modifikace

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

- implementace systému bude provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.
- návrh a provedení akceptačních testů k ověření dodané a implementované funkcionality.

Kupující v rámci svého stávajícího prostředí požaduje konfiguraci prodávajícím za účelem předávání logů a dalších hlášení i u následujících zařízení a software:

- serverové operační systémy Windows, včetně domény a Active Directory
- virtualizační řešení VMware
- zálohovací software Veeam
- storage NetApp FAS2650
- síťové přepínače Dell PowerEdge FN410S
- servery DELL PowerEdge FC630, Dell T420

Kupující požaduje dodávku SIEM minimálně s následujícími parametry:

Parametr	Popis povinného parametru
Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií
Ovládání	Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídicí konzole s jednotným GUI.
Správa prvků	Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat - logů a událostí.
Skupiny Prvků	Podpora zařazování Prvků do skupin/kategorií dle vlastností (typ, operační systém, dostupné služby, síť apod.) i metadat (umístění, hodnota apod.)
Metadata Prvků	Možnost konfigurace metadat Prvku - min. hodnota, priorit a spolehlivost (věrohodnost) událostí
Monitorování Prvků	Automatické monitorování stavu Prvku - min. dostupnost poskytované služby a základní dostupnost (odezva na ping)
Vyhledávání Prvků	Víceparametrové vyhledávání a filtrování Prvků podle vlastností i metadat, export do souboru v běžném strojově zpracovatelném formátu (např. csv, xml apod.)
Vazby	Detekce síťových prvků standardními protokoly a mapování jejich vazeb
Detekce zranitelností	Automatická ruční i plánovaná detekce zranitelností Prvků (i nezařazených) - porovnání stavu Prvků s databází známých zranitelností průběžně aktualizovanou výrobcem
Profily zranitelností	Vestavěné i uživatelsky definované profily detekce zranitelností - definice typů zranitelností, které mají být kontrolovány.
Autentizace	Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému Prvku.
Detekce průniku	Víceúrovňová detekce průniku (intrusion detection) - min. na úrovni sledování síťového provozu a na úrovni Prvků.
Instalace agentů	Podpora vzdálené instalace ID agentů (intrusion detection) min. pro operační systémy Microsoft Windows
Detekce průniku - assety	Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů, rootkitů či obdobného škodlivého kódu
Detekce průníků - síť	Analýza monitorovaných síťových toků a detekce anomálií indikujících možné narušení bezpečnosti politiky (NBA - Network Behavior Analysis)
Síťové toky	Monitorování síťových toků technologií netflow (min. verze 5,9,10) či kompatibilní (ipfix, netstream) dle nabízených přepínačů a firewallů.
Síťové toky hypervizor	Podpora sledování síťových toků virtuálních síťových přepínačů VMware vSphere
Viditelnost síťových toků	Viditelnost síťového provozu - zobrazení, prohledávání, filtrování síťových toků včetně historie
IP reputace	Integrovaná služba aktualizovaná výrobcem ohodnocující reputaci a spolehlivost veřejné IP adresy s možností změny priorit událostí, alarmů apod. Reputace založena na detekovaných (aktivitách IP adresy (spam, skenování, phishing, distribuce malware, botnet apod.
Protokoly	Podporované protokoly min. syslog, windows events collection (pomocí agenta i bezagentově (např. WMI), snmp, s/ftp, nfs, cifs, netflow
Ukládání logů	Bezpečné ukládání logů s řízeným přístupem v nezměněné (nefiltrované) podobě (tzv. raw logy)
Zpracování logů	Centrální zpracování logů, jejich normalizace, korelace, grafická interpretace a archivace, včetně logů generovaných samotným řešením
Rozšíření logů	Vytváření vlastních atributů v událostech. Automatické doplňování atributů aktuálními hodnotami z externích zdrojů. Podpora atributů v celém systému - vyhledávání, filtrace, korelace atd.

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

Parametr	Popis povinného parametru
Prohledávání logů	Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání
Expirace logů	Podpora automatické rotace raw logů s nastavením doby expirace
Zálohování logů	Podpora zálohování logů na externí síťové úložiště
Ochrana logů	Zajištění integrity raw logů aplikací digitální podpisu. Možnost jednoduchého uživatelského ověření integrity
Centralizace logů	Konsolidace logů na jednom centrálním místě.
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě
Doplňování názvů	Automatické doplňování reverzních DNS a hostname záznamů k IP adresám.
Identifikace MAC	Automatické doplňování výrobce zařízení podle MAC adresy
Grafy událostí	Grafické znázornění událostí - četnost, typ, časová osa
Parsery	Možnost vytváření uživatelských parserů bez nutnosti externí spolupráce
Ladění parserů	On-line ladění uživatelsky vytvářených parserů v reálném čase- okamžité zobrazení rozparovaných dat při vložení testovací zprávy/události.
Standardizace logů	Standardizace přijatých logů do jednotného formátu, parsování parametrů do předepsaných polí
Pohledy	Předpřipravené pohledy a podpora vytváření vlastních pohledů na data uživateli a jejich ukládání pro pozdější využití a zpracování dat. Včetně grafické reprezentace dat - grafy, mapy apod.
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových reportů. Včetně grafické reprezentace dat - grafy, mapy apod.
Upozornění	Zasílání uživatelsky vytvořených upozornění podle uživatelsky definovaných podmínek. Možnost zahrnutí přijatých rozparovaných dat do upozornění.
Správa uživatelů	Správa uživatelů systému musí být integrovatelná s MS Active Directory. Systém musí umožňovat i přihlašování pomocí lokálních účtů při nedostupnosti Active Directory. Podpora granularního (lokálního) nastavení uživatelských oprávnění
Tikety	Možnost vytváření tiketů k bezpečnostním událostem s možností přiřazení řešiteli. Možnost sledování průběhu tiketů včetně historie - obsah, vykonané činnosti, eskalace. Podpora jednoduchého manuálního vytváření tiketů v průběhu vyšetřování incidentu.
Automatizace tiketů	Tickety lze vytvářet automaticky na základě vytvořené politiky k jednotlivým událostem / zranitelnostem.
Politiky	Podpora vestavěných a tvorby vlastních komplexních politik zpracování událostí - Politiky musí umožnit spustit minimálně následující akce: odeslání emailu, vytvoření ticketu, spuštění skriptu.
Korelace	Podpora korelací událostí na základě definovaných parametru bez závislosti na typu zdroje. Vestavěné a výrobcem aktualizované korelace, podpora vytváření vlastních
Rozšířené korelace	Systém musí umožňovat tvorbu korelací nejen napříč zdroji, ale také napříč daty z interních subsystémů (např. detekce zranitelnosti, průníků, IP reputace). V závislosti na datech interních subsystémů je případně upravena vážnost incidentu (oproti standardní korelaci).
Upozornění	Podpora vytváření upozornění (alertů) na základě korelovaných událostí včetně zahrnutí rozšířených korelací. Vestavěná upozornění i podpora ručního vytváření.
IT Compliance	Podpora compliance (jednání v souladu s pravidly") - certifikace dle obvyklých bezpečnostních standardů a norem PCI DSS, HIPAA
Auditní reporty	Vestavěné, výrobcem aktualizované šablony reportů pro podporu kontrolních a certifikačních auditů - min. dle standardů PCI DSS, HIPAA, NIST CSF, ISO 27001
Legislativa	Systém musí zajistit bezpečné, úplné a nepochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č.316/2014 Sb. (VKB), o kybernetické bezpečnosti, a to v platných zněních
Provedení	Centrální část systému bude realizována jako jedna virtuální appliance
Licence	Licence pro min. 150 sledovaných systémů (Prvků), bez licenčního omezení velikosti aktivních i archivních dat či jiných funkcionalit systému.
Výkon	Trvalé zpracování min 1000 EPS (events per second - událostí za sekundu)
Škálovatelnost	Možnost zvýšení výkonu doplněním dalších appliance pro sběr dat a vykovávání funkcí systémů, popřípadě rozdělením systému na více serverů.
Vysoká dostupnost	Integrovaná podpora pro možnost doplnění dalšího systému (nodu) a sestavení clusteru – min. 2 systém min, režim active/passive

Záruka a podpora:

- Nárok na podporu výrobce a nové verze software, včetně aktualizací bezpečnostních a funkčních signatur (zranitelnosti, korelační pravidla, detekce průniku, detekce Prvků (typy zařízení, aplikace, operační systémy), aktualizací reportů po dobu 2 let.

Záruka a podpora bude hrazena jednorázově společně s dodávkou systému na výše uvedenou dobu.

2.3.1 Server pro SIEM a posílení systémových prostředků

Pro zajištění trvalého běhu SIEM, který zajistí záznam a analýzy událostí požaduje kupující dodávku serveru do (záložní) technické místnosti. Tím dojde k navýšení systémových prostředků tak, aby byl zajištěn provoz SIEM při výpadku systémových prostředků v hlavní technické místnosti.

Dále kupující požaduje navýšit operační paměť RAM dvou stávajících server Dell FC630 o 128 GB (každý server), a to s ohledem na potřebu zachování kompatibility se stávajícím serverovým prostředím a využitím jeho již existujících a připravených technologií.

Licenci virtualizačního software pro dodávaný server a možnost jeho provozu ve stávající virtualizované farmě (VMware) kupujícího poskytne prodávajícímu kupující, a proto tato licence nebude součástí tohoto předmětu plnění.

Kupující požaduje dodávku serveru minimálně s následujícími parametry:

Parametr	Popis povinného parametru
Provedení	rackové provedení max. 1U včetně výsuvných kolejnic a montážního materiálu do racku
CPU	1 x procesor, 16 fyzických jader Výkon procesoru dle https://www.cpubenchmark.net/ min. 19 000 bodů
RAM	128 GB, min. 2600 MT/s
Úložiště	Min. 2x SSD 240 GB, hardwarový RAID1, provedení M.2 v PCI slotu (nezabírá pozice HDD) - pro hypervizor VMware ESXi
LAN	LAN 4x 10Gb SFP+ s podporou virtualizace - VMware NetQueue. Podpora NIC partitioning (NPAR), FCoE offload, iSCSI offload, RDMA RoCEv2
USB	min. 3 USB konektory - min. 1x verze 3.0, min. 1x umístění na čelním panelu s podporou bootování, min. 1x interní
Management	Servisní modul s možností samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora http/s, ssh, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace)
Provozní podmínky	Určen pro provoz v běžném neklimatizovaném prostředí do 40 (nárazově až 45) stupňů Celsia
Napájení	2x napájecí zdroj, redundance, min. Platinum specifikace dle 80 PLUS https://cs.wikipedia.org/wiki/80_Plus
Management	Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozních stavů či parametrů (min. napájení, teplota, vada HDD. Aktivní indikace standardního provozního stavu. V případě závady zobrazuje její popis v textové formě.

Záruka a podpora:

- Záruční servis min. 5 let. Oprava do druhého pracovního dne v místě instalace.
- Nárok na aktualizace firmware a podporu výrobce po dobu záručního servisu

Záruka a podpora bude hrazena jednorázově společně s dodávkou systému na výše uvedenou dobu.

Pro posílení systémových prostředků požaduje kupující dodávku modulů RAM minimálně s následujícími parametry:

Parametr	Popis povinného parametru
RAM	8 ks 32 GB originální RAM modul pro server Dell FC630, min. 2400 MT/s

Záruka a podpora:

- Dodané moduly musí být kryté zárukou výrobce serveru, v němž budou instalovány, po celou dobu platnosti záruky serveru bez ohledu na délku trvání

Záruka a podpora bude hrazena jednorázově společně s dodávkou systému na výše uvedenou dobu.

