

KUPNÍ SMLOUVA

Č.j. R-23/16-2024

uzavřená níže uvedeného dne, měsíce a roku podle § 2079 a násl. a § 2085 a násl.
zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Čl. 1 Smluvní strany

Kupující: **Město Ostrov**

Sídlo: Jáchymovská 1, Ostrov 363 01

IČ: 00254843

DIČ: CZ00254843

Zastoupený: Bc. Pavel Čekan, starosta

Kontaktní osoba: Tomáš Bujanský, informatik

Telefon: (+420) 354 224 814

e-mail: tbujansky@ostrov.cz

Bankovní spojení: Komerční banka a.s.

Číslo účtu: 19-920341/0100

jako kupující, na straně jedné

(dále jen „kupující“)

a

Prodávající: **Aricoma Systems a.s.**

Sídlo: Hornoplní 3322/34, 702 00 Ostrava

IČ: 04308697

DIČ: CZ04308697

Zastoupený/Jednající: Jaroslav Dvořák, Vice President, člen představenstva

Kontaktní osoba: Jiří Kubát

Bankovní spojení: Česká spořitelna a.s.

Číslo účtu: 6563752/0800

Zápis v OR: vedeném u Krajského soudu v Ostravě spisová značka B 11012

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 IT technologií pro zvýšení kybernetické bezpečnosti“, 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.
- 2.3. Plněním této smlouvy dochází k realizaci následujících projektových záměrů kupujícího
 - registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008378, název projektu Zvýšení kybernetické bezpečnosti města Ostrov
- 2.4. Výše uvedený projekt stanoví dílčí specifika, která jsou promítnuta i do obsahu této smlouvy.

Čl. 3 Vlastnické vztahy

- 3.1. Prodávající prohlašuje, že je výlučným vlastníkem předmětu plnění smlouvy a jeho příslušenství, které je předmětem plnění této smlouvy.
- 3.2. Detailní technická specifikace předmětu plnění této smlouvy a počtu kusů jednotlivého zboží a jeho 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 a nehmotný majetek v podobě licencí, obojí včetně příslušenství. Předmět smlouvy je detailně specifikován v příloze č. 1 a 2 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 přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu, které jsou blíže specifikovány v příloze č. 1 této smlouvy. Bez provedení těchto služeb a prací nebude možné považovat předmět koupě za řádně dodaný.
- 4.3. Prodávající se zavazuje dodat předmět smlouvy kupujícímu s veškerými doklady nutnými k převzetí a zejména k užívání dodaných zařízení a software a provést všechny požadované související služby a práce.
- 4.4. Prodávající touto smlouvou prodává kupujícímu do výlučného vlastnictví předmět kupní smlouvy definovaný v odst. 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 prodáváných 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., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) a ustanovení § 2358 a následující zákona č. 89/2012 Sb., občanský zákoník, 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 odst. 2.1 této smlouvy, přičemž se skládá z ceny dodávky jednotlivých zařízení a licencí. Kupní cenu je možné hradit po částech plnění, pro která tato smlouva stanoví samostatné termíny plnění.
- 6.2. Kupující se zavazuje zaplatit prodávajícímu za předmět spočívající v dodávce plnění uvedený v Čl. 4 této smlouvy kupní cenu ve výši
- 11 520 389,00 Kč bez DPH,
13 939 670,69 Kč včetně DPH,
když DPH ve výši 21 % činí 2 419 281,69 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. Kompletní skladba kupní ceny a její rozklad je obsažen v příloze č. 3 této smlouvy.
- 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. Prodávající na základě svého práva vystavit daňový doklad (fakturu) vystaví samostatnou fakturu za předmět koupě dle této smlouvy.
- 6.8. Kupující požaduje vyhotovení samostatných faktur pro jednotlivé projekty uvedené v článku 2.3 této smlouvy, a to na základě předání a převzetí rozhodných předmětů plnění podle této smlouvy a jejích příloh.
- 6.9. 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. Součástí daňového dokladu rovněž musí být název relevantního projektu a číslo projektu – viz odst. 6.12.
- 6.10. Splatnost daňového dokladu je 30 dnů ode dne jeho doručení kupujícímu.
- 6.11. 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., občanský zákoník. 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.
- 6.12. Všechny faktury dle této smlouvy musí obsahovat relevantní název a registrační číslo projektu, který je:
 - registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008378, název projektu Zvýšení kybernetické bezpečnosti města Ostrov
- 6.13. 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 dani z přidané hodnoty, 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

- 7.1. Prodávající předá kupujícímu předmět plnění této smlouvy do 25 týdnů od nabytí účinnosti této smlouvy, a to včetně realizace všech souvisejících služeb.
- 7.2. Místa dodání a předání předmětu plnění této smlouvy jsou na následujících adresách
 - technologická místnost na adrese MěÚ Ostrov, Jáchymovská 1, Ostrov,
 - technologická místnost na adrese Městská policie Ostrov, Hlavní tř. 797, Ostrov
- 7.3. Vlastnické právo k předmětu plnění přechází na kupujícího v okamžiku jeho předání prodávajícím a převzetí kupujícím potvrzeného na předávacím protokolu.
- 7.4. Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností předmětu plnění včetně užitku přechází na kupujícího současně s nabytím vlastnictví.

- 7.5. Náklady spojené s předáním předmětu plnění, zejména dopravu, nese prodávající a náklady spojené s převzetím nese kupující.
- 7.6. 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 kontaktní osoba kupujícího uvedená v článku 1. této smlouvy.
- 7.7. 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., občanský zákoník, se nepoužijí.

Čl. 8 Součinnost

- 8.1. Kupující požaduje, aby maximum prací odvedl prodávající samostatně, bez zatěžování pracovníků kupujícího. Součinnost kupujícího bude omezena na nezbytnou míru a bude se vztahovat především na schvalování výstupů prodávajícího v předem definovaných kontrolních dnech a na nezbytnou IT podporu nutnou k nasazení technologií.
- 8.2. Rozsah součinnosti bude odsouhlasen před zahájením implementačních a instalačních služeb, včetně termínů jejího poskytování.
- 8.3. V případě následného požadavku prodávajícího na součinnost nad dohodnutý rámec má kupující právo součinnost odmítnout, případně ji poskytnout v termínu a rozsahu dle svých možností, a to bez dopadu na harmonogram realizace a z něj vyplývající sankce za nedodržení termínů.
- 8.4. Neposkytnutí součinnosti jako důvod pro posun smluvních termínů bude akceptován pouze tam, kde byla součinnost kupujícím přislíbena při zahájení implementačních a instalačních prací.

Čl. 9 Projektový tým (seznam techniků)

- 9.1. Proávající se zavazuje předmět plnění smlouvy realizovat prostřednictvím projektového týmu (seznamu techniků), kterým prokázal kvalifikaci ve veřejné zakázce, na jejímž základě je uzavírána tato smlouva. Projektový tým (seznam techniků) prodávajícího je odpovědný za plnění této smlouvy.
- 9.2. Proávající se zavazuje realizovat předmět plnění této smlouvy prostřednictvím projektového týmu (seznamu techniků) v tomto složení na těchto pozicích:
Projektový manažer (Vedoucí realizačního týmu) – **Filip Junga**
Technický specialista – architekt podnikové ICT architektury – **Petr Michálek**
Technický specialista - kybernetická bezpečnost – **Luděk Mandok**
Technický specialista – správa logů – **Ondřej Šinták**
Technický specialista – síťová infrastruktura – **Richard Vodička**
Technický specialista – ověřovací systémy – **Petr Kasan**
- 9.3. Změna konkrétní osoby na pozici člena projektového týmu prodávajícího je možná pouze za předpokladu prokázání potřebné kvalifikace novou osobou v rozsahu stanoveném pro danou pozici člena projektového týmu stanovenou ve veřejné zakázce, na jejímž základě je uzavřena tato smlouva. Taková změna musí být prodávajícím řádně iniciována písemně dokladována a prokázána kvalifikace nové osoby na pozici člena projektového týmu před jeho zapojením do realizace plnění dle této smlouvy (včetně všech souvisejících požadavků na projektový tým stanovený v zadávacích podmínkách, na jejichž základě je uzavřena tato smlouva, jako např. max. počet pozic obsazených jednou osobou apod.).

Čl. 10 Další práva a povinnosti smluvních stran

- 10.1. 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.
- 10.2. Prodávající se dále zavazuje předat kupujícímu listinné potvrzení dodaných licencí, které jsou předmětem plnění této kupní smlouvy.

Čl. 11 Práva z vadného plnění a smluvní záruka

- 11.1. Kupující požaduje a prodávající se zavazuje držet záruku 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.
- 11.2. 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.
- 11.3. 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.
- 11.4. Na příslušenství a provedené implementační práce bude prodávajícím poskytována záruka v délce dvou (2) let. 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. V případě vady provedené implementační práce se prodávající zavazuje odstranit závadu do 14 kalendářních dnů ode dne nahlášení vady kupujícím.
- 11.5. 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.
- 11.6. 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.
- 11.7. 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 nevážnou práva třetích osob.
- 11.8. 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.
- 11.9. Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.
- 11.10. Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.

Čl. 12 Smluvní pokuty

- 12.1. 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.

- 12.2. 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.
- 12.3. V případě prodlení prodávajícího s odstraněním nahlášené závady ve lhůtě uvedené v odst. 11.5 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.
- 12.4. V případě prodlení prodávajícího s odstraněním nahlášené závady na příslušenství nebo provedených implementačních pracích se stanovuje smluvní pokuta ve výši 200,- za každý celý kalendářní týden prodlení.
- 12.5. V případě prodlení prodávajícího s odstraněním nahlášené závady v podobě provedených implementačních a konfiguračních prací se stanovuje smluvní pokuta ve výši 500,- za každý celý pracovní den prodlení.
- 12.6. V případě realizace předmětu plnění této smlouvy projektovým týmem prodávajícího v jiném složení, než které je uvedeno v odst. 9.2 této smlouvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 20.000,- Kč za každý zjištěný případ.
- 12.7. V případě nedodržení komunikace v českém jazyce na základě této smlouvy podle odst. 11.8 smlouvy je kupující oprávněn vyúčtovat smluvní pokutu ve výši 1.000,- Kč za každý případ.
- 12.8. Zaplacením smluvní pokuty nezaniká povinnost druhé strany závazek splnit a není tím dotčeno právo poškozené strany na náhradu škody, které nesplněním povinnosti vznikla.
- 12.9. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30-ti dnů od doručení jejího vyúčtování.

Čl. 13 Pojištění

- 13.1. Prodávající prohlašuje, že má uzavřenou pojistnou smlouvu se společností Generali Česká pojišťovna a.s., Spálená 75/16, Nové Město, 110 00 Praha 1, Česká republika, IČO 45272956 proti škodám způsobeným třetím osobám jeho činností, včetně možných škod způsobených jeho pracovníky, a to ve výši pojistného plnění ve výši minimálně 5 mil. Kč. Současně se zavazuje udržovat pojistnou smlouvu v platnosti po celou dobu plnění této smlouvy.
- 13.2. Nebude-li prodávající udržovat platné pojištění ve smyslu ustanovení odst. 13.1 tohoto článku po celou dobu trvání smlouvy, bude tato skutečnost považována za podstatné porušení povinností vyplývajících z této smlouvy.
- 13.3. Smluvní strany shodně konstatují, že v souladu s obecnými podmínkami pojištění odpovědnosti prodávajícího a dle příslušných zákonných ustanovení bude případně pojistné plnění z titulu náhrady škody způsobené prodávajícím nebo jeho sub dodavateli na základě této smlouvy hrazeno pojišťovnou přímo kupujícímu.

Čl. 14 Odstoupení od smlouvy

- 14.1. 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., občanský zákoník, ve znění pozdějších předpisů.
- 14.2. 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.

- 14.3. 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.
- 14.4. Realizace smlouvy je podmíněna přidělením dotace. Kupující nedisponuje vlastními finančními prostředky v objemu zajišťujícím provedení dodávky. Z uvedeného důvodu si kupující vyhrazuje právo odstoupit od této smlouvy v případě nepřidělení finančních prostředků dotačním orgánem. Pokud kupující odstoupí od této smlouvy z důvodu nedostatečnosti finančních prostředků, nevzniká prodávajícímu vůči kupujícímu jakýkoliv nárok.
- 14.5. Kupující požaduje, aby prodávající před uzavřením smlouvy předložil potvrzení od lokálního zastoupení výrobce, že nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. V případě, že prodávající uvedený požadavek kupujícího nesplní, vyhrazuje si kupující právo odstoupit od uzavření smlouvy s okamžitou platností bez jakýchkoliv sankcí.

Čl. 15 Registr smluv – doložka

- 15.1. Proávající 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.
- 15.2. Proávající 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.
- 15.3. Zveřejnění smlouvy a metadata v registru smluv zajistí kupující.

Čl. 16 Závěrečná ustanovení

- 16.1. Tato smlouva je vyhotovena v elektronickém originále, jenž po podpisu druhou ze smluvních stran obdrží obě smluvní strany.
- 16.2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
- 16.3. Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními zákona č. 89/2012 Sb., občanský zákoník.
- 16.4. Přílohami této smlouvy jsou:
 - Příloha č. 1 – Technická specifikace zadavatele – dodávka IT
 - Příloha č. 2 – Technická specifikace dodavatele
 - Příloha č. 3 – Cenová tabulka
 - Příloha č. 4 - Smluvní podmínky k sociálně odpovědnému zadávání
- 16.5. Strany této smlouvy berou na vědomí, že kupující jako správce osobních údajů je oprávněn zpracovávat zde uvedené osobní údaje v souladu s článkem 6 odst. 1 písm. b) Obecného nařízení (toto zpracování je nezbytné pro splnění smlouvy) a písm. c) (toto zpracování je nezbytné pro splnění právní povinnosti správce zveřejnit smlouvu na profilu zadavatele dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, postupy podle zákona

č. 106/1999 Sb., o svobodném přístupu k informacím nebo na své úřední desce dle zákona č. 128/2000 Sb., o obcích).

- 16.6. Předmět veřejné zakázky bude spolufinancován z prostředků Národního plánu obnovy, výzva č. 41 s názvem „Kybernetická bezpečnost – obce“, název projektu: „Zvýšení kybernetické bezpečnosti města Ostrov“, reg. č. projektu CZ.31.2.0/0.0/0.0/23_093/0008378. Z tohoto důvodu:
- a) je prodávající, povinen minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací projektu (předmětu plnění této smlouvy) zaměstnancům nebo zmocněncům pověřených orgánů (MV 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,
 - b) prodávající výslovně souhlasí s tím, že kupující je oprávněn za účelem kontroly postupu kupujícího poskytnout oprávněným osobám veškeré dokumenty (včetně nabídky prodávajícího),
 - c) prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu (veřejné zakázky/dotace) včetně účetních dokladů minimálně do konce roku 2035,
 - d) prodávající je povinen spolupůsobit při výkonu finanční kontroly ve smyslu § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.
- 16.7. V případě, že po podpisu této smlouvy na prodávajícího anebo jeho poddodavatele budou dopadat mezinárodní sankce podle zákona upravujícího provádění mezinárodních sankcí č. 69/2006 Sb. ve smyslu zákona č. 240/2022 Sb. účinného od 1. 9. 2022, je povinen to prodávající písemně oznámit kupujícímu. V případě, že oznámení neprovede a kupující zjistí, že na prodávajícího anebo jeho poddodavatele mezinárodní sankce dopadají, vyzve prodávajícího k vysvětlení nebo nápravě formou vyjmutí osoby ze sankčního seznamu. V případě že náprava není možná, odstoupí kupující od této smlouvy, přičemž účinnost odstoupení nastává doručením odstoupení prodávajícímu.
- 16.8. 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

V Ostrově

Bc. Pavel Čekan
starosta

Za prodávajícího

V Jihlavě

Jaroslav Dvořák
Vice President, člen představenstva

Obsah

1	TECHNICKÁ SPECIFIKACE KUPUJÍCÍHO (ZADAVATELE) PRO PROJEKT KYBERNETICKÉ BEZPEČNOSTI MĚSTA	
2	POPIS PLNĚNÍ PODLE TÉTO TECHNICKÉ DOKUMENTACE.....	3
3	POŽADAVKY NA TECHNICKÉ ŘEŠENÍ	5
3.1	OBECNÉ POŽADAVKY NA JEDNOTLIVÉ ČÁSTI A OBLASTI PLNĚNÍ.....	5
3.2	FUNKČNÍ POŽADAVKY NA ŘEŠENÍ	8
3.2.1	<i>Oblast zvýšení zabezpečení komunikační sítě</i>	<i>9</i>
3.2.2	<i>Oblast vytvoření serverového prostředí s vysokou dostupností pro provoz IS.....</i>	<i>13</i>
3.2.3	<i>Oblast řízení privilegovaných účtů a zařízení</i>	<i>17</i>
3.2.4	<i>Oblast vícefaktorové autentizace</i>	<i>18</i>
3.2.5	<i>Oblast zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů..</i>	<i>20</i>
4	INSTALACE A ZPROVOZNĚNÍ	25
4.1	OBECNÉ POŽADAVKY NA INSTALAČNÍ SLUŽBY	25
4.2	PODROBNÝ POPIS INSTALAČNÍCH SLUŽEB	25
4.3	DOKUMENTACE K DODÁVANÉMU ŘEŠENÍ	27
4.3.1	<i>Prováděcí dokumentace</i>	<i>27</i>
4.3.2	<i>Provozní dokumentace</i>	<i>28</i>
4.4	ZAŠKOLENÍ IT ADMINISTRÁTORŮ	28
4.5	TESTOVACÍ PROVOZ	28
4.6	AKCEPTAČNÍ ŘÍZENÍ.....	28
4.6.1	<i>Dílčí akceptační řízení</i>	<i>28</i>
4.6.2	<i>Souhrnné akceptační řízení - akceptace</i>	<i>28</i>
4.6.3	<i>Opakované akceptační řízení</i>	<i>29</i>
4.7	HARMONOGRAM PLNĚNÍ	30
4.8	PROJEKTOVÉ ŘÍZENÍ	31

1 Technická specifikace kupujícího (zadavatele) pro projekt kybernetické bezpečnosti města

Zadavatel požaduje dodávku jednotlivých komponent dle této technické specifikace včetně příslušenství v níže uvedené minimální specifikaci.

