Veřejná zakázka na dodávky

zadávaná v otevřeném řízení podle ustanovení § 3 písmeno b), § 14 odstavec (1), § 15 odstavec (1) a (2), § 25, § 56 souvisejících zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění platném ke dni zahájení tohoto zadávacího řízení (dále rovněž jen „Zákon“) s názvem:

„ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI VE FN BRNO – OPAKOVANÉ ZADÁVACÍ ŘÍZENÍ“

ve vztahu k Zákonu se jedná o veřejnou zakázku nadlimitní

NADLIMITNÍ REŽIM

OPAKOVANÉ OTEVŘENÉ ŘÍZENÍ

Veřejná zakázka bude realizována na základě podpory projektu s názvem „Zvýšení kybernetické bezpečnosti ve FN Brno“, registrační číslo projektu č. CZ.06.3.05/0.0/0.0/15_011/0006912 v rámci Integrovaného regionálního operačního programu, prioritní osy 3, specifického cíle 3.2, výzvy č. 10 – „Kybernetická bezpečnost“ a bude spolufinancována z prostředků EU v rámci IROP.

TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY

Obsah

1 Popis stávající infrastruktury

FN Brno je poskytovatelem základní služby, ve smyslu Zákona o kybernetické bezpečnosti. Do skupiny systémů základní služby spadají NIS, LIS, RIS, TIS, Farmis, MPI, EHR, PACS a další systémy s vysokou mírou důležitosti pro bezproblémové poskytování zdravotních služeb FN Brno. Tyto základní služby je třeba zajišťovat s vysokou dostupností pro koncového zákazníka (pacienta + zdravotnického pracovníka), což představuje mj. i potřebu zabezpečení vysoké robustnosti podpůrných aktiv a jejich způsobilost pro provoz 24x7x365. Současně je třeba dbát na fyzickou bezpečnost HW i SW komponent prostředí, resp. zabezpečovat odpovídající kontrolu pohybu osob, ochrany majetku a dat.

FN Brno poskytuje své služby ve třech areálech v Brně [Jihlavská 20 (PMDV); Černopolní 9 (PDM); Obilní trh 11 (PRM)] a dále na jednom samostatném pracovišti v Třebíči. Prvky perimetru zajišťující konektivitu do Internetu a Cisco wireless řadiče jsou umístěné v datových centrech v jednom z areálů; výpadek stávající MAN vede k nedostupnosti všech služeb ve zbývajících areálech.

V rámci jednotlivých areálů jsou vybudovány datové rozvody, které s ohledem na jejich stáří již zvolna přestávají vyhovovat požadavkům. Fyzická i morální životnost optických rozvodů je na hranici bezpečného provozu. Dochází k problémům s konektivitou na úrovni optických spojů a s ohledem na zastaralou technologii MM také k omezením kvality přenosu dat a výpadkům při dosažení hraničních vzdáleností u optických tras. Stávající MM optické rozvody znemožňují rozvoj navyšování propustnosti datové sítě. Optické trasy neposkytují redundanci distribučních bodů, což při výpadku znamená nedostupnost služeb ve velkém rozsahu areálů FN Brno.

Datové rozvaděče se nacházejí v prostorách dostupných veřejnosti často bez možnosti zabezpečeného přístupu do těchto rozvaděčů; racky jsou zabezpečené standardním mechanickým zámkem. Datové rozvaděče mají v současnosti omezenou kapacitu pro rozšíření (již není možné do současných racků vložit další prvky technologie), jsou bez zálohovaného napájení a dostatečného chlazení.

Síťová infrastruktura je založena na technologii Cisco. Používané přepínače Cisco Catalyst již dosahují konce své fyzické a morální životnosti. Většina těchto zařízení je již několik let provozována bez podpory výrobce nebo mají stanoven termín ukončení podpory výrobce v řádu měsíců. Dále je provozováno Cisco ISE v standalone řešení, které tak nezajišťuje redundanci pro plnohodnotné nasazení zabezpečení 802.1X na drátové i bezdrátové síti a aplikaci Identity PSK.

FN Brno provozuje cca 50 fyzických serverů (např. Fujitsu PRIMERGY RX2540 M2 (Horizon farma), HP ProLiant DL380p Gen8 (serverová farma), Fujitsu PRIMERGY RX2540 M1 (serverová farma), 3x HP ProLiant BL460c Gen8 (Blade chasis testovací farma), HP ProLiant BL460c Gen7 (Blade chasis testovací farma), které slouží převážně pro virtualizační platformu VMware vCloud Suite a poskytují prostředí pro provoz cca 420 virtuálních serverů.

Co se týče datového úložiště, FN Brno provozuje produkční diskové pole Netapp 8040 v stretched Metrocluster modu a jako zálohovací pole slouží Netapp 8020. Produkční pole je již na hraně nejen kapacitní, ale zejména v oblasti poskytovaných IOPS pro aktiva systémů Základních služeb. Je

žádoucí zajistit nové výkonné řadiče v Server Cluster módu s využitím stávajících polic a již pořízené diskové kapacity.

FN Brno na části infrastruktury provozuje hyperkonvergované úložiště tvořené VMware vSAN na úrovni virtuálních desktopů. Je žádoucí rozšířit tuto IOPS orientovanou diskovou kapacitu i do oblasti serverové farmy (pro výše uvedených 450 virtuálních serverů).

Data jsou zálohována prostřednictvím dosluhující velkokapacitní (150 TB) páskové jednotky IBM TS 3584 a nově prostřednictvím Veeam na výše uvedené diskové pole Netapp 8020. Část zálohovacího pole je vyčleněna jako certifikované dlouhodobé důvěryhodné úložiště.

FN Brno provozuje cca 3000 koncových stanic a cca 1200 virtuálních desktopů (VMware Horizon). PC stanice jsou převážně osazeny HW konfigurací CPU intel s benchmarking scórem 2149 bodů , 4 GB RAM, 320 GB HDD s Windows 7 Pro. Virtuální desktopy jsou využívány pro pružnou škálovatelnost výkonu a bezpečnost provozu.

Prostory FN Brno jsou pokryty signálem bezdrátové sítě (WiFi). Nároky na WiFi v posledním období významně narůstají. Díky intenzivnímu nasazování mobilních aplikací (mj. ošetřovatelská dokumentace, použití zdravotechnického přístroje na pacienta, monitoring životních funkcí pacienta, lokalizace pacientů a zdravotnické techniky) se začíná projevovat nedostatečné pokrytí WiFi signálem. S ohledem na jasný trend nárůstu poptávky po mobilním připojení zdravotechnických prostředků (jak v tradiční podobě, tak v podobě IoT zařízení) je žádoucí zvýšit počet přístupových bodů.

Pro správu a monitoring jsou využívány tyto nástroje: VMware vSphere, vRealize Operations Manager, NetApp Grafana, System Center Operations Manager (SCOM). Z pohledu zvýšení kybernetické bezopečnosti je žádoucí tyto systémy rozšířit a konsolidovat pro rychlou orientaci administrátorů a získat přehled možných detekcí problémů na jedno místo, pro co nejrychlejší a správnou reakci správců systémů.

Jako bezpečnostní prvek je nasazen Firewalll Forcepoint Sidewinder (McAfee Firewall Enterprise). Stávající appliance je ovšem již End-of-Life, tudíž na ni není možné dokoupit podporu, ale musel by se udělat kompletní upgrade zařízení. Proto je nutné řešit kompletní bezpečnostní politiku v oblasti Firewallu a zadávání pravidel dle ZKB.

Z pohledu problematiky zabezpečení vysoké dostupnosti služeb je třeba rovněž poukázat na vysokou latenci na infrastruktuře a limitovanou propustnost sítě, která zapříčiňuje dočasnou nedostupnost těchto služeb a nedostatečnou odezvu systémů. Centrální prvky jsou trvale přetížené a dochází již ke zpomalení, limitaci provozu a z hlediska bezpečnosti není v současnosti možné aplikovat pravidla pro filtrování nežádoucího provozu. Jsou evidovány rovněž relativně časté výpadky poskytovaných služeb zapříčiněné ztrátou napájení (pravidelné zkoušky záložních napájecích zdrojů) a tím pádem kolapsem napájecích zdrojů v DR u LAN prvků a technologií.