2.4 Zabezpečení fyzického vstupu do serverovny

Prodávající pro kupujícího provede dodávku a instalaci **4 kusů** IP kamer včetně objektivů a licence software pro správu, archivaci a analýzu záznamů z dodaných kamer.

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

Kupující pro možnost instalace kamer zajistí v místě jejich umístění dostupnost UTP a 220V infrastruktury ze svého stávajícího prostředí.

Samotné kamery budou umístěny ve dvojicích tak, aby vždy pro každou ze dvou technologických místností zajistili pohled na vchod do místnosti a dále na samotné technologie. Technické místnosti jsou dle rozpisu obsažené na úvod této technické dokumentace v suterénu budovy C a v budově A ve druhém patře.

Prodávající provede pro kupujícího konfiguraci a uvedení celku kamer a software do rutinního provozu - záznamu lokalit prostřednictvím kamer a jeho zpracovávání a vyhodnocování prostřednictvím dodaného softwarového řešení.

Kupující požaduje dodávku kamerového systému minimálně s následujícími parametry:

Parametr	Popis povinného parametru
Kamery	
Provedení	IP dome kamera, vnitřní provedení včetně montážního materiálu na strop/zeď
Rozlišení	4 Mpx (2688x1520) nativně
Objektiv	2.8 - 12 mm, manuálně nastavitelný pro čip 1/3.2" nebo odpovídající pro větší čip (menší není přípustný)
Světelnost	F 2.2 nebo lepší při nejméně příznivém nastavení objektivu, automatické řízení clony
Napájení	PoE (spotřeba do 10W) a samostatný napájecí konektor, včetně napájecího adaptéru
Porty	LAN min. 100 Mb
Přísvit	infračervený, min. 20 m, min. 8x LED
Protisvětlo	Korekce protisvětla, resp. široký dynamický rozsah (WDR – wide dynamic range)
Data, ukládání	min. streamy H.264, lokální ukládání na SD kartu. Karta min. 32 GB součástí dodávky
Rozlišení, snímková frekvence	min. 2560x1440, 24 fps při zapnutém WDR. Min. 3 datové streamy s nezávislým nastavením kvality obrazu
Zvuk	vestavěný mikrofon
Detekce událostí	Detekce pohybu (min. 4 nezávislá okna), periodické události, demontáž kamery
Kompatibilita	Podpora standardu ONVIF
Obslužný software	
Provedení	Profesionální systém pro sledování, záznam a centrální správu IP kamerového systému
Přístupy	Integrovaná správa uživatelů a oprávnění, podpora Active Directory
Zobrazení	Podpora maticového zobrazení (min. 4 x 4 okna) přehrávaných záznamů i živých streamů na jednom monitoru
Vzdálený přístup	Vzdálený přístup k nahrávacímu serveru prostřednictvím webového rozhraní i "tlustého" klienta
Události	Podpora upozornění a událostí za nabízených kamer
Přehlednost	Integrovaná "živá" mapa pro přehled o rozmístění kamer možností prokliku (aktivace) náhledu obrazu kamery přímo v mapě
Pokročilé funkce	Detekce překročení hranice, detekce shlukování, sledování vyznačených oblastí apod.
Detekce událostí	Detekce pohybu (min. 4 nezávislá okna), periodické události, demontáž kamery
Optimalizace	Pokročilé způsoby řízení záznamu a snížení datových nároků (detekce událostí/pohybu vyvolá zvýšení rychlosti/kvality nahrávání)
Operační systém	Provoz v prostředí Windows nebo virtuální appliance VMware
Kompatibilita	zvýšení rychlosti/kvality nahrávání)
Retence	Správu nahrávek včetně automatické retence nahrávek po určené době.

Záruka a podpora:

- Záruční servis min. 3 let. Oprava hardware do deseti pracovních dnů
- Nárok na aktualizace firmware a nové verze software po dobu záručního servisu

Záruka a podpora bude hrazena jednorázově společně s dodávkou na výše uvedenou dobu.

2.5 Modernizace správy elektronické pošty

V rámci předmětu plnění prodávající dodá a implementuje systému elektronické pošty s plnohodnotnou podporou groupwarových funkcí (správa kontaktů, kalendářů, schůzek, úkolů apod.) a zabezpečením e-mailového provozu před škodlivým a obtěžujícím kódem. Zabezpečení bude realizováno jako min. dvouúrovňové s využitím odpovídajících bezpečnostních funkcí nabízeného firewallu pro jednu z úrovní. Součástí zabezpečení budou i kontroly a optimalizace nastavení souvisejících systémů (DNS, firewall, zálohování apod.) dle doporučených postupů výrobce systému.

*Veřejná zakázka s názvem
Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení*

Za účelem efektivního využití systému prodávající v rámci předmětu plnění provede napojení na MS Active Directory v prostředí kupujícího. Součástí této integrace dle standardizované služby AD společnosti Microsoft bude i revize konfigurace a struktury uživatelů a skupin uživatelů za účelem optimalizace předmětné struktury pro napojení poštovního serveru na služby AD. Součástí návrhu revize struktury AD bude i provedení potřebných úprav na základě odsouhlasení kupujícího.

Pro provoz poštovního serveru není možné poskytnout stávající licenci OS stávajícího majoritního serverového operačního systému Windows kupujícího. Potřebnou licenci OS proto musí prodávající v potřebném rozsahu zahrnout do ceny své dodávky.

Kupujícím pro provoz daného řešení bude prodávajícímu poskytnuta licence virtualizace (VMware) a zálohování (Veeam), tedy technologie stávající, na nichž je serverové prostředí kupujícího vybudováno.

Kupující požaduje dodávku systému správy elektronické pošty minimálně s následujícími parametry:

Parametr	Popis povinného parametru
Systém elektronické pošty	
Základní funkce	Zajištění elektronické komunikace včetně e-mailů, správy kontaktů a úkolů, organizace času a poznámek včetně sdílení údajů na základě nastavitelných oprávnění a jejich delegace
Podpora MS Office	On-line spolupráce uživatelů s nativní vazbou na klienta Microsoft Outlook a řešení Microsoft Office s možností plnohodnotné off-line práce klienta systému.
Úložiště	K ukládání dat musí systém využívat integrované databázové úložiště a umožnit jeho replikaci v režimu vysoké dostupnosti.
Podpora AD	Integrace s Microsoft Active Directory včetně načítání vztahu nadřízený - podřízený
Skupiny	Dynamické komunikační skupiny – automatické plnění dle přednastavených pravidel
Správa	Centralizovaná správa pomocí grafického rozhraní i prostřednictvím příkazové řádky a skriptů.
Politiky	Možnost nastavení centrálních transportních a retenčních (správa a udržování dat) politik.
Rozhraní	Webové rozhraní pro klienty i svěřenou administraci v českém jazyce.
Šifrování	Licencované prostředí pro plný počet uživatelů se zabezpečeným (SSL šifrovaným) přístupem a možností práce se šifrovanými zprávami.
Synchronizace	Automatická zabezpečená plná synchronizace Microsoft Outlook přes internet bez nutnosti připojení přes VPN.
Automatizace	Automatická konfigurace klientů při použití Microsoft Outlook a mobilních klientů Android a IOS.
Protokoly	Podpora protokolů MAPI, POP, IMAP, SMTP a zabezpečení SSL a PKI. Plná podpora Active Sync
Ochrana dat	Ochrana dokumentů - implementace transportních pravidel a DRM (Document Rights Management). Ochrana proti ztrátě citlivých dat - DLP (data lost protection)
Diagnostika	Integrovaní průvodci pro řešení problémů, nástroje pro analýzu stavu systému.
Řízení schránek	Podpora globálních i uživatelských nastavení schránek - limity pro velikost obsahu, odeslaných zpráv, nastavení zastupitelnosti
Delegace oprávnění	Delegace oprávnění pro určité oblasti správy na vybrané uživatele (například aktualizace osobních údajů a kontaktů na personální oddělení) jednoduchým způsobem, přes webové rozhraní nebo přímo z prostředí MS Outlook.
Sdílení	Sdílené adresáře, složky, kalendáře. Delegace oprávnění pro sdílení osobních složek mezi uživateli.
Rezervace	Podpora rezervací a plánování zdrojů - zasedací místnosti, vozidla apod.
Vyhledávání	Indexování, plnohodnotné rychlé fulltextové vyhledávání v klientu i webovém rozhraní
Mobilní zařízení	Podpora synchronizace mobilních zařízení (smartphone, tablety) s možností definovat a aplikovat politiky pro přístup pouze schválených zařízení, vynucení přístupu pomocí kódu PIN apod.
Bezpečnost	Podpora vzdáleného vymazání mobilního zařízení uživatelem i administrátorem při ztrátě či kompromitaci.
Licence	1 server, 200 zařízení, 350 uživatelů
Zabezpečení systému elektronické pošty	
Základní funkce	Antivirová a antispamová (anti-x) ochrana komunikačního systému pošty
Integrace	Integrace s nabízeným komunikačním systémem - ukládání spamů do složky „Nevyžádaná pošta“ uživatelů
Architektura	Lokální provoz (není přípustné přesměrování MX záznamů mimo prostředky zadavatele)
Logování	Integrované detailní logování a analýzy veškeré komunikace včetně všech prováděných kontrol
Bezpečnost	Poskytování obvyklých detekčních a obranných technik proti spamu (SBL, RBL, white/black listy, graylisting, Bayes filtr, DKIM, heuristiku, Sender ID, SPF, Phishing filtr, Backscatter), blokování a výjimky dle běžných pravidel založených na IP adresách, typech souborů, typech obsahu, doménách, jazycích/zemích apod.
Antivir	Systém musí poskytovat antivirovou kontrolu a ochranu průchozí elektronické komunikace
Kompatibilita	Systém musí být možno provozovat jako služba na Windows Serveru
Licence	1 server, 200 zařízení a 350 uživatelů komunikačního systému

Záruka a podpora:

- Nárok na podporu výrobce a opravné verze software včetně aktualizací bezpečnostních signatur po dobu 5 let.

Záruka a podpora bude hrazena jednorázově společně s dodávkou na výše uvedenou dobu.

3 Harmonogram dodávky

Kupující požaduje realizaci předmětu plnění dle následujícího harmonogramu. Harmonogram je sestaven tak, aby jednotlivé práce na sebe logicky navazovaly a zároveň byl v souladu s požadavky výzvy číslo 10 IROP, ze které má být předmět plnění spolufinancován (s ohledem na termín dokončení předmětu plnění). S ohledem na možnost kontroly realizace plnění z pohledu času (tj. dílčí vyhodnocování dodržování harmonogramu realizace) je harmonogram doplněn milníky. Započetí každého milníku je možné pouze za předpokladu, že bude provedena akceptace všech milníků předcházejících, s výjimkou přípravných prací, k nimž není potřeba součinnosti pracovníků kupujícího. To je vyžadováno zejména s ohledem na omezené kapacity pracovníků kupujícího a potřebu řízeného přístupu k realizaci jednotlivých prací.

Harmonogram plnění

1. Dodávka a instalace aktivních prvků v podobě Firewallů a síťových přepínačů - do 5 týdnů od uzavření kupní smlouvy
2. Dodávka a instalace prvků zajištění fyzické bezpečnosti datových center a technologických místností - do 7 týdnů od uzavření kupní smlouvy
3. Dodávka a instalace poštovního serveru - do 9 týdnů od uzavření kupní smlouvy
4. Dodávka a instalace sběru a vyhodnocování kybernetických události (SIEM) - do 20 týdnů od uzavření smlouvy

4 Projektové řízení

Jako součástí plnění jsou požadovány pravidelné projektové schůzky v sídle kupujícího min. 1× každých 21 dní a dále ad-hoc pracovní schůzky k problematice řešení jednotlivých částí plnění, včetně projednání a odsouhlasení výstupů pro konfiguraci a nastavení jednotlivých částí plnění pro potřebu kupujícího.

