

1. Technická specifikace - požadavky na předmět dodávek a služeb

Zvýšení kybernetické bezpečnosti města Duchcova – 2. etap

2. Předmět plnění

Předmětem plnění veřejné zakázky je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele v souladu se standardy kybernetické bezpečnosti (dále také jen „dodávka“, „systém“, „řešení“ nebo „technologie“) včetně nezbytných služeb, podrobná specifikace dodávek a služeb je uvedena v dalších kapitolách tohoto dokumentu. Řešení musí být navrženo tak, aby náklady na provoz systému byly co nejmenší.

I u technických parametrů, u kterých není výslovně uvedeno, že jde o požadovanou minimální či maximální hodnotu, lze nabídnout i řešení „lepší“, tedy řešení přesahující (ve smyslu výhodnějším z pohledu užitné hodnoty) hodnotu stanoveného požadavku, ledaže ze zadávacích podmínek výslovně vyplývá, že musí být splněna přesně daná hodnota.

3. Popis současného stavu

Město Duchcov v současnosti primárně využívá dva fyzické servery. Na serverech je provozován hypervisor Hyper-V a celkem 8 virtuálních serverů. Servery jsou replikovány mezi sebou a zálohovány pomocí Veeam Backup&Replication.

Servery i zálohovací úložiště jsou připojeny rychlostí 10Gbe. Serverovna je připojena do dalšího rozvaděče 1Gbe metalickou linkou. Z toho rozvaděče je pak optickým propojem připojena další budova naproti přes ulici.

Město Duchcov používá jako firewall zařízení Mikrotik bez UTM funkcí. Switche jsou různých výrobců, WiFi AP jsou Unifi, avšak již nepodporované výrobcem.

4. Cílový stav

Cílovým stavem je posílení zabezpečení WAN/LAN města Duchcov, posílení bezpečnosti v oblasti zálohování a monitoringu, nasazení logování a terminálového provozu.

Cílového stavu bude dosaženo dodávkou dvou firewallů typu NGFW, které budou v clusteru. Výměnou 4 aktivních prvků (z toho dva budou PoE) a výměnou Wifi AP, celkem 5ks.

Zálohování bude posíleno o další úložiště, které bude umístěné v druhé budově, mimo hlavní serverovnu. Požadováno je zařízení s nastavitelnou retencí ukládaných dat (záloh) tak, aby uložená data nebylo možné po určité (nastavitelnou) dobu změnit. Z pohledu zálohovacího systému půjde o zařízení typu WORM (Write One, Read Many). Protože počet zálohovaných zařízení překročí 10ks, součástí dodávky bude i licence pro zálohovací řešení pro Veeam Backup&Replication, které už v současnosti město Duchcov využívá. Licence musí pokrývat min. 15ks virtuálních serverů, včetně licencí pro Veeam ONE, který je také využíván.

Součástí výměny aktivních prvků bude nasazení segmentace sítě, implementace 802.1X, natažení datových rozvodů pro WiFi AP, připojení archivu k LAN úřadu a vybudování páteřního optického rozvodu mezi serverovnou a podružnými datovými rozvaděči. Archiv je samostatná budova, která je vzdálena cca 10m od serverovny přes dvůr v zadním traktu městského úřadu.

Centrální přepínače budou tvořeny dvěma centrálními přepínači propojenými mezi sebou rychlostí min. 40Gbe. K těmto switchům budou připojeny vždy dvěma linkami další 3 klientské přepínače, dva servery a NAS rychlostí 10Gbe.

Součástí řešení bude i doplnění infrastruktury o systém určený pro sběr a archivaci logů ze všech používaných i nově dodávaných řešení.

Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Data budou ukládána do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. přepínače/netflow a firewall/syslog).

Veškeré dále požadované informace si bude systém automaticky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními protokoly ze síťových a dalších aktivních zařízení a Windows server systémů.

Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích prostřednictvím firewallu a dalších přístupových a autentifikačních systémů (např. radius logy). Dále budou získávány informace o překladu zdrojových, vnitřních IP adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně.

Pro nasazení systému VDI budou pořízeny nezbytné softwarové serverové licence, klientské licence RDS (Remote Desktop Services). Pro bezpečné zpřístupnění virtualizovaných aplikací externím uživatelů (zaměstnanci pracující mimo MěÚ Duchcov, zaměstnanci spolupracujících organizací apod.) bude vybudován webový aplikační portál.