2 Požadavky na zpracování Cílového konceptu (Solution Design)

Zadavatel požaduje po dodavateli zpracování Cílového konceptu – dokumentu, který bude obsahovat časový plán prací a činností, které je nutné provést k úspěšné realizaci předmětu plnění této veřejné zakázky a věcný popis všech etap realizace a vzájemných závislostí a vazeb této veřejné zakázky. Vybraný účastník může zahájit realizaci ostatních etap této veřejné zakázky až po schválení Cílového konceptu zadavatelem.

Zadavatel požaduje po dodavateli vytvoření popisného dokumentu, který obsahuje min. tyto oblasti:

- Definice projektu (důvod realizace projektu, cíl projektu, výstupy a bezpečnostní požadavky),
- Návrh řešení (business architektura, aplikační a datová architektura, technologická architektura),
- Bezpečnost (identifikace business hrozeb, požadavky na dostupnost, důvěrnost a integritu, požadavky na logování, požadavky na detekci, prevenci a zvládání incidentů, požadavky na Hardening),
- Realizace a nastavení (aplikace, infrastruktura, licence),
- Testování a školení (nástroj pro řízení testování, testovací scénáře, školící prostředí, školení),
- Provoz systému (plán zálohování, plán dohledu, strategie obnovy, patchování, upgrade, aktualizace prostředí, neprodukční prostředí, servisní model),
- Řízení projektu (harmonogram realizace, analýza rizik projektu, součinnost, akceptační kritéria, otevřené body),
- Přílohy.

Uzná-li dodavatel za vhodné, může výše uvedenou oblast v popisném dokumentu označit jako – „nerelevantní“ a danou oblast v Cílovém konceptu nespecifikovat.

Harmonogram může být doplněn technickými a organizačními pomůckami, které usnadní jejich interpretaci koncovému uživateli.

Pozn. Vzor Cílového konceptu tvoří přílohu č. 2 této technické specifikace.

3 Vybudování nových síťových tras

Vybudování nových síťových tras bude zahrnovat:

a) instalaci a zprovoznění nových optických tras;

b) instalaci a zprovoznění nových metalických tras pro infrastrukturu bezdrátové sítě WiFi;

c) instalaci a zprovoznění rozvodů pro rozšíření kamerového systému[1];

a to vč. provedení nezbytných stavebních prací, v souladu s dokumentací pro provedení stavby „*Dokumentace datových rozvodů pro zvýšení kybernetické bezpečnosti*", která tvoří samostatnou přílohu Zadávací dokumentace v režimu důvěrných informací, a kterou obdrží účastník v souladu s pravidly definovanými v Zadávací dokumentaci.

Základní specifikace:

Trasy nových datových rozvodů budou vedeny uvnitř stávajících objektů, resp. stávajících podzemních kolektorů. Mimo trasy podzemních kolektorů budou rozvody vedeny v zemi. Pro tyto trasy bude třeba zajistit nezbytně nutné výkopy. Všechny nezbytné výkopové práce budou realizovány v ploše uzavřených areálů Fakultní nemocnice Brno. Všechny plánované práce jsou v souladu s územním plánováním města Brna. Navržené řešení musí být po technické stránce kompatibilní se stávajícím řešením využívaným ve FN Brno.

Požadavky na trasy vedené v zemi jsou následující:

- Rýhy pro nové rozvody budou šíře 800 mm a hloubky 1200 mm. V případě hloubky vyšší jak 1200 mm je nezbytně provést pažení rýhy. Výkopy rýh mohou být provedeny jak ručně, tak strojně. S ohledem na skutečnost, že se v areálu nachází mnoho podzemních sítí, se doporučuje provádět výkopy ručně.
- Před započetím výkopových prací je nezbytně nutné provést vytýčení všech stávajících podzemních sítí.
- Okraje výkopů křižující komunikace budou zabezpečeny proti pádu osob pochozí plochou a zábradlím minimální výšky 900 mm.
- Nová kabeláž slaboproudých rozvodů bude uložena do pískového lože tloušťky 80 mm a následně obsypána další vrstvou písku tloušťky 80 mm. Po provedení pískového obsypu bude rýha zasypána hutněnou zeminou z výkopu. Ve vrstvě cca 200 mm nad pískový obsyp bude nad trasou kabeláže položen výstražný pruh fólie.
- Finální zapravení rýhy bude dle místa, kde se rýha nachází – ohumusování, doplnění zámkové dlažby, doplnění skladby komunikace atd.

Požadavky na trasy vedené uvnitř stávajících objektů jsou následující:

[1] *dle kap. 6 tohoto dokumentu*

- Nové optické rozvody, rozvody wifi a rozvody pro kamerový systém budou umisťovány do prostor stávajících podhledů. Stávající podhledy jsou tvořeny kazetovými podhledy, kovovými lamelovými podhledy, SDK podhledy.
- Kazetové a lamelové podhledy budou rozebrány v nezbytně nutném rozsahu, kazety či lamely budou uschovány a po montáži rozvodů budou opět použity k osazení. V případě SDK podhledu bude provedeno odstranění SDK podhledových desek v nezbytně nutném rozsahu. Tento rozsah bude přesně určen během realizace prací.
- Po montáži rozvodů bude provedeno zpětné vyspravení podhledu s použitím SDK desek shodného typu a technických parametrů, jako je zbytek podhledu.
- V místech bez pohledů budou rozvody přisponkovány k pevnému stropu a zakryty krycími lištami.

Technické parametry optických rozvodů

Při návrhu a budování přenosových tras je vyžadován postup v souladu s technickými požadavky na přenosové technologie a trasy dle ČSN EN 50174 „Informační technologie". Předpokládá se nahrazení stávajících MM tras nově vytvořenými SM trasami. Nové SM trasy budou vedeny z Distribution DR do Access DR, dle PD. Konkrétní trasy optických kabelů, resp. rozmístění prvků je patrné ze zpracované výkresové dokumentace a jejich vzájemné propojení z blokových schémat.

Optická vlákna budou zavařena, nikoliv lepena. U všech optických rozvodů budou provedeny příslušné zkoušky, a rovněž odpovídající vyznačení tras v terénu. Na základě problematiky s umístěním optických van do datových rozvaděčů je třeba současně vyřešit přesun a doplnění části datových rozvaděčů.

S ohledem na požadavek jednotné identifikace klíčových technologických prvků a rozvodů, bude v rámci dodávky provedeno označení každého rozvaděče elektronickou kartou – RFI (bude poskytnuta databáze rozvaděčů s jednotnou identifikací, údaji a dokumenty, které jsou předmětem dodávky (manuály, revize, termíny, prohlídky a ostatní).

Co se týče technologie, předpokládá se využití samonosného optického kabelu DROP 09/125 G.657.A1 LSOH - J/A-N(ZN)H - 7A01 zafouknutého do mikro trubičky LSHF vnitřní tenkostěnné 10/8mm, pro indoor použití, vnitřní lubrikační vrstva SILICORE pro snížení tření, min. povolený poloměr ohybu 10cm, pro zafouknutí kabelů do průměru 6mm. Požadované vlastnosti optického kabelu jsou podrobně specifikovány ve zpracované PD.

Optické kabely v budovách budou uloženy dle norem částečně do PVC žlabů na omítce a v podhledech, částečně v kovových žlabech – rozvody na dlouhých chodbách. Rozvody na páteřní trase – po dlouhých chodbách - budou provedeny samostatně pro datové rozvody a pro silnoproudé rozvody. V případě nutnosti a při souběhu vedení u plastových žlabů se využije kovová stínící vložka do plastového žlabu

Optické kabely budou ukončeny v příslušných datových rozvaděčích, dle projektové dokumentace. V rámci akce se neplánuje optický kabel spojkovat; bude zatažen do mikro trubiček v celém úseku bez přerušení. Parametry svárů jsou definovány v PD

Součástí zprovoznění bude rovněž provedení měření, dle PD, a dále zkušební provoz (po provedení výchozí revize) po dobu min. 14 dní.