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

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí zadavatele (dále též „kupující“) k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

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.

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

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

V případě, že se tato dokumentace odkazuje na přílohu s označením „**NDA**“, jedná se o „Popis stávajícího technologického prostředí“, který bude poskytnut na základě podpisu smlouvy o ochraně důvěrných informací.

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.

2 Popis plnění podle této technické dokumentace

Předmětem plnění této technické specifikace je dodávka a implementace opatření v oblasti kybernetické bezpečnosti, a to včetně nedílně souvisejících požadavků typu dodání licencí, zaškolení, zpracování dokumentace a služeb technické podpory.

V rámci plnění dojde k rozšíření stávajícího prostředí realizací opatření v dále vyjmenovaných oblastech. Pro zajištění kupující požaduje dodávku následujících zařízení a SW licencí:

Oblast Kybernetické bezpečnosti	Typ	Název položky
Oblast Zvýšení zabezpečení komunikační sítě	SW	Licence software pro řízení přístupu do sítě založeného na protokolu 802.1x
	HW	Páteří přepínače s příslušenstvím Přístupové přepínače s příslušenstvím Přístupové body Wi-Fi (AP) s příslušenstvím Next-Generation Firewally s příslušenstvím
Oblast Vytvoření serverového prostředí s vysokou dostupností pro provoz IS	HW	Hyperkonvergované (HCI) servery Úložiště záloh s řízenou retencí
	SW	Licence serverové virtualizace Licence diskové virtualizace Licence serverových operačních systémů Licence klientské přístupové k serverovému operačnímu systému Licence aplikační virtualizace
Oblast Řízení privilegovaných účtů a zařízení	SW	Licence SW pro správu a zabezpečení privilegovaných účtů
Oblast Vícefaktorová autentizace	SW	Licence SW pro autentizaci uživatelů pomocí identifikačních karet Licence SW pro správu identifikačních karet a interních a veřejných certifikátů včetně PKI
	HW	Klávesnice s integrovanou čtečkou karet Hybridní identifikační karty
Oblast Zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů	HW	Úložiště pro logování Nástroj pro sběr a vyhodnocování síťových toků
	SW	Licence SW pro sběr a správu logů
a související příslušenství		

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Předmětem plnění jsou následující činnosti dodavatele (dále též „prodávající“):

- dodávka licencí, implementace, testovací provoz a předání do řádného užívání jednotlivých oblastí plnění.

Pro výše uvedený rozsah plnění:

- začlenění nabízených technologií do stávajícího prostředí,
- úprava dodaného řešení dle potřeb a požadavků kupujícího,
- zaškolení IT administrátorů kupujícího.

Dále je předmětem plnění dodávka:

- dokumentace k dodanému plnění v požadovaném rozsahu,
- dalších licencí potřebných pro provoz SW komponent,
- listinného potvrzení dodaných licencí co do jejich počtu a rozsahu.

3 Požadavky na technické řešení

Hlavním cílem je zvýšení kybernetické bezpečnosti a naplnění požadavků daných zákonem číslo 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), tj. v souhrnu zajištění a zvýšení bezpečnosti informačních a komunikačních systémů kupujícího.

Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

Pokud dodavatelem nabízené řešení vyžaduje komponenty nebo služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

Zadavatel z důvodů jednotné správy IT infrastruktury a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.

Veškeré komponenty, které dodavatel dodává v rámci předmětu plnění, musí splňovat následující podmínky:

Jedná se o nové a nerepasované komponenty.
Byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce.
Mají plnou záruku od výrobce.
Mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce.
Obsahují všechny nezbytné licence na používání příslušného softwaru.
Jsou v databázi výrobce uvedeny jako prodaná kupujícímu – zadavateli.
Zadavatel 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.

3.1 Obecné požadavky na jednotlivé části a oblasti plnění

Oblast Zvýšení zabezpečení komunikační sítě
Bude provedeno nasazení nových přístupových přepínačů (i na stávající pozice) pro možnost plošné implementace technologie 802.1X.
Budou dodány a implementovány přístupové body WiFi s centrální správou.
Architektura WiFi bude založena na řešení s centrální správou prováděnou kontrolérem (řadičem), který bude součástí firmwaru síťových prvků a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatickou detekci a reakci na rušení cizím signálem.
V celé LAN bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby Active Directory založené na standardu IEEE 802.1X. Stejný standard řízení přístupů bude implementován i pro zařízení bez podpory Active Directory, pouze pro autentizaci bude využit jiný, zařízením podporovaný, způsob – certifikát apod.
Bude implementován vysoce dostupný síťový / perimetrový firewall pro provádění hloubkové kontroly komunikace mezi interními subjekty (uživatel, zaměstnanec, server) a interními i veřejnými zdroji (internet), ověřování validity komunikačních a aplikačních protokolů, filtrací nežádoucích adres a antimalwarovou kontrolou. Ochrání tak interní systémy před zavlečením škodlivého kódu z prostředí internetu či jiných veřejných/externích sítí. Bude poskytovat také prostředky VPN pro vzdálený přístup uživatelů a ochranu aplikací publikovaných z interní sítě do internetu. Firewall nahradí stávající řešení a převezme jeho vhodná konfigurační nastavení.
Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky bude vzorová konfigurace 802.1x na

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

všech typech koncových zařízení Kupujícího.
Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). WiFi bude nabízet více SSID (např. zaměstnanci, hosté, veřejnost), které budou obsluhovány samostatnými VLAN a budou napojeny na radius servery. Zaměstnanci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) bude provedeno dle 802.11i, tedy – WPA2/3 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty, popř. veřejnost, kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál nabízeného systému řízení 802.1X s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.
Pro hosty a veřejnost budou zřízeny samostatná VLAN (, které bude komunikačně odděleny od vnitřních sítí organizace. Tyto VLAN bude mít své L3 rozhraní až na úrovni firewallu tak, aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro zaměstnance.
Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s přepínáním provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.
Bude vybudován, resp. modernizován systém základních síťových služeb (DHCP, DNS včetně validujícího resolveru DNSSEC) a dalších podpůrných služeb nezbytných pro provoz dodávaných technologií.

Oblast Vytvoření serverového prostředí s vysokou dostupností pro provoz IS
Bude provedena instalace a implementace obou HCI (hyper converged infrastructure) serverů včetně serverové a diskové virtualizace a začlenění do stávající infrastruktury.
HCI servery budou tvořit samostatný cluster, funkčně a z pohledu správy nezávislý na stávající virtualizační platformě.
Bude vybudována plnohodnotná platforma aplikační virtualizace (terminálových služeb) včetně webového portálu s publikovanými aplikacemi pro lokální i vzdálený přístup uživatelů a centrálního přístupového bodu zajišťující vyrovnavání zátěže mezi jednotlivými aplikačními servery. Součástí implementace je vybudování aplikačního prostředí uživatele – tj. instalace a konfigurace klientských aplikací (Office, Acrobat). Dodavatel plnění dle této technické specifikace se dále zavazuje poskytnout součinnost dodavatelům IS kupujícího VITA a GINIS, které ve stávajícím prostředí kupující provozuje, při jejich přenosu do nově vybudovaného prostředí těmito dodavateli. Tato součinnost je předpokládána zejména na úrovni potřebných konfigurací virtualizační platformy, dodaného prostředí serverových OS a centrálně konfigurovaných bezpečnostních pravidel.
Bude provedena konsolidace stávajícího serverového prostředí – migrace stávajících virtuálních serverů do nově vybudované virtualizační platformy a jejich optimalizace. Seznam VM určených k takové migraci je obsažen v části podléhající NDA – Popisu stávajícího prostředí.
Zálohovací systém bude rozšířen o bezpečné úložiště s nastavitelnou retencí uložených záloh a jejich ochranou proti změně časovými zámky. Součástí plnění jsou i další nezbytné konfigurační změny stávajícího zálohovacího prostředí v souvislosti s implementací nových technologií dle této technické specifikace.

Oblast řízení privilegovaných účtů a zařízení
Pro oblast řízení privilegovaných účtů a zařízení bude implementován systém, který bude sloužit jako vstupní bod pro místní i externí správce, kteří jeho prostřednictvím budou přistupovat ke spravovaným systémům. V tomto bodě bude činnost správců zaznamenávána a logována. Systém dále zajistí automatickou změnu hesel ve spravovaných systémech s otevřenou a veřejně dostupnou dokumentací (tzv. rotaci hesel).

Oblast Vícefaktorová autentizace
Bude implementován nástroj autentizace uživatelů s využitím více faktorové (víceúrovňové) autentizace.
Ověřování uživatele při přihlašování ke koncovému zařízení (resp. jeho operačnímu systému) bude prováděno pomocí identifikačních karet typu Smart card, které budou sloužit jako bezpečné úložiště uživatelských certifikátů, kterými bude

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

ověřována identita uživatele.
Autentizační prostředky (karty smart card) budou certifikovány jako kvalifikovaný prostředek pro vytvoření a používání kvalifikovaného elektronického podpisu při uložení příslušných uživatelských certifikátů vydávaných veřejnými certifikačními autoritami. Autentizační prostředky musí splňovat požadavky nařízení eIDAS č.910/2014.
Autentizační prostředky budou vedle kontaktní části (smart card) obsahovat i bezkontaktní část, která umožní využívání pro autentizaci uživatelů v docházkovém/přístupovém systému (konfigurace těchto systémů není součástí předmětu plnění), popřípadě dalších systémech založených na stejné technologii.
Součástí plnění bude komplexní nástroj pro evidenci a řízení celého životního cyklu karet a uložených certifikátů, včetně jednoduché automatické obnovy certifikátu uživatelem pomocí grafického průvodce před vypršením platnosti certifikátu.
Součástí dodávky a implementace jsou i veškeré nezbytné podpůrné systémy – zejména vybudování PKI (Public Key Infrastructure) včetně certifikační autority a vhodné sady šablon vystavovaných certifikátů.
Řešení musí umožňovat jednoduchou správu identifikačních prostředků tak, aby mohla být prováděna zaškoleným uživatelem – např. personalistou, a to včetně prvotního vydání karty a certifikátu uživateli.

Oblast Zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů
Nástroj pro sběr a správu logů (systém centrálního logování).
Bude implementován nástroj pro správu logů (tzv. log management). Nástroj bude sbírat, normalizovat a spravovat logy a data síťových toků KS bezpečnostní a provozní povahy napříč KS a IS.
Uložené logy bude možné snadno prohledávat či filtrovat na základě multikriteriálních dotazů napříč zdroji logů.
Zavedený nástroj bude obsahovat notifikační systém, kdy notifikace bude možné navázat na výskyt provozní či bezpečnostní události.
Zdroje dat/ logů pro budou vybrány z tzv. primárních a podpůrných (technických) aktiv kupujícího. K jejich určení bude využito Vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí kupujícího (kupující neprovozuje významný informační systém). Nezbytné konfigurační zdrojových (popř. dalších navázaných) systémů jsou součástí plnění, případnou potřebnou součinnost dodavatelů agendových IS (pokud má dojít ke sběru jejich logů) zajišťuje na svůj náklad kupující.
Nástroj bude implementován tak, aby jeho provoz nebyl závislý na infrastruktuře kupujícího a byl tak schopen zaznamenávání činnosti a detekce bezpečnostních či nestandardních událostí i v nestandardních provozních stavech infrastruktury kupujícího (přetížení, start, nestabilita, bezpečnostní událost/incident apod.).
Nástroj pro sběr a vyhodnocování síťových toků
Pro získání schopnosti detekce a identifikace bezpečnostní události na úrovni síťového provozu bude implementován nástroj pro sběr a vyhodnocování síťových toků, který bude provádět sledování a hloubkovou analýzu síťových toků (netflow) na perimetru sítě a v libovolném jejím segmentu podle aktuálních potřeb a požadavků.
Nástroj bude ukládat historii síťového provozu (resp. síťových toků) po dobu min. 1 měsíc pro účely operativní analýzy a podpory při řešení kybernetických událostí a incidentů nebo provozních problémů. Současně bude ukládat získané informace a také informace o své činnosti (změny konfigurací, aktualizace) do nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů.
Nástroj bude disponovat pokročilou tzv. behaviorální analýzou, tj. detekcí nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, detekce provozních problémů apod.) a bude umožňovat detekci anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.
Nástroj bude implementován tak, aby jeho provoz nebyl závislý na infrastruktuře kupujícího a byl tak schopen zaznamenávání činnosti a detekce bezpečnostních či nestandardních událostí i v nestandardních provozních stavech infrastruktury kupujícího (přetížení, start, nestabilita, bezpečnostní událost/incident apod.).

Společné požadavky

Všechny systémy budou dodány a vybudovány jako lokální (on-premise) v prostředí kupujícího. Jejich funkčnost bude nezávislá na dostupnosti externích zdrojů a internetové konektivitě s výjimkou případného ověřování licenčních klíčů a manuálně řízeného stahování funkčních a bezpečnostních aktualizací.

3.2 Funkční požadavky na řešení

V této části jsou uvedeny povinné minimální parametry prvků nabízeného řešení a jejich minimální funkcionality. Dodavatel může pro plnění nabídnout technologie s touto minimální nebo vyšší úrovní.

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

Dodavatel 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 výrobci a obchodním (nebo typovým) označení.

Konkrétní parametry jednotlivých komponent dodavatel 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.

Zadavatel výslovně upozorňuje, že popis způsobu naplnění každého povinného parametru musí být konkrétní, úplný a musí výslovně prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku zadavatele), že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru. Nesplnění požadovaného způsobu prokázání splnění povinných parametrů je považováno za nesplnění zadávacích podmínek.

3.2.1 Oblast zvýšení zabezpečení komunikační sítě

2x Páteří přepínače

Parametr	Popis parametru
Provedení	L2/L3 přepínač v rackovém provedení, 1U včetně montážního materiálu
Porty	24x 10 Gb SFP+ a 2x 100 Gb QSFP28 (kompatibilní s 40Gb QSFP+ a podporou rozdělení každého na 4x 10/25Gb porty)
Propustnost	Neblokovaná architektura, přepínací kapacita min. 880 Gbps
Agregace portů	Podpora LACP, min. 20 portů v agregační skupině, bez omezení počtu skupin
Směrování	Hardwarové statické routování včetně VLAN, dynamické směrování (min. RIP, OSPF, BGP), směrování založené na politikách, min. 8000 routovacích záznamů pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p
VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření, podpora IEEE 802.1ad (Q-in-Q), podpora VXLAN, min. 4000 VLAN
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS
MAC	Podpora min. 60 000 MAC adres
Síťové toky	Plný přímý export síťových toků - Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent)
Rozšířené stohování	Pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG/MCLAG (Multi-Chassis Link Aggregation) nebo obdobná
Zrcadlení provozu	Podpora RSPAN (Remote SPAN) a ERSPAN (Encapsulated Remote SPAN)
Napájení	Redundantní interní napájecí zdroje, vyměnitelné za provozu (hot-swap)
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci. Vyhrazený 1 Gb port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
Záruka	Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den

21x Přístupový přepínač

Parametr	Popis parametru
Provedení	L2+ přepínač v rackovém provedení max. 1U a hloubka do 32 cm, neblokovaná architektura
Porty	Min. 48x 1 GbE PoE+, 4x 10 Gb SFP+
Propustnost	Neblokovaná architektura, přepínání/směrování min. 176 Gbps
Power on Ethernet	Podpora PoE/PoE+ 802.3af/at na všech metalických portech, celkový PoE výkon min. 700 W
Agregace portů	Podpora LACP, min. 8 portů v agregační skupině, min. 12 skupin
Směrování	Statické routování
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN na základě 802.1X ověření
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS
MAC	Podpora min. 30 000 MAC adres
Zrcadlení provozu	Zrcadlení síťového provozu portu(ů), podpora SPAN
Napájení	Interní napájecí zdroj
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
Hlučnost	Max. hlučnost 47 dB pro umístění v pracovních prostorech
Záruka	Záruka a servisní podpora výrobce min. 60 měsíců

40× Přístupový bod WiFi s příslušenstvím

Parametr	Popis parametru
Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na strop a zeď
Frekvence	Min. 3 nezávislé rádiové moduly činnost v rádiovém pásmu 2,4 a 5 GHz současně, s podporou standardu OFDMA min. u 2 modulů
Architektura	Homogenní WiFi síť s rychlým a spolehlivým roamingem klientů, podpora Mesh (https://en.wikipedia.org/wiki/Wireless_mesh_network)
Anténní systém	Interní systém, optimalizovaný pro montáž na strop
Současná obsluha více klientů	Podpora MU–MIMO (Multi–User MIMO) – multi–user multiple input/multiple output
Přenosové rychlosti	5 GHz min. 1200Mbps, 2.4 GHz min. 550Mbps
Standardy	Podpora standardů 802.3at, 802.11n, 802.11ax, 802.11k, 802.11n, 802.11r, 802.11v, Hotspot 2.0
Multi SSID	Podpora vysílání min. 8 SSID (WiFi sítí) na 2.4 i 5 GHz současně, podpora přiřazení každého SSID do samostatné VLAN
Zatížení	Min. 300 přiřazených (asociovaných) klientů na rádiový modul
Řízení zátěže	Automatické rozkládání zátěže přístupových bodů předáváním klientů a automatickým směrováním klientů na 5 GHz (pokud klienti podporují)
Porty	Min. 2x 1Gb, min 1x PoE s podporou standardů 802.3at a 802.3af
Bezpečnost	Trvalá detekce cizích přístupových bodů/klientů nezávislým radiem, spektrální analýza
Kontroler	Centrální kontroler pro kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů součástí dodávky. Kontroler musí být provozován v interní síti zadavatele a být integrální součástí firmware nabízených síťových prvků. Grafické webové rozhraní pro správu
Autentizace, autorizace	Podpora standardu WPA3 (Wi-Fi Protected Access III), integrovaný portál pro autentizaci uživatelů (Captive portal), ověření klientů (min. hardware, uživatel, operační systém, certifikát) s využitím protokolu 802.1X
IoT a lokalizace	Integrovaná hardwarová podpora standardu 802.15.4 (Zigbee) a BLE (Bluetooth Low Energy)
Správa	Plná podpora CLI, SSH, SNMP, syslog, web rozhraní, hromadná aktualizace firmware a konfigurace