Virtualizací aplikací dojde ke sjednocení pracovních prostředí uživatelů, významně se sníží náročnost jeho správy a dojde k prodloužení životního cyklu uživatelských zařízení. Současně dojde k přesunu uživatelských dat na servery, čímž se zlepší jejich zabezpečení z pohledu poškození i kompromitace.

Oba používané servery mají dostatek výkonu pro provoz poptávaných řešení, pouze celé řešení musí být doplněno o jednu licenci Windows Serveru.

Pro poštovní služby a spolupráci MěÚ Duchcov využívá platformu Office 365.

5. Implementační služby

5.1. Obecné požadavky

Zadavatel požaduje provést minimálně následující implementační práce. Dodavatel je dále povinen zahrnout do plnění veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobcí a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

V rámci implementace předmětu plnění dodavatel realizuje následující služby:

- Vytvoření cílového konceptu – výstupem bude prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí cílového konceptu bude také návrh akceptačních testů. Prováděcí dokumentace musí být před zahájením realizace dodávek výslovně schválena zadavatelem.
- Dodávka a implementace předmětu plnění podle cílového konceptu.
- Zajištění projektového vedení realizace předmětu plnění.
- Zajištění školení pro administrátora v rozsahu min 16 hodin.
- Dodavatel zajistí zkušební provoz v délce minimálně 14 dnů včetně technické podpory minimálně 2 specialistů na dodané řešení s dojezdem maximálně do 1 hodiny od nahlášení požadavku v pracovní den v době od 08:00 do 17:00.
- Provedení akceptačních a testů vysoké dostupnosti dle schválené prováděcí dokumentace.
- Předání do plného provozu. Předání do plného provozu bude zadavatelem akceptováno pouze po dokončení bezproblémového zkušebního provozu a po provedení akceptačních a testů vysoké dostupnosti.

Náklady na provedení implementačních služeb a školení musí být zahrnuty v nabídkové ceně k položkám, ke kterým se vztahují (nevyčísľují se zvlášť).

Dodavatel dle svého uvážení může doplnit v nabídce další služby, které jsou dle jeho názoru nezbytné pro úspěšnou realizaci zakázky.

5.2.Specifické požadavky

5.2.1. Firewally

- Dodávka nových firewallů
- Konfigurace firewallů v HA režimu dle best practices výrobce
- Aktualizace na nejnovější verzi OS
- Přenesení a revize pravidel ze stávajícího řešení

5.2.2. Switche a Wifi

- Montáž do racku a zapojení portů (management, LAN) dodávaných switchů
- Montáž nově dodávaných WiFi AP
- Switche budou připojeny k centrální dvojici switchů dvěma linkami
- Upgrade SW vybavení.
- Konfigurace portů pro připojení serveru a dalších dodávaných technologií, nastavení VLAN pro oddělení provozu dle cílového konceptu
- Konfigurace koncových zařízení (cca 50ks) v souvislosti se zavedením 802.1x

5.2.3. Propojení archivu

- Montáž wifi pojitka
- Zprovoznění spoje mezi serverovnou a archivem

5.2.4. Logování

- Návrh a implementace systému pro centrální logování, především, ale nejen:

- 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
- monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. netflow) – systém pro monitorování a sběr provozně - lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení
- Provedení souvisejících konfigurací monitorovaných systémů

5.2.5. Zálohování

- Zalicencování současného zálohovacího řešení
- Zprovoznění zálohovacího řešení, s maximální možnou ochranou proti průniku, smazání či přepsání záloh – immutable backup, dle best practices výrobce.
- Zálohovací úloha/úlohy budou zálohovat celého prostředí.
- Data budou ukládána na současné NAS úložiště a následně do datového trezoru
- Provedení testovací obnovy celého VM, i jednotlivé položky z datového trezoru.
- Celé řešení musí prokazatelně fungovat bez závad min. po dobu zkušebního provozu

5.2.6. Monitoring

- Zalicencování řešení Veeam ONE
- Konfigurace monitoringu min na tyto události:
 - Detekce možného ransomware útoku
 - Pokus o smazání záloh
 - Neobvyklou (podezřelou) velikost zálohy
 - Nezvyklá délka záloh
 - Auditování změn v zálohovacích úlohách
 - Změnu retenční doby na tzv. neměnné zálohy
 - Stav tzv. neměnných zálohy
 - Zakázání zálohovací či jiné úlohy
 - Failed pokusy při přihlášení do Hyper-V
- Zprovoznění min. SMTP notifikací