Technické parametry rozvodů pro WiFi

Navržené řešení musí být koncipováno s ohledem na kompatibilitu a jednotnou správu s již instalovaným stávajícím systémem. Pro vlastní rozšíření bezdrátové sítě, je tedy nutné zvolit stejné technologie, jiné technologie nebudou kompatibilní se stávající strukturou.

Požadované pokrytí je specifikováno ve dvou technologických rovinách. Pokrytí signálem pro účely běžné datové komunikace WiFi terminálů a pokrytí signálem a dostatečný počet AP pro případné nasazení VoIP služeb a RTLS lokalizačních služeb. Rozmístění prvků je v rámci PD určeno s velkou mírou přesnosti dle měření a studií 802.11 a/b/g/n WiFi Site Survey, studie proveditelnosti nasazení centrálně řízené WiFi sítě v areálech FN Brno – Jihlavská, Obilní trh a Černopolní, které poskytuje dostatečné podklady pro návrh RTLS topologie z výsledného modelu radiové prostupnosti stavby.

Předpokládá se, že řešení naváže na již používané a osvědčené technologie s jednotným managementem. Celá síť bude centrálně řízená. Pro všechna nová přípojná místa bude použito shodné přenosové médium – metalický kabel CAT6a LSOH. Kabely budou zakončeny v datových rozváděčích do modulárních CAT6a patch panelů. Fyzické přepojování umožňují patch panely v datových rozváděčích pomocí propojovacích patch kabelů. Celé řešení bude dimenzováno s určitou rezervou pro snadný rozvoj a možnost změn v konfiguraci jak kabeláže, tak i aktivních a wireless prvků.

Konkrétní rozmístění požadovaných prvků je patrné z výkresové dokumentace a jejich vzájemné propojení z blokových schémat. Wifi access pointy budou provozovány v nepřetržitém provozu[2].

Součástí dodávky bude rovněž odpovídající množství propojovacích kabelů pro požadovaná zapojení jednotlivých zásuvek v datových rozvaděčích a ze zásuvek do wifi přístupových bodů, dle PD.

Součástí zprovoznění bude rovněž provedení měření, dle PD, a dále zkušební provoz (po provedení výchozí revize) po dobu min. 14 dní. Měření musí splnit požadavky pro standard Ethernet při rychlosti 10 Gbits .

Organizační zabezpečení:

S ohledem na skutečnost, že se jedná o instalaci v rozsáhlém areálu s velkým počtem pohybujících se externích osob a personálu, bude nutné zajistit odpovídající organizační zajištění ve spolupráci s investorem a koordinaci s dalšími aktivitami, které mohou probíhat v místě plnění. Samozřejmostí je rovněž zabezpečení bezpečnosti a ochrany zdraví

[2] *Požadovaný počet a konkrétní tech. parametry pro WiFi access pointy jsou specifikovány v kap. 4.8*

4 Rozšíření síťové infrastruktury

4.1 Kontroler pro PDM a záložní kontroler pro PDM

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní** účastník **dle nabízeného o zařízení**
Kontrolery bezdrátové sítě – dvojice (1ks primární - Kontroler pro PDM a 1ks redundantní - Záložní kontroler pro PDM) zařízení pro doplnění Mobility domény stávajících kontrolerů CT5520 provozovaných Zadavatelem	ANO	
Minimální počet 10G SFP portů per kontroler s aktivními 10m Twinax kabely pro všechny porty součástí dodávky	2	
Redundantní napájecí zdroj součástí dodávky	ANO	
Minimální propustnost pro data Gb/s	20 Gb/s	
Licence dle počtu nově pořizovaných AP, možnost upgradu až na 1500 registrovaných AP	ANO	
Možnost přenosu licencí mezi nově pořizovaným a stávajícím párem kontrolerů Zadavatele	ANO	
Podpora stávajících AP řady CAP1702I, které má Zadavatel nasazeny ve své infrastruktuře, a nově pořizovaných AP	ANO	
Redundance na úrovni kontrolerů a jejich portů, výpadek aktivního kontroleru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace)	ANO	
Možnost postupného upgradu dvojice nově pořizovaných a stávajících kontrolerů, možnost přesunu všech či libovolné části současných i nově pořizovaných AP Zadavatele mezi dvojicemi kontrolerů z důvodu zkrácení doby výpadku při upgradu SW kontrolerů a AP	ANO	
Lokální síť - možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost	ANO	
Mesh síť - podpora indoor a outdoor mesh sítí, současné připojení normálních a mesh AP k jednomu kontroleru	ANO	
Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP	ANO	
Šifrovaná řídící komunikace AP-kontroler	ANO	
Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů	ANO	
Bezpečnost a Guest Access		
Kontrolery musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
802.1x/EAP autentizace: PEAP, EAP-FAST, EAP-TLS, ...	ANO	
PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID	ANO	
Možnost autentizace nových klientů k AP v módu lokálního bridgování dat pomocí 802.1x/EAP i v případě výpadku centrálního kontroleru	ANO	
Podpora standardu „802.11w" pro ochranu řídících rámců na AP a klientovi	ANO	
Podpora standardu „802.11u" pro výběr SSID a autentizaci klienta	ANO	
Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP	ANO	
Integrovaná správa návštěvnických účtů s možností definice jejich platnosti	ANO	
Možnost omezit počet klientů per SSID	ANO	
Lokální profilování zařízení – per uživatel a per zařízení	ANO	
Integrovaný IDS systém pro detekci útoků na bezdrátovou síť (wireless IDS), detekce cizích AP (Rogue AP) a klientů v AdHoc režimu, možnost vynuceného odpojení klientů od cizích AP	ANO	
Podpora plného NetFlow v9 (RFC 3954) exportu záznamů o datových tocích uživatelů (vč. zdrojové a cílové IP adresy, portů, WLAN ID, počtu paketů a objemu přenesených dat) směrem k externímu kolektoru	ANO	
Rychlý roaming	ANO	
Automatizované řešení roamingu uživatelů v rámci AP připojených na nově pořizovaný i stávající pár kontrolerů Zadavatele , L2/L3	ANO	
Podpora standardu „802.11r" pro rychlý roaming klientů mezi AP, možnost selektivního využití 802.11r na sdíleném SSID pouze pro zařízení, které tento standard podporují	ANO	
Podpora standardu „802.11k" pro optimalizaci roamingu	ANO	
Podpora standardu „802.11v" pro optimalizaci připojení klienta	ANO	
QoS a řízení provozu v bezdrátové síti		
Podpora 802.11e/WMM	ANO	
Diferenciace úrovní QoS pro různé služby a skupiny uživatelů (zaměstnance a návštěvníky), možnost obousměrného omezení propustnosti per klient, možnost nastavit konkrétní QoS profil na Apple klientech přímo z kontroleru	ANO	
Mechanismy řízení přístupu (Call Admission Control) pro hasový i video provoz. Konfigurovatelné parametry max. zátěže a šířky pásma.	ANO	
Podpora Video-streamingu se spolehlivým multicastem	ANO	
Optimalizace multicast provozu v bezdrátové síti (IGMP snooping)	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
Aplikační inspekce přenášeného provozu (DPI na 7. vrstvě ISO/OSI na základě aplikačních signatur) umožňující rozpoznání jednotlivých aplikací, grafické zobrazení statistik a možnost řízení QoS per rozpoznaná aplikace	ANO	
Podpora Apple Bojour protokolu, zpracování mDNS paketů, možnost filtrování služeb mezi subnety	ANO	
Správa frekvenčního pásma		
Automatizovaná centrální správa frekvenčního pásma, spolupráce RRM mezi kontrolery nově pořizovaného i stávajícího páru kontrolerů Zadavatele	ANO	
Monitoring rádiového spektra vč. 20/40/80/160 MHz kanálů, možnost okamžité automatické centralizovaně řízené reakce (změna kanálu nebo jeho šířky, změna vysílacího výkonu), grafické vyobrazení informací o kvalitě signálu	ANO	
Automatické zvýšení vysílacího výkonu okolních AP při výpadku AP („self healing“)	ANO	
Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur	ANO	
Mesh síť – automatický výběr vhodného kanálu pro backhaul, automatické sestavení optimálního mesh stromu, monitorování všech kanálů na pozadí s rychlou konvergencí v případě výpadku primárního nadřazeného AP	ANO	
Troubleshooting radiového signálu a automatické řešení problému rušivého signálu, generování alarmů na základě překročení prahových hodnot kvality signálu	ANO	
Možnost členění AP do skupin, konfigurace AP podle příslušnosti do skupiny	ANO	
Možnost vytváření rádiových profilů (nastavení kanálů, rychlostí)	ANO	
Nastavení různého rádiového profilu pro různé skupiny AP	ANO	
Podpora IPv6		
Podpora IPv6 – management kontroleru (vč. Syslog, radius)	ANO	
Podpora IPv6 – komunikace AP-kontroler	ANO	
Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty	ANO	
Podpora IPv6 – IPv6 multicast, MLD snooping	ANO	
Podpora IPv6 – bezpečnost (RAGuard, IPv6 Source Guard, DHCPv6 Server Guard, ACL)	ANO	
Podpora IPv6 – video-streaming se spolehlivým multicastem	ANO	
Podpora IPv6 – ND cache na kontroleru, optimalizace přenosu ND zpráv, rate-limiting pro RA	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/ vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
Dohled a správa kontroleru		
Centrální administrace správců s granularitou přístupových práv	ANO	
Podpora správy přes serial CLI nebo přes IPv4 a IPv6 pomocí SSH/telnet, http a https web GUI, SNMP, aplikace pro dohled pro Android a Apple mobilní platformy	ANO	
RJ45 konzolový port a/nebo USB konzolový port	ANO	