S ohledem na rozsah plnění a dopad jeho zavedení do produkčního provozu na výkon činnosti kupujícího je v rámci předmětu plnění kupujícím požadováno aplikování základních principů projektového řízení ze strany prodávajícího. Jedná se zejména o řízení projektových prací v souladu s uzavřenou smlouvou s ohledem na:

- věcné plnění – rozsah, posloupnost a hloubku prací,
- závazný harmonogram projektu – dodržování termínů v harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem ke kupujícímu, aktivní řešení výše uvedených nestandardních situací).

Dále se jedná o zpracování pravdivých, úplných a věcně jasných a vypovídajících zápisů ze všech konzultačních a projektových schůzek a pracovních jednání (s cílem zaznamenání klíčových rozhodnutí, ujednání, navržených nebo dohodnutých způsobů řešení dílčích částí projektu atd.). Uvedené zápisy budou zpracovány během schůzek a jednání, případně budou zpracovány a předány kupujícímu nejpozději do dvou pracovních dnů po těchto jednáních.

5 Školení

Prodávající zrealizuje v sídle kupujícího prezenční zaškolení pro IT administrátory kupujícího minimálně v rozsahu provozní dokumentace. Školení bude pokrývat všechny komponenty dodávané v rámci předmětu plnění, a to minimálně v rozsahu:

- běžných administrátorských činností pro implementovaná řešení,
- standardní údržby řešení pro administrátory kupujícího,
- základní identifikace nestandardních stavů řešení a jejich příčin.

Minimální požadovaný rozsah zaškolení pro administrátory je 24 hodin.

Předpokládaný počet administrátorů – účastníků školení – je max. 5

Kupující pro účely zaškolení zajistí a zpřístupní učebnu vybavenou notebooky, prezentační technikou (ve smyslu projektor, tabule pro psaní / kreslení) a dále zajistí konektivitu do vnitřní sítě kupujícího.

Příloha č. 2 - Technická specifikace z nabídky účastníka (prodávajícího)

7 Technický popis nabízených komponent

7.1 Fortinet FG-101E

FortiGate - firewall, zabezpečení internetu, VPN

FortiGate appliance jsou primárním Fortinet produktem pro firewall a VPN. Tvoří jádro zabezpečení přístupu do internetu a celé zabezpečovací infrastruktury sítě. FortiGate zařízení řídí speciálně vyvinutý operační systém FortiOS 4. Obrovskou výhodou FortiGate produktů je, že většinu funkcí nalezneme již v základním modelu FortiGate-50B.

FortiGate appliance nabízí několik úrovní zabezpečení pro širokou škálu aplikací a typů obsahu včetně webu, e-mailu, FTP, IM/P2P a NNTP. Mezi hlavní funkce FortiGate zařízení patří:



- Firewall, VPN (virtuální privátní síť IPSec a SSL VPN), Traffic Shaping
- Intrusion Prevention System IPS (detekce průniku do systému)
- Antivirus, Antispyware, Antimalware
- Web Filtering (kontrola webového obsahu)
- Antispam
- Application Control (např. IM nebo P2P síť)
- podpora VoIP (H.323 a SCCP)
- směrování na 2/3 vrstvě
- **FSAE** (aktivní ověřování uživatelů vůči Active Directory)
- Dual WAN (záloha nebo load balancing primárního připojení do internetu se sekundárním)
- Data Loss Prevention DLP (prevence proti úniku informací)
- WAN optimization (optimalizace datových toků a akcelerace výkonu linky)
- Network Access Control NAC (kontrola koncových stanic)
- Vulnerability management
- High Availability HA v režimu active/active nebo active/passive (vysoká dostupnost zajištěná spojením dvou a více FortiGate)
- Virtual Domain VDOM (rozdělení jednoho fyzického FortiGate do více virtuálních)
- Wireless Controller

FortiGate v současnosti představuje produkt s nejrozsáhlejší sadou bezpečnostních a síťových služeb v rámci jednoho zařízení na dnešním trhu.

7.1.1 Antivirus a Antispyware

Ve FortiGate produktech nalezneme až čtyři kanály, jakými se lze bránit proti malware. První tři jsou tři proxy-based antivirové databáze. Jako čtvrtou možností je použití antivirové ochrany přímo v datových tocích, tím je tak zajištěna nezávislost kontroly na velikosti kontrolovaného souboru. Dále je možné nastavit úroveň kontroly antiviru a tím tak flexibilně řídit požadavky na výkon nebo vyšší zabezpečení.



7.1.2 WAN Optimization (WAN optimalizace)

WAN Optimization (WAN optimalizace) poskytuje akceleraci pro aplikace procházející přes pomalejší konektivity, které jsou zpravidla spoje typu WAN. V kombinaci s multi-threat security, optimalizací datových toků (traffic optimization) a VPN technologiemi poskytuje zabezpečenou a rychlou komunikaci.



7.1.3 Application Control (aplikační kontrola)

Application Control (aplikační kontrola) používá dynamický aplikační identifikační modul, který rozpoznává aplikace na základě jejich chování. Ve spojení aplikační kontroly s dalšími bezpečnostními politikami a funkcí traffic shaping mohou administrátoři dosáhnout komplexnější ochrany. Vše lze aplikovat na jednotlivé aplikace nebo skupiny aplikací. K dispozici je i analýza popularity jednotlivých aplikací a logování provozu/využití šířky pásma.



7.1.4 Data Loss Prevention (prevence proti úniku informací)

Data Loss Prevention (DLP) pracuje na základě nalezené shody v podporovaných protokolech. Za pomoci této služby je možné chránit firemní síť proti úniku citlivých informací. Mezi podporované protokoly patří: e-mail (SMTP, IMAP, POP3, SMTPS, IMAPS, POP3S), HTTP(S) (POST, GET), FTP (PUT, GET), NNTP, IM (AIM, ICQ, MSN, Yahoo), session control. DLP technologie dále umožňuje vykonávat auditorské požadavky, které jsou vyžadovány v legislativě.



7.1.5 SSL Inspection (SSL inspekce)

SSL Inspection (SSL inspekce) zajišťuje ochranu před malwarem, která může být maskována zabezpečenými protokoly. SSL inspekce dešifruje SSL komunikaci a na dešifrovanou komunikaci pak mohou být použity všechny bezpečnostní kontroly.



7.1.6 Web Filtering (filtrování webu)

Fortinet Web Filtering kategorizuje více než 57 miliónů webových stránek do více než 75 kategorií. Na základě zařazení stránek do jednotlivých kategorií mohou administrátoři jednoduše zablokovat přístupy na všechny stejně tématicky laděné weby. Je také možné přidělovat časové kvóty jednotlivým uživatelům pro přístup na jednotlivé skupiny webových stránek.



7.2 HPE FlexFabric 5710 48SFP+ 6QSFP+ or 2QSFP28

Datasheet v Angličtině

Řada přepínačů HPE Flex Fabric 5700 je řada vysoce výkonných přepínačů s vysokou hustotou, špičkovou latencí a špičkou "ToR", která je součástí řešení HPE FlexFabric společnosti Hewlett Packard Enterprise (HPE) FlexNetwork .

Ideální pro nasazení na serverové přístupové vrstvě velkých podnikových datových center. Řada přepínačů HPE 5700 je navržena tak, aby poskytovala cenově výhodné řešení, které je stále dostatečně výkonné, aby zvládlo nárůst virtualizovaných aplikací a přenosu ze serverů na server, splňuje potřeby zákazníků, kteří nyní vyžadují inovace ToR, pro vyšší výkonnost připojení k serveru,

konvergenci Ethernetu a úložiště dat, schopnost pracovat s virtuálními prostředím a velmi nízkou latencí v jednom zařízení.

Management:	Fully Managed
Layer 3 Dynamic:	L2 switching / L3 Static routing / RIP routing
48x 10/100/1000 RJ45 portů + 4x 1000/10000 SFP+ porty + 2x OSPF+	
IRF stacking	až 9 switchů do stohu
Redundantní zdroje	Nejsou součástí balení. Nutno dokoupit zvlášť – JG900A, JG901A, JC680A, JC681A nebo JH336A
Redundantní větráky	Nejsou součástí balení. Nutno dokoupit zvlášť – JC682A nebo JC683A



7.2.1 Technické parametry

Porty	48SFP+ 6QSFP+ or 2QSFP2
Paměť a CPU	1 GB flash, 4 GB SDRAM
Velikost bufferu :	12 MB
Latence:	<1.5 μs (64-byte packet)
Propustnost :	1 071 Mpps
Kapacita switchování:	1 440 Gbps
Vstupní napětí:	100 VAC–240 VAC
Výkon:	74W
Rozměry v palcích (H x W x D)	1.73" × 17.32" × 15.75"

7.3 HPE 5130 24G PoE+ 4SFP+ EI

Série **výkonných přepínačů**, které svými vlastnostmi a širokou nabídkou bezpečnostních technologií vyhoví nárokům větších firem a uskupení. Přístroj nabízí **firemní úroveň QoS, stohování, podporu třetí vrstvy**, RIP i fixních **10GbE uplinků**. Switche využívají výhod **IPv6** řešení a energeticky úsporných technik.

7.3.1 Vylepšená kontrola nad síťovým provozem

Majitel tohoto přepínače dostane do rukou **vylepšený QoS nástroj** pro snadnou a rychlou implementaci kontroly nad síťovým provozem - může ovlivňovat rychlost přístupu na základě mnoha parametrů, **lze určovat úroveň priority a omezovat provoz na vybraném portu**, VLAN nebo celém switchi. Redukovat tak lze nežádoucí síťový provoz bez větších nároků na administrativní náročnost.

7.3.2 Výborná bezpečnostní kontrola

Přístupy do sítě se musejí hlídat a tento přepínač právě takovému požadavku díky zařazení technik **802.1x a MAC Authentication** plně vyhovuje. Podporuje také **ACL, VLAN ALC a IPv6 ACL**. O bezpečnost dat se stará šifrování na bázi **SSHv2, SSL a SNMPv3**, zařazena je i DHCP ochrana. O správu sítě pečuje HPE Intelligent Management Center (IMC).

7.3.3 Klíčové vlastnosti

Síťový přepínač, který podporuje L3 vrstvu a stohování včetně napájení přes Ethernet (až 370 W).

Rozhraní: 24 x RJ-45 autosensing 10/100/1000 porty; 4 x SFP+ 1000/10000 porty. K dispozici jsou protokoly 802.1x a MAC Authentication či ACL, VLAN ALC a IPv6 ACL. Mnoho dalších technik brání vaši síť před zákeřnými útoky. Podporovány jsou SSL a SSHv2 šifrování a SNMPv3.

Záruka na dobu životnosti (99 let) + NBD (servis do druhého pracovního dne na místě zákazníka) po celou dobu životnosti + 3 měsíce 24x7 softwarová podpora v ceně.