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
Monitoring	Detailní monitoring a diagnostika provozu v reálném čase - parametry připojení a komunikace klienta, stav přístupových bodů (počty klientů, vytížení kanálů, signál, cizí (rogue) přístupové body)
Úsporné napájení	Podpora standardu 802.3az - Energy-Efficient Ethernet (EEE)
Záruka	Min. 60 měsíců poskytovaná výrobcem zařízením

2× Next-generation firewall

Parametr	Popis parametru
Porty	Min. 2x 10 Gb SFP+ a 2x 10x GbE (mohou být sdílené), 8x 1GbE, USB pro ext. záložní 4G modem
NGFW	Min. základní funkce Next-generation firewall- viz https://en.wikipedia.org/wiki/Next-generation_firewall-firewall , aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
Architektura	Založená na využití specializovaných čipů (ASIC) pro akceleraci klíčových funkcí a vyšší bezpečnost
Počet současných spojení	Min. 1,3 milionu
Propustnost SSL VPN	Min. 1 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů
Propustnost SSL inspekce	Min. 2.5 Gbps
Propustnost firewallu	Min. 25 Gbps (pro UDP pakety >= 512 bytů)
Propustnost NGFW	Min. 2.5 Gbps
Propustnost IPS	Min. 4.5 Gbps
Propustnost detekce škodlivého kódu	Min. 2 Gbps
Virtualizace	Min. 5 virtuálních kontextů
Vysoká dostupnost	Režimy Active/Passive i Active/Active se společnou konfigurací
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	Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd.)
Kategorizace a blokáce provozu	Založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne
Antispam	Antispamová a antivirová inspekce elektronické pošty
Sandbox	Integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba součástí dodávky)
Aktualizace	Automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu
Management a monitoring	HTTP/S, SSH, SNMP, syslog
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
SD-WAN	Integrovaná podpora SD WAN-min. rozkládání zátěže a vysoká dostupnost více internetových přípojek
Sledování toků	Export síťových toků (Netflow nebo ekvivalent)
Bezpečnost	Integrovaný TPM (Trusted Platform Module) čip pro ukládání citlivých údajů
Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů
Záruční servis	Záruka a podpora výrobce min. 60 měsíců v režimu 24x7. Odeslání náhradního zařízení nejdéle následující pracovní den po nahlášení závady. Včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí-URL filtrace, IPS, antimalware, antisipam, aplikační kontrola, sandbox)

Licence software pro řízení přístupu do sítě založeného na protokolu 802.1x

Parametr	Popis parametru
Provedení	Software nebo softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN
Základní autentizační metody	Min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, autorizace proti externí SQL databázi
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth)
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory
Externí identity	Podpora autentizace externími identitami - min. Microsoft, Google
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
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

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu
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.
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-bit.
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, modality, technologické prvky, IoT
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance není součástí dodávky
Licence	Trvalá licence pro min. 500 současných (konkurenčních) koncových zařízení ověřených pomocí 802.1X bez omezení počtu uživatelů
Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA
Kompatibilita	Software nebo appliance určen pro provoz v prostředí stávající serverové virtualizace
Podpora	Podpora výrobce 60 měsíců včetně nároku na nové verze a aktualizace software

Síťové příslušenství

Parametr	Popis parametru
Optické moduly	90x SFP+ 10Gb, SM, LC, min. 1 km, včetně diagnostiky, kompatibilní s nabízenými přepínači 6x SFP+ 10Gb, SM, LC, min. 1 km, kompatibilní s nabízenými servery
Vysokorychlostní kabely	1x kabel QSFP28 – QSFP28, 100 Gb, 0,5 m, kompatibilní s nabízenými přepínači 2x kabel QSFP28 - 4x SFP28+ 25Gb, 5 m, kompatibilní s nabízenými přepínači a servery
Optické kabely	90x patch kabel SM LC-SC, 3 m 10x patch kabel SM LC-LC, 3 m
Záruka	36 měsíců

3.2.2 Oblast vytvoření serverového prostředí s vysokou dostupností pro provoz IS

2x Hyperkonvergováný (HCI – hyperconverged infrastructure) server, včetně příslušenství

Parametr	Popis parametru
Provedení	Rackové provedení max. 1U včetně výsuvných kolejnic a montážního materiálu do racku
CPU	1x procesor maximálně 32 jádrový (kvůli licencování provozovaného software) Výkon server dle https://spec.org SPECrate®2017_int_base =350 SPECrate®2017_fp_base =400
RAM	768 GB, DDR-5, všechny paměťové kanály CPU musí být využity

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Úložiště pro hypervizor	Min. 2x SSD 480 GB, RAID1, provedení M.2, nezabírá pozice HDD
Bezpečnost	Integrovaný modul TPM 2.0
Úložiště	Min. 8x 3,84 TB NVMe SSD, 1 DWPD (Drive Writes Per Day) po dobu záruky SSD výměnné za provozu (hot-plug), kompatibilní s nabízenou diskovou virtualizací
HDD/SSD řadič	NVMe, HBA i RAID režim (RAID 5,6,50,60), kompatibilní s nabízenou diskovou virtualizací
LAN	3x 2 portová NIC10/25Gb SFP28 s podporou virtualizace-VMware NetQueue, Microsoft VMQ a podporou NPAR (Network Partitioning) 1x 1GbE samostatný port pro vzdálený management
USB	Min. 3x USB port 3.x, min. 1x na čelním panelu s podporou bootování
Vzdálená správa	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)
Napájení	Redundantní napájecí zdroje min. 500W, musí splňovat požadavky na certifikaci energetické účinnosti Platinum dle 80 PLUS (https://cs.wikipedia.org/wiki/80_Plus) nebo lepší; případně na stejné nebo vyšší úrovni účinnosti podle jiné certifikace
Příslušenství	1x kabel SFP28 – SFP28 (25 Gb) 2 m (pro každý server)
Záruční servis	Záruční servis na dobu 60 měsíců poskytovaný výrobcem, oprava následující pracovní den od nahlášení v místě instalace, technická podpora výrobce v českém jazyce. Dostupnost ovladačů a dokumentace na webu výrobce dle výrobního/sériového čísla serveru.

Licence serverové virtualizace

Parametr	Popis parametru
Provedení	Licence software pro virtualizaci nabízených HCI serverů
Základní funkce	Hypervizor instalovaný přímo na hardware, umožňující plnou virtualizaci libovolného x86-64 serveru
Souborový systém	Integrovaný clusterový souborový systém sdílený mezi více hypervizory s podporou snapshotů
Migrace a replikace virtuálních serverů	Online bezvýpadková migrace virtuálních serverů/strojů (VM) mezi hypervizory, včetně současné změny úložiště VM. Podpora vícenásobných souběžných migrací. Online bezvýpadková replikace VM mezi hypervizory
Vysoká dostupnost	V případě výpadku hypervizoru automatický restart VM na jiném hypervizoru
Úspora výpočetních zdrojů	Podpora thin provisioning, RAM over-provisioning, snapshot management
Síťová komunikace	Virtuální síťový přepínač integrovaný v hypervizoru
Správa	Centralizovaná správa všech hypervizorů z jedné konzole
Úložiště	Podpora lokálních i SAN úložišť (SAS, iSCSI, FC)
Zálohování	Kompatibilita se současným systémem zálohování, včetně možnosti zálohování celých VM bez nutnosti instalace agentů do OS
Podpora	Podpora výrobce, včetně nároku na opravné verze po dobu min 60 měsíců

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Licence diskové virtualizace

Parametr	Popis parametru
Provedení	Licence software vysoce dostupného virtualizovaného softwarově definovaného diskového úložiště pro nabízené HCI servery
Replikace	Software musí umožnit minimálně synchronní replikace dat (zrcadlení, RAID1) mezi uzly SDS (virtualizačními servery)
Vysoká dostupnost	Automatické překlenutí výpadku jednoho prvku systému – jednoho serveru či jeho komponenty (např. jednoho disku). Včetně podpory zotavení a obnovení
Podpora virtualizace	Software bude provozován v úrovni hypervizorů nabízené serverové virtualizace s přímým přístupem k lokálnímu úložišti (nikoli jako VM)
Vyrovnávací paměť	Integrovaná podpora vyrovnávací paměti pro čtení i zápis s využitím flash médií (SSD, NVMe disků apod.) a RAM
Škálovatelnost výkonu	Podpora přidání dalších uzlů SDS s rozptřčením stávajících dat mezi uzly SDS. Podpora navýšování kapacity přidáním / zvětšením disků v rámci uzlu (licence nebude kapacitně omezena)
Serverová virtualizace - integrace	Podpora technologií nabízené serverové virtualizace – replikace virtuálních strojů, podpora virtuálních distribuovaných přepínačů, správa politik úložišť
iSCSI	Integrovaná podpora publikace kapacity SDS prostřednictvím protokolu iSCSI (tzv. iSCSI target) a NFS
Podpora	Podpora výrobce, včetně nároku na nové verze po dobu min 60 měsíců

Licence operačních systémů

Parametr	Popis parametru
Serverové operační systémy	Licence 64-bitového serverového operačního systému v aktuální verzi pro každý nabízený HCI server . Licence musí umožnit provoz hypervizoru a min. 20 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech souvisejících aplikací, nabízených systémů a aplikací a management nástrojů
Klientské přístupové licence k serverovému operačnímu systému	Klientské licence pro nabízené operační systémy umožňující využívat těchto systémů 130 uživatelům bez omezení počtu přístupových zařízení
Klientské licence aplikační virtualizace	Klientské licence pro nabízené operační systém umožňující využívat služeb aplikační virtualizace Windows aplikací(též terminálové služby) systémů 130 uživatelům bez omezení počtu přístupových zařízení
Vysoká dostupnost	Veškeré nabízené licence musí umožňovat legální provoz ve virtualizovaném prostředí s vysokou dostupností – tj. automatickým přesouváním virtuálních serverů mezi hypervizory (fyzickými servery)
Podpora	60 měsíců včetně nároku na bezpečnostní a opravné aktualizace

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

V případě dodávky licencí produktů společnosti MICROSOFT jsou požadovány licence, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv MICROSOFT.

V případě dodávky licencí produktů společnosti MICROSOFT dodavatel zároveň poskytne dokumentaci, ze které bude jasný původ, resp. prodejní kanál licencí nebo zajistí zpracování smlouvy se společností Microsoft (Microsoft - SELECT Plus, Open, CSP, MPSA, EA) ve prospěch kupujícího.

V případě dodávky licencí produktů společnosti MICROSOFT se vyžaduje dodání licencí formou licenčního portálu vázaného na koncového zákazníka (kupujícího), jehož součástí budou:

- Seznam nabízených licencí a jejich počet,
- Instalační médium,
- Instalační klíče,
- resp. další informace vztahujících se k licencím.

Pro zdokumentování jasného původu požaduje zadavatel poskytnout dokumentaci obsahující označení prvního nabyvatele softwaru a také číslo smlouvy, pod kterou byl software pořízen, úplný řetězec vlastníků softwaru, potvrzení o odinstalaci od každého z předchozích vlastníků.

1x Zabezpečené úložiště záloh s řízenou retencí

Parametr	Popis parametru
Provedení	Rackové provedení max. 2U včetně výsuvných kolejnic a montážního materiálu do racku
CPU	Minimálně 1x procesor min. osmijádrový. Výkon procesoru dle https://www.cpubenchmark.net/ min. 23 000 bodů
RAM	32 GB, min. min DDR5 - 3200
Úložiště firmware	Min. 2x SSD 480 GB, Enterprise provedení min. 1 DWPD, výměnné za provozu (hot-plug)
Úložiště dat	Min. 10x 20TB, 7 200 ot/min, výměnné za provozu (hot-plug)
RAID hardware	SATA/SAS 12Gb, RAID 1,5,6, zálohovaná zapisovací cache min. 8 GB, podpora HBA režimu
LAN	2x 1GbE, 2x 10Gb SFP+
USB	Min. 3 USB konektory-min. 1x verze 3.0, min. 1x na čelním panelu s podporou bootování
Vzdálená správa	Servisní modul s možností samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, virtuální média, možnost bootování se vzdáleného média
Napájení	Redundantní napájecí zdroje min. 800W, musí splňovat požadavky na certifikaci energetické účinnosti Platinum dle 80 PLUS (https://cs.wikipedia.org/wiki/80_Plus) nebo lepší; případně na stejné nebo vyšší úrovni účinnosti podle jiné certifikace
Souborový systém	XFS
Protokoly	SMB/CIFS, SNMP, http/s a ssh (management)
Výkon	Zápis min. 2 TB GB / hod.
Ochrana dat	Min. RAID5, automatická relokační vadných datových bloků
Retence dat	Programově nastavitelné retenční lhůty na uložený objekt (např. soubor), po dobu retence nelze objekt modifikovat
Redundance	Redundantní rotační díly a napájecí zdroje
Ochrana proti přepisu dat	Režim WORM (Write Once - Read many times Memory)
Kompatibilita	Kompatibilita se stávajícím zálohovacím software, podpora ukládání záloh, řízení jejich historie a řízení retenčních lhůt
Záruka	60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze firmware / software

3.2.3 Oblast řízení privilegovaných účtů a zařízení

1x Software pro správu a zabezpečení privilegovaných účtů

Parametr	Popis parametru
Základní funkčnost	Proxy brána určená pro správu a monitoring privilegovaných přístupů
Záznam relací	Zaznamenávání relací privilegovaných uživatelských účtů včetně vytváření logů
Licence	Licence pro monitorování a záznam min. 10 současně pracujících (privilegovaných) uživatelů na min. 100 definovaných cílových systémech
Logování relací	Nepozměnitelné podklady pro audit a analytické reporty uživatelského chování
Metadata	Ukládání metadat záznamů pro snadnou orientaci při prohlížení a vyhledávání (kliknutí myši, změna obrazovky apod.)
Architektura	Virtuální appliance, bezagentové řešení (bez nutnosti instalace agentů na monitorované systémy)
Autentizace	Min. Microsoft Active Directory, podpora vícefaktorové autentizace (MFA)
Autorizace	Integrované workflow pro autorizaci (min. povolené časy a trvání relace)
Bezpečné přihlášení	Uživatel privilegovaného účtu se přihlašuje pouze k proxy. Přihlášení k cílovému systému zajišťuje proxy - uživatel nezná přístupové údaje k cílovému systému
Přístupové protokoly a aplikace	Proxy umožňuje zprostředkované (bez znalosti hesla cílového systému) přihlášení k cílovým systémům min. RDP, SSH, webová GUI)
Notifikace	Zasílání notifikací o zahájení definované relace
Řízení v reálném čase	Monitorování relací v reálném čase a jejich okamžité ukončení v případě potřeby
Rozšiřitelnost	Podpora modulů (plug - in či obdobných) pro integraci s dalšími technologiemi / technologickými partnery
Rozhraní	Webové rozhraní pro přístup uživatelů k konfiguraci, bezpečná publikace do internetu (šifrovaná komunikace)
Zabezpečení přístupových údajů	Integrované bezpečné (šifrované) úložiště přístupových údajů k cílovým systémům
Rotace hesel	Automatická změna (rotace) hesel přístupových účtů ke spravovaným systémům s otevřenou a veřejně dostupnou dokumentací
Logy	Uložení auditních záznamů s přístupem pouze oprávněných uživatelů, podpora napojení na systém centrálního logování a/nebo SIEM
Podpora	Podpora výrobce po dobu 60 měsíců – nárok na nové verze software, včetně aktualizací

3.2.4 Oblast vícefaktorové autentizace

1x Software pro autentizaci uživatelů pomocí identifikačních karet

Parametr	Popis parametru
Základní popis	Systém pro autentizaci uživatele identifikačním prostředkem typu Smart card vůči adresářové službě Active Directory
Rozhraní	Grafické rozhraní v českém jazyce
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a automatické vyvolání uživatelského průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik
Autentizace	Autentizace uživatele v aktuálně výrobcem podporovaných operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft)
Správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK atd.)
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti
Licence	Pro 200 uživatelů (včetně externích)
Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze

1x Software pro správu identifikačních karet a interních a veřejných certifikátů včetně PKI

Parametr	Popis parametru
Provedení	Systém pro správu identifikačních prostředků (karet) a certifikátů
Rozhraní	Grafické rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti
Předávání veřejných doménových klíčů	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory
Prostředky	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků
Evidence	Systém umožní evidovat minimálně - typ prostředku (zejména kontaktní, bezkontaktní, hybridní) - druh prostředku (zejména uživatelský, administrační, operátorský) - stav prostředku (zejména používaný, k recyklaci, skartovaný) - historii prostředku (zejména datum zavedení do evidence, vydání uživateli, recyklace) - držitele prostředku (zejména aktuálního držitele i všechny předchozí držitele) - data uložená v prostředku (zejména certifikáty a další data, včetně historie dat)
Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance - včasné (konfigurovatelné) e-mailové upozornění na vypršení platnosti certifikátu
Certifikační autority	Systém musí umožnit použití jakékoliv certifikačních autority od kvalifikovaných poskytovatelů certifikačních služeb (https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx).
Operace	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů
Personifikace	Integrované prostředí pro generování podkladů pro potisk identifikačních karet i na vlastní tiskárně
Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečeti pro systémy třetích stran včetně dokumentace.
Notifikace	E-mailové upozornění uživatelů i správců na nestandardní stavy či nutnost zásahu (např. expirace certifikátu – nutnost obnovy)
PKI	Součástí řešení bude kompatibilní infrastruktura PKI (public key infrastructure) pro zajištění celého životního cyklu osobních přihlašovacích certifikátů a jejich šablon
Licence	Pro 200 uživatelů, včetně externích
Podpora	Podpora výrobce po dobu 60 měsíců – nárok na nové verze software, včetně aktualizací