4.2 Jednotný management pro LAN a Wifi Infrastrukturu

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník**dle nabízeného zařízení**
Jednotný WLAN + LAN management	ANO	
Existující formát zařízení	Virtuální server pro prostředí VMware	
Rozšiřující licence do existujícího systému Prime Infrastructure dle počtu a typu poptávaných aktivních prvků + rozšiřující licence pro v současné době požívaných 68ks switchů řady Catalyst 2960X,	ANO	
Možnost navýšení počtu spravovaných zařízení formou dokoupení licence	ANO	
Kompletní správa životního cyklu infrastruktury (nasazení, administrace, monitoring, odstraňování problémů)	ANO	
Grafické web rozhraní pro správu	ANO	
Přístup ke GUI i pomocí aplikace pro mobilní zařízení	ANO	
Nástroje monitorování, monitorování v reálném čase a odstraňování problémů	ANO	
Automatická archivace konfigurací, porovnávání konfigurací, porovnávání konfigurací vůči šablonám	ANO	
Konfigurační šablony dle "best practice" a designových příruček	ANO	
Inventarizace nasazeného HW v síti	ANO	
Inventarizace, nasazení, správa firmware do síťových zařízení	ANO	
Monitorování výskytu koncových zařízení, IP telefonů a uživatelů v síti	ANO	
Generování reportů bezpečnostních problémů infrastruktury	ANO	
Zobrazení L2, L3 topologické mapy	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník**dle nabízeného zařízení**
Kompletní správa životního cyklu bezdrátové sítě (plánování, nasazení, monitoring, troubleshooting, reporting)	ANO	
Monitoring připojení koncových zařízení napříč pevnou i bezdrátovou sítí	ANO	
Monitoring IPv6 připojení koncových zařízení napříč pevnou i bezdrátovou sítí	ANO	
Integrace se znalostní bází výrobce pro usnadnění řešení problémů a správy	ANO	
Podpora API pro programatický přístup do databází aplikace správy	ANO	
Hierarchické mapy zobrazující umístění AP, šíření signálu a podporou zobrazení aktuální pozice wifi klientů (notebooků, PDA, WiFi telefonů, WiFi RFID tagů apod.)	ANO	
Centrální konfigurace bezdrátových sítí včetně bezpečnostních politik, QoS profilů	ANO	
Nástroje pro detekci a řešení problémů v bezdrátové síti (grafy obsazenosti kanálů, grafy odpovídající provozu klientů, atd.)	ANO	
Nástroje pro plánování WLAN sítě	ANO	
Nástroje pro plánování, nasazení, monitorování a optimalizaci hlasových služeb do bezdrátové sítě	ANO	
Podpora SNMPv1, SNMPv2, SNMPv3	ANO	
Podpora autorizace a autentizace vůči TACACS+	ANO	
Technologický dashboard pro zobrazování výsledků měření kvality signálu bezdrátové sítě	ANO	
Zobrazování současných i historických hodnot a trendu kvality signálu bezdrátové sítě	ANO	
Zobrazování alarmů týkajících se kvality signálu	ANO	
Možnost pokročilého vyhledávání zdrojů interference v bezdrátové síti	ANO	
Nástroj pro troubleshooting klientů s funkcí identifikace zdrojů interference, které ovlivňují klienty	ANO	
Integrovaný nástroj pro sběr diagnostických dat o kontrolerech a AP v bezdrátové síti	ANO	
Automatické dohledání portu pevné sítě s připojeným falešným Access Pointem	ANO	
Komplexní zobrazení veškerých relevantních údajů pro jednotlivé zařízení a jednotlivého uživatele v souhrnném pohledu (kontextově) pro rychlejší troubleshooting	ANO	