7.3.4 Technické parametry

Počet LAN 1000 Mbps:	24
Počet portů SFP:	4
QoS:	Ano
Max. přenosová rychlost [Gbps]:	128
Podporované rychlosti [Mb/s]:	1 000
• Porty	
Počet portů SFP:	4
Počet LAN 1000 Mbps:	24
• Parametry	
Provedení:	Rackmount
Web management:	Ano
Funkce:	QoS, Stohovatelný, VLAN
PoE:	Ano
Podporované PoE standardy:	802.3af, 802.3at
Počet PoE Out portů:	24
PoE budget [W]:	370
• Rychlosti	
Max. přenosová rychlost [Gbps]:	128
Podporované rychlosti [Mb/s]:	1 000

7.4 HPE IMC Standard Software

Viz Datasheet v příloze č. 10.1

7.5 Aruba ClearPass Cx000V VM Appliance E-LTU

Viz Datasheet v příloze č. 10.1

7.6 Aruba ClearPass NL AC 500 CE E-LTU

Viz Datasheet v příloze č. 10.1

7.7 Aruba IAP-304 a Aruba IAP-305

Datasheet v Angličtině

7.7.1 Aruba IAP-304

Model Aruba Instant IAP-304 (RW) patří mezi základní produkty rychlé WiFi sítě. Nabízí bezdrátové rozhraní standardu 802.11n/ac s konfigurací antén typu 2x2:2/3x3:3 MU-MIMO. Přístroj má integrované rovněž Bluetooth rozhraní. Obsahuje tři duální RP-SMA konektory pro externí antény.

Vysoká přenosová rychlost

Jednotka nabízí svižné přenosové rychlosti, které sahají až do kadence 1300 megabytů za vteřinu v 5GHz pásmu a až 300 Mbps v pásmu 2,4GHz. Zařízení rozpoznává MU-MIMO přístroje, a automaticky je umí nasměrovat k nejbližšímu přístupovému bodu z rodiny Aruba.

Klíčové vlastnosti

Rychlý přístupový bod výrobce Hewlett-Packard, který je dvoupásmový (2,4 a 5 GHz). Jeho celková přenosová rychlost dosahuje až 1600 Mbps. Přístroj rovněž podporuje Bluetooth technologii. Rozhraní: 1 x 10/100/1000 RJ-45 (LAN), 1 x USB 2.0, 1 x sériové konzolové rozhraní, kensington bezpečnostní slot.

Technické parametry

- Frekvenční rozsah (GHz): 2.4, 5
- Přenosové rychlosti pro WLAN (Wifi) [Mb/s]: 1300 + 400
- Rozhraní: Bluetooth, RJ-45, WiFi
- Počet portů RJ-45: 1
- Access Point: Ano
- Typ routeru: Access point, MU-MIMO
- WLAN (Wifi) standardy: 802.11a, 802.11ac, 802.11b, 802.11g, 802.11n
- Frekvenční rozsah (GHz): 2.4, 5
- Management: Ano
- Typ antény: Vestavěná
- Přenosové rychlosti pro WLAN (Wifi) [Mb/s]: 1300 + 400

7.7.2 Aruba IAP-305

Přístupový bod řady Aruba 305 se středním rozsahem a značnou přenosovou rychlostí, který je **vhodný pro nasazení ve firemním prostředí**, jako jsou maloobchodní pobočky, sklady, hotely a podnikové kanceláře či školní jednotky. Zařízení využívá technologie **802.11ac**.

Vysoká přenosová rychlost

Kompaktní Aruba 305 Series AP poskytuje maximální přenosovou rychlost **1300 Mb/s v pásmu 5 GHz (3x3 MIMO) a 300 Mb/s v pásmu 2.4 GHz (2x2 MIMO)** při celkové rychlosti datového toku 1.6 Gb/s. S integrovaným rozhraním **Bluetooth Aruba Beacon** nabízí serie AP 305 pokročilou možnost lokalizace a služby upozornění založené na bezdrátové komunikaci. Současně zjednodušuje dálkovou správu baterií Aruba Beacons.

Více možností použití

Přístroj Aruba 305 nabízí řadu **provozních režimů**. V režimu controller-managed nabízí centralizovanou konfiguraci, šifrování dat, vynucování zásad a síťové služby, stejně jako distribuované a centralizované předávání zpráv. V režimu "Instant" automaticky předává konfiguraci sítě jiným AP ve stejném módu v

síti WLAN. Kromě jiného nabízí zařízení také bezdrátové monitorování zarušení sítě a dokonce také identifikaci zdrojů rušení vysokofrekvenčními zářeními.

Klíčové vlastnosti

Značkový **přístupový bod ze série HP Aruba**, který poslouží zejména v kancelářském prostředí. Podporuje **Wi-Fi rozhraní 802.11ac** a nabízí práci ve dvou frekvenčních pásmech (2.4 a 5 GHz). Rozhraní: 1 x 10/100/1000 RJ-45 LAN, 1 x USB 2.0 (typ A), Bluetooth.

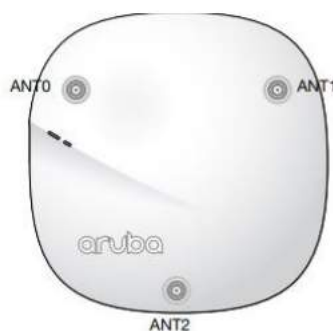
Rozměry: 165 x 165 x 38 mm. Hmotnost: 460 g.

Technické parametry

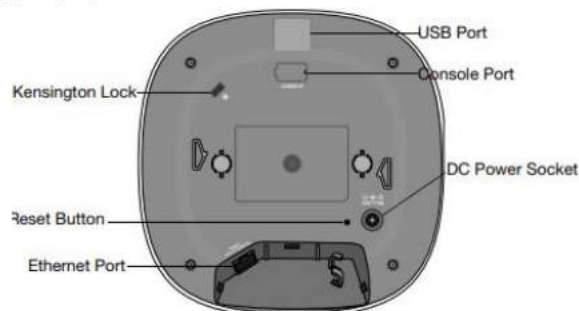
- Frekvenční rozsah (GHz): 2.4, 5
- Přenosové rychlosti pro WLAN (Wifi) [Mb/s]: 1300 + 400

- Rozhraní: RJ-45, USB 2.0, WiFi
- Počet portů RJ-45: 1
- Access Point: Ano
- Typ routeru: Access point
- WLAN (Wifi) standardy: 802.11a, 802.11ac, 802.11b, 802.11g, 802.11n

- Frekvenční rozsah (GHz): 2.4, 5
- Management: Ano
- Typ antény: Vestavěná
- Přenosové rychlosti pro WLAN (Wifi) [Mb/s]: 1300 + 400



Obrázek 2 Externí anténí konektory



Obrázek 1 zadní pohled (oba modely stejné)

7.8 AT&T Cybersecurity

Viz Datasheet v příloze č. 10.1

7.9 Dell EMC PowerEdge R640 rack server



Nekompromisní výkon a vysoká kapacita pro produktivitu a škálovatelnost datových center PowerEdge R640 je ideální 2soketová platforma pro vysokokapacitní škálovací výpočetní úkoly v datových centrech a úložiště. Využijte flexibilitu 2,5palcových nebo 3,5palcových disků, výkon NVMe a integrovanou inteligenci k zajištění optimalizovaného výkonu aplikací v zabezpečené platformě. S pomocí integrované diagnostiky a funkce SupportAssist poskytuje server R640 maximální dobu běhu systému a provoz bez starostí.

Ideální úlohy:

- Vysokokapacitní softwarově definované úložiště
 - Poskytovatelé služeb: aplikační vrstva
 - Vysokokapacitní privátní cloud
 - Virtualizace
 - HPC
- Zjednodušte nasazení a dosáhněte snadného škálování od 3 do více než 1 000 uzlů pro softwarově definované úložiště s bloky Dell EMC Ready Node pro ScaleIO.
 - Maximalizujte výkon úložiště s až 8 disky NVMe.
 - Škálování výpočetních zdrojů s procesory Intel® Xeon® SP přináší 27% navýšení výpočetních jader a 50% navýšení šířky pásma oproti předchozí generaci procesorů Xeon².

Automatizujte produktivitu pomocí inteligentní integrované správy

- Automatizace Dell EMC a inteligentní správa znamenají, že věnujete méně času rutinní údržbě a můžete se zaměřit na vyšší priority.
- Maximalizujte provozní dobu pomocí proaktivní diagnostiky a automatizovaných oprav, které zvyšují produktivitu až o 90 %³.
- Využijte existující konzole pro správu s možností snadné integrace nástrojů VMware® vSphere®, Microsoft® System Center a Nagios®.
- Zvyšte produktivitu pomocí řadiče Dell EMC iDRAC9 bez agentů, určeného pro automatizovanou, efektivní správu.
- Zjednodušte nasazení pomocí konzole OpenManage příští generace a serverových profilů, s jejichž pomocí lze rychlým, škálovatelným způsobem plně konfigurovat a připravovat servery.

7.9.1 Technické údaje :

Procesor	Až dva škálovatelné procesory Intel® Xeon®, až 28 jader na procesor
Operační systém	Canonical® Ubuntu® LTS Citrix® XenServer® Microsoft Windows Server® s technologií Hyper-V Red Hat® Enterprise Linux SUSE® Linux Enterprise Server VMware® ESXi
Paměť	24 slotů na paměti DIMM DDR4, podporuje RDIMM/LRDIMM, zrychlení až na 2 666, maximálně 1,5 TB Až 12 modulů NVDIMM, nejvýše 192 GB Podporuje pouze registrované moduly DIMM DDR4 ECC
Diskové pozice	
Přední pozice:	Až 10 x 2,5palcový disk s až 8 disky NVMe, disky SAS/SATA/SSD/NVMe, max. 58 TB Až 4 x 3,5palcový disk SAS/SATA, max. 40 TB
Zadní pozice na pevné disky:	Až 2 x 2,5palcový disk SAS/SATA/SSD/NVMe, max. 12 TB
Rozměry	
Uspořádání:	Rack (1U)
Hloubka šasi:	705,05 mm
Ochrana dat :	TPM 1.2/2.0 optional Cryptographically signed firmware Secure Boot System Lockdown Secure erase
Porty	
Možnosti síťových karet NDC:	4x 1 GE nebo 2x 10 GbE + 2x 1 GE nebo 4x 10 GE nebo 2x 25 GE
Přední porty:	Video, 1x USB 2.0, k dispozici rozhraní USB 3.0, vyhrazený řadič iDRAC Direct USB
Zadní porty:	Video, sériový port, 2x USB 3.0, vyhrazený síťový port iDRAC
Grafická karta:	VGA, NVIDIA NVS310 k dispozici jako karta PCIe, až 3 sloty Gen3, vše x16 karty
Šasi	Volitelný displej LCD nebo bezpečnostní čelní kryt (bezel)
Napájení	Titanium 750 W, Platinum 495 W, 750 W, 1 100 W a 1 600 W 48 V ss. 1 100 W, 380 V smíšený režim 1 100 W, 240 V smíšený režim 750 W Napájecí zdroje připojitelné za provozu s volitelnou plnou redundancí, až 8 ventilátorů připojitelných za provozu s plnou redundancí

Řadiče RAID

Interní řadiče: PERC H330, H730p, H740p, HBA330, softwarové pole RAID (SWRAID) S140

Úložný subsystém optimalizovaný pro spuštění:

HWRAID se 2 disky SSD M.2, 120 GB, 240 GB

Externí řadič PERC (RAID): H840

Externí adaptéry HBA (bez podpory pole RAID):
HBA SAS, 12 Gb/s

Správa

Integrované / At-the-Server Řadič iDRAC9 s modulem Lifecycle Controller (Express, Enterprise)

iDRAC Direct

iDRAC REST API s Redfish

BLE / bezdrátový modul Quick Sync 2

Konzole

OpenManage Enterprise (již brzy)

OpenManage Essentials

OpenManage Power Center

Mobilita

OpenManage Mobile

Nástroje

Modul služby iDRAC

OpenManage Server Administrator

OpenManage Storage Services

Dell EMC Repository Manager

Dell EMC System Update

Dell EMC Server Update Utility

Dell EMC Update Catalogs

OpenManage Integrations

Microsoft® System Center

VMware® vCenter™

Software BMC (k dispozici od BMC)