140x Klávesnice s integrovanou čtečkou karet

Parametr	Popis parametru
Provedení	PC klávesnice s integrovanou čtečkou nabízených čipových (SmartCard) karet, připojitelná přes USB
Rozložení kláves	České rozložení a popis klávese samostatným numerickým blokem, české popisy kláves. Kvalitní ergonomické provedení
Kompatibilita	Standardní PC a notebooky, Windows 7 a vyšší (32 a 64 bit), Linux
Záruka	24 měsíců

130x Hybridní identifikační karty

Parametr	Popis parametru
Základní popis	Hybridní identifikační karta s kontaktní částí Smart card a bezkontaktní částí typu EMARINE, kompatibilní s nabízeným čtečkami a splňující požadavky nařízení eIDAS č.910/2014
Veřejné certifikáty	Karta musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit – zejména Postsignum, která nyní kupující používá
Identity	Karta musí umožnit ukládání více identit
Kvalifikovaný prostředek	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)
Softwarová podpora	Součástí dodávky bude software pro zpřístupnění jejich rozhraní v operačním systému včetně rozšířených funkcionalit, tzv. Middleware
Záruka	24 měsíců

3.2.5 Oblast zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů

1x Licence software pro sběr a správu logů (systém centrálního logování)

Parametr	Popis parametru
Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware
Ovládání	Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení.
Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze
Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému
Sběr dat (logů)	Bezagentový sběr logů s výjimkou systémů Windows
Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených), šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem
Protokoly	Příjem a zpracování logů, událostí a další strojově generovaných dat minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELp, nešifrovaně) a TCP 20515 (RELp, šifrovaně)
Formáty logů	Min. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog
Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv
Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy
Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.
Vizualizace logů	Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrovaná podpora zobrazení TOP X událostí za zvolené časové období
Pracovní plochy	Předpřipravené pohledy (dashboards) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání
Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min. 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti
Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - např. umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům dat, aplikacím, zařízením, IP rozsahů apod.
Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova
Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy
Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém
Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalostí (např. SQL dotazů apod.) napříč všemi typy dat a zařízení
Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Průběžná aktualizace přednastavených reportů výrobcem
Integrace	Integrované REST API rozhraní musí umožnit autorizovaný přístup ke strukturované databázi logů
Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparserovaných testovacích dat včetně případných chyb
Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Vmware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortinet, HPE/Aruba, Dell servery, Synology, Linux, Apache, nabízený Systém pro analýzu síťového provozu
Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP
Výkon	Min. 2000 EPS (events per second), krátkodobá (min. 10 min) přetížitelnost systému až 200%
Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat
Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade
Zálohování	Integrované zálohování a obnova konfigurace
Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden
Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce
Podpora	Min. 60 včetně nároku na nové verze firmware/software a aktualizace

1x Úložiště pro logování - produkční

Parametr	Popis parametru
Základní funkce	Úložiště a výpočetní zdroje pro software systému centrálního logování - software systému centrálního logování
Architektura	Integrovaná appliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávisle na infrastruktuře zadavatele
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška max. 2U
Kapacita	Využitelná diskové kapacita pro ukládání data min. 12 TB, disky musí být chráněny min. RAID 5
Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis i čtení) o kapacitě min. 2 GB
Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)
LAN konektivita	Min. 2x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent
Záruka	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace

Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

1x Úložiště pro logování - archivační

Parametr	Popis parametru
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška max. 2U
Výkon	64 bit CPU, min. 6 jader
HDD	Min. 12 pozic pro HDD, rozšiřitelné min. na 30 HDD
Rozšiřitelnost	Podpora připojení externích disků přes USB 3.0 (min. 2 porty)
Hot-swap	Disky vyměnitelné za chodu.
SSD HDD	Podpora SSD disků pro ukládání dat i akceleraci rotačních HDD
Kapacita	Osazeno min. 6x 12 TB HDD SATAIII/256MB cache, 7200 ot/min oficiálně podporovanými výrobcem zařízení
Konektivita	Min. 4 x 1 GbE a 2x 10Gb SFP+ porty s podporou agregace linek a redundance
Výkon	Rychlost zápisu min. 1 700 MB/sec při RAID5 a CIFS
Kompatibilita	Plná podpora Microsoft Hyper-V a Windows Active Directory a ACL
Komunikace LAN	Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
RAM	Min. 8 GB, využitelná jako cache, rozšiřitelná min na 64 GB
Ochrana dat	Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10, integrovaný systém pro automatické vytváření a správu snapshotů (snímků dat)
Napájení	Vestavěné redundantní napájecí zdroje
Záruka	60 měsíců, oprava v místě instalace (včetně HDD)

1x Nástroj pro sběr a vyhodnocování síťových toků

Parametr	Popis parametru
Základní funkce	Monitorování síťové aktivity v reálném čase, identifikace potenciální kybernetické hrozby, bezpečnostního rizika a anomálního chování a tvorba upozornění o jejich výskytu v reálném čase.
Architektura	Integrovaná appliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), provozovaný v prostředí zadavatele. Samostatně funkční nezávisle na infrastruktuře zadavatele či dalších (např. cloudových) službách.
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška max. 1U, hloubka max. 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.
Ovládání	Grafická webová konzole (HTTPS) pro administrátory i operátory, pro správu a používání systému. SSH pro CLI - automatizace, monitorování.
Viditelnost	Systém zajišťuje detailní viditelnost do síťové komunikace s "drill down" prokliky na veškerá uložená data.
Sběr dat	Systém bude získávat data na základě zrcadleného síťového provozu bez potřeby instalace agentů na zařízení v síti.
Zrcadlení komunikace	Podpora SPAN portů a síťových TAPů pro získávání dat zrcadlené komunikace.
Pasivní sběr	Systém bude zcela pasivní vůči síťovému provozu, monitorovaný provoz přes systém nebude procházet a systém jej nebude nijak ovlivňovat.
Netflow protokoly	Systém umožní analyzovat síť na základě zpracování statistických protokolů typu NetFlow v5, NetFlow v9, IPFIX, NetStream a případně dalších ekvivalentních.

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Záznam provozu	Zaznamenávání síťového provozu, minimálně základních parametrů: cílová a zdrojová IP/MAC adresa, podsít, využitý protokol, IPv4 nebo IPv6.
Integrace	Integrace s nabízeným Systémem pro správu, minimálně v úrovni syslog.
Kontextuální informace	Získávání, vizualizace a integrace kontextuálních informací v jednotném grafickém rozhraní: - Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS provozu a Active Directory, - IP geolokace.
Monitorování zařízení	Identifikace zařízení v síti (koncová zařízení, servery, IoT, síťové prvky), rozpoznání změn v síti a notifikace výskytu nového zařízení (obecně assetu).
Analýza	Integrovaný modul pro detailní analýzu sítě - vytváření dlouhodobých grafů a přehledů o komunikaci na síti s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), SSL a DNS provozu, VoIP statistik, SMB/CIFS, DHCP a e-mail provozu.
Vizualizace, vyhledávání	Zobrazení provozu a jeho hloubková analýza - okamžité vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez speciálního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů.
HTTP komunikace	Podpora pro příjem a analýzu HTTP provozu – včetně položek typu URL a hostname.
Detekce anomálií	Integrované samostatné učení na základě matematických metod (např. strojové učení) pro analýzu síťové aktivity, vytváření a automatická průběžná modifikace modelů chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb. Schopnost identifikace nestandardního síťového chování na základě modelu chování daného zařízení a jeho služeb.
Detekce hrozeb	Schopnost detekce neznámých hrozeb, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Minimálně identifikace příznaků potenciálně škodlivého chování: - průzkumné aktivity v síti, - potenciální úniky dat, - detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, - detekce příznaků těžení kryptoměn, - útoky hrubou silou a enumerace dat.
Behaviorální analýza	Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.
False-positive události	Integrovaná podpora identifikace neplatných událostí pomocí mechanismu false-positives, potlačení identifikovaných událostí při příštím výskytu.
Autentizace	Podpora autentizace vůči LDAP, včetně podpory RBAC (přiřazení úrovně oprávnění na základě členství uživatele v konkrétní LDAP skupině).
Reporting	Tvorba dlouhodobých grafů a přehledů s různými typy pohledů dle kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH). Generování statistik a podrobných výpisů ve volitelných časových intervalech. Tvorba tzv. Top N statistik podle různých kritérií (počet přenesených bytů, paketů, toků atd.) pro výpis nejaktivnějších či anomálně komunikujících assetů.
Automatizace reportingu	Vytváření automatizovaných manažerských reportů včetně možnosti exportu do PDF a CSV (nebo obdobného strojově čitelného) formátu. Automatické zasílání reportů emailem, předpřipravené reporty v českém a anglickém jazyce.
Alerty, notifikace	Notifikace na základě překročení prahových hodnot definovaných při implementaci či v průběhu provozu. Systém musí být schopen upozorňovat uživatele prostřednictvím e-mailu o: - všech identifikovaných událostech, - událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. Logování notifikací.
Výkon	Min. 0,2 Gb/s trvalý síťový provoz, min. 200 Netflow/sec.
Kapacita	Úložná kapacita SSD s ochranou min. RAID 1 pro min. 30 denní historii při plném výkonu.
Konektivita	Min. 1x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent.
Záruka a podpora	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace.

4 Instalace a zprovoznění

4.1 Obecné požadavky na instalační služby

Kupující požaduje provést minimálně dále uvedené práce na dodaných komponentech a případně dalších souvisejících zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení předmětu plnění v rozsahu doporučeném výrobcí a dle tzv. nejlepších praktik, i případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

V rámci předmětu plnění kupující požaduje provedení min. následujících služeb:

- doprava jednotlivých komponent do místa plnění (uvedena v kupní smlouvě)
- zpracování a předání dokumentace,
- vlastní nasazení řešení splňující požadované parametry technického řešení,
- začlenění nabízených technologií do stávajícího prostředí,
- zajištění testovacího provozu,
- provedení akceptačních testů,
- dodávka a aktivace požadovaných SW licencí, kontrola aktivací musí být součástí akceptačních testů
- zaškolení IT administrátorů na dodané technologie v rozsahu min. 16 hodin.

4.2 Podrobný popis instalačních služeb

Kupující požaduje provést minimálně uvedené instalační a implementační práce na dodaných komponentech a případně dalších souvisejících zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení předmětu plnění v rozsahu doporučeném výrobcí a dle tzv. nejlepších praktik, i případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

Náklady na provedení instalačních a implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

Zvýšení zabezpečení komunikační sítě
- analýza stávajícího síťového prostředí a návrh nové architektury LAN, - implementace pořízených technologií, - provedení segmentace sítě – VLAN, adresování, routování, - zavedení DNSSEC, vybudování DNSSEC resolveru pro LAN úřadu, - návrh a implementace systému 802.1X pro LAN a WiFi včetně definice přístupových politik. Systém 802.1x musí být integrován s adresářovou službou Active Directory, - implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál, - zpracování uživatelské dokumentace konfigurace obvyklých zařízení a jejich systémů pro systém 802.1X – PC, notebooky, chytré telefony, tablety, tiskárny – Windows, Linux, MacOS, Android, IOS, embedded systémy periférií. Provedení vzorové migrace a konfigurace všech kategorií koncových zařízení (1 zařízení každé kategorie) do systému s ověřováním 802.1X, - návrh a vybudování vhodné architektury WiFi s více SSID pro zaměstnance, jejich osobní zařízení a veřejnost s vhodným způsobem ověřování a politikami řízení provozu, - návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií, zajištění bezpečné publikace interních zdrojů úřadu, vybudování VPN na bázi webového portálu, - převzetí komunikačních pravidel ze stávajícího firewallu a jejich implementace do nového firewallu

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

včetně optimalizací využívajících pokročilých vlastností nového řešení. Export pravidel ze stávajícího firewallu zajistí kupující, - provedení potřebných migrací a konfigurací stávajících systémů – export konfigurací stávajících síťových systémů provede kupující, - návrh a provedení akceptačních testů.
Vytvoření serverového prostředí s vysokou dostupností pro provoz IS
- analýza současného prostředí s ohledem na systémové a kapacitní nároky systém a aplikací - návrh a rozšíření virtualizační platformy v kontextu nově dodávaných technologií a zvýšení dostupnosti provozovaného prostředí jako celku, a to pro provoz současných a dodaných systémů - návrh a vybudování platformy aplikační virtualizace včetně nastavení uživatelského prostředí a vhodných politik - začlenění veškerých dodaných systémů do zálohovacích plánů organizace - provedení potřebných migrací - provedení potřebných konfigurací souvisejících systémů - návrh a provedení akceptačních testů
Nasazení systému řízení privilegovaných účtů a zařízení
Privilegované účty - analýza ICT prostředí se zaměřením na vyhledání a inventarizace privilegovaných účtů - vybudování systému pro správu a řízení privilegovaných účtů včetně napojení monitorovaných systémů a nastavení rotace hesel - provedení potřebných konfigurací souvisejících systémů - návrh a provedení akceptačních testů
Vícefaktorová autentizace
- analýza prostředí se zaměřením na zavedení vícefaktorové autentizace - vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority integrované s Active Directory, návrh a implementace šablon certifikátů - vybudování systému vícefaktorové autentizace s využitím kontaktních identifikačních prostředků (čipových/Smart karet). Instalace externích čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění. - návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (karet a doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti - návrh procesů souvisejících se řízením životního cyklu karet a certifikátů včetně jejich vystavování a přidělování zaměstnancům personálním oddělením - návrh a realizace zálohování - provedení potřebných konfigurací souvisejících systémů - návrh a provedení akceptačních testů včetně výkonových testů
Zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů
Sběr a správa logů - analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí - návrh a vybudování systému centrálního logování pro zaznamenávání činnosti informačního a komunikačního systému, jeho uživatelů a administrátorů

- monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených pracovních stanic (aplikační virtualizace) apod.
- monitorování IP datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) dle RFC3954 nebo ekvivalentu (např. netflow) – minimálně na úrovni rozhraní WAN
- provedení souvisejících konfigurací monitorovaných systémů
- návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů

Sběr a vyhodnocení síťových toků

- analýza komunikačního systému a návrh způsobu sběru a obsahu síťových toků a logovaných událostí
- vybudování systému sběru a analýzy síťových toků a souvisejících bezpečnostních událostí
- provedení souvisejících konfigurací monitorovaných systémů
- ukládání informací (min. o bezpečnostních událostech incidentech do systémů sběru a správy logů)
- návrh a provedení akceptačních testů

4.3 Dokumentace k dodávanému řešení

V rámci předmětu plnění kupující požaduje zpracování a předání níže uvedené dokumentace. Dokumentace musí být zhotovena v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. DOC, ODT, PDF atd.) na datovém nosiči.

4.3.1 Prováděcí dokumentace

Prováděcí dokumentace bude sloužit jako podklad pro vlastní instalaci a implementaci řešení do prostředí kupujícího. Prováděcí dokumentace bude zahrnovat detailní popis cílového stavu a způsobu jeho dosažení, včetně:

- detailního popisu cílového stavu včetně funkcionalit jednotlivých částí systému,
- nutné a doporučené optimalizační a konfigurační změny dodávaných systémů i všech navázaných systémů (serverová infrastruktura, LAN, zálohování, monitorování atd.),
- způsob zajištění potřebného HW a SW,
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
- detailní návrh a popis postupu instalace a implementace předmětu plnění,
- detailní popis zajištění bezpečnosti informací,
- detailní harmonogram realizace včetně uvedení kritických milníků,
- návrh designu síťového a bezpečnostního řešení a jeho konfigurace,
- návrh designu aplikačních řešení,
- vazby na stávající systémy a jejich konfigurace,
- integrace implementovaných softwarových systémů,
- rekonfigurace stávajících systémů, které nevyžadují součinnost ani souhlas třetí strany a které mají veřejně a otevřeně dostupnou dokumentaci umožňující rekonfiguraci neomezenému okruhu kvalifikovaných osob,
- dopady implementace na dostupnost a funkčnost stávajících služeb,
- posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon),
- požadované součinnosti kupujícího a jejich rozsah,
- návrh akceptačních kritérií a akceptačních testů.

4.3.2 Provozní dokumentace

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy:

4.4 Zaškolení IT administrátorů

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 implementované systémy,
- standardní údržby systémů pro administrátory kupujícího,
- základní identifikace nestandardních stavů systému a jejich příčin.

Minimální požadovaný rozsah zaškolení pro administrátory je 16 hodin.

Předpokládaný počet administrátorů (účastníků školení) je max. 8 osob.

4.5 Testovací provoz

Testovací provoz proběhne po dobu uvedenou v harmonogramu realizace, a to se zvýšeným dohledem a podporou ze strany prodávajícího.

Cílem testovacího provozu je poskytnout metodické vedení a prostor uživatelům pro ověření funkcionalit a vlastní funkčnosti dodaného řešení, pro cvičnou práci se systémem a prostor pro prodávajícího pro identifikaci a opravu případných chyb a neshod. Dalším cílem testovacího provozu je možnost případné definice změnových požadavků ze strany kupujícího. Během testovacího provozu provede prodávající aktualizaci Prováděcí dokumentace na Dokumentaci skutečného provedení, včetně záznamu konkrétních provedených konfigurací. Úspěšný průběh testovacího provozu, jehož výstupem bude faktické uživatelské ověření schopnosti nasazení nového řešení v prostředí kupujícího na základě této technické specifikace a jejich příloh, je jednou z nezbytných podmínek kupujícího pro možnost akceptace plnění na základě této technické specifikace a jejich příloh.