4.3 Core switche v DC

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
HW specifikace		
Počet	2ks	
Typ hardwarového přepínače	L3 přepínač	
Formát přepínače	Modulární	
Velikost přepínače maximálně (RU)	10	
Minimální počet slotů v šasi	7	
Orientace slotů v šasi	horizontální	
Celková minimální propustnost přepínacího subsystému	6 Tb/s	
Minimální kapacita interní sběrnice na 1 slot přepínače	440 Gb/s	
Minimální počet 128 000 záznamů v MAC adresní tabulce	ANO	
Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	256000	
Minimální počet záznamů ve směrovací tabulce – IPv6 unicast	128000	
Minimální počet aktivních VLAN	4000	
Řídící modul s integrovanými rozhraními 10GE	ANO	
Řídící modul s integrovanými rozhraními 40GE	ANO	
Redundantní řídící modul	ANO	
Neměnná propustnost i při výpadku redundantního řídícího modulu	ANO	
Přepínač musí být schopen vytvořit s již v síti provozovaným přepínačem Catalyst 6807-XL s řídícím modulem Supervisor-6T dvojici takovým způsobem, že dohromady budou vystupovat jako jedna logická entita v L2 i L3 síťových protokolech	ANO	
Napájecí zdroj, max. dosažitelný výkon	ANO, alespoň 2500W	
Interní redundantní napájecí zdroje, max, dosažitelný výkon	ANO, alespoň 2500W	
Celkový počet napájecích zdrojů pro N+1 redundanci	4	
Minimální počet 10GE SFP+ portů s volitelným fyzickým rozhraním s lokálním přepínáním	48	
Standard 802.1ae na 10GE portech s volitelným fyzickým rozhraním	ANO	
Minimální počet 40Gbit/s portů s volitelným fyzickým rozhraním	28	
Standard 802.1ae na 40Gbit/s portech s volitelným fyzickým rozhraním	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
Povýšitelnost 10Gbit/s portů na 40Gbit/s porty (externím kabelem)	ANO	
Linkové karty musí být funkční i v již provozovaných přepínačích Catalyst 6807-XL s řídícím modulem Supervisor-6T	ANO	
Funkční specifikace		
Virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního šasi (jediná entita z pohledu L2 i L3 protokolů)	ANO	
Ochranné mechanismy rozpadnutí virtuálního šasi bez nutnosti využití dodatečných zařízení	ANO	
Stavové přepnutí mezi řídicími moduly v jednom fyzickém šasi (ekvivalent funkce Statefull Switchover/SSO)	ANO	
Stavové přepnutí mezi řídícími moduly v logickém šasi (ekvivalent funkce Statefull Switchover/SSO mezi fyzickými šasi)	ANO	
Prvek tvoří součást architektury, která zajistí velkou a funkční L2 doménu rozprostřenu libovolně kdekoli po celé LAN síti	ANO	
Prvek tvoří součást architektury, která zajistí IP subnet rozprostřený libovolně po celé síti	ANO	
Směrování protokolů IPv4 a IPv6 v hardware (duální podpora IPv4 a IPv6, tedy možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, *dual-stack*)	ANO	
HW podpora MPLS a VPLS	ANO	
Tunelovací protokoly (např. GRE) v hardware	ANO	
Překlad adres/NAT v hardware	ANO	
IEEE 802.3ad	ANO	
IEEE 802.3ad přes více modulů	ANO	
IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)	ANO	
IEEE 802.1Q	ANO	
IEEE 802.1ak	ANO	
tunelování 802.1Q v 802.1Q	ANO	
IEEE 802.1s - multiple spanning trees	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
IEEE 802.1p	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“	ANO	
Detekce jednosměrnosti optické linky (např. UDLD)	ANO	
QoS classification – dle ACL, IP Prec, DSCP, CoS	ANO	
QoS marking –dle IP Prec, DSCP, CoS	ANO	
QoS Policing	ANO	
Policing i na hodnotu agregovANOu ze všech karet s lokálním přepínáním	ANO	
Policing per-flow (např. microflow policing nebo funkčně ekvivalentní)	ANO	
Konfigurovatelné HW prostředky ochrany CPU před útoky typu DoS	ANO	
Hardwarová filtrace (access list) na fyzickém i logickém L2 i L3 rozhraní	ANO	
Hardwarová filtrace (access list) dle L2, L3 i L4 informací	ANO	
Provádění dílčích změn v access listu nemá vliv na filtraci datových toků neměněnou částí access listu	ANO, povýšením SW	
Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)	ANO	
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ANO	
Propagace bezpečnostní role uživatele nebo koncového zařízení pro každý datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní)	ANO	
Zabezpečení a analýza DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní)	ANO	
Ochrana ARP protokolu (např. Dynamic ARP Inspection, DAI nebo funkčně ekvivalentní)	ANO	
Ochrana podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
Switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
MPLS směrování	ANO, povýšením SW	
VPLS směrování	ANO, povýšením SW	
BGPv4, MP-BGP	ANO	
OSPFv2, OSPFv3	ANO	
OSPF s MD5 a NSSA	ANO	
RIPv2, RIPng	ANO	
IS-IS pro IPv4 a IPv6	ANO	
Router Redundancy protokol pro IPv4 (např. VRRP, HSRP)	ANO	
Policy-based routing podle ACL	ANO	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO	
PIM-SM (Protocol Independent Multicast, sparse mód)	ANO	
PIM SSM (PIM Source Specific Multicast)	ANO	
Bidirectional Protocol Independent Multicast (RFC 5015)	ANO	
IGMPv2, IGMPv3	ANO	
Antispoofingová kontrola ekvivalentní funkci RPFC, *reverse path forwarding check* dle RFC3704 a RFC3178 pro IPv4 i IPv6	ANO	
Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830)	ANO, povýšením SW	
IPv6 services (HTTP, DNS, SSH, ACL, ICMP, DHCP)	ANO	
Router Redundancy protokol pro IPv6 (např. VRRP, HSRP)	ANO	
IPv6 First Hop Security (IPv6 Port ACL, RA guard, Secure Neighbor Discovery)	ANO	
IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)	ANO	
IPv6 over GRE v hardware	ANO	
ISATAP v hardware	ANO	
IPv6 QoS	ANO	
Vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače/směrovače pro tvorbu VPN (podpora virtualizace směrovacích tabulek - např. funkční ekvivalent Virtual Routing and Forwarding/Multi-VRF)	ANO	
Protokoly a služby per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO	
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) a Flexible NetFlow (nebo funkčně ekvivalentní) pro IPv4 i IPv6	ANO	
NetFlow na vstupu i výstupu	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ANO	
Statistiky určovány z každého paketu daného "flow"	ANO	
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ANO	
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"	ANO	
Zobrazení sbíraných infromací o "flow" přímo v přepínači. I včetně "TopN" pohledu.	ANO	
Export statistik "flow" selektivně na více kolektorů	ANO	
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	
Konfigurovatelná autodiagnostika při startu i za provozu zařízení	ANO	
Nástroj měření odezev sítě (např. IP SLA) pro IPv4 i IPv6	ANO, povýšením SW	
Měření a ovládání spotřeby energie k LAN připojených koncových zařízení	ANO	
Textové řádkově orientované/CLI konfigurační rozhraní	ANO	
Konfigurace zařízení v člověku čitelné textové formě	ANO	
Povýšování operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ANO	
Nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ANO	
Přepínač může sloužit pro automatickou zálohu a obnovu firmware včetně konfigurace pro podřízený/é přepínač/e	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ANO	
Sériová konzolová linka	ANO	
SSHv2	ANO	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO	
Synchronizace času protokolem NTPv3 (klient i server)	ANO	
SNMPv2	ANO	
SNMPv3	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní** účastník **dle nabízeného zařízení**
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
TACACS+ klient	ANO	
Zrcadlení portů (funkční ekvivalent SPAN)	ANO	
Vzdálené zrcadlení portů (funkční ekvivalent RSPAN)	ANO	
Pokročilé interní nástroje pro ladění/debugging procházejícího provozu	ANO	
Syslog	ANO	

4.4 Rozšíření DC LAN

4.4.1 Vzdálené distribuované optické linkové karty/moduly

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Distribuované rozšiřující moduly (virtuální vzdálené rozšiřujících moduly umístěné v jiném fyzickém šasi) k používané řadě DC switchů Nexus 9300	ANO	
Počet požadovaných virtuálních vzdálených rozšiřujících modulů	4ks	
Formát požadovaného virtuálního vzdáleného rozšiřujícího modulu - osaditelný do rackové skříně, maximální velkost 1RU	ANO	
Počty a typy portů virtuálního vzdáleného modulu	48x1/10GE SFP+ 6x40G QSFP	
Licence pro DC management nástroj pro 4ks používaných switchů Nexus 9300	ANO	

4.4.2 Víceúčelové switche do DC

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Počet	4ks	
Typ přepínače	L2/L3 přepínač	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Formát přepínače	Stohovatelný	
Počet dedikovaných stohovacích portů	2	
Minimální počet zařízení ve stohu	8	
Minimální kapacita sběrnice stohu	400 Gb/s	
Sdílení výkonu napájecích zdrojů napříč celým stohem	ANO	
Stateful Switch Over v rámci stohu	ANO	
Non-stop Forwarding	ANO, povýšením firmware	
Možnost instalovat interní redundantní napájecí zdroj	ANO	
Interní redundantní napájecí zdroj požadován	ANO	
Datový stohovací kabel požadován	ANO	
Napájecí stohovací kabel požadován	ANO	
Počet portů 10/100/1000 Base-TX s PoE napájením	48	
Minimální PoE budget	1000W	
Uplink porty	8x10GE SFP+	
Min. velikost sdíleného systémového bufferu	16MB	
Velikost MAC address tabulky	30000	
Min. počet IPv4 routes	600	
Min. počet IPv6 routes	300	
Min. počet konfigurovatelných security ACL	5000	
IEEE 802.3ad (Link Aggregation)	ANO	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků	128	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
Provoz 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, povýšením firmware	
ISIS	ANO, povýšením firmware	
BGPv4	ANO, povýšením firmware	
Graceful Insertion and Removal	ANO, povýšením firmware	
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, povýšením firmware	
MPLS VPN	ANO, povýšením firmware	
MPLS VPN - 6VPE	ANO, povýšením firmware	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO, povýšením firmware	
Reverse path check (uRPF) pro IPv4 i IPv6	ANO, povýšením firmware	
IGMPv2, IGMPv3	ANO	
IGMP snooping	ANO	
MLD snooping	ANO	
DHCP relay	ANO	
Minimální počet HW QoS front	8	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
QoS - Strict Priority Queue	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
QoS-Per Flow policing	ANO	
QoS-Hierarchical QoS	ANO, min. 2 úrovně	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	
IPv6 QoS	ANO	
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	
IPv6 Port ACL, VLAN ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
PACL, VACL	ANO	
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	
IEEE 802.1ae na uplink portech	ANO	
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO, povýšením firmware	
Switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	
IEEE 802.3af	ANO	
IEEE 802.3at	ANO	
IEEE 802.3az	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Multicast DNS (mDNS) gateway	ANO, povýšením firmware	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO, povýšením firmware	
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ANO, povýšením firmware	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	
Python scripting	ANO	
Linux shell	ANO	
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	
Application hosting	ANO, povýšením firmware	
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO, povýšením firmware	
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	
SNMPv2/v3	ANO	
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	
Podpora network boot (iPXE) pres IPv4 i IPv6	ANO	
Inventarizovatelnost komponent integrovANOu RFID identifikací	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
Vzdálený port mirroring (ERSPAN)	ANO, povýšením firmware	
NTPv3 server	ANO	