OpenManage Connections

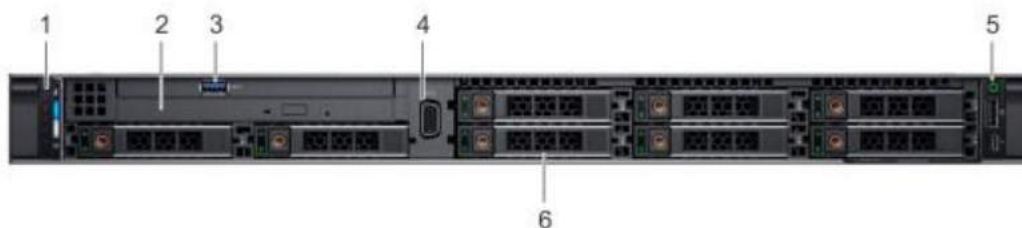
Nagios Core a Nagios XI

HPE Operations Manager i (OMi)

IBM Tivoli® Netcool/OMNIbus (již brzy)

IBM Tivoli® Network Manager IP Edition (již brzy)

7.9.2 Možnosti provedení



Obrázek 3 čelní pohled na provedení 8 x

Popis jednotlivých pozic

1. Levý kontrolní panel

obsahuje systémové informace o stavu systému a



Obrázek 4 Levý kontrolní

ID systému, stavové LED a indikátor iDRAC Quick Sync (bezdrátový)

- 1) Status LED
- 2) systémové informace o stavu systému
- 3) iDRAC Quick Sync 2 wireless indicator (volitelně)

2. Volitelně optická mechanika
3. Volitelně USB port
4. VGA port
5. Pravý kontrolní panel



Obrázek 5 pravý

obsahuje tlačítko POWER, USB port, iDRAC Direct micro port, a iDRAC Direct status LED.

- 1) Tlačítko pro vypnutí a zapnutí
- 2) USB 3.0
- 3) LED kontrolka Direct iDRAC
- 4) iDRAC Direct port (Micro-AB USB)

6. Diskové pozice
7. Informační tag servisní

jedná se o Informační štítek který po vysunutí, obsahuje systémové informace jako je

TAG, NIC, MAC adresa a podobně. Pokud je při konfiguraci zvolen bezpečný výchozí přístup k iDRAC tak štítek také obsahuje předvolené heslo iDRAC.

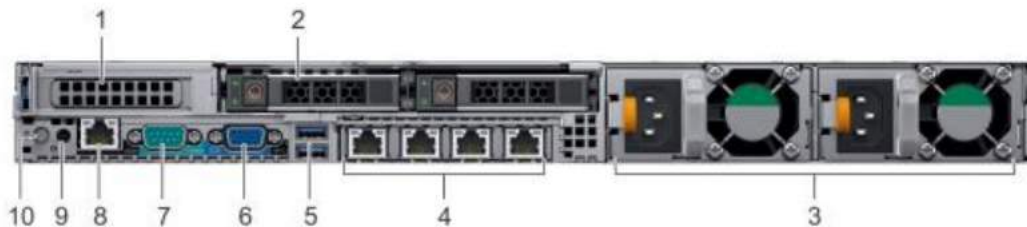


Obrázek 6 čelní pohled na provedení 4 x 3,5" HDD



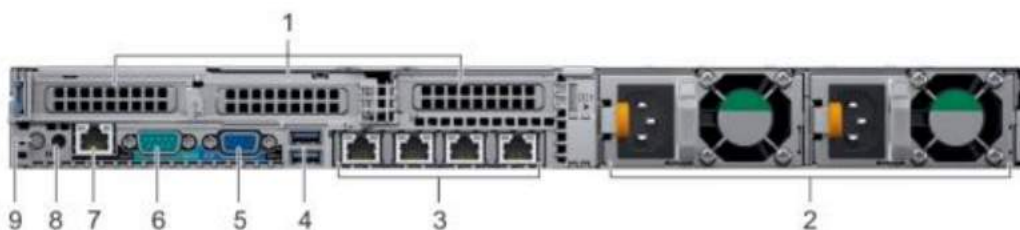
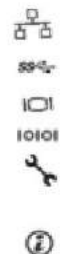
Obrázek 7 čelní pohled na provedení 10 x 2,5" HDD

1. Levý kontrolní panel
2. Diskové pozice
3. VGA port
4. Pravý kontrolní panel
5. Informační tag



Obrázek 8 zadní pohled na provedení 2 x 2,5" HDD s 1 x PCIe rozšiřujícím slotem


1. PCIe expansion card slot
2. Sloty pro HDD v zadních pozicích
3. Napájecí zdroje
4. Ethernet porty
5. USB 3.0 porty
6. VGA port
7. Sériový port
8. iDRAC9 dedikovaný port pro management
9. CMA napájecí port
10. Identifikační tlačítko pro označení systému v RACKu

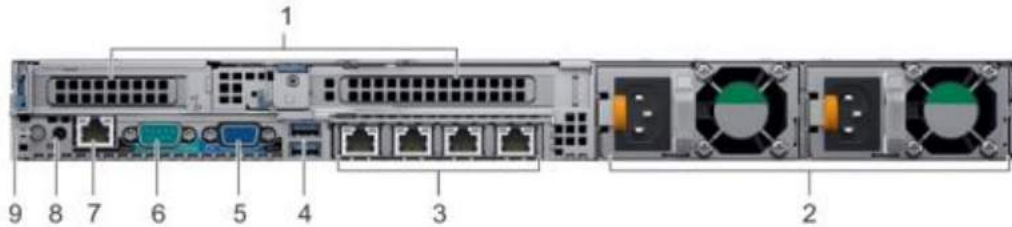


Obrázek 9 zadní pohled na provedení s 3 x PCIe

1. PCIe expansion card slot 3 x
2. Napájecí zdroje
3. Ethernet porty
4. USB 3.0 porty
5. VGA port
6. Sériový port
7. iDRAC9 dedikovaný port pro management

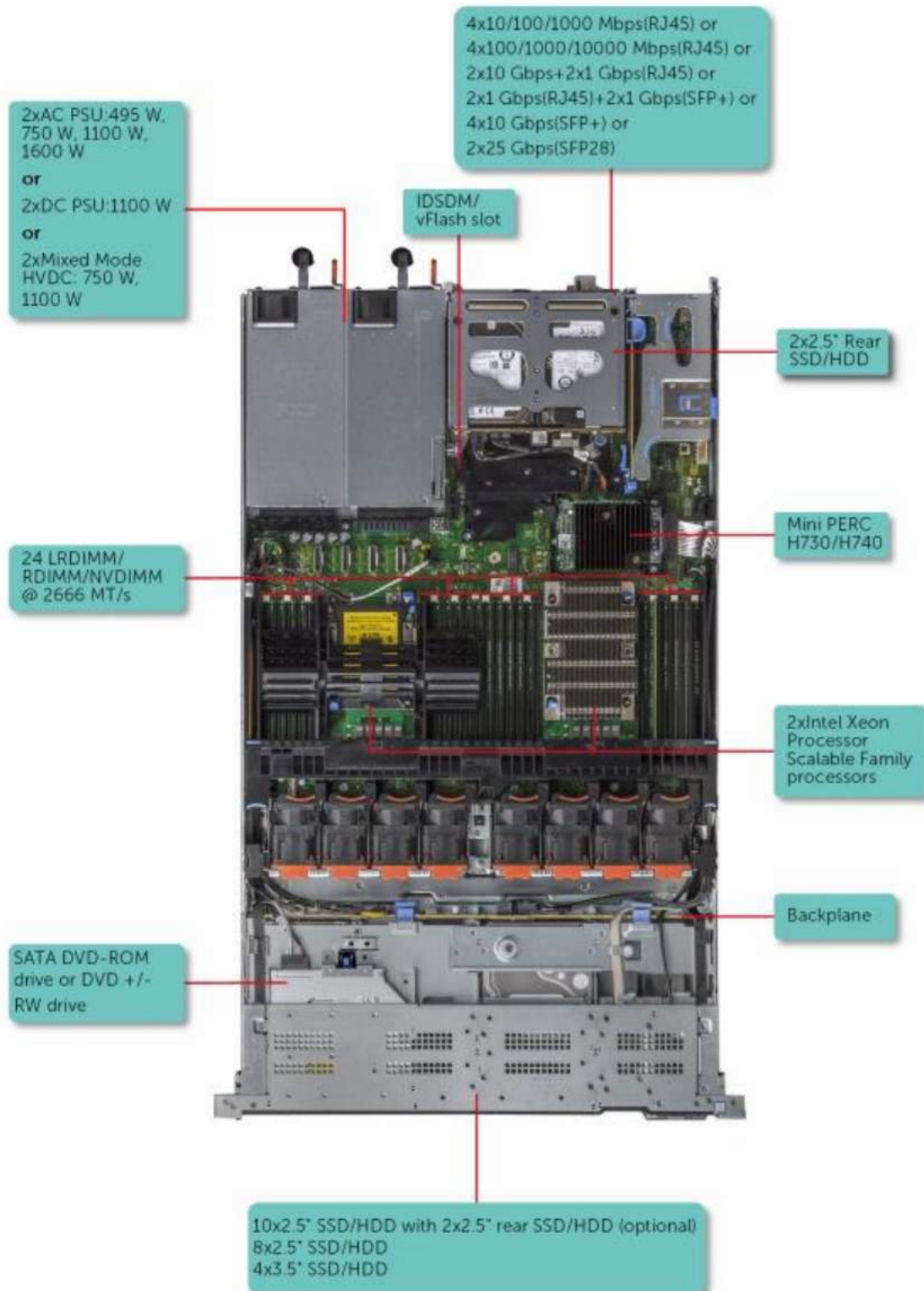


8. CMA napájecí port
9. Identifikační tlačítko pro označení systému v RACKu 



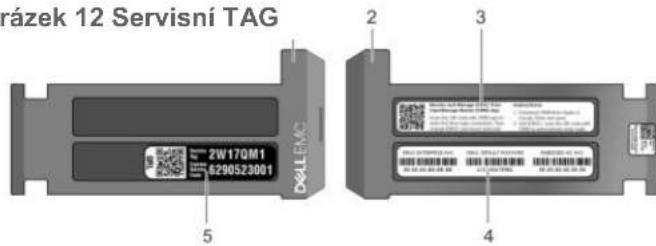
Obrázek 10 zadní pohled na systém s 2 x PCIe