4.6 Akceptační řízení

4.6.1 Dílčí akceptační řízení

Dílčí akceptační řízení bude provedeno jednotlivé oblasti plnění dle této technické specifikace. Dílčí akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům této technické specifikace a jejím přílohám a požadavků daných prováděcí dokumentací.

Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno (Akceptováno) nebo Nesplněno (Neakceptováno), podepsaný oprávněnými osobami smluvních stran.

Součástí akceptačního protokolu ke každé oblasti plnění bude i soupis předaných prvků včetně jejich sériových čísel.

Dílčí akceptace mohou probíhat v libovolném pořadí, je-li to technicky a organizačně možné a vhodné.

4.6.2 Souhrnné akceptační řízení - akceptace

Souhrnné akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům kupní smlouvy a této technické specifikace, která je její přílohou, a jejich příloh, funkčního i nefunkčního charakteru – licence a příslušenství.

Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno (Akceptováno) / Splněno (Akceptováno) s výhradou / Nesplněno (Neakceptováno), podepsaný oprávněnými osobami smluvních stran, a to s výsledným uvedením každé části na tomto akceptačním protokolu a výsledku akceptačního řízení.

Klasifikace Splněno (Akceptováno) s výhradou umožní pokračování v realizaci v případě vad drobných, pro které může být opakování akceptačního řízení zbytečně nákladné.

4.6.3 Opakované akceptační řízení

Jestliže plnění nesplňuje podmínky stanovené pro akceptaci, bude obsahem akceptačního protokolu vyjádření Nesplněno (Neakceptováno) spolu s popisem závad a uvedením termínů pro jejich nápravu. Prodávající napraví tyto nedostatky a akceptační řízení v odpovídajícím rozsahu bude provedeno znovu. Proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně. Proces testování a následných oprav lze opakovat, dokud prodávající nesplní požadavky pro akceptaci řádnou s výsledkem Splněno (Akceptováno), nejvýše však 2× (dvakrát).

V situaci, kdy by bylo nutné opakovat akceptační řízení více jak 2× (dvakrát), bude takové opakování považováno za podstatné porušení smlouvy ze strany prodávajícího a kupující bude oprávněn odstoupit od smlouvy. Prodlení vzniklé v souvislosti s potřebou opakování akceptačních řízení bude považováno vždy za prodlení vzniklé na straně prodávajícího se zachováním důsledků takového prodlení, tedy zejména smluvních pokut na základě uvažené kupní smlouvy.

Opakované akceptační řízení bude probíhat jednotlivě samostatně pro jednotlivé části či oblasti tak, aby na již akceptované části dané opakované akceptační řízení nemělo vliv.

4.7 Harmonogram plnění

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, 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.

Aktivita projektu	Termín nejpozději do
Zpracování prováděcí dokumentace, připomínkování ze strany kupujícího, vypořádání připomínek, finalizace dokumentu.	4 týdny
Akceptační řízení prováděcí dokumentace	1 týden
Předání prováděcí dokumentace	T + 5 týdnů
Dodávky komponent řešení a instalace Implementace dodaného řešení prováděcí dokumentace – nastavení / konfigurace / parametrizace jednotlivých oblastí, provedení integrací na spolupracující systémy atd. Zpracování a dodávka provozní dokumentace. Zpracování školicích materiálů.	15 týdnů
Připravené prostředí pro testovací provoz, předání do testovacího provozu.	T + 20 týdnů
Prezenční zaškolení IT administrátorů. Předání do testovacího provozu.	1 týden
Testovací provoz s dohledem a podporou prodávajícího. Oprava chyb a neshod, případná definice změnových požadavků. Aktualizace dokumentace Dodávka licencí (listinné potvrzení dodaných licencí co do jejich počtu a rozsahu).	3 týdny
Akceptační řízení – porovnání skutečných vlastností se požadavky smlouvy.	1 týden
Akceptace projektu, předání systému do rutinního provozu.	T + 25 týdnů

Poznámka: Ve sloupci „Termín nejpozději do:“ znak „T“ vyjadřuje datum účinnosti smlouvy.

4.8 Projektové řízení

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

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti kupujícího je v rámci předmětu plnění objednatel 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 projektových prací,
- závazný harmonogram projektu – dodržování termínů v harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem k objednateli, 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.

Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

Technická specifikace Prodávajícího pro projekt kybernetické bezpečnosti města

Obsah

TECHNICKÁ SPECIFIKACE PRODÁVÁJÍCÍHO PRO PROJEKT KYBERNETICKÉ BEZPEČNOSTI MĚSTA.....	1
1 POŽADAVKY NA TECHNICKÉ ŘEŠENÍ	2
1.1 PLNĚNÍ OBECNÝCH POŽADAVKŮ NA JEDNOTLIVÉ ČÁSTI A OBLASTI PLNĚNÍ	2
1.2 PLNĚNÍ FUNKČNÍCH POŽADAVKŮ NA ŘEŠENÍ	5
1.2.1 Oblast zvýšení zabezpečení komunikační sítě	5
1.2.2 Oblast vytvoření serverového prostředí s vysokou dostupností pro provoz IS.....	10
1.2.3 Oblast řízení privilegovaných účtů a zařízení	14
1.2.4 Oblast vícefaktorové autentizace	15
1.2.5 Oblast zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů..	17
2 INSTALACE A ZPROVOZNĚNÍ	22
2.1 INSTALAČNÍ SLUŽBY.....	22
2.2 PODROBNÝ POPIS INSTALAČNÍCH SLUŽEB	22
2.3 DOKUMENTACE K DODÁVANÉMU ŘEŠENÍ	24
2.3.1 Prováděcí dokumentace	24
2.3.2 Provozní dokumentace	24
2.4 ZAŠKOLENÍ IT ADMINISTRÁTORŮ	24
2.5 TESTOVACÍ PROVOZ	25
2.6 AKCEPTAČNÍ ŘÍZENÍ.....	25
2.6.1 Dílčí akceptační řízení	25
2.6.2 Souhrnné akceptační řízení - akceptace	25
2.6.3 Opakované akceptační řízení	25
2.7 HARMONOGRAM PLNĚNÍ	26
2.8 PROJEKTOVÉ ŘÍZENÍ	27

1 Požadavky na technické řešení

Veškeré komponenty, které prodávající dodává v rámci předmětu plnění, musí splňovat následující podmínky:

Jedná se o nové a nerepasované komponenty.
Byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce.
Mají plnou záruku od výrobce.
Mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce.
Obsahují všechny nezbytné licence na používání příslušného softwaru.
Jsou v databázi výrobce uvedeny jako prodaná kupujícímu – zadavateli.
Zadavatel 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.

1.1 Plnění obecných požadavků na jednotlivé části a oblasti plnění

Oblast Zvýšení zabezpečení komunikační sítě
Bude provedeno nasazení nových přístupových přepínačů (i na stávající pozice) pro možnost plošné implementace technologie 802.1X.
Budou dodány a implementovány přístupové body WiFi s centrální správou.
Architektura WiFi bude založena na řešení s centrální správou prováděnou kontrolérem (řadičem), který bude součástí firmwaru síťových prvků a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatickou detekci a reakci na rušení cizím signálem.
V celé LAN bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby Active Directory založené na standardu IEEE 802.1X. Stejný standard řízení přístupů bude implementován i pro zařízení bez podpory Active Directory, pouze pro autentizaci bude využit jiný, zařízením podporovaný, způsob – certifikát apod.
Bude implementován vysoce dostupný síťový / perimetrový firewall pro provádění hloubkové kontroly komunikace mezi interními subjekty (uživatel, zaměstnanec, server) a interními i veřejnými zdroji (internet), ověřování validity komunikačních a aplikačních protokolů, filtrací nežádoucích adres a antimalwarovou kontrolou. Ochrání tak interní systémy před zavlečením škodlivého kódu z prostředí internetu či jiných veřejných/externích sítí. Bude poskytovat také prostředky VPN pro vzdálený přístup uživatelů a ochranu aplikací publikovaných z interní sítě do internetu. Firewall nahradí stávající řešení a převezme jeho vhodná konfigurační nastavení.
Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky bude vzorová konfigurace 802.1x na všech typech koncových zařízení Kupujícího.
Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). WiFi bude nabízet více SSID (např. zaměstnanci, hosté, veřejnost), které budou obsluhovány samostatnými VLAN a budou napojeny na radius servery. Zaměstnanci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) bude provedeno dle 802.11i, tedy – WPA2/3 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty, popř. veřejnost, kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kuponů. Preferován bude captive portál nabízeného systému řízení 802.1X s tzv. lobby přístupem pro správu a generování účtů/kuponů ne-technickou osobou.
Pro hosty a veřejnost budou zřízeny samostatná VLAN (, které bude komunikačně odděleny od vnitřních sítí organizace. Tyto VLAN bude mít své L3 rozhraní až na úrovni firewallu tak, aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro zaměstnance.
Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s přepínáním provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Bude vybudován, resp. modernizován systém základních síťových služeb (DHCP, DNS včetně validujícího resolveru DNSSEC) a dalších podpůrných služeb nezbytných pro provoz dodávaných technologií.

Oblast Vytvoření serverového prostředí s vysokou dostupností pro provoz IS

Bude provedena instalace a implementace obou HCI (hyper converged infrastructure) serverů včetně serverové a diskové virtualizace a začlenění do stávající infrastruktury.

HCI servery budou tvořit samostatný cluster, funkčně a z pohledu správy nezávislý na stávající virtualizační platformě.

Bude vybudována plnohodnotná platforma aplikační virtualizace (terminálových služeb) včetně webového portálu s publikovanými aplikacemi pro lokální i vzdálený přístup uživatelů a centrálního přístupového bodu zajišťující vyrovnavání zátěže mezi jednotlivými aplikačními servery. Součástí implementace je vybudování aplikačního prostředí uživatele – tj. instalace a konfigurace klientských aplikací (Office, Acrobat).

Dodavatel plnění dle této technické specifikace se dále zavazuje poskytnout součinnost dodavatelům IS kupujícího VITA a GINIS, které ve stávajícím prostředí kupující provozuje, při jejich přenosu do nově vybudovaného prostředí těmito dodavateli. Tato součinnost je předpokládána zejména na úrovni potřebných konfigurací virtualizační platformy, dodaného prostředí serverových OS a centrálně konfigurovaných bezpečnostních pravidel.

Bude provedena konsolidace stávajícího serverového prostředí – migrace stávajících virtuálních serverů do nově vybudované virtualizační platformy a jejich optimalizace. Seznam VM určených k takové migraci je obsažen v části podléhající NDA – Popisu stávajícího prostředí.

Zálohovací systém bude rozšířen o bezpečné úložiště s nastavitelnou retencí uložených záloh a jejich ochranou proti změně časovými zámky. Součástí plnění jsou i další nezbytné konfigurační změny stávajícího zálohovacího prostředí v souvislosti s implementací nových technologií dle této technické specifikace.

Oblast řízení privilegovaných účtů a zařízení

Pro oblast řízení privilegovaných účtů a zařízení bude implementován systém, který bude sloužit jako vstupní bod pro místní i externí správce, kteří jeho prostřednictvím budou přistupovat ke spravovaným systémům. V tomto bodě bude činnost správců zaznamenávána a logována. Systém dále zajistí automatickou změnu hesel ve spravovaných systémech s otevřenou a veřejně dostupnou dokumentací (tzv. rotaci hesel).

Oblast Vícefaktorová autentizace

Bude implementován nástroj autentizace uživatelů s využitím více faktorové (víceúrovňové) autentizace.

Ověřování uživatele při přihlašování ke koncovému zařízení (resp. jeho operačnímu systému) bude prováděno pomocí identifikačních karet typu Smart card, které budou sloužit jako bezpečné úložiště uživatelských certifikátů, kterými bude ověřována identita uživatele.

Autentizační prostředky (karty smart card) budou certifikovány jako kvalifikovaný prostředek pro vytvoření a používání kvalifikovaného elektronického podpisu při uložení příslušných uživatelských certifikátů vydávaných veřejnými certifikačními autoritami. Autentizační prostředky musí splňovat požadavky nařízení eIDAS č.910/2014.

Autentizační prostředky budou vedle kontaktní části (smart card) obsahovat i bezkontaktní část, která umožní využívání pro autentizaci uživatelů v docházkovém/přístupovém systému (konfigurace těchto systémů není součástí předmětu plnění), popřípadě dalších systémech založených na stejné technologii.

Součástí plnění bude komplexní nástroj pro evidenci a řízení celého životního cyklu karet a uložených certifikátů, včetně jednoduché automatické obnovy certifikátu uživatelem pomocí grafického průvodce před vypršením platnosti certifikátu.

Součástí dodávky a implementace jsou i veškeré nezbytné podpůrné systémy – zejména vybudování PKI (Public Key Infrastructure) včetně certifikační autority a vhodné sady šablon vystavovaných certifikátů.

Řešení musí umožňovat jednoduchou správu identifikačních prostředků tak, aby mohla být prováděna zaškoleným uživatelem – např. personalistou, a to včetně prvotního vydání karty a certifikátu uživateli.

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Oblast Zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů
Nástroj pro sběr a správu logů (systém centrálního logování).
Bude implementován nástroj pro správu logů (tzv. log management). Nástroj bude sbírat, normalizovat a spravovat logy a data síťových toků KS bezpečnostní a provozní povahy napříč KS a IS.
Uložené logy bude možné snadno prohledávat či filtrovat na základě multikriteriálních dotazů napříč zdroji logů.
Zavedený nástroj bude obsahovat notifikační systém, kdy notifikace bude možné navázat na výskyt provozní či bezpečnostní události.
Zdroje dat/ logů pro budou vybrány z tzv. primárních a podpůrných (technických) aktiv kupujícího. K jejich určení bude využito Vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritérií přiměřeně uzpůsobených a aplikovaných na prostředí kupujícího (kupující neprovozuje významný informační systém). Nezbytné konfigurace zdrojových (popř. dalších navázaných) systémů jsou součástí plnění, případnou potřebnou součinnost dodavatelů agendových IS (pokud má dojít ke sběru jejich logů) zajišťuje na svůj náklad kupující.
Nástroj bude implementován tak, aby jeho provoz nebyl závislý na infrastruktuře kupujícího a byl tak schopen zaznamenávání činnosti a detekce bezpečnostních či nestandardních událostí i v nestandardních provozních stavech infrastruktury kupujícího (přetížení, start, nestabilita, bezpečnostní událost/incident apod.).
Nástroj pro sběr a vyhodnocování síťových toků
Pro získání schopnosti detekce a identifikace bezpečnostní události na úrovni síťového provozu bude implementován nástroj pro sběr a vyhodnocování síťových toků, který bude provádět sledování a hloubkovou analýzu síťových toků (netflow) na perimetru sítě a v libovolném jejím segmentu podle aktuálních potřeb a požadavků.
Nástroj bude ukládat historii síťového provozu (resp. síťových toků) po dobu min. 1 měsíc pro účely operativní analýzy a podpory při řešení kybernetických událostí a incidentů nebo provozních problémů. Současně bude ukládat získané informace a také informace o své činnosti (změny konfigurací, aktualizace) do nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů.
Nástroj bude disponovat pokročilou tzv. behaviorální analýzou, tj. detekcí nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, detekce provozních problémů apod.) a bude umožňovat detekci anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.
Nástroj bude implementován tak, aby jeho provoz nebyl závislý na infrastruktuře kupujícího a byl tak schopen zaznamenávání činnosti a detekce bezpečnostních či nestandardních událostí i v nestandardních provozních stavech infrastruktury kupujícího (přetížení, start, nestabilita, bezpečnostní událost/incident apod.).
Společné požadavky
Všechny systémy budou dodány a vybudovány jako lokální (on-premise) v prostředí kupujícího. Jejich funkčnost bude nezávislá na dostupnosti externích zdrojů a internetové konektivitě s výjimkou případného ověřování licenčních klíčů a manuálně řízeného stahování funkčních a bezpečnostních aktualizací.