4.5 Distribuční switche ve všech areálech

4.5.1 Obecné minimální požadavky pro všechny typy distribučních switchů v lokalitách Bohunice L04, Bohunice Z01a a Dětská F02 + G01a

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
HW specifikace		
Typ hardwarového přepínače	L3 přepínač	
Formát přepínače	Modulární	
Velikost přepínače maximálně (RU)	10	
Minimální počet slotů v šasi	7	
Orientace slotů v šasi	horizontální	
Celková minimální propustnost přepínacího subsystému	6 Tb/s	
Minimální kapacita interní sběrnice na 1 slot přepínače	440 Gb/s	
Minimální počet 128 000 záznamů v MAC adresní tabulce	ANO	
Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	256000	
Minimální počet záznamů ve směrovací tabulce – IPv6 unicast	128000	
Minimální počet aktivních VLAN	4000	
Řídící modul s integrovanými rozhraními 10GE	ANO	
Řídící modul s integrovanými rozhraními 40GE	ANO	
Redundantní řídící modul	ANO	
Neměnná propustnost i při výpadku redundantního řídícího modulu	ANO	
Přepínač musí být schopen vytvořit s již v síti provozovaným přepínačem Catalyst 6807-XL s řídícím modulem Supervisor-6T dvojici takovým způsobem, že dohromady budou vystupovat jako jedna logická entita v L2 i L3 síťových protokolech	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Napájecí zdroj, max. dosažitelný výkon	ANO, alespoň 2500W	
Interní redundantní napájecí zdroje, max, dosažitelný výkon	ANO, alespoň 2500W	
Celkový počet napájecích zdrojů pro N+1 redundanci	3	
Standard 802.1ae na 10GE portech s volitelným fyzickým rozhraním	ANO	
Minimální počet 40Gbit/s portů s volitelným fyzickým rozhraním	4	
Standard 802.1ae na 40Gbit/s portech s volitelným fyzickým rozhraním	ANO	
Povýšitelnost 10Gbit/s portů na 40Gbit/s porty (externím kabelem)	ANO	
Linkové karty musí být funkční i v již provozovaných přepínačích Catalyst 6807-XL s řídícím modulem Supervisor-6T	ANO	
Funkční specifikace		
Virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního šasi (jediná entita z pohledu L2 i L3 protokolů)	ANO	
Ochranné mechanismy rozpadnutí virtuálního šasi bez nutnosti využití dodatečných zařízení	ANO	
Stavové přepnutí mezi řídicími moduly v jednom fyzickém šasi (ekvivalent funkce Statefull Switchover/SSO)	ANO	
Stavové přepnutí mezi řídícími moduly v logickém šasi (ekvivalent funkce Statefull Switchover/SSO mezi fyzickými šasi)	ANO	
Prvek tvoří součást architektury, která zajistí velkou a funkční L2 doménu rozprostřenu libovolně kdekoli po celé LAN síti	ANO	
Prvek tvoří součást architektury, která zajistí IP subnet rozprostřený libovolně po celé síti	ANO	
Směrování protokolů IPv4 a IPv6 v hardware (duální podpora IPv4 a IPv6, tedy možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, *dual-stack*)	ANO	
HW podpora MPLS a VPLS	ANO	
Tunelovací protokoly (např. GRE) v hardware	ANO	
Překlad adres/NAT v hardware	ANO	
IEEE 802.3ad	ANO	
IEEE 802.3ad přes více modulů	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)	ANO	
IEEE 802.1Q	ANO	
IEEE 802.1ak	ANO	
tunelování 802.1Q v 802.1Q	ANO	
IEEE 802.1s - multiple spanning trees	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
IEEE 802.1p	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“	ANO	
Detekce jednosměrnosti optické linky (např. UDLD)	ANO	
QoS classification – dle ACL, IP Prec, DSCP, CoS	ANO	
QoS marking –dle IP Prec, DSCP, CoS	ANO	
QoS Policing	ANO	
Policing i na hodnotu agregovANOu ze všech karet s lokálním přepínáním	ANO	
Policing per-flow (např. microflow policing nebo funkčně ekvivalentní)	ANO	
Konfigurovatelné HW prostředky ochrany CPU před útoky typu DoS	ANO	
Hardwarová filtrace (access list) na fyzickém i logickém L2 i L3 rozhraní	ANO	
Hardwarová filtrace (access list) dle L2, L3 i L4 informací	ANO	
Provádění dílčích změn v access listu nemá vliv na filtraci datových toků neměněnou částí access listu	ANO, povýšením SW	
Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)	ANO	
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ANO	
Propagace bezpečnostní role uživatele nebo koncového zařízení pro každý datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní)	ANO	
Zabezpečení a analýza DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní)	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Ochrana ARP protokolu (např. Dynamic ARP Inspection, DAI nebo funkčně ekvivalentní)	ANO	
Ochrana podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
Switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
MPLS směrování	ANO, povýšením SW	
VPLS směrování	ANO, povýšením SW	
BGPv4, MP-BGP	ANO	
OSPFv2, OSPFv3	ANO	
OSPF s MD5 a NSSA	ANO	
RIPv2, RIPng	ANO	
IS-IS pro IPv4 a IPv6	ANO	
Router Redundancy protokol pro IPv4 (např. VRRP, HSRP)	ANO	
Policy-based routing podle ACL	ANO	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO	
PIM-SM (Protocol Independent Multicast, sparse mód)	ANO	
PIM SSM (PIM Source Specific Multicast)	ANO	
Bidirectional Protocol Independent Multicast (RFC 5015)	ANO	
IGMPv2, IGMPv3	ANO	
Antispoofingová kontrola ekvivalentní funkci RPFC, *reverse path forwarding check* dle RFC3704 a RFC3178 pro IPv4 i IPv6	ANO	
Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830)	ANO, povýšením SW	
IPv6 services (HTTP, DNS, SSH, ACL, ICMP, DHCP)	ANO	
Router Redundancy protokol pro IPv6 (např. VRRP, HSRP)	ANO	
IPv6 First Hop Security (IPv6 Port ACL, RA guard, Secure Neighbor Discovery)	ANO	
IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)	ANO	
IPv6 over GRE v hardware	ANO	
ISATAP v hardware	ANO	
IPv6 QoS	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače/směrovače pro tvorbu VPN (podpora virtualizace směrovacích tabulek - např. funkční ekvivalent Virtual Routing and Forwarding/Multi-VRF)	ANO	
Protokoly a služby per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO	
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) a Flexible NetFlow (nebo funkčně ekvivalentní) pro IPv4 i IPv6	ANO	
NetFlow na vstupu i výstupu	ANO	
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ANO	
Statistiky určovány z každého paketu daného "flow"	ANO	
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ANO	
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"	ANO	
Zobrazení sbíraných infromací o "flow" přímo v přepínači. I včetně "TopN" pohledu.	ANO	
Export statistik "flow" selektivně na více kolektorů	ANO	
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	
Konfigurovatelná autodiagnostika při startu i za provozu zařízení	ANO	
Nástroj měření odezev sítě (např. IP SLA) pro IPv4 i IPv6	ANO, povýšením SW	
Měření a ovládání spotřeby energie k LAN připojených koncových zařízení	ANO	
Textové řádkově orientované/CLI konfigurační rozhraní	ANO	
Konfigurace zařízení v člověku čitelné textové formě	ANO	
Povýšování operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ANO	
Nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ANO	
Přepínač může sloužit pro automatickou zálohu a obnovu firmware včetně konfigurace pro podřízený/é přepínač/e	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ANO	
Sériová konzolová linka	ANO	
SSHv2	ANO	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO	
Synchronizace času protokolem NTPv3 (klient i server)	ANO	
SNMPv2	ANO	
SNMPv3	ANO	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
TACACS+ klient	ANO	
Zrcadlení portů (funkční ekvivalent SPAN)	ANO	
Vzdálené zrcadlení portů (funkční ekvivalent RSPAN)	ANO	
Pokročilé interní nástroje pro ladění/debugging procházejícího provozu	ANO	
Syslog	ANO	