5.2.7. RDS

- Příprava pilotního projektu pro 10 uživatelů
- Řešení nesmí být typu All in One z důvodu budoucího možného rozšiřování.
- Návrh a zabezpečení host serveru
- Instalace aplikací, provedení testů aplikací, tiskáren apod.
- Instalace Office 365 (plán Microsoft 365 Business Premium)
- Publikace pomocí webového portálu zabezpečeného hvězdičkovým certifikátem, který město Duchcov vlastní
- Vyhodnocení testů
- Upřesnění technického návrhu

- Ověřovací provoz

5.2.8. SQL

- Příprava nového virtuálního serveru
- Výkonnostní analýza původního řešení a návrh konfigurace nového řešení
- Instalace SQL dle původní konfigurace s přihlédnutím na best practices výrobce
- Konfigurace zálohování

5.2.9. Požadavky na úpravu LAN

Serverovna se nachází ve 3NP MěÚ Duchcov. Distribuční rozvaděč se nachází o jedno patro níže. Do toho rozvaděče je přiveden optický propoj z další budovy a jsou zde dva 48 portové přepínače. Se serverovnou je tento rozvaděč připojen metalickým rozvodem neumožňující propoj rychlostí 10Gbe. Nově bude vybudována optická trasa tvořená jedním 16vláknem typu MM mezi tímto rozvaděčem a serverovnou tak, aby bylo možné propoj z vedlejší budovy i samotné přepínače zapojit redundantně pomocí 10Gbe propoje do centrálních přepínačů v serverovně.

V budově bude nově umístěno 4ks Wifi AP ke kterým je nutné zakončit v rozvaděči ve 2NP, kde bude provozován jeden z dodávaných PoE přepínačů. Další Wifi AP se bude nacházet v druhé budově.

V Archivu, který bude propojen se serverovnou bezdrátovým propojem, bude umístěn malý rozvaděč s PoE switchem, jedním WiFi AP a jednou datovou dvojzásuvkou.

6. Akceptační testy

Akceptační testy budou pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti, dále prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná. Dále pro každou komoditu navrhuje účastník vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení. Návrh vhodných akceptačních kritérií je součástí nabídky, zadavatel může v průběhu zpracování Prováděcí dokumentace provést jejich upřesnění či rozšíření.

Test	Požadovaný výsledek
Zavedení 802.1x	Všechny připojené zařízení jsou autentikovány pomocí 802.1x. Neautorizované zařízení se k LAN/Wifi nepřipojí (nedostane IP adresu)
Rozpojení clusteru firewallů	Nedojde k výpadku poskytovaných služeb
Funkční RDS farma	Je možné se připojit z LAN i Internetu pomocí HTTPS do RDS farmy, uživatel vidí svá data a profil
Ověření logování	Veškerá zařízení (HW, servery, managementy apod.) budou ukládat své logy do log managementu
Pokus o smazání záloh z datového trezoru	Zálohy nebude možné smazat
Testovací obnova	Bude úspěšná provedena testovací obnova VM z datového trezoru

Redundantní zapojení	Bude vytažen jeden datový kabel ze zařízení typu server, switch apod. Úspěšný test bude v případě, že u zařízení nedojde ke ztrátě konektivity
----------------------	--

7. Požadované parametry technického řešení

7.1. Obecné požadavky

Zadavatel při výstavbě, správě a provozu technologií striktně dodržuje hledisko technologické neutrality, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.

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

Za předpokladu, že účastníkem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, úložiště, komunikační prvky atd.) neobsaženou v popisu předmětu plnění, zahrne účastník do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

Pro každý softwarový produkt, který účastník nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.

Účastník ve své nabídce detailně popíše vazby na stávající systémy Zadavatele, které jsou nezbytné pro správné fungování řešení nabízeného účastníkem.

Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že účastník vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky – není přípustné implementovat např. další serverovou virtualizační platformu, adresářovou službu apod.