1.2 Plnění funkčních požadavků na řešení

1.2.1 Oblast zvýšení zabezpečení komunikační sítě

2x Páteří přepínače

Parametr	Popis parametru
Provedení	L2/L3 přepínač v rackovém provedení, 1U včetně montážního materiálu
Porty	24x 10 Gb SFP+ a 2x 100 Gb QSFP28 (kompatibilní s 40Gb QSFP+ a podporou rozdělení každého na 4x 10/25Gb porty) [REDACTED]
Propustnost	Neblokovaná architektura, přepínací kapacita 880 Gbps
Agregace portů	Podpora LACP, 20 portů v agregační skupině, bez omezení počtu skupin
Směrování	Hardwarové statické routování včetně VLAN, dynamické směrování (min. RIP, OSPF, BGP), směrování založené na politikách, min. 8000 routovacích záznamů pro IPv4 i IPv6
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p
VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření, podpora IEEE 802.1ad (Q-in-Q), podpora VXLAN, min. 4000 VLAN
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS
MAC	Podpora min. 60 000 MAC adres
Síťové toky	Plný přímý export síťových toků - Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent)
Rozšířené stohování	Pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG/MCLAG (Multi-Chassis Link Aggregation) nebo obdobná
Zrcadlení provozu	Podpora RSPAN (Remote SPAN) a ERSPAN (Encapsulated Remote SPAN)
Napájení	Redundantní interní napájecí zdroje, vyměnitelné za provozu (hot-swap)
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci. Vyhrazený 1 Gb port pro správu (out-of-band management) - nezapočítává se do požadovaného počtu portů (viz Porty)
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
Záruka	Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den

21x Přístupový přepínač

Parametr	Popis parametru
Provedení	L2+ přepínač v rackovém provedení 1U a hloubka do 31 cm, neblokovaná architektura
Porty	48x 1 GbE PoE+, 4x 10 Gb SFP+

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Propustnost	Neblokovaná architektura, přepínání/směrování 176 Gbps
Power on Ethernet	Podpora PoE/PoE+ 802.3af/at na všech metalických portech, celkový PoE výkon 740 W
Agregace portů	Podpora LACP, 8 portů v agregační skupině, 12 skupin
Směrování	Statické routování
Řízení provozu	Víceúrovňový QoS, podpora standardu 802.1p
VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN na základě 802.1X ověření
Ověřování uživatelů a zařízení	Plná podpora IEEE 802.1X
Dualstack	Plný IPv4 a IPv6 dualstack včetně směrování a QoS
MAC	Podpora 32 000 MAC adres
Zrcadlení provozu	Zrcadlení síťového provozu portu(ů), podpora SPAN
Napájení	Interní napájecí zdroj
Monitoring a správa	Plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
Hlučnost	hlučnost 46,5 dB pro umístění v pracovních prostorech
Záruka	Záruka a servisní podpora výrobce 60 měsíců

40x Přístupový bod WiFi s příslušenstvím

Parametr	Popis parametru
Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na strop a zeď
Frekvence	3 nezávislé radiové moduly činnost v radiovém pásmu 2,4 a 5 GHz současně, s podporou standardu OFDMA min. u 2 modulů
Architektura	Homogenní WiFi síť s rychlým a spolehlivým roamingem klientů, podpora Mesh (https://en.wikipedia.org/wiki/Wireless_mesh_network)
Anténní systém	Interní systém, optimalizovaný pro montáž na strop
Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) – multi-user multiple input/multiple output
Přenosové rychlosti	5 GHz 1200Mbps, 2.4 GHz 550Mbps
Standardy	Podpora standardů 802.3at, 802.11n, 802.11ax, 802.11k, 802.11n, 802.11r, 802.11v, Hotspot 2.0
Multi SSID	Podpora vysílání min. 8 SSID (WiFi sítí) na 2.4 i 5 GHz současně, podpora přiřazení každého SSID do samostatné VLAN
Zatížení	300 přiřazených (asociovaných) klientů na radiový modul

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Řízení zátěže	Automatické rozkládání zátěže přístupových bodů předáváním klientů a automatickým směrováním klientů na 5 GHz (pokud klienti podporují) [REDACTED]
Porty	2x 1Gb, 1x PoE s podporou standardů 802.3at a 802.3af
Bezpečnost	Trvalá detekce cizích přístupových bodů/klientů nezávislým radiem, spektrální analýza
Kontroler	Centrální kontroler pro kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů součástí dodávky. Kontroler musí být provozován v interní síti zadavatele a být integrální součástí firmware nabízených síťových prvků. Grafické webové rozhraní pro správu [REDACTED]
Autentizace, autorizace	Podpora standardu WPA3 (Wi-Fi Protected Access III), integrovaný portál pro autentizaci uživatelů (Captive portal), ověření klientů (min. hardware, uživatel, operační systém, certifikát) s využitím protokolu 802.1X
IoT a lokalizace	Integrovaná hardwarová podpora standardu 802.15.4 (Zigbee) a BLE (Bluetooth Low Energy)
Správa	Plná podpora CLI, SSH, SNMP, syslog, web rozhraní, hromadná aktualizace firmware a konfigurace
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
Monitoring	Detailní monitoring a diagnostika provozu v reálném čase - parametry připojení a komunikace klienta, stav přístupových bodů (počty klientů, vytížení kanálů, signál, cizí (rogue) přístupové body)
Úsporné napájení	Podpora standardu 802.3az - Energy-Efficient Ethernet (EEE)
Záruka	60 měsíců poskytovaná výrobcem zařízením

2x Next-generation firewall

Parametr	Popis parametru
Porty	2x 10 Gb SFP+ a 2x 10x GbE (mohou být sdílené), 8x 1GbE, USB pro ext. záložní 4G modem
NGFW	Min. základní funkce Next-generation firewall- viz https://en.wikipedia.org/wiki/Next-generation_firewall-firewall , aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.
Architektura	Založená na využití specializovaných čipů (ASIC) pro akceleraci klíčových funkcí a vyšší bezpečnost
Počet současných spojení	3 milionu
Propustnost SSL VPN	1,4 Gbps
Propustnost SSL inspekce	2.6 Gbps
Propustnost firewallu	Min. 25 Gbps (pro UDP pakety >= 512 bytů)
Propustnost NGFW	2.5 Gbps
Propustnost IPS	4.5 Gbps
Propustnost detekce škodlivého	2 Gbps

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
kód	
Virtualizace	10 virtuálních kontextů
Vysoká dostupnost	Režimy Active/Passive i Active/Active se společnou konfigurací
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	Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd.)
Kategorizace a blokáce provozu	Založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorií na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne
Antispam	Antispamová a antivirová inspekce elektronické pošty
Sandbox	Integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba součástí dodávky)
Aktualizace	Automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení
Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu
Management a monitoring	HTTP/S, SSH, SNMP, syslog
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků (přepínače, WiFi, firewally)
SD-WAN	Integrovaná podpora SD WAN-min. rozkládání zátěže a vysoká dostupnost více internetových přípojek
Sledování toků	Export síťových toků (Netflow nebo ekvivalent)
Bezpečnost	Integrovaný TPM (Trusted Platform Module) čip pro ukládání citlivých údajů
Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů
Záruční servis	Záruka a podpora výrobce min. 60 měsíců v režimu 24x7. Odeslání náhradního zařízení nejdéle následující pracovní den po nahlášení závady. Včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí-URL filtrace, IPS, antimalware, antispam, aplikační kontrola, sandbox)

Licence software pro řízení přístupu do sítě založeného na protokolu 802.1x

Parametr	Popis parametru
Provedení	Software nebo softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení
Nastavení přístupů	Nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém
Autentizace	Zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Základní autentizační metody	PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty
Identity	Vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC
Nezávislá autentizace a autorizace	Úplné oddělení autentizace a autorizace, autentizace proti službě Active Directory, autorizace proti externí SQL databázi
Rozšířená autentizace a autorizace	Podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth)
Kontextová autorizace	Autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory
Externí identity	Podpora autentizace externími identitami - Microsoft, Google
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, pro odpojení nebo karanténu koncových zařízení
Bezpečnost	Podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení)
Správa	Vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení
Portál	Captive portál pro uživatele a jejich rozšířenou autentizaci, podpora více graficky i obsahově unikátních portálů provozovaných souběžně. Integrovaná podpora úpravy vzhledu
Rychlé přihlášení	Podpora přihlášení prostřednictvím QR kódu. Zapamatování úspěšně autentizovaných/registrovaných klientů a zjednodušení opakovaných přihlášení (jen potvrzení uvítací/informační) stránky
Registrace	Podpora samoobslužné registrace s ověřením SMS, e-mailem
Ochrana identit	Veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES 128-bit.
Speciální zařízení	Podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, modality, technologické prvky, IoT
Vysoká dostupnost	Integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru 2 appliance. Druhá appliance není součástí dodávky
Licence	Trvalá licence pro 500 současných (konkurenčních) koncových zařízení ověřených pomocí 802.1X bez omezení počtu uživatelů
Automatizace a integrace	REST-API rozhraní pro základní funkce AAA
Kompatibilita	Software nebo appliance určen pro provoz v prostředí stávající serverové virtualizace
Podpora	Podpora výrobce 60 měsíců včetně nároku na nové verze a aktualizace software

Síťové příslušenství

Parametr	Popis parametru
Optické moduly	90x SFP+ 10Gb, SM, LC, min. 1 km, včetně diagnostiky , kompatibilní s nabízenými přepínači Fortinet

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	6x SFP+ 10Gb, SM, LC, min. 1 km, kompatibilní s nabízenými servery DELL
Vysokorychlostní kabely	1x kabel QSFP28 – QSFP28, 100 Gb, 0,5 m, kompatibilní s nabízenými přepínači Fortinet 2x kabel QSFP28 - 4x SFP28+ 25Gb, 5 m, kompatibilní s nabízenými přepínači Fortinet a servery DELL
Optické kabely	90x patch kabel SM LC-SC, 3 m 10x patch kabel SM LC-LC, 3 m
Záruka	36 měsíců

1.2.2 Oblast vytvoření serverového prostředí s vysokou dostupností pro provoz IS

2x Hyperkonvergováný (HCI – hyperconverged infrastructure) server, včetně příslušenství

Parametr	Popis parametru
Provedení	Rackové provedení max. 1U včetně výsuvných kolejnic a montážního materiálu do racku
CPU	1x procesor AMD EPYC 9354P 3.25GHz, 32C/64T, 256M Cache Výkon server dle https://spec.org SPECrate®2017_int_base =371 SPECrate®2017_fp_base =447
RAM	768 GB, DDR-5, všechny paměťové kanály CPU musí být využity
Úložiště pro hypervizor	2x SSD 480 GB, RAID1, provedení M.2, nezabírá pozice HDD
Bezpečnost	Integrovaný modul TPM 2.0
Úložiště	8x 3,84 TB NVMe SSD, 1 DWPD (Drive Writes Per Day) po dobu záruky SSD výměnné za provozu (hot-plug), kompatibilní s nabízenou diskovou virtualizací
HDD/SSD řadič	PERC H755N - NVMe, HBA i RAID režim (RAID 5,6,50,60), kompatibilní s nabízenou diskovou virtualizací
LAN	3x 2 portová NIC10/25Gb SFP28 [REDACTED] podporou virtualizace-VMware NetQueue, Microsoft VMQ a podporou NPAR (Network Partitioning) 1x 1GbE samostatný port pro vzdálený management
USB	3x USB port 3.x, min. 1x na čelním panelu s podporou bootování
Vzdálená správa	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)
Napájení	Redundantní napájecí zdroje min. 500W, musí splňovat požadavky na certifikaci energetické účinnosti Platinum dle 80 PLUS (https://cs.wikipedia.org/wiki/80_Plus) nebo lepší; případně na stejné nebo vyšší úrovni účinnosti podle jiné certifikace
Příslušenství	1x kabel SFP28 – SFP28 (25 Gb) 2 m (pro každý server)
Záruční servis	Záruční servis na dobu 60 měsíců poskytovaný výrobcem, oprava následující pracovní den od nahlášení v místě instalace, technická podpora výrobce v českém jazyce. Dostupnost ovladačů a dokumentace na webu výrobce dle výrobního/sériového čísla serveru.

Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

Licence serverové virtualizace

Parametr	Popis parametru
Provedení	Licence software pro virtualizaci nabízených HCI serverů [REDACTED]
Základní funkce	Hypervizor instalovaný přímo na hardware, umožňující plnou virtualizaci libovolného x86-64 serveru [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Souborový systém	Integrovaný clusterový souborový systém sdílený mezi více hypervizory s podporou snapshotů [REDACTED] [REDACTED] [REDACTED]
Migrace a replikace virtuálních serverů	Online bezvýpadková migrace virtuálních serverů/strojů (VM) mezi hypervizory, včetně současné změny úložiště VM. Podpora vícenásobných souběžných migrací. Online bezvýpadková replikace VM mezi hypervizory [REDACTED] [REDACTED]
Vysoká dostupnost	V případě výpadku hypervizoru automatický restart VM na jiném hypervizoru [REDACTED] [REDACTED]
Úspora výpočetních zdrojů	Podpora thin provisioning, RAM over-provisioning, snapshot management [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Síťová komunikace	Virtuální síťový přepínač integrovaný v hypervizoru [REDACTED] [REDACTED] [REDACTED]
Správa	Centralizovaná správa všech hypervizorů z jedné konzole [REDACTED] [REDACTED]
Úložiště	Podpora lokálních i SAN úložišť (SAS, iSCSI, FC)
Zálohování	Kompatibilita se současným systémem zálohování, včetně možnosti zálohování celých VM bez nutnosti instalace agentů do OS [REDACTED] [REDACTED]
Podpora	Podpora výrobce, včetně nároku na opravné verze po dobu 60 měsíců [REDACTED] [REDACTED]

Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

Licence diskové virtualizace

[REDACTED]

Parametr	Popis parametru
Provedení	Licence software vysoce dostupného virtualizovaného softwarově definovaného diskového úložiště pro nabízené HCI servery [REDACTED]
Replikace	Software musí umožnit minimálně synchronní replikace dat (zrcadlení, RAID1) mezi uzly SDS (virtualizačními servery) [REDACTED]
Vysoká dostupnost	Automatické překlenutí výpadku jednoho prvku systému – jednoho serveru či jeho komponenty (např. jednoho disku). Včetně podpory zotavení a obnovení [REDACTED]
Podpora virtualizace	Software bude provozován v úrovni hypervizorů nabízené serverové virtualizace s přímým přístupem k lokálnímu úložišti (nikoli jako VM) [REDACTED]
Vyrovnávací paměť	Integrovaná podpora vyrovnávací paměti pro čtení i zápis s využitím flash médií (SSD, NVMe disků apod.) a RAM [REDACTED]
Škálovatelnost výkonu	Podpora přidání dalších uzlů SDS s rozptřčením stávajících dat mezi uzly SDS. Podpora navýšování kapacity přidáním / zvětšením disků v rámci uzlu (licence nebude kapacitně omezena) [REDACTED]
Serverová virtualizace - integrace	Podpora technologií nabízené serverové virtualizace – replikace virtuálních strojů, podpora virtuálních distribuovaných přepínačů, správa politik úložišť [REDACTED]
iSCSI	Integrovaná podpora publikace kapacity SDS prostřednictvím protokolu iSCSI (tzv. iSCSI target) a NFS [REDACTED]
Podpora	Podpora výrobce, včetně nároku na nové verze po dobu 60 měsíců

Licence operačních systémů

[REDACTED]

[REDACTED]

[REDACTED]

Parametr	Popis parametru
Serverové operační systémy	Licence 64-bitového serverového operačního systému v aktuální verzi pro každý nabízený HCI server . Licence musí umožnit provoz hypervizoru a min. 20 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech souvisejících aplikací, nabízených

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	systémů a aplikací a management nástrojů
Klientské přístupové licence k serverovému operačnímu systému	Klientské licence pro nabízené operační systémy umožňující využívat těchto systémů 130 uživatelům bez omezení počtu přístupových zařízení
Klientské licence aplikační virtualizace	Klientské licence pro nabízené operační systém umožňující využívat služeb aplikační virtualizace Windows aplikací(též terminálové služby) systémů 130 uživatelům bez omezení počtu přístupových zařízení
Vysoká dostupnost	Veškeré nabízené licence umožňují legální provoz ve virtualizovaném prostředí s vysokou dostupností – tj. automatickým přesouváním virtuálních serverů mezi hypervizory (fyzickými servery)
Podpora	60 měsíců včetně nároku na bezpečnostní a opravné aktualizace

Licence Microsoft - SELECT Plus (nové) - dodání licencí formou licenčního portálu vázaného na koncového zákazníka (kupujícího), jehož součástí budou:

- Seznam nabízených licencí a jejich počet,
- Instalační médium,
- Instalační klíče,
- resp. další informace vztahujících se k licencím.

1x Zabezpečené úložiště záloh s řízenou retencí

Parametr	Popis parametru
Provedení	Rackové provedení 2U včetně výsuvných kolejnic a montážního materiálu do racku
CPU	Minimálně 1x procesor Intel Xeon Silver 4410Y 2G, 12C/24T Výkon procesoru dle https://www.cpubenchmark.net/ 24357 bodů
RAM	32 GB, DDR5 - 5600
Úložiště firmware	2x SSD 480 GB, Enterprise provedení 1 DWPD, výměnné za provozu (hot-plug)
Úložiště dat	10x 20TB, 7 200 ot/min, výměnné za provozu (hot-plug)
RAID hardware	PERC H755, SATA/SAS 12Gb, RAID 1,5,6, zálohovaná zapisovací cache 8 GB, podpora HBA režimu
LAN	2x 1GbE, 2x 10Gb SFP
USB	3 USB konektory, 1x verze 3.0, 1x na čelním panelu s podporou bootování
Vzdálená správa	Servisní modul s možností samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, virtuální média, možnost bootování se vzdáleného média
Napájení	Redundantní napájecí zdroje 800W, musí splňovat požadavky na certifikaci energetické účinnosti Platinum dle 80 PLUS (https://cs.wikipedia.org/wiki/80_Plus) nebo lepší; případně na stejné nebo vyšší úrovni účinnosti podle jiné certifikace
Souborový systém	XFS
Protokoly	SMB/CIFS, SNMP, http/s a ssh (management)
Výkon	Zápis 2 TB GB / hod.