1. PCIe expansion card slot 2 x
Ostatní je totožné s předchozím vyobrazením

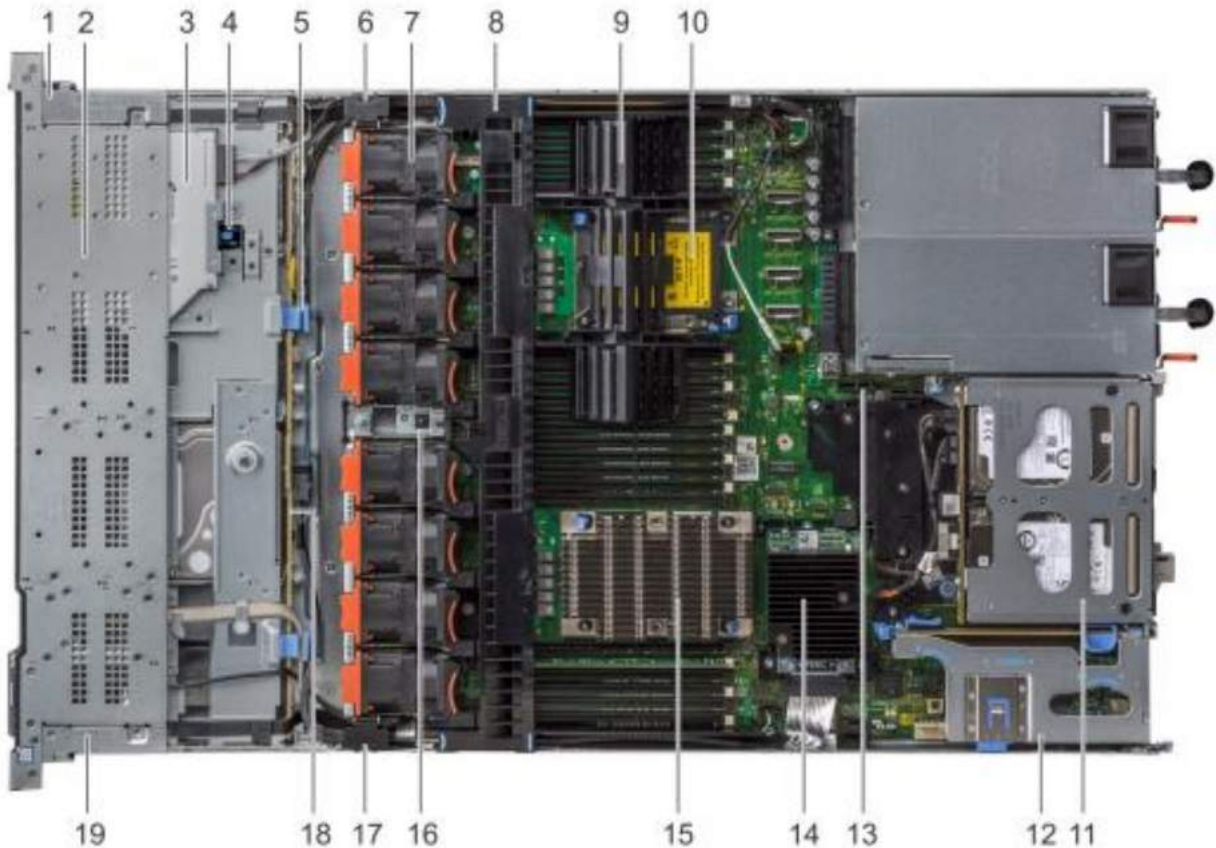


Obrázek 11 pohled na vnitřní uspořádání

Obrázek 12 Servisní TAG

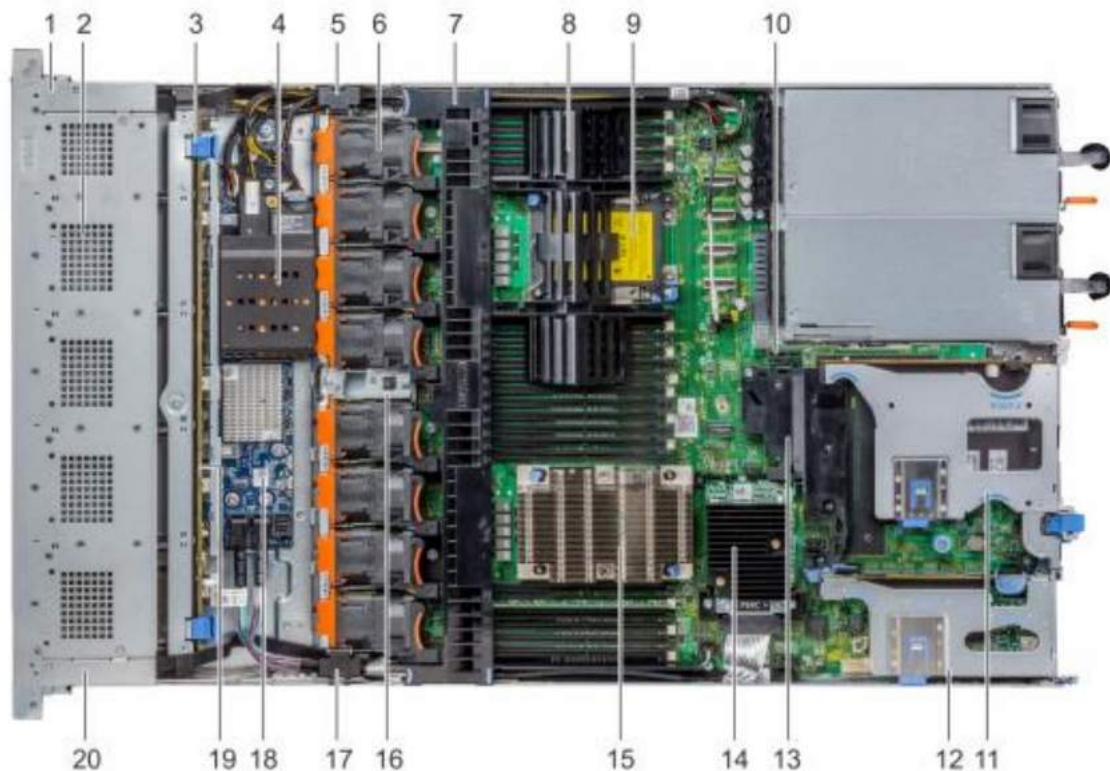


1. Informativní TAG (čelní pohled)
2. Informativní TAG (zadní pohled)
3. OpenManage Mobile (OMM) label
4. iDRAC MAC address and iDRAC secure password label
5. Service Tag



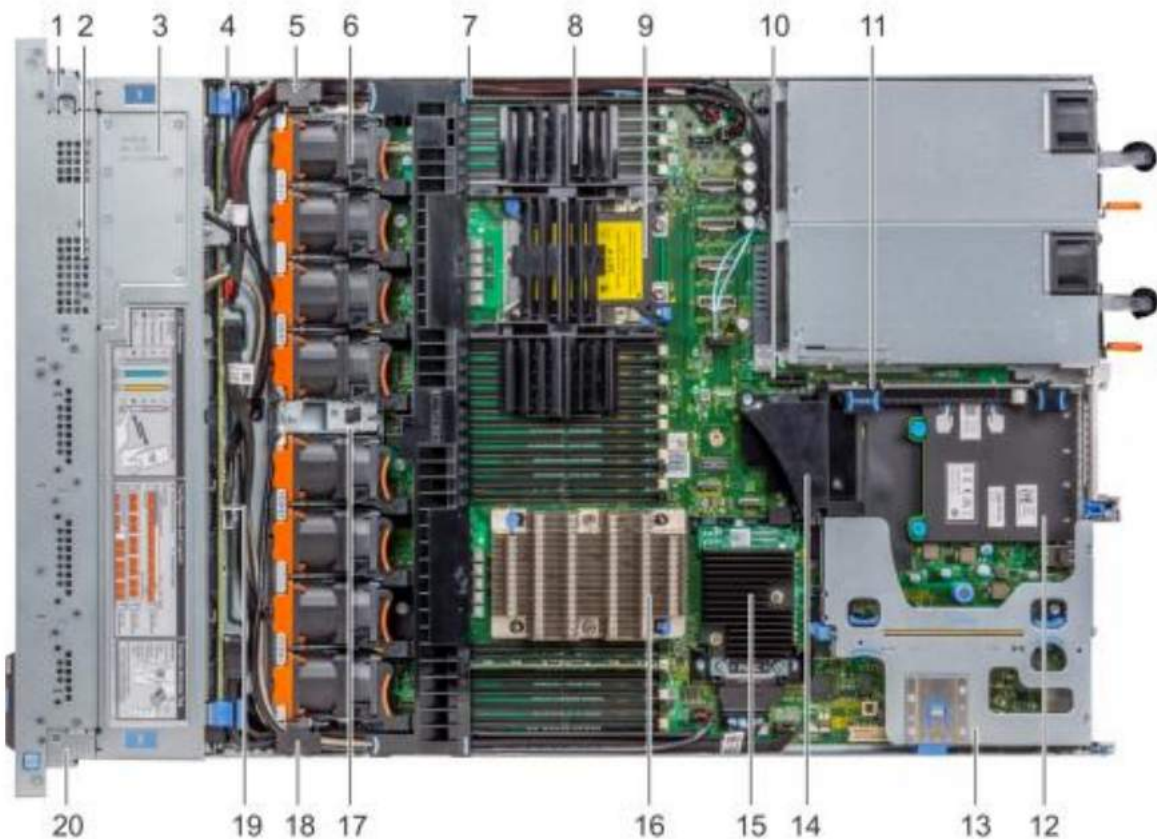
Obrázek 13 vnitřní pohled na provedení s 1 x PCIe rozšiřujícím slotem

- | | |
|--|---|
| <ol style="list-style-type: none"> 1. kryt kabelu pravého ovládacího panelu 2. Pozice pro HDD 3. Optická mechanika 4. uvolňovací západka optické jednotky 5. backplane uvolňovací západka 6. západka kabeláže 7. ventilátor chlazení 8. vzduchový kryt ventilátorů chlazení 9. slot pro procesor a prázdné DIMM sloty | <ol style="list-style-type: none"> 10. slot pro procesor číslo 2 11. zadní modul pevného disku 12. rozšiřující redukce PCI karet 13. slot pro IDSDM / vFlash modul 14. integrovaná karta diskového řadiče 15. slot pro procesor číslo 1 16. protipozice západky víka case 17. kabelová západka 18. backplane pro pevné disky 19. kryt kabelu levého ovládacího panelu |
|--|---|



Obrázek 14 vnitřní pohled na provedení se dvěma PCIe rozšiřujícími sloty

1. kryt kabelu pravého ovládacího panelu
2. Pozice pro HDD
3. backplane uvolňovací západka
4. NVDIMM-N battery
5. západka kabeláže
6. ventilátor chlazení
7. vzduchový kryt ventilátorů chlazení
8. slot pro procesor a prázdné DIMM sloty
9. slot pro procesor číslo 2
10. slot pro IDSDM / vFlash modul
11. rozšiřující redukce PCI karet 2 B
12. rozšiřující redukce PCI karet 1 B
13. kryt PCIe
14. integrovaná karta diskového řadiče
15. slot pro procesor číslo 1
16. protipozice západky víka case
17. kabelová západka
18. SAS expansní deska
19. backplane pro pevné disky
20. kryt kabelu levého ovládacího panelu



1. kryt kabelu pravého ovládacího panelu
2. Pozice pro HDD
3. backplane uvolňovací západka
4. NVDIMM-N battery
5. západka kabeláže
6. ventilátor chlazení
7. vzduchový kryt ventilátorů chlazení
8. slot pro procesor a prázdné DIMM sloty
9. slot pro procesor číslo 2
10. slot pro IDSDM / vFlash modul
11. rozšiřující redukce PCI karet 2 A
12. modulární karta s LAN porty
13. rozšiřující redukce PCI karet 1 A
14. kryt PCIe
15. integrovaná karta diskového řadiče
16. slot pro procesor číslo 1
17. protipozice západky víka case
18. kabelová západka
19. backplane pro pevné disky
20. kryt kabelu levého ovládacího panelu

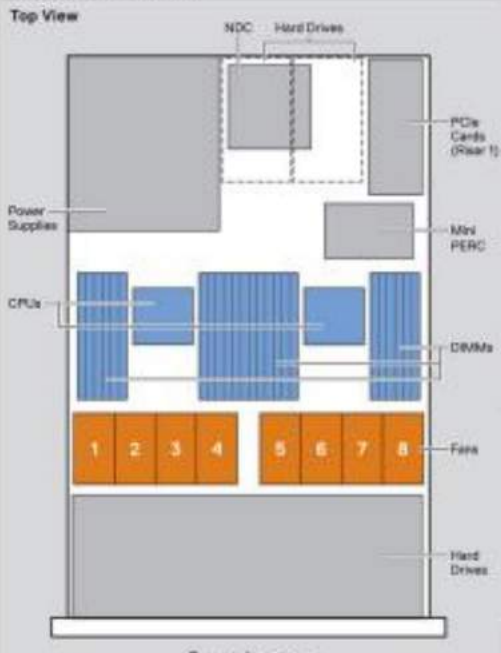
Service Information

System Touchpoints

- Hot swap touchpoints: Components with terracotta touchpoints can be serviced while the system is running.
- Cold swap touchpoints: Components with blue touchpoints require a full system shutdown before servicing.