Účastník prokáže, že všechny dodávky, které dodá Zadavateli:

- (a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
- (b) mají plnou záruku od výrobce,
- (c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
- (d) obsahují licenci na používání příslušného softwaru,
- (e) jsou určeny pro provoz v České republice,
- (f) z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti účastník doloží čestným prohlášením. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

7.1.1. Specifické požadavky – povinné parametry řešení

(1) V dále uvedených tabulkách jsou uvedeny minimální požadované (povinné) parametry dodávaného řešení.

(2) Účastník ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Účastník tedy uvede konkrétní technické parametry nabízeného zboží, vč. uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry mohou být buď rovněž doplněny do tabulky, nebo mohou být doloženy jinde v nabídce např. formou katalogových listů apod., v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit. Zadavatel umožňuje v nabídce uvést funkční, veřejně a bezplatně přístupný přímý odkaz na externí zdroj požadovaných informací – bez nutnosti zadavatelova vyhledávání na internetových stránkách, takový zdroj bude považován za nefunkční a požadavek nebude splněn.

(3) Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku Zadavatele), že nabízené řešení jednoznačně splňuje všechny požadavky.

(4) V případě nesplnění povinných parametrů může být nabídka vyřazena z hodnocení a účastník ze zadávacího řízení vyloučen.

8. Popis požadavků zadavatele

WAN/LAN				
Část	Parametr	Popis povinného parametru	Účastník popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Účastník uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
Firewally 2ks	Provedení	Do racku 1U, včetně montážního kitu		
	Porty	min 10x 1GbE (min. 2x WAN) a 2x 1 Gb SFP (mohou být sdílené), USB pro ext. 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.		
	Počet současných spojení	min. 0,7 milionu		
	Propustnost SSL VPN	min. 900 Mbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů		
	Propustnost SSL inspekce	min. 600 Mbps		
	Propustnost firewallu	min. 10 Gbps pro pakety 512 bytů a větší		
	Propustnost NGFW	min. 600 Mbps		
	Propustnost IPS	min. 1200 Mbps		
	Propustnost detekce škodlivého kódu	min. 600 Mbps		
	Logování	Interní disk pro uchovávání logů min 128GB typu SSD		
	Zabezpečení VPN	Dvoufaktorové ověřování pomocí mobilní aplikace min. pro 10 uživatelů		
	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 určité době během dne		
	Antispam	antispamová a antivirová inspekce elektronické pošty		
	Sandbox	Možnost integrovaného sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky)		
	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení		

WAN/LAN				
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu		
	Management a monitoring	HTTP/S, SSH, SNMP, syslog,		
	Záruka	min. 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalware, antispam, aplikační kontrola)		
Sítové přepínače	Společné parametry			
	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U, neblokovaná architektura		
	Agregace portů	podpora LACP		
	Směrování	hardwarové statické routování včetně VLAN, policy based routing		
	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		
	Ověřování uživatelů a zařízení	Podpora 802.1X		
	Základní parametry	L2/L3 přepínač v rackovém provedení max. 1U, neblokovaná architektura		
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS		
	MAC	podpora min. 15 000 MAC adres		
	Síťové toky	plný přímý export síťových toků - Netflow, IPFIX nebo ekvivalent (sFlow není ekvivalent)		
	Monitoring a správa	plná podpora CLI, SSH, SNMP, syslog, sFlow, web rozhraní, REST nebo SOAP/WDSL API pro automatizaci (např. z IDM)		
	Nezávislý management	vyhrazený samostatný síťový port pro management (nezapočítává se do požadovaného počtu portů)		
	Centrální správa	jednotná správa, monitorování a aktualizace firmware z centrální grafické konzole obsažené ve firmware nabízených síťových prvků.		
	Administrativní rozhraní	Centrální administrativní rozhraní je jednotné pro přepínače i nabízený firewall.		
	Stohování	pokročilé stohování s rozložením LAG (link aggregation group) mezi více přepínačů ve stohu - např. technologie MLAG (Multi-Chassis Link Aggregation nebo obdobná		
	Záruka	Min. 60 měsíců poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware.		
	Specifické parametry			
	Počty, porty a propustnost, napájení	2x centrální přepínač - 24x 1 Gb RJ-45 + 4x 10 Gb SFP+, 2x 40GE QSFP porty , propustnost min. 285 Gbps 1x přístupový přepínač - 24x 1 Gb RJ-45 + 4x 10 Gb SFP+, porty PoE/PoE+ (802.3af/at), propustnost min. 125 Gbps		