4.5.2 Specifické minimální požadavky pro distribučních switche v lokalitě Bohunice L04

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Počet	1ks	
Minimální počet 10GE SFP+ portů s volitelným fyzickým rozhraním s lokálním přepínáním	176	

4.5.3 Specifické minimální požadavky pro distribučních switche v lokalitě Bohunice Z01a

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Počet	1ks	

Minimální počet 10GE SFP+ portů s volitelným fyzickým rozhraním s lokálním přepínáním	144	

4.5.4 Specifické minimální požadavky pro distribučních switche v lokalitě Dětská F02 + G01a

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Počet	2ks	
Minimální počet 10GE SFP+ portů s volitelným fyzickým rozhraním s lokálním přepínáním	80	

4.5.5 Distribuce - Lokalita Bohunice D00

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
HW specifikace		
Počet	2ks	
Typ hardwarového přepínače	L3 zařízení	
Formát přepínače	fixní konfigurace	
Velikost přepínače maximálně (RU)	2	
Celková minimální propustnost přepínacího subsystému	950 Gb/s	
Minimální počet 128 000 záznamů v MAC adresní tabulce	ANO	
Minimální počet záznamů ve směrovací tabulce - IPv4 unicast	256000	
Minimální počet záznamů ve směrovací tabulce – IPv6 unicast	128000	
Minimální počet aktivních VLAN	4000	
Interní redundantní napájecí zdroj	ANO	
Minimální počet 10GE portů s volitelným fyzickým rozhraním s lokálním přepínáním	40	
Standard 802.1ae na 10Gbit/s portech s volitelným fyzickým rozhraním	ANO	
Minimální počet 40Gbit/s portů s volitelným fyzickým rozhraním	2	
Standard 802.1ae na 40Gbit/s portech s volitelným fyzickým rozhraním	ANO	
Funkční specifikace		

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Virtualizace – možnost sloučit alespoň dvě fyzická šasi do jednoho logického celku – virtuálního šasi (jediná entita z pohledu L2 i L3 protokolů)	ANO	
Ochranné mechanismy rozpadnutí virtuálního šasi bez nutnosti využití dodatečných zařízení	ANO	
Stavové přepnutí mezi řídícími moduly v logickém šasi (ekvivalent funkce Statefull Switchover/SSO mezi fyzickými šasi)	ANO	
Prvek tvoří součást architektury, která zajistí velkou a funkční L2 doménu rozprostřenu libovolně kdekoli po celé LAN síti	ANO	
Prvek tvoří součást architektury, která zajistí IP subnet rozprostřený libovolně po celé síti	ANO	
Směrování protokolů IPv4 a IPv6 v hardware (duální podpora IPv4 a IPv6, tedy možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, *dual-stack*)	ANO	
HW podpora MPLS a VPLS	ANO	
Tunelovací protokoly (např. GRE) v hardware	ANO	
Překlad adres/NAT v hardware	ANO	
IEEE 802.3ad	ANO	
IEEE 802.3ad přes více modulů	ANO	
IEEE 802.3ad přes více šasi (funkční ekvivalent Multichassis Etherchannel)	ANO	
IEEE 802.1Q	ANO	
IEEE 802.1ak	ANO	
tunelování 802.1Q v 802.1Q	ANO	
IEEE 802.1s - multiple spanning trees	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
IEEE 802.1p	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Hardwarová podpora dlouhých ethernetových rámců, tzv. „jumbo frames“	ANO	
Detekce jednosměrnosti optické linky (např. UDLD)	ANO	
QoS classification – dle ACL, IP Prec, DSCP, CoS	ANO	
QoS marking –dle IP Prec, DSCP, CoS	ANO	
QoS Policing	ANO	
Policing per-flow (např. microflow policing nebo funkčně ekvivalentní)	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Konfigurovatelné HW prostředky ochrany CPU před útoky typu DoS	ANO	
Hardwarová filtrace (access list) na fyzickém i logickém L2 i L3 rozhraní	ANO	
Hardwarová filtrace (access list) dle L2, L3 i L4 informací	ANO	
Provádění dílčích změn v access listu nemá vliv na filtraci datových toků neměněnou částí access listu	ANO, povýšením SW	
Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)	ANO	
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ANO	
Propagace bezpečnostní role uživatele nebo koncového zařízení pro každý datový rámec (např. Security Group Tagging nebo funkčně ekvivalentní)	ANO	
Zabezpečení a analýza DHCP protokolu (např. DHCP snoopingu nebo funkčně ekvivalentní)	ANO	
Ochrana ARP protokolu (např. Dynamic ARP Inspection, DAI nebo funkčně ekvivalentní)	ANO	
Ochrana podvrženého mapování IP/MAC adresy (např. IP Source Guard/IPSG nebo funkčně ekvivalentní)	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení	ANO	
MPLS směrování	ANO, povýšením SW	
VPLS směrování	ANO, povýšením SW	
BGPv4, MP-BGP	ANO	
OSPFv2, OSPFv3	ANO	
OSPF s MD5 a NSSA	ANO	
RIPv2, RIPng	ANO	
IS-IS pro IPv4 a IPv6	ANO	
Router Redundancy protokol pro IPv4 (např. VRRP, HSRP)	ANO	
Policy-based routing podle ACL	ANO	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO	
PIM-SM (Protocol Independent Multicast, sparse mód)	ANO	
PIM SSM (PIM Source Specific Multicast)	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Bidirectional Protocol Independent Multicast (RFC 5015)	ANO	
IGMPv2, IGMPv3	ANO	
Antispoofingová kontrola ekvivalentní funkci RPFC, *reverse path forwarding check* dle RFC3704 a RFC3178 pro IPv4 i IPv6	ANO	
Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830)	ANO, povýšením SW	
IPv6 services (HTTP, DNS, SSH, ACL, ICMP, DHCP)	ANO	
Router Redundancy protokol pro IPv6 (např. VRRP, HSRP)	ANO	
IPv6 First Hop Security (IPv6 Port ACL, RA guard, Secure Neighbor Discovery)	ANO	
IPv6 Multicast (MLDv1 & v2, PIM SSM, PIM SM)	ANO	
IPv6 over GRE v hardware	ANO	
ISATAP v hardware	ANO	
IPv6 QoS	ANO	
Vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače/směrovače pro tvorbu VPN (podpora virtualizace směrovacích tabulek - např. funkční ekvivalent Virtual Routing and Forwarding/Multi-VRF)	ANO	
Protokoly a služby per VRF (TACACS+, VRRP nebo HSRP, SNMP, Syslog, NTP, PING)	ANO	
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955) a Flexible NetFlow (nebo funkčně ekvivalentní) pro IPv4 i IPv6	ANO	
NetFlow (nebo funkčně ekvivalentní) na vstupu i výstupu	ANO	
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ANO	
Statistiky určovány z každého paketu daného "flow"	ANO	
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ANO	
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"	ANO	
Zobrazení sbíraných infromací o "flow" přímo v přepínači. I včetně "TopN" pohledu.	ANO	
Export statistik "flow" selektivně na více kolektorů	ANO	
Switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
Interpretace uživatelských CLI a Tcl skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Konfigurovatelná autodiagnostika při startu i za provozu zařízení	ANO	
Nástroj měření odezev sítě (např. IP SLA) pro IPv4 i IPv6	ANO	
Měření a ovládání spotřeby energie k LAN připojených koncových zařízení	ANO	
Textové řádkově orientované/CLI konfigurační rozhraní	ANO	
Konfigurace zařízení v člověku čitelné textové formě	ANO	
Povýšování operačního software zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ANO	
Nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a HTTP	ANO	
Přepínač může sloužit pro automatickou zálohu a obnovu firmware včetně konfigurace pro podřízený/é přepínač/e	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ANO	
Sériová konzolová linka	ANO	
SSHv2	ANO	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO	
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	
Synchronizace času protokolem NTPv3 (klient i server)	ANO	
SNMPv2	ANO	
SNMPv3	ANO	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
TACACS+ klient	ANO	
Zrcadlení portů (funkční ekvivalent SPAN)	ANO	
Vzdálené zrcadlení portů (funkční ekvivalent RSPAN)	ANO	
Pokročilé interní nástroje pro ladění/debugging procházejícího provozu	ANO	
Syslog	ANO	