Mechanical Overview

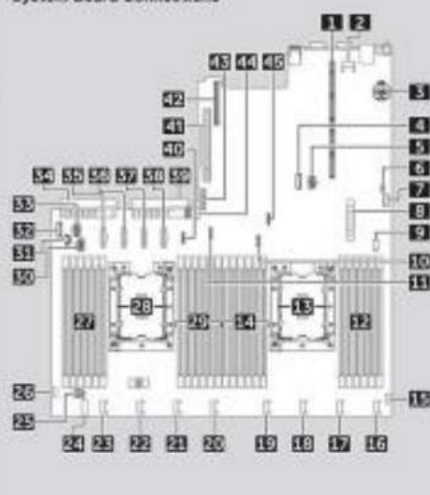
Top View



Front of system

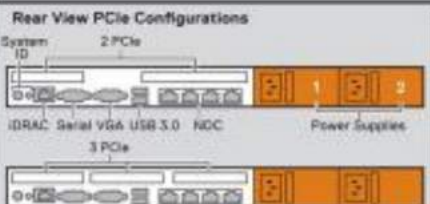
Electrical Overview

System Board Connections




1 Riser 1	33 NVDIMM Battery Power
2 TPM Docking	34 Left CP
3 Coin Cell Battery	35 DIMMs for CPU 2 Channels 3, 4, 5
4 Rear Backplane Signal	36 CPU 2
5 Rear Backplane Power	37 DIMMs for CPU 2 Channels 0, 1, 2
6 Jumpers	38 EXP Power
7 VGA	39 ODD Power
8 MiniPERC	40 Backplane Signal
9 USB 2.0	41 Backplane Power
10 PCH SATA-B	42 PSU 2
11 PCH SATA-D	43 Backplane HDDs 2-3
12 DIMMs for CPU 1 Channels 0, 1, 2	44 Backplane HDDs 4-5
13 CPU 1	45 Backplane HDDs 6-7
14 DIMMs for CPU 1 Channels 3, 4, 5	46 Backplane HDDs 8-9
15 Right CP	47 PSU 1
16 Fan 8	48 ODD Signal
17 Fan 7	49 Riser 2
18 Fan 6	50 NDC
19 Fan 5	51 iSDCM + vFlash
20 Fan 4	52 Internal USB 3.0
21 Fan 3	
22 Fan 2	
23 Fan 1	
24 NVDIMM Battery Signal	

Rear View PCIe Configurations



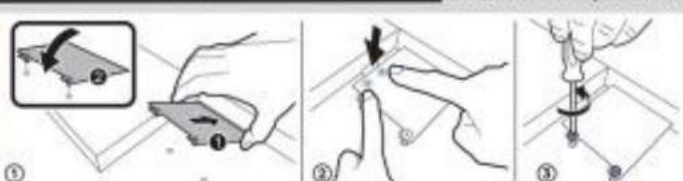
Rear View Hard Drive Configurations




Caution: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that came with the product.

System Tasks

Network Daughter Card Installation








MiniPERC



Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Non-A90-21 Label Part No: 8MNUJ4

Obrázek 15 servisní informace

Jumper Settings

Jumper	Setting	Description
PWRD_EN	 (default)	BIOS password is enabled.
		BIOS password is disabled. iDRAC local access unlocked at next AC power cycle. iDRAC password reset is enabled in F2 iDRAC settings menu.
	 (default)	BIOS configuration settings retained at system boot.
NVRAM_CLR		BIOS configuration settings cleared at system boot.

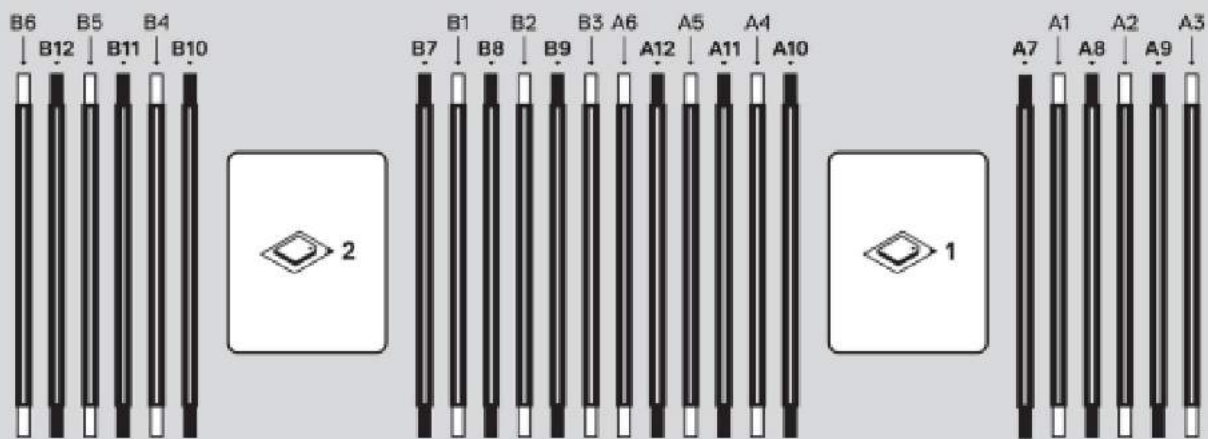
Scan to see hardware servicing and software setup videos, how-to's, and documentation.



To learn more about this Dell product or to order additional or replacement parts, go to Dell.com/support

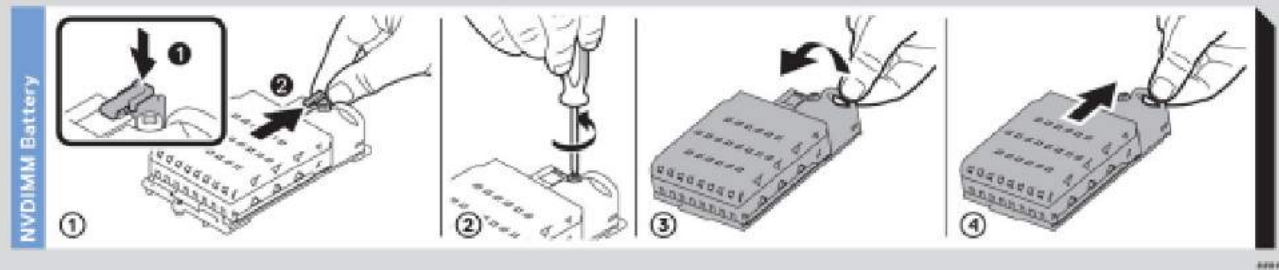
Memory Information

⚠ Caution: Memory (DIMMs) and CPUs may be hot during servicing.



Configuration	Sequence
Memory-Optimized	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Mirroring	(1,2) (3,4) (5,6) (7,8) (9,10) (11,12)

Memory Sparing details are documented in the *Installation and Service Manual*.



Obrázek 16 informace o operační paměti a nastavení

Odkaz na podrobnější informace:
https://topics-cdn.dell.com/pdf/poweredge-r640_owners-manual_en-us.pdf

7.10 Kamery Vivotek FD8177-H

VIVOTEK FD8177-H je vnitřní IP kamera s vysokým rozlišením, pokročilými funkcemi pro zvýšení kvality obrazu a integrovaným inteligentním nočním IR přísvitem.

7.10.1 Nadstandartní vlastnosti IP kamery VIVOTEK FD8177-H

- Vysoké 4Mpx rozlišení **2688 x 1520 bodů** při 30 snímcích za sekundu (vypnuté WDR Pro)
- Vysoké rozlišení **2560 x 1440 bodů** při 24 snímcích za sekundu (zapnuté WDR Pro)
- **WDR Pro (110db), 3D redukce šumu, vysoká citlivost v noci**
- Varifokální objektiv s **úhly záběru 33° až 105°** s automaticky řízenou clonou DC-iris
- Otočení obrazu po 90° - hlídání chodeb nebo dlouhých a úzkých míst
- Kompresi H.264 a MJPEG
- Multistreaming - 3 nezávislé streamy pro libovolné nastavení kvality obrazu
- **Smart Stream II** - inteligentní nastavení datového toku IP kamery
- Podpora den a noc funkcí s odklopitelem IR filtrem
- Integrovaný inteligentní IR přísvit s efektivním dosvitem až 30 metrů
- Vestavěný slot paměťových karet microSD/SDHC/SDXC
- Podpora napájení po datovém kabelu **PoE** dle normy 802.3af
- Podpora VIVOTEK VCA - video analýza obrazu

7.10.2 Bezpečnostní funkce IP kamery VIVOTEK FD8177-H

Video detekce pohybu, odesílání e-mailů při poplachu, spuštění záznamu na paměťovou kartu při poplachu, ukládání videa na FTP či síťové úložiště při poplachu.

7.10.3 Video analýza obrazu VIVOTEK VCA v IP kameře VIVOTEK FD8177-H

Video analýza obrazu - inteligentní bezpečnostní funkce překročení nastavené hranice, hlídání vytyčené oblasti před vložením či odcizením předmětu a detekce poflakování.

7.10.4 Způsob záznamu z IP kamery VIVOTEK FD8177-H

Záznam videa na paměťovou kartu, odeslání snímku nebo krátkého videa na e-mail, FTP či síťové úložiště. Doporučujeme záznam pomocí zdarma dodávaného softwaru VIVOTEK VAST v českém jazyce nebo pomocí záznamového zařízení (je třeba dokoupit).

7.10.5 Připojení k IP kameře pomocí počítače, mobilního telefonu a tabletu

Sledovat obraz z IP kamery VIVOTEK FD8177-H můžete z libovolného počítače (Windows, Linux, Apple), chytrého telefonu (Android a iOS - Apple) a tabletu (Android a iOS - Apple).

Pro nastavení IP kamery doporučujeme použít počítač s MS Windows a prohlížečem Internet Explorer do verze 10 s podporou Active X. Internet Explorer 11 a vyšší lze též použít, ovšem v kompatibilním módu verze IE 7 - 10. Pomocí ostatních prohlížečů se můžete připojit a sledovat obraz s omezenými možnostmi v nastavení.

IP kamera VIVOTEK FD8177-H podporuje MJPEG stream s libovolným definováním URL pro snadnou integraci do inteligentních systémů pro inteligentní domy.

7.10.6 Připojení IP kamery VIVOTEK FD8177-H do systému

IP kameru můžete připojit pomocí datového kabelu FTP cat. 5e, doporučujeme vždy použít stíněný. Napájení po datovém kabelu pomocí PoE dle normy IEEE 802.3af (délka kabelu až 100m).