WAN/LAN				
		1x přístupový přepínač - 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, porty PoE/PoE+ (802.3af/at), propustnost min. 175 Gbps 1x přístupový přepínač - 48x 1 Gb RJ-45 + 4x 10 Gb SFP+, propustnost min. 175 Gbps 1x přístupový přepínač - 8x 1 Gb RJ-45 + 2x 1 Gb SFP, propustnost min. 20 Gbps		
WiFi AP 6ks	Základní funkce	Přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na strop		
	Frekvence	min. 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)		
	Antennní 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	5GHz 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 radiový 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		
	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	záruka min. 60 měsíců		
Bezdrátový propoj 2ks	Použití	Venkovní/vnitřní		
	Rychlost LAN	Min. 1Gbps		
	Rychlost Wi-Fi	Min. 900Mbit/s		
	RAM	Min. 256MB		

WAN/LAN				
	Bezdrátová síť	Vestavěná 60 GHz 802.11ad		
	PoE	Zařízení podporuje napájení pomocí PoE		
	Záruka	Min. 2 roky		
UPS a PDU	Battery pack	Rozšíření stávající UPS Eaton 5PX 3000i RT3U G2 o 1ks battery packu o jmenovité hodnotě baterie min. 12 V/9 Ah		
	Provedení PDU	do racku		
	Kapacita výstupního výkonu	max. 10A zatížení, 2300VA		
	Výstupní zásuvky	8x zásuvka pro připojení zařízení (7x IEC320 C13 pro spotřebiče + 1x IEC320 C14 pro připojení)		

Zálohování				
Část	Parametr	Popis povinného parametru	Účastník popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Účastník uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
Bezpečné úložiště 1ks	Provedení	Provedení tower. Barevně označené hot-plug komponenty. Pro přístup ke všem komponentám není nutné nářadí. Uzamykatelný čelní panel.		
	CPU	Minimálně 1x procesor 4 jádrový. Výkon serveru dle http://www.spec.org : SPECrate®2017_int_base min. 40 bodů SPECrate®2017_fp_base min. 41 bodů		
	RAM	16 GB, min. 3200 MT/s		
	Úložiště firmware	Min. 2x SSD 480 GB, read intensive, samostatný HW řadič RAID1 Tyto disky nesmí zabírat pozice pro disky určené pro data Disky musí být typu hot-plug a přístupné z přední nebo zadní strany serveru.		
	Úložiště data	Min. 6x 12 TB, NLSAS 12Gb, min. 7 200 ot/min		
	RAID hardware	SAS 12Gb, RAID 1,5,6, zálohovaná zapisovací cache min. 8 GB		
	LAN	2x 1GbE RJ-45 + 2x 10/25 GbE SFP28 1x 1Gb RJ-45 - samostatný port pro vzdálený management		
	USB	min. 2 USB konektory - min. 1x verze 3.0, min. min 1x na čelním panelu s podporou bootování		
	Management	Servisní modul s možností samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora HTTP/S, SSH, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace)		
	Napájení	2x napájecí zdroj min. 600 W, redundance		
	Souborový systém	XFS		

Zálohování				
	Protokoly	SMB/CIFS, SNMP, http/s a SSH (management)		
	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 systémem, podpora ukládání záloh, řízení jejich historie a řízení retenčních lhůt		
	Záruka	Záruka min. 60 měsíců Dostupnost podpory 24 hodin denně, 365 dní v roce Reakční doba do konce následujícího pracovního dne od nahlášení na linku podpory. Servis je poskytován přímo výrobcem hardware. Oprava v místě instalace hardware. Možnost automatického generování servisního incidentu přímo u výrobce hardware (zařízení musí být schopno automatizovaného předávání závad a otevírání servisních požadavků na helpdesk výrobce). Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty serveru. Podpora prostřednictvím Internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení bez nutnosti vytvoření uživatelského účtu pro danou činnost.		