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Ochrana dat	RAID5, automatická relokační vadných datových bloků
Retence dat	Programově nastavitelné retenční lhůty na uložený objekt (např. soubor), po dobu retence nelze objekt modifikovat
Redundance	Redundantní rotační díly a napájecí zdroje
Ochrana proti přepisu dat	Režim WORM (Write Once - Read many times Memory)
Kompatibilita	Kompatibilita se stávajícím zálohovacím software, podpora ukládání záloh, řízení jejich historie a řízení retenčních lhůt
Záruka	60 měsíců, oprava druhý pracovní den v místě instalace, nárok na podporu výrobce a nové verze firmware / software

1.2.3 Oblast řízení privilegovaných účtů a zařízení

1x Software pro správu a zabezpečení privilegovaných účtů

Parametr	Popis parametru
Základní funkčnost	Proxy brána určená pro správu a monitoring privilegovaných přístupů
Záznam relací	Zaznamenávání relací privilegovaných uživatelských účtů včetně vytváření logů
Licence	Licence pro monitorování a záznam min. 10 současně pracujících (privilegovaných) uživatelů na 100 definovaných cílových systémech
Logování relací	Nepozměnitelné podklady pro audit a analytické reporty uživatelského chování
Metadata	Ukládání metadat záznamů pro snadnou orientaci při prohlížení a vyhledávání (kliknutí myši, změna obrazovky)
Architektura	Virtuální appliance, bezagentové řešení (bez nutnosti instalace agentů na monitorované systémy)
Autentizace	Microsoft Active Directory, podpora vícefaktorové autentizace (MFA)
Autorizace	Integrované workflow pro autorizaci (min. povolené časy a trvání relace)
Bezpečné přihlášení	Uživatel privilegovaného účtu se přihlašuje pouze k proxy. Přihlášení k cílovému systému zajišťuje proxy - uživatel nezná přístupové údaje k cílovému systému
Přístupové protokoly a aplikace	Proxy umožňuje zprostředkované (bez znalosti hesla cílového systému) přihlášení k cílovým systémům min. RDP, SSH, webová GUI)
Notifikace	Zasílání notifikací o zahájení definované relace
Řízení v reálném čase	Monitorování relací v reálném čase a jejich okamžité ukončení v případě potřeby
Rozšiřitelnost	Podpora modulů (plug - in či obdobných) pro integraci s dalšími technologiemi / technologickými partnery
Rozhraní	Webové rozhraní pro přístup uživatelů i konfiguraci, bezpečná publikace do internetu (šifrovaná komunikace)
Zabezpečení přístupových údajů	Integrované bezpečné (šifrované) úložiště přístupových údajů k cílovým systémům
Rotace hesel	Automatická změna (rotace) hesel přístupových účtů ke spravovaným systémům s otevřenou a veřejně dostupnou dokumentací
Logy	Uložení auditních záznamů s přístupem pouze oprávněných uživatelů, podpora napojení na systém

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	centrálního logování a/nebo SIEM
Podpora	Podpora výrobce po dobu 60 měsíců – nárok na nové verze software, včetně aktualizací

1.2.4 Oblast vícefaktorové autentizace

1x Software pro autentizaci uživatelů pomocí identifikačních karet

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Parametr	Popis parametru
Základní popis	Systém pro autentizaci uživatele identifikačním prostředkem typu Smart card vůči adresářové službě Active Directory
Rozhraní	Grafické rozhraní v českém jazyce
Obnova certifikátů	Automatické hlídání expirace uživatelských doménových i kvalifikovaných certifikátů a automatické vyvolání uživatelského průvodce pro jeho jednoduchou automatizovanou uživatelskou obnovu podle nastavených politik
Autentizace	Autentizace uživatele v aktuálně výrobcem podporovaných operačních systémech Windows včetně RDS (Remote Desktop Services) všech verzích aktuálně podporovaných výrobcem (Microsoft)
Správa	Uživatelská správa uložených certifikátů a bezpečnostních údajů (PIN, QPIN, PUK atd.)
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti
Licence	Pro 250 uživatelů (včetně externích)
Záruka	Záruka 60 měsíců včetně podpory výrobce a nároku na nové a opravné verze

1x Software pro správu identifikačních karet a interních a veřejných certifikátů včetně PKI

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Parametr	Popis parametru
Provedení	Systém pro správu identifikačních prostředků (karet) a certifikátů
Rozhraní	Grafické rozhraní v českém jazyce s podporou SSO uživatele přihlášeného do domény Active Directory
Správa certifikátů	Export / import certifikátů/klíčů, z/na identifikační prostředek, smazání certifikátů nebo privátního

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	klíče, od/registrace certifikátu ve Windows, testování integrity a použitelnosti
Předávání veřejných doménových klíčů	Automatizované předávání veřejných klíčů doménových certifikátů do stávajícího systému Microsoft Active Directory
Prostředky	Podpora kontaktních, bezkontaktních i hybridních identifikačních prostředků
Evidence	Systém umožní evidovat minimálně - typ prostředku (zejména kontaktní, bezkontaktní, hybridní) - druh prostředku (zejména uživatelský, administrační, operátorský) - stav prostředku (zejména používání, k recyklaci, skartovaný) - historii prostředku (zejména datum zavedení do evidence, vydání uživateli, recyklace) - držitele prostředku (zejména aktuálního držitele i všechny předchozí držitele) - data uložená v prostředku (zejména certifikáty a další data, včetně historie dat)
Integrace	Napojení na Active Directory (zdroj dat o uživatelích, autentizace uživatelů, řízení rolí podle členství ve skupinách) a interní certifikační autoritu (certifikáty)
Správa certifikátů	Správa certifikátů (doménových i kvalifikovaných) ve webovém prostředí systému: - vydávání (ukládání) certifikátů na identifikační prostředek, vytvoření a tisk protokolu o vystavení - odvolání certifikátu - vydávání "v zastoupení" - např. personalista vydá novému zaměstnanci identifikační prostředek včetně certifikátu zaměstnance - včasné (konfigurovatelné) e-mailové upozornění na vypršení platnosti certifikátu
Certifikační autority	Systém musí umožnit použití jakékoliv certifikační autority od kvalifikovaných poskytovatelů certifikačních služeb (https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx).
Operace	Recyklace identifikačních prostředků s pevným i náhodným PIN/PUK, změna uživatele, odblokování PIN (i vzdálené), tisk protokolů
Personifikace	Integrované prostředí pro generování podkladů pro potisk identifikačních karet i na vlastní tiskárně
Rozhraní	Integrované aktivní aplikační rozhraní (API) pro bezpečné (autorizované) poskytování veřejných informací o uložených prostředcích, certifikátech a kvalifikovaných elektronických pečeti pro systémy třetích stran včetně dokumentace.
Notifikace	E-mailové upozornění uživatelů i správců na nestandardní stavy či nutnost zásahu (např. expirace certifikátu – nutnost obnovy)
PKI	Součástí řešení bude kompatibilní infrastruktura PKI (public key infrastructure) pro zajištění celého životního cyklu osobních přihlašovacích certifikátů a jejich šablon
Licence	Pro 250 uživatelů, včetně externích
Podpora	Podpora výrobce po dobu 60 měsíců – nárok na nové verze software, včetně aktualizací

140x Klávesnice s integrovanou čtečkou karet

Parametr	Popis parametru
Provedení	PC klávesnice s integrovanou čtečkou nabízených čipových (SmartCard) karet, připojitelná přes USB
Rozložení kláves	České rozložení a popis klávese samostatným numerickým blokem, české popisy kláves. Kvalitní ergonomické provedení
Kompatibilita	Standardní PC a notebooky, Windows 7 a vyšší (32 a 64 bit), Linux
Záruka	24 měsíců

130x Hybridní identifikační karty

Parametr	Popis parametru
Základní popis	Hybridní identifikační karta s kontaktní částí Smart card a bezkontaktní částí typu EMARINE, kompatibilní s nabízeným čtečkami a splňující požadavky nařízení eIDAS č.910/2014
Veřejné certifikáty	Karta musí umožnit ukládání a používání vlastních certifikátů a certifikátů veřejných certifikačních autorit – zejména Postsignum, která nyní kupující používá
Identity	Karta musí umožnit ukládání více identit
Kvalifikovaný prostředek	Karta musí být možno využívat pro elektronický podpis nejvyšší úrovně (kvalifikovaný podpis uložený na QSCD prostředku)
Softwarová podpora	Součástí dodávky bude software pro zpřístupnění jejich rozhraní v operačním systému včetně rozšířených funkcionalit, tzv. Middleware
Záruka	24 měsíců

1.2.5 Oblast zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů

1x Licence software pro sběr a správu logů (systém centrálního logování)

Parametr	Popis parametru
Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware
Ovládání	Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení.
Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze
Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému
Sběr dat (logů)	Bezagentový sběr logů s výjimkou systémů Windows
Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených), šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem
Protokoly	Příjem a zpracování logů, událostí a další strojově generovaných dat minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELp, nešifrovaně) a TCP 20515 (RELp, šifrovaně)
Formáty logů	RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog
Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv
Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy
Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.
Vizualizace logů	Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období
Pracovní plochy	Předpřipravené pohledy (dashboards) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání
Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min. 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti
Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - např. umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům dat, aplikacím, zařízením, IP rozsahů apod.
Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova
Rozpoznávání IP, MAC	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy
Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém
Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalostí (např. SQL dotazů apod.) napříč všemi typy dat a zařízení
Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Průběžná aktualizace přednastavených reportů výrobcem
Integrace	Integrované REST API rozhraní musí umožnit autorizovaný přístup ke strukturované databázi logů
Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparserovaných testovacích dat včetně případných chyb
Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Vmware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortinet, HPE/Aruba, Dell servery, Synology, Linux, Apache, nabízený Systém pro analýzu síťového provozu
Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP
Výkon	2000 EPS (events per second), krátkodobá (10 min) přetžitelnost systému až 200%
Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat
Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade
Zálohování	Integrované zálohování a obnova konfigurace
Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden
Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce
Podpora	60 včetně nároku na nové verze firmware/software a aktualizace

Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

1x Úložiště pro logování – produkční

Parametr	Popis parametru
Základní funkce	Úložiště a výpočetní zdroje pro software systému centrálního logování - software systému centrálního logování
Architektura	Integrovaná appliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávisle na infrastruktuře zadavatele
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška 2U
Kapacita	Využitelná diskové kapacita pro ukládání data min. 12 TB, disky musí být chráněny RAID 5
Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis i čtení) o kapacitě 2 GB
Napájení	Systém musí mít redundantní napájení (2 nezávislé zdroje)
LAN konektivita	2x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent
Záruka	60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace

1x Úložiště pro logování – archivační

Parametr	Popis parametru
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška 2U
Výkon	64 bit CPU, 6 jader, Intel® Xeon® D-1531
HDD	12 pozic pro HDD, rozšiřitelné na 30 HDD
Rozšiřitelnost	Podpora připojení externích disků přes USB 3.0 (2 porty)
Hot-swap	Disky vyměnitelné za chodu.
SSD HDD	Podpora SSD disků pro ukládání dat i akceleraci rotačních HDD
Kapacita	Osazeno 12 TB HDD SATAIII/256MB cache, 7200 ot/min oficiálně podporovanými výrobcem zařízení
Konektivita	4 x 1 GbE a 2x 10Gb SFP+ porty s podporou agregace linek a redundance
Výkon	Rychlost zápisu min. 1 700 MB/sec při RAID5 a CIFS
Kompatibilita	Plná podpora Microsoft Hyper-V a Windows Active Directory a ACL
Komunikace LAN	Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s
UPS	Podpora korektního vypnutí signálem z UPS přes LAN při výpadku napájení
RAM	8 GB, využitelná jako cache, rozšiřitelná na 64 GB
Ochrana dat	Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10, integrovaný systém pro automatické vytváření a správu snapshotů (snímků dat)
Napájení	Vestavěné redundantní napájecí zdroje

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
Záruka	60 měsíců, oprava v místě instalace (včetně HDD)

1x Nástroj pro sběr a vyhodnocování síťových toků

Parametr	Popis parametru
Základní funkce	Monitorování síťové aktivity v reálném čase, identifikace potenciální kybernetické hrozby, bezpečnostního rizika a anomálního chování a tvorba upozornění o jejich výskytu v reálném čase.
Architektura	Integrovaná appliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), provozovaný v prostředí zadavatele. Samostatně funkční nezávisle na infrastruktuře zadavatele či dalších (cloudových) službách.
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška 1U, hloubka 900 mm, včetně výsuvných kolejnic a ramene pro vedení kabelů.
Ovládání	Grafická webová konzole (HTTPS) pro administrátory i operátory, pro správu a používání systému. SSH pro CLI - automatizace, monitorování.
Viditelnost	Systém zajišťuje detailní viditelnost do síťové komunikace s "drill down" prokliky na veškerá uložená data.
Sběr dat	Systém bude získávat data na základě zrcadleného síťového provozu bez potřeby instalace agentů na zařízení v síti.
Zrcadlení komunikace	Podpora SPAN portů a síťových TAPů pro získávání dat zrcadlené komunikace.
Pasivní sběr	Systém bude zcela pasivní vůči síťovému provozu, monitorovaný provoz přes systém nebude procházet a systém jej nebude nijak ovlivňovat.
Netflow protokoly	Systém umožní analyzovat síť na základě zpracování statistických protokolů typu NetFlow v5, NetFlow v9, IPFIX, NetStream a případně dalších ekvivalentních.
Záznam provozu	Zaznamenávání síťového provozu, minimálně základních parametrů: cílová a zdrojová IP/MAC adresa, podsítě, využitý protokol, IPv4 nebo IPv6.
Integrace	Integrace s nabízeným Systémem pro správu, minimálně v úrovni syslog.
Kontextuální informace	Získávání, vizualizace a integrace kontextuálních informací v jednotném grafickém rozhraní: - Hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS provozu a Active Directory, - IP geolokace.
Monitorování zařízení	Identifikace zařízení v síti (koncová zařízení, servery, IoT, síťové prvky), rozpoznání změn v síti a notifikace výskytu nového zařízení (obecně assetu).
Analýza	Integrovaný modul pro detailní analýzu sítě - vytváření dlouhodobých grafů a přehledů o komunikaci na síti s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH), SSL a DNS provozu, VoIP statistik, SMB/CIFS, DHCP a e-mail provozu.
Vizualizace, vyhledávání	Zobrazení provozu a jeho hloubková analýza - okamžité vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez speciálního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů.
HTTP komunikace	Podpora pro příjem a analýzu HTTP provozu – včetně položek typu URL a hostname.
Detekce anomálií	Integrované samostatné učení na základě matematických metod (např. strojové učení) pro

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

Parametr	Popis parametru
	analýzu síťové aktivity, vytváření a automatická průběžná modifikace modelů chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb. Schopnost identifikace nestandardního síťového chování na základě modelu chování daného zařízení a jeho služeb.
Detekce hrozeb	Schopnost detekce neznámých hrozeb, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Minimálně identifikace příznaků potenciálně škodlivého chování: - průzkumné aktivity v síti, - potenciální úniky dat, - detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, - detekce příznaků těžení kryptoměn, - útoky hrubou silou a enumerace dat.
Behaviorální analýza	Detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů). Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti.
False-positive události	Integrovaná podpora identifikace neplatných událostí pomocí mechanismu false-positives, potlačení identifikovaných událostí při příštím výskytu.
Autentizace	Podpora autentizace vůči LDAP, včetně podpory RBAC (přiřazení úrovně oprávnění na základě členství uživatele v konkrétní LDAP skupině).
Reporting	Tvorba dlouhodobých grafů a přehledů s různými typy pohledů dle kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (http, IMAP, SSH). Generování statistik a podrobných výpisů ve volitelných časových intervalech. Tvorba tzv. Top N statistik podle různých kritérií (počet přenesených bytů, paketů, toků atd.) pro výpis nejaktivnějších či anomálně komunikujících assety.
Automatizace reportingu	Vytváření automatizovaných manažerských reportů včetně možnosti exportu do PDF a CSV (nebo obdobného strojově čitelného) formátu. Automatické zasílání reportů emailem, předpřipravené reporty v českém a anglickém jazyce.
Alerty, notifikace	Notifikace na základě překročení prahových hodnot definovaných při implementaci či v průběhu provozu. Systém musí být schopen upozorňovat uživatele prostřednictvím e-mailu o: - všech identifikovaných událostech, - událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. Logování notifikací.
Výkon	0,2 Gb/s trvalý síťový provoz, 500 Netflow/sec.
Kapacita	Úložná kapacita SSD s ochranou RAID 1 pro 30 denní historii při plném výkonu.
Konektivita	1x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent.
Záruka a podpora	60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace.

2 Instalace a zprovoznění

2.1 Instalační služby

Budou provedeny uvedené práce na dodaných komponentech a případně dalších souvisejících zařízeních.

V rámci předmětu plnění kupující požaduje provedení následujících služeb:

- doprava jednotlivých komponent do místa plnění (uvedena v kupní smlouvě)
- zpracování a předání dokumentace,
- vlastní nasazení řešení splňující požadované parametry technického řešení,
- začlenění nabízených technologií do stávajícího prostředí,
- zajištění testovacího provozu,
- provedení akceptačních testů,
- dodávka a aktivace požadovaných SW licencí, kontrola aktivací musí být součástí akceptačních testů
- zaškolení IT administrátorů na dodané technologie v rozsahu min. 16 hodin.

2.2 Podrobný popis instalačních služeb

Budou provedeny uvedené instalační a implementační práce na dodaných komponentech a případně dalších souvisejících zařízeních.