7.11 Parametry

7.11.1 Nadstandardní vlastnosti kamery

- Smart Stream II: ano
- 3D redukce šumu: ano
- Obrazové profily: ano
- Otoční obrazu po 90° pro hlídání koridoru: ano
- Integrovaný přísvit: ano
- Smart IR: ano
- Přístup pomocí mobilního telefonu: ano
- VCA - videoanalýza obrazu: ano
- Podpora standardu ONVIF: ano

7.11.2 Čip a optické vlastnosti

- Snímací čip: 1/3" progressive CMOS
- Vlastnosti snímacího čipu: 1/5 až 1/32000s., AGC, AWB
- Citlivost (barevně): 0,1 lx
- Citlivost (ČB): 0,01 lx
- Den/Noc: ano
- Podpora WDR: ano - WDR Pro (110dB)
- Podpora automaticky řízené clony: ano
- Mechanicky odklopitelný IR filtr: ano
- Objektiv: ano - integrovaný
- Integrovaný IR přísvit: ano
- Max. dosvit IR přísvitu: 30m
- Parametry IR přísvitu: 10x SMT IR LED, inteligentní IR

7.11.3 Vlastnosti objektivu

- Min. ohnisková vzdálenost: f 2,8 mm
- Max. ohnisková vzdálenost: f 12 mm
- Optický zoom: 3x
- Minimální úhel (horizontální): 33°
- Maximální úhel (horizontální): 105°
- Clonové číslo: F 1,4
- Průměr (velikost snímače): 1/3"
- Podpora IR (den/noc): ano
- Regulace clony: automatická (DC-drive)
- Max. doporučené rozlišení kamery: 4 Mpix
- Asférický objektiv: ano

7.11.4 Video

- Kompresce: MJPEG a H.264
- Maximální rozlišení: 2688 x 1520 px
- Počet snímků při max. rozlišení: 30 s.
- Max. počet snímků: 30 s.
- Multi-streaming: ano
- Počet streamů: 3
- Max. počet klientů: až 10

7.11.5 Audio

- Kompresce: G.711, G.726
- Integrovaný mikrofón: ano

7.11.6 Rozhraní

- Síťové rozhraní: 1x RJ-45 10 Base-T / 100BaseTX Ethernet
- Protokoly: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X, UDP, ICMP, ARP, SSL, TLS
- Slot paměťových karet: 1x MicroSD/SDHC/SDXC

7.11.7 Mechanické provedení

- Provedení: vnitřní
- Typ kamery: dome - půlkoule
- Šířka: 129 mm
- Výška: 129 mm
- Hloubka: 94 mm
- Vlhkost: 90% HR
- Hmotnost: 417 g
- Min. provozní teplota: 0°C
- Max. provozní teplota: 50°C
- Schválení a normy: CE, LVD, FCC Class A, VCCI, C-Tick, UL

7.11.8 Napájení zařízení

- Podpora PoE dle normy IEEE 802.3af: ano
- Spotřeba při napájení PoE 802.3af: 10 W



- i. Na stranách 49-50 u centrálních switchů nabídka obsahuje standardní texty a konfigurační možnosti z datového listu výrobce. Hodnotící komise vyzývá k objasnění: Upřesněte nabízenou konfiguraci (redundantní zdroje a větráky).

Objasnění účastníka:

Ano, požadovaná funkcionality redundantních zdrojů a větráků je obsažena v nabídce, viz konkrétní konfigurace centrálních switchů v následující tabulce:

Text	Množství	Jednotka
Centrální switche	1,00	ks.
HPE 5710 48SFP+ 6QSFP+/2QSFP28 Switch, P/N: JL585A	2,00	ks
HPE 5710 250W FB AC PSU, P/N: JL589A	4,00	ks
HPE X721 FB Fan Tray, P/N: JL594A	4,00	ks
HPE 5Y FC NBD Exchange 5710 48G SVC, P/N: HB4B6E	2,00	ks

- ii. Na straně 55 u serveru nabídka obsahuje standardní texty a konfigurační možnosti z datového listu výrobce. Hodnotící komise vyzývá k objasnění: Upřesněte nabízenou konfiguraci.

Objasnění účastníka:

Níže naleznete kompletní konfiguraci nabízeného serveru:

Product Name	Module Name	Option Name	Qty
PowerEdge R640	Základna	PowerEdge R640 Server	1
	Konfigurace šasi	No Hard Drive, No Backplane Chassis	1
	Modul TPM (Trusted Platform Module)	Trusted Platform Module 2.0	1
	Procesor	Intel® Xeon® Gold 6130 2.1G,16C/32T,10.4GT/s,22M Cache,Turbo,HT (125W) DDR4-2666	1
	Další procesor	No Additional Processor	1
	Konfigurace řízení teploty procesoru	1 Standard Heatsink for 165W or less CPU	1
	Typ konfigurace paměti	Performance Optimized	1
	Typ a rychlost paměti DIMM	2666MT/s RDIMMs	1
	Kapacita paměti	32GB RDIMM, 2666MT/s, Dual Rank	4
	Operační systémy instalované ve výrobě:	VMware ESXi 6.7 U2 Embedded Image (License Not Included)	1
	Sekundární operační systém	Windows Server® 2016, Standard Ed,Secondary OS, No MEDIA,16 CORE	1

Sady médií operačního systému	Windows Server® 2016, Standard Edition, Secondary OS, Media Kit	1
Boot Optimized Storage Cards	BOSS controller card + with 2 M.2 Sticks 240G (RAID 1), LP	1
Konfigurace pole RAID	CO, Diskless Configuration (No RAID, No Controller)	1
Řadič pole RAID	Embedded SATA	1
Pevné disky	No Hard Drive	1
Nastavení řízení spotřeby v systému BIOS	Power Saving Dell Active Power Controller	1
Chlazení	5 Standard Fans for R640	1
Napájecí zdroj	Dual, Hot-plug, Redundant Power Supply (1+1), 495W	1
Napájecí kabely	Rack Power Cord 2M (C13/C14 10A)	2
Riser PCIe	Riser Config 4, 2x16 LP	1
Správa integrovaných systémů (Multi)	iDRAC9, Enterprise	1
Adaptér SNA (Select Network Adapter)	QLogic FastLinQ 41164 Quad Port 10GbE SFP+, rNDC	1
Čelní kryt (bezel)	LCD Bezel for x4 and x8 chassis	1
Quick Sync	No Quick Sync	1
Ližiny racku	ReadyRails™ Sliding Rails Without Cable Management Arm	1
Heslo	iDRAC, factory Random Password	1
Nástroj Group Manager	iDRAC Group Manager, Enabled	1
Interní optická jednotka	No Internal Optical Drive	1
Další štítky na přepravní krabici	Order Configuration Shipbox Label (Ship Date, Model, Processor Speed, HDD Size, RAM)	1
Přepravní materiál	PowerEdge R640 Shipping Material for 8 HDD chassis	1
Spedice	PowerEdge R640 Shipping EMEA2 (English/Slovenian/Slovakian/Polish/Czech/Hungary/Greek/Arab)	1
Standardní záruka	3Yr Basic Warranty - Next Business Day - Minimum Warranty	1
Rozšířené služby	5Yr Basic Warranty - Next Business Day	1

iii. Na straně 2 je uvedeno, že „Předmětem plnění veřejné zakázky je dodávka a nasazení nových technologií do prostředí zadavatele za účelem zvýšení jeho kybernetické bezpečnosti“ a předmětem plnění je dodávka mailového serverového software. Na straně 46 (tabulka) je i vyčíslena cena nabízeného řešení. Hodnotící komise vyzývá účastníka k předložení dokladů a objasnění naplnění požadavků zadavatele na mailový serverový software, který je součástí nabídky účastníka a který umožní ověření naplnění požadavků na tento software stanovených zadavatelem v zadávacích podmínkách.

Objasnění účastníka:

Jako systém pro správu elektronické pošty je navržen produkt Microsoft Exchange Server 2016 Standard, který bude provozován na operačním systému Microsoft Server 2016 Standard. Dle požadavků byl zvolen pro Exchange licenční model pro klientská zařízení (DvcCAL licence). Jako doplněk pro zabezpečení pošty je použit produkt XWall for Microsoft Exchange, který bude integrován se stávajícím antivirovým systémem Zadavetele:

Text	Množství	Jednotka
Mailový klient	1,00	ks.
ExchgSvrStd 2019 SNGL OLP NL	1,00	ks
ExchgStdCAL 2019 SNGL OLP NL DvcCAL	200,00	ks
Win Svr Std 2019 64Bit ENG 16 Core	1,00	ks
XWall for Microsoft Exchange	1,00	ks

Detailní informace o nabízených produktech jsou k dispozici na odkazech:

<https://products.office.com/cs-cz/exchange/microsoft-exchange-server>

<https://docs.microsoft.com/cs-cz/Exchange/exchange-server?view=exchserver-2019>

<https://www.dataenter.co.at/products/xwall.htm>

V Praze dne 21. 8. 2019.

Milan
Hlišák
Digitálně
podepsal Milan
Hlišák
Datum:
2019.08.22
08:42:17 +02'00'

Milan Hlišák

Předseda představenstva

5 Cenová tabulka

Příloha č. 2 Zadávací dokumentace - Cenová tabulka

Dodávka technologií za účelem zvýšení kybernetické bezpečnosti - druhé vyhlášení

Zadavatel Nemocnice Slaný, Sídlo: Politických vězňů 576, 274 01 Slaný, IČO: 00875295

Cena technologie a jejich implementaci, včetně příslušenství	Cena v Kč bez DPH
FireWall 2 ks - dodávka včetně implementace	639 760 Kč
Služby záručního servisu a technické podpory v délce 5 let k Firewallům	755 200 Kč
Centrální přepínače 2 ks - dodávka včetně implementace	779 820 Kč
Služby záručního servisu a technické podpory v délce 5 let k centrálním přepínačům a jejich příslušenství	53 728 Kč
Přepínače (síťové switche) 24 ks - dodávka včetně implementace	2 212 248 Kč
Služby záručního servisu a technické podpory v délce 5 let k přepínačům a jejich příslušenství	50 640 Kč
Systém pro centrální správu aktivních prvků a ověřování uživatelů (systém zabezpečení síťových portů)	1 470 554 Kč
Podpora systému pro centrální správu aktivních prvků a ověřování uživatelů (systém zabezpečení síťových portů) v délce 5 let	519 280 Kč
Wi-Fi Access pointy 40 ks - dodávka včetně implementace	912 736 Kč
Služby záručního servisu a technické podpory v délce 5 let k access pointům	38 960 Kč
Sběr a vyhodnocování kybernetických událostí - SIEM (systém pro centralizovanou správu eventů a logů) - dodávka včetně implementace	1 027 861 Kč
Služby technické podpory SIEM v délce 2 roky pro SIEM	276 889 Kč
Server pro SIEM - dodávka včetně implementace	410 367 Kč
Služby záručního servisu pro server pro SIEM v délce 5 let	22 461 Kč
Posílení systémových prostředků - dodávka RAM	262 346 Kč
Zabezpečení fyzického vstupu do serveroven (kamery 4ks včetně ovládacího software) - dodávka včetně implementace	138 000 Kč
Zabezpečení fyzického vstupu do serveroven (kamery 4ks včetně ovládacího software) - záruční servis a podpora v délce 3 let	19 480 Kč
Software modernizace správy elektronické pošty - včetně dodávky a implementace	1 317 830 Kč
Software modernizace správy elektronické pošty - podpora 5 let	61 840 Kč
Nabídková cena celkem v Kč bez DPH	10 970 000,00 Kč
Nabídková cena celkem v Kč včetně DPH	13 273 700,00 Kč

Dne 18.7.2019 provedla nacenění společnost s názvem STORAGE ONE,a.s., IČ 023 01 245, zastoupená Milanem Hlišákem, Předsedou představenstva

Milan Hlišák

Digitálně podepsal Milan Hlišák

Datum: 2019.07.18 10:00:23

+02'00'

Podpis osoby oprávněné jednat jménem či za účastníka