Logování				
Část	Parametr	Popis povinného parametru	Účastník popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Účastník uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
	Základní funkce	Sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů		
	Protokoly sběru logů	syslog, TCP, UDP, HTTP, JSON		
	Sběr síťových toků	netflow kompatibilní dle nabízeného firewallu a centrálního přepínače		
	Zdroje logů	Min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a Netflow, ostatní aktivní prvky - syslog, SNMP trap, Office 365, Sysmon (windows)		
	Parsování logů	Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod.		
	Retence	Uchovávání logů 6 měsíců, automatická retence logů a indexů		
	Geolokace	Podpora automatického doplňování logů o informaci o lokalitě podle IP adresy		
	Normalizace logů	Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji		

Logování				
Logování 1ks	Rozšíření logů	Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem.		
	Bezpečnost	Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)		
	Výkon	500 EPS (event per second), 5000 FPM (flows per minute)		
	Dashboardy	Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)		
	Export dat	Export dat do csv - výsledky hledání		
	Kanály	Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.		
	Alerty, notifikace	Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílání upozornění		
	Active Directory	integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění administrator a operator		
	Vyhledávání	Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - výběrem v kontextovém menu vybraného pole uloženého záznamu.		
	Ovládání	Intuitivní grafické rozhraní		
	Kompatibilita	Podpora provozu v prostředí nabízené serverové virtualizace		
	Ukládání dat	do databáze, případná databázová licence je součástí dodávky		
	Výstupy	Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem		
	Integrace	Nástroj musí mít podporu pro integraci se sysmon a zpracování jeho dat, systém tím pádem umí hlídat spuštěné příkazy přes powershell, procesy, CMD atd.		
	Detekce zranitelností	Řešení umí získávat informace o nainstalovaném software + o nasazených KB a díky tomu provádět kontrolu vůči seznamu vydaných zranitelností.		
	Bezpečnostní funkce	Řešení skenuje monitorovaný systém a hledá malware, rootkity a neobvyklé chování		
	Záruka	Záruka na 60 měsíců včetně poskytnutí opravných verzí		

Licence				
Část	Parametr	Popis povinného parametru	Účastník popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Účastník uvede odkaz na příloženou část nabídky, kde je možné ověřit naplnění parametru
Licence	Zálohování	Licence typu předplatné, pro Veeam Backup&Replication pro min. 15ks virtuálních serverů a Veeam ONE na 1 rok		
	OS Windows	Licence OS Windows Server v nejnovější verzi pro min. 2 virtuální servery		
	SQL	Licence SQL v nejnovější verzi pro min. 25 současně pracujících uživatelů		
	RDS CAL	10 licencí typu USER		

9. Výkaz výměr – kabeláž - optický propoj, Wifi AP, archiv

P.č.	Název položky	MJ	množství
Díl:	Zednické práce		
1	Vybourání otvor. zed' cihel. 0,0225 m2, tl. 30cm, MVC	kus	9,00000
2	Vybourání otvor. zed'/strop železobeton	kus	3,00000
3	Zednické přípomoce a začištění - kabelová trasa	kpl	1,00000
Díl:	Komponenty		
4	Police 19" 500mm 40kg	ks	1,00000
5	19" osazený panel 24portů pro CAT6	ks	1,00000
6	19" Vyvazovací panel s oky 1-U	ks	1,00000
7	19" rozvaděč 6U, hloubka 600mm	ks	1,00000
8	Patch kabel CAT6a PVC 1m do racku	ks	6,00000
Díl:	Elektroinstalace		
9	Lišta elektroinstalační PVC š.do 40 mm, vč. montáže	m	70,00000
10	Lišta elektroinstalační PVC š.do 240 mm (optický kabel), vč. rohů a montáže	m	20,00000
	Montáž sdělovací a zabezp.tech		
11	Zakončení v optické vaně	kus	24,00000
12	Propojovací pole optických systému, 24 portů	kus	4,00000
13	Svar opt.vláknů vč.ochrany a pigtailu, první svar	kus	16,00000
14	Svar opt.vláknů vč.ochrany a pigtailu, další svar	kus	16,00000
15	Vyhotovení protokolu o měření optických kabelů	hod	2,00000
16	Měření optic.kabelů reflektometr.metoda, 1. měř.	kus	16,00000
17	Měření optic.kabel.reflektometr.metoda další měř.	kus	16,00000
18	Kabel optický 16 vláken, vč. uložení	m	60,00000
19	Demontáž a zpětná montáž zařízení v racku	kpl	1,00000
20	Datová dvojzásuvka, vč. keystone a montáže	kus	1,00000
21	Uložení kabelu Cat6 U-FTP, včetně dodávky kabelu a keystoneů	m	90,00000
22	Příslušenství ke strukturované kabeláži, měření	kpl	1,00000
Díl:	VRN		
23	Ostatní práce spojené se zprovozněním sítě	kus	1,00000