Zvýšení zabezpečení komunikační sítě
- analýza stávajícího síťového prostředí a návrh nové architektury LAN, - implementace pořízených technologií, - provedení segmentace sítě – VLAN, adresování, routování, - zavedení DNSSEC, vybudování DNSSEC resolveru pro LAN úřadu, - návrh a implementace systému 802.1X pro LAN a WiFi včetně definice přístupových politik. Systém 802.1x musí být integrován s adresářovou službou Active Directory, - implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál, - zpracování uživatelské dokumentace konfigurace obvyklých zařízení a jejich systémů pro systém 802.1X – PC, notebooky, chytré telefony, tablety, tiskárny – Windows, Linux, MacOS, Android, IOS, embedded systémy periferií. Provedení vzorové migrace a konfigurace všech kategorií koncových zařízení (1 zařízení každé kategorie) do systému s ověřováním 802.1X, - návrh a vybudování vhodné architektury WiFi s více SSID pro zaměstnance, jejich osobní zařízení a veřejnost s vhodným způsobem ověřování a politikami řízení provozu, - návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií, zajištění bezpečné publikace interních zdrojů úřadu, vybudování VPN na bázi webového portálu, - převzetí komunikačních pravidel ze stávajícího firewallu a jejich implementace do nového firewallu včetně optimalizací využívajících pokročilých vlastností nového řešení. Export pravidel ze stávajícího firewallu zajistí kupující, - provedení potřebných migrací a konfigurací stávajících systémů – export konfigurací stávajících síťových systémů provede kupující, - návrh a provedení akceptačních testů.
Vytvoření serverového prostředí s vysokou dostupností pro provoz IS
- analýza současného prostředí s ohledem na systémové a kapacitní nároky systém a aplikací - návrh a rozšíření virtualizační platformy v kontextu nově dodávaných technologií a zvýšení dostupnosti provozovaného prostředí jako celku, a to pro provoz současných a dodaných systémů

*Veřejná zakázka s názvem
„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“*

- návrh a vybudování platformy aplikační virtualizace včetně nastavení uživatelského prostředí a vhodných politik - začlenění veškerých dodaných systémů do zálohovacích plánů organizace - provedení potřebných migrací - provedení potřebných konfigurací souvisejících systémů - návrh a provedení akceptačních testů
Nasazení systému řízení privilegovaných účtů a zařízení
Privilegované účty - analýza ICT prostředí se zaměřením na vyhledání a inventarizace privilegovaných účtů - vybudování systému pro správu a řízení privilegovaných účtů včetně napojení monitorovaných systémů a nastavení rotace hesel - provedení potřebných konfigurací souvisejících systémů - návrh a provedení akceptačních testů
Vícefaktorová autentizace
- analýza prostředí se zaměřením na zavedení vícefaktorové autentizace - vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority integrované s Active Directory, návrh a implementace šablon certifikátů - vybudování systému vícefaktorové autentizace s využitím kontaktních identifikačních prostředků (čipových/Smart karet). Instalace externích čteček na koncová zařízení ani distribuce identifikačních medií uživatelům není součástí plnění. - návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (karet a doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti - návrh procesů souvisejících se řízením životního cyklu karet a certifikátů včetně jejich vystavování a přidělování zaměstnancům personálním oddělením - návrh a realizace zálohování - provedení potřebných konfigurací souvisejících systémů - návrh a provedení akceptačních testů včetně výkonových testů
Zavedení nástroje pro zaznamenávání činnosti IS a KS, jeho uživatelů a administrátorů
Sběr a správa logů - analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí - návrh a vybudování systému centrálního logování pro zaznamenávání činnosti informačního a komunikačního systému, jeho uživatelů a administrátorů - monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem) - logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených pracovních stanic (aplikační virtualizace) apod. - monitorování IP datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) dle RFC3954 nebo ekvivalentu (např. netflow) – minimálně na úrovni rozhraní WAN - provedení souvisejících konfigurací monitorovaných systémů - návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů

Sběr a vyhodnocení síťových toků

- analýza komunikačního systému a návrh způsobu sběru a obsahu síťových toků a logovaných událostí
- vybudování systému sběru a analýzy síťových toků a souvisejících bezpečnostních událostí
- provedení souvisejících konfigurací monitorovaných systémů
- ukládání informací (min. o bezpečnostních událostech incidentech do systémů sběru a správy logů)
- návrh a provedení akceptačních testů

2.3 Dokumentace k dodávanému řešení

Bude zpracována a dodána níže uvedené dokumentace. Dokumentace bude zhotovena v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. DOC, ODT, PDF atd.) na datovém nosiči.

2.3.1 Prováděcí dokumentace

Prováděcí dokumentace bude sloužit jako podklad pro vlastní instalaci a implementaci řešení do prostředí kupujícího. Prováděcí dokumentace bude zahrnovat detailní popis cílového stavu a způsobu jeho dosažení, včetně:

- detailního popisu cílového stavu včetně funkcionalit jednotlivých částí systému,
- nutné a doporučené optimalizační a konfigurační změny dodávaných systémů i všech navázaných systémů (serverová infrastruktura, LAN, zálohování, monitorování atd.),
- způsob zajištění potřebného HW a SW,
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem,
- detailní návrh a popis postupu instalace a implementace předmětu plnění,
- detailní popis zajištění bezpečnosti informací,
- detailní harmonogram realizace včetně uvedení kritických milníků,
- návrh designu síťového a bezpečnostního řešení a jeho konfigurace,
- návrh designu aplikačních řešení,
- vazby na stávající systémy a jejich konfigurace,
- integrace implementovaných softwarových systémů,
- rekonfigurace stávajících systémů, které nevyžadují součinnost ani souhlas třetí strany a které mají veřejně a otevřeně dostupnou dokumentaci umožňující rekonfiguraci neomezenému okruhu kvalifikovaných osob,
- dopady implementace na dostupnost a funkčnost stávajících služeb,
- posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon),
- požadované součinnosti kupujícího a jejich rozsah,
- návrh akceptačních kritérií a akceptačních testů.

2.3.2 Provozní dokumentace

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy:

2.4 Zaškolení IT administrátorů

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 v rozsahu:

- běžných administrátorských činností pro implementované systémy,
- standardní údržby systémů pro administrátory kupujícího,
- základní identifikace nestandardních stavů systému a jejich příčin.

Rozsah zaškolení pro administrátory je 16 hodin.

Předpokládaný počet administrátorů (účastníků školení) je max. 8 osob.

2.5 Testovací provoz

Testovací provoz proběhne po dobu uvedenou v harmonogramu realizace, a to se zvýšeným dohledem a podporou ze strany prodávajícího.

Cílem testovacího provozu je poskytnout metodické vedení a prostor uživatelům pro ověření funkcionality a vlastní funkčnosti dodaného řešení, pro cvičnou práci se systémem a prostor pro prodávajícího pro identifikaci a opravu případných chyb a neshod. Dalším cílem testovacího provozu je možnost případné definice změnových požadavků ze strany kupujícího. Během testovacího provozu provede prodávající aktualizaci Prováděcí dokumentace na Dokumentaci skutečného provedení, včetně záznamu konkrétních provedených konfigurací. Úspěšný průběh testovacího provozu, jehož výstupem bude faktické uživatelské ověření schopnosti nasazení nového řešení v prostředí kupujícího na základě této technické specifikace a jejich příloh, je jednou z nezbytných podmínek kupujícího pro možnost akceptace plnění na základě této technické specifikace a jejich příloh.

2.6 Akceptační řízení

2.6.1 Dílčí akceptační řízení

Dílčí akceptační řízení bude provedeno jednotlivé oblasti plnění dle této technické specifikace. Dílčí akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům této technické specifikace a jejím přílohám a požadavků daných prováděcí dokumentací.

Výsledkem dílčího akceptačního řízení je akceptační protokol s výsledkem Splněno (Akceptováno) nebo Nesplněno (Neakceptováno), podepsaný oprávněnými osobami smluvních stran.

Součástí akceptačního protokolu ke každé oblasti plnění bude i soupis předaných prvků včetně jejich sériových čísel.

Dílčí akceptace mohou probíhat v libovolném pořadí, je-li to technicky a organizačně možné a vhodné.

2.6.2 Souhrnné akceptační řízení - akceptace

Souhrnné akceptační řízení bude zahrnovat porovnání skutečného stavu vůči požadavkům kupní smlouvy a této technické specifikace, která je její přílohou, a jejich příloh, funkčního i nefunkčního charakteru – licence a příslušenství.

Výsledkem souhrnného akceptačního řízení je akceptační protokol s výsledkem Splněno (Akceptováno) / Splněno (Akceptováno) s výhradou / Nesplněno (Neakceptováno), podepsaný oprávněnými osobami smluvních stran, a to s výsledným uvedením každé části na tomto akceptačním protokolu a výsledku akceptačního řízení. Klasifikace Splněno (Akceptováno) s výhradou umožní pokračování v realizaci v případě vad drobných, pro které může být opakování akceptačního řízení zbytečně nákladné.

2.6.3 Opakované akceptační řízení

Jestliže plnění nesplňuje podmínky stanovené pro akceptaci, bude obsahem akceptačního protokolu vyjádření Nesplněno (Neakceptováno) spolu s popisem závad a uvedením termínů pro jejich nápravu. Proávající napraví tyto nedostatky a akceptační řízení v odpovídajícím rozsahu bude provedeno znovu. Proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně. Proces testování a následných oprav lze opakovat, dokud prodávající nesplní požadavky pro akceptaci řádnou s výsledkem Splněno (Akceptováno), nejvýše však 2x (dvakrát).

V situaci, kdy by bylo nutné opakovat akceptační řízení více jak 2x (dvakrát), bude takové opakování považováno za podstatné porušení smlouvy ze strany prodávajícího a kupující bude oprávněn odstoupit od smlouvy. Prodlení vzniklé v souvislosti s potřebou opakování akceptačních řízení bude považováno vždy za prodlení vzniklé na straně prodávajícího se zachováním důsledků takového prodlení, tedy zejména smluvních pokut na základě uvažené kupní smlouvy.

Opakované akceptační řízení bude probíhat jednotlivě samostatně pro jednotlivé části či oblasti tak, aby na již akceptované části dané opakované akceptační řízení nemělo vliv.

2.7 Harmonogram plnění

Harmonogram je sestaven tak, aby jednotlivé práce na sebe logicky navazovaly a zároveň byl v souladu s požadavky výzvy, 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.

Aktivita projektu	Termín nejpozději do
Zpracování prováděcí dokumentace, připomínkování ze strany kupujícího, vypořádání připomínek, finalizace dokumentu.	4 týdny
Akceptační řízení prováděcí dokumentace	1 týden
Předání prováděcí dokumentace	T + 5 týdnů
Dodávky komponent řešení a instalace Implementace dodaného řešení prováděcí dokumentace – nastavení / konfigurace / parametrizace jednotlivých oblastí, provedení integrací na spolupracující systémy atd. Zpracování a dodávka provozní dokumentace. Zpracování školicích materiálů.	15 týdnů
Připravené prostředí pro testovací provoz, předání do testovacího provozu.	T + 20 týdnů
Prezenční zaškolení IT administrátorů. Předání do testovacího provozu.	1 týden
Testovací provoz s dohledem a podporou prodávajícího. Oprava chyb a neshod, případná definice změnových požadavků. Aktualizace dokumentace Dodávka licencí (listinné potvrzení dodaných licencí co do jejich počtu a rozsahu).	3 týdny
Akceptační řízení – porovnání skutečných vlastností se požadavky smlouvy.	1 týden
Akceptace projektu, předání systému do rutinního provozu.	T + 25 týdnů

Poznámka: Ve sloupci „Termín nejpozději do:“ znak „T“ vyjadřuje datum účinnosti smlouvy.

2.8 Projektové řízení

Jako součástí plnění budou pravidelné projektové schůzky 1x měsíčně a dále ad-hoc pracovní schůzky k problematice řešení jednotlivých oblastí plnění, včetně projednání a odsouhlasení výstupů pro konfiguraci a nastavení jednotlivých oblastí plnění pro potřebu kupujícího.

S ohledem na rozsah projektu a dopad jeho zavedení do produkčního provozu na výkon činnosti kupujícího je v rámci předmětu plnění objednatelem 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 projektových prací,
- závazný harmonogram projektu – dodržování termínů v harmonogramu, podchycení případných kolizí, zpoždění nebo vznikajících rizik a jejich reportování směrem k objednateli, 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.

Cenová tabulka veřejné zakázky s názvem „Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

1. Dodavatel cenovou tabulku vyplní a cenu vypočte pouze v buňkách označených:
2. Dodavatel vyplní do tabulky jednotlivé ceny dodávek a služeb včetně jejich příslušenství.
3. Pro stanovení nabídkové ceny dodavatel do ceny zařízení zaneše i cenu standardní záruky, která je k zařízení dodávána. Nadstandardní záruku, záruční servis a podporu dodavatel nacení samostatně do příslušné položky k zařízení v tabulce níže. Podpora zařízení a podpora software za předpokladu, že první rok podpory je součástí dodávky licence nebo zařízení může být součástí ceny zařízení a licence, každý další rok musí být naceněn samostatně ve sloupečku E této tabulky, jako samostatná podpora, není-li v technické dokumentaci (příloha č. 1 ZD) uvedeno jinak.
4. Náklady na implementační služby budou zohledněny v ceně dodávek zařízení.

Dodávka IT technologie projektu Zvýšení kybernetické bezpečnosti města Ostrov, registrační číslo projektu CZ.31.2.0/0.0/0.0/23_093/0008378				
Položka	Počet	Celková cena za uvedený Počet [Kč bez DPH]	Cena za prodlouženou záruku a záruční servis k zařízení dle specifikace [Kč bez DPH]	Tech. podpora po dobu 5 let (maintenance, bezpečnostní update, patche, subskribce, nároky na aktualizační balíčky dat atd.) [Kč bez DPH]
Páteční přepínač s příslušenstvím	2	718 616 Kč	236 985 Kč	---
Přístupový přepínač s příslušenstvím	21	807 285 Kč	219 692 Kč	---
Přístupový bod WiFi s příslušenstvím	40	403 320 Kč	12 490 Kč	---
Next-generation firewall s příslušenstvím	2	316 834 Kč	44 200 Kč	38 700 Kč
Licence SW pro řízení přístupu do sítě 802.1x	1	360 838 Kč	---	48 500 Kč
Hyperkonvergováný server, včetně příslušenství	2	1 073 259 Kč	88 400 Kč	---
Licence serverové virtualizace	2	76 154 Kč	---	18 000 Kč
Licence diskové virtualizace	2	283 169 Kč	---	63 630 Kč
Licence operačních systémů serverů	2	624 084 Kč	---	46 800 Kč
Klientské licence operačních systémů	130	171 918 Kč	---	---
Klientské licence aplikační virtualizace operačních systém serverů	130	598 599 Kč	---	---
Úložiště záloh s řízenou retencí	1	297 028 Kč	22 300 Kč	---
Licence SW pro správu a zabezpečení privilegovaných účtů	1	1 090 851 Kč	---	186 000 Kč
Licence SW pro autentizaci uživatelů pomocí identifikačních karet	1	674 546 Kč	---	78 500 Kč
Licence SW pro správu identifikačních karet a interních a veřejných certifikátů včetně PKI	1	341 246 Kč	---	12 600 Kč
Klávesnice s integrovanou čtečkou karet	140	129 758 Kč	---	---
Hybridní karty	130	265 385 Kč	---	---
Licence SW pro sběr a správu logů (systém centrálního logování)	1	810 426 Kč	---	123 800 Kč
Úložiště pro logování	1	197 609 Kč	18 600 Kč	---
Nástroj pro sběr a vyhodnocování síťových toků	1	904 667 Kč	56 700 Kč	58 900 Kč

Nabídková cena celkem v Kč bez DPH	11 520 389,00 Kč
DPH ve výši 21 %	2 419 281,69 Kč
Nabídková cena celkem v Kč včetně DPH	13 939 670,69 Kč

Smluvní podmínky k sociálně odpovědnému zadávání

k veřejné zakázce zadávané v otevřeném řízení podle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, s názvem

„Dodávka IT technologií pro zvýšení kybernetické bezpečnosti“

Znění přílohy smlouvy uzavírané na plnění předmětné veřejné zakázky k zohlednění zásad sociálně odpovědného zadávání:

- 1) Prodávající (resp. dodavatel, zhotovitel) prohlašuje, že si je vědom skutečnosti, že kupující (objednatel) má zájem na plnění této smlouvy v souladu se zásadami společensky odpovědného zadávání veřejných zakázek. Prodávající se zavazuje po celou dobu trvání smlouvy zajistit dodržování veškerých právních předpisů, zejména pak pracovníprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a zákona č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovníprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovníprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci), a to vůči všem osobám, které se na plnění smlouvy podílejí a bez ohledu na to, zda bude podle této smlouvy plněno prodávajícím či jeho poddodavatelem.
- 2) Prodávající je povinen po dobu trvání této smlouvy vždy na výzvu kupujícího předložit čestné prohlášení, v němž uvede jmenný seznam všech svých zaměstnanců, agenturních zaměstnanců, živnostníků a dalších osob, se kterými se na realizaci smlouvy podílel v době od uzavření smlouvy či od poslední výzvy k předložení prohlášení. V čestném prohlášení musí být uvedeno, zda všechny osoby v seznamu uvedené jsou vedeny v příslušných registrech, zejména živnostenském rejstříku, registru pojištěnců ČSSZ a mají příslušná povolení k pobytu v ČR a k výkonu pracovní činnosti. Dále zde bude potvrzeno, že uvedené osoby byly proškoleny z problematiky BOZP a že jsou v případě potřeby vybaveny osobními ochrannými pracovními prostředky dle platné legislativy. Prodávající bere na vědomí, že tato prohlášení je kupující oprávněn poskytnout příslušným orgánům státní správy ČR. Tato povinnost platí bez ohledu na to, zda bude plnění podle této smlouvy prováděno prodávajícím či jeho poddodavatelem.
- 3) Prodávající je oprávněn průběžně kontrolovat dodržování povinností kupujícího dle odst. 1 a 2, a to i přímo u pracovníků provádějících služby, přičemž prodávající je povinen tuto kontrolu umožnit, strpět a poskytnout kupujícímu veškerou nezbytnou součinnost k jejímu provedení.
- 4) Prodávající je povinen oznámit kupujícímu, že vůči němu či jeho poddodavateli bylo orgánem státní správy (zejména Státním úřadem inspekce práce či oblastními inspektoráty, Krajskou hygienickou stanicí apod.) zahájeno řízení pro porušení právních předpisů, jichž se dotýká ujednání v odst. 1 a odst. 2, a k němuž došlo při provádění smlouvy nebo v souvislosti s ní, a to nejpozději do 10 dnů od doručení oznámení o zahájení řízení. Součástí oznámení prodávajícího bude též informace o datu doručení oznámení o zahájení řízení.
- 5) Prodávající je povinen předat kupujícímu kopii pravomocného rozhodnutí, jímž se řízení ve věci dle předchozího odstavce končí, a to nejpozději do 7 dnů ode dne, kdy rozhodnutí nabude právní moci. Současně s kopií pravomocného rozhodnutí prodávající poskytne kupujícímu informaci o datu nabytí právní moci rozhodnutí. V případě, že prodávající (či

jeho poddodavatel) bude v rámci řízení zahájeného dle předchozího odstavce pravomocně uznán vinným ze spáchání přestupku, správního deliktu či jiného obdobného protiprávního jednání, je prodávající povinen přijmout nápravná opatření a o těchto, včetně jejich realizace, písemně informovat kupujícího, a to v přiměřené lhůtě.

- 6) Prodávající prohlašuje, že v případě výběru poddodavatelů, bude-li to s ohledem na poptávané práce a činnosti vhodné, resp. možné, upřednostní poddodavatele zaměstnávající osoby znevýhodněné na trhu práce nebo pracovníky se zdravotním postižením.
- 7) Prodávající výslovně souhlasí s tím, že kupující je oprávněn v případě prodávajícím neuhrazené faktury svému poddodavateli v době splatnosti, pozastavit úhradu faktury vystavené kupujícím.