4.5.6 Distribuce - druhý typ switche – Minimální požadavky pro lokality Bohunice D00 a Dětská F02 + G01a

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Typ přepínače	L2/L3 přepínač	
Počet pro lokalitu Bohunice D00	1 ks	
Počet pro lokalitu Dětská F02 + G01a	2 ks	
Formát přepínače	Stohovatelný	
Počet dedikovaných stohovacích portů	2	
Minimální počet zařízení ve stohu	8	
Minimální kapacita sběrnice stohu	400 Gb/s	
Sdílení výkonu napájecích zdrojů napříč celým stohem	ANO	
Stateful Switch Over v rámci stohu	ANO	
Non-stop Forwarding	ANO, povýšením firmware	
Možnost instalovat interní redundantní napájecí zdroj	ANO	
Interní redundantní napájecí zdroj požadován	ANO	
Datový stohovací kabel požadován	ANO	
Napájecí stohovací kabel požadován	ANO	
Počet portů 10/100/1000 Base-TX s PoE napájením	24	
Minimální PoE budget	720W	
Uplink porty	8x10GE SFP+	
Min. velikost sdíleného systémového bufferu	16MB	
Velikost MAC address tabulky	30000	
Min. počet IPv4 routes	600	
Min. počet IPv6 routes	300	
Min. počet konfigurovatelných security ACL	5000	
IEEE 802.3ad (Link Aggregation)	ANO	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků	128	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
Provoz 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO, povýšením firmware	
ISIS	ANO, povýšením firmware	
BGPv4	ANO, povýšením firmware	
Graceful Insertion and Removal	ANO, povýšením firmware	
IP Multicast (PIM SSM, PIM SM)	ANO, povýšením firmware	
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO, povýšením firmware	
MPLS VPN	ANO, povýšením firmware	
MPLS VPN - 6VPE	ANO, povýšením firmware	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO, povýšením firmware	
Reverse path check (uRPF) pro IPv4 i IPv6	ANO, povýšením firmware	
IGMPv2, IGMPv3	ANO	
IGMP snooping	ANO	
MLD snooping	ANO	
DHCP relay	ANO	
Minimální počet HW QoS front	8	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
QoS - Strict Priority Queue	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
QoS-Per Flow policing	ANO	
QoS-Hierarchical QoS	ANO, min. 2 úrovně	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	
IPv6 QoS	ANO	
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	
IPv6 Port ACL, VLAN ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
PACL, VACL	ANO	
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO, povýšením firmware	
IEEE 802.1ae na uplink portech	ANO	
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO, povýšením firmware	
Switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	
IEEE 802.3af	ANO	
IEEE 802.3at	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
IEEE 802.3az	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Multicast DNS (mDNS) gateway	ANO, povýšením firmware	
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO, povýšením firmware	
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ANO, povýšením firmware	
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	
Python scripting	ANO	
Linux shell	ANO	
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	
Application hosting	ANO, povýšením firmware	
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO, povýšením firmware	
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	
SNMPv2/v3	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	
Podpora network boot (iPXE) pres IPv4 i IPv6	ANO	
Inventarizovatelnost komponent integrovANOu RFID identifikací	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
Vzdálený port mirroring (ERSPAN)	ANO, povýšením firmware	
NTPv3 server	ANO	

4.5.7 Distribuce – lokalita Porodnice A1

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Základní vlastnosti		
Třída zařízení	L3 switch	
Formát zařízení	fixní konfigurací, 1RU	
Stohovatelný bez snížení počtu ethernet portů	ANO	
Stohování požadováno	ANO	
Počet portů 10 Gbit/s a jejich typ	28x SFP+	
možnost volby 1Gbit/s nebo 10Gbit/s rychlosti uplink portu vhodným rozšiřujícím modulem a transcieverem	ANO	
Redundantní interní napájecí zdroj, vyměnitelný za chodu	ANO	
Možnost kombinace AC a DC zdroje v jednom zařízení	ANO	
Možnost připojit externí redundantní zdroj	ANO	
Redundantní ventilátor	ANO	
Směrovací protokoly	ANO	
Výkonnostní parametry		
Minimální propustnost přepínacího subsystému	600 Gbit/s	
Minimální paketový výkon přepínače	450 milionu paketů/vteřinu	
Rychlost stohovacího propojení	alespoň 460 Gbit/s	
Minimální počet MAC adres	30000	
Vlastnosti stohování		
sdílení výkonu napájecích zdrojů napříč celým stohem	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
minimální počet přepínačů ve stohu	9	
automatická kontrola a sjednocení verze software přepínačů ve stohu	ANO	
možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ANO	
seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ANO	
kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance)	ANO	
synchronizace všech stavů mezi aktivním řídícím prvkem a jedním ze záložních pro minimalizaci vlivu výpadků	ANO	
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ANO	
IEEE 802.3ad	ANO	
Podpora "jumbo rámců"	ANO	
Protokoly 2. vrstvy		
IEEE 802.1D	ANO	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
Tunelování 802.1Q v 802.1Q	ANO	
IEEE 802.1X - Port Based Network Access Control	ANO	
IEEE 802.1s - multiple spanning trees	ANO	
IEEE 802.1w - Rapid Tree Spanning Protocol	ANO	
IEEE 802.1p - Minimální počet vnitřních front	8	
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ANO	
Detekce protilehlého zařízení (např. CDP, LLDP)	ANO	
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ANO	
Protokol pro definici šířených VLAN (IEEE 802.1ak nebo VTP)	ANO	
Detekce jednosměrnosti optické linky (např. UDLD)	ANO	
STP root guard	ANO	
STP loop guard	ANO	
Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)	ANO	
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ANO	
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ANO	
QoS	ANO	
QoS i na stohovacím propoji	ANO	
možnost konfigurovat QoS na stohovacím propoji	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
DHCP relay	ANO	
Protokol IPv6		
Certifikace IPv6 ready logo – Phase II	ANO	
HSRP nebo VRRP pro IPv6	ANO	
IPv6 ACL	ANO	
IPv6 QoS	ANO	
IPv6 services (DNS, Telnet, SSH, Syslog, ICMP)	ANO	
HTTP, SNMP over IPv6	ANO	
RADIUS, TACACS+ over IPv6	ANO	
OSPFv3	ANO	
IPv6 MLDv2 snooping	ANO	
IPv6 Port ACL	ANO	
IPv6 First Hop Security RA guard	ANO	
IPv6 First Hop Security DHCPv6 guard	ANO	
IPv6 First Hop Security IPv6 SourceGuard	ANO	
IPv6 First Hop Security IPv6 Binding Integrity Guard	ANO	
DHCPv6 Server and Relay	ANO	
Směrovací protokoly		
BGPv4	ANO	
OSPFv2, OSPFv3	ANO	
OSPF s MD5 a NSSA	ANO	
RIPv2	ANO	
statické směrování	ANO	
Policy-based routing podle ACL	ANO	
EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868)	ANO	
Virtualizace směrovacích funkcí (např. Multi-VRF)	ANO	
Směrování multicastu		
PIM (dense i sparse mód)	ANO	
PIM		
IGMPv2 snooping	ANO	
IGMPv3 snooping	ANO	
IPv6 MLDv1 & v2 snooping	ANO	
Bezpečnost		
Switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
Reverse path check (uRPF)	ANO	
ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.3ad)	ANO	
ACL pro IP	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
ACL pro ethernetové rámce	ANO	
IPv6 ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
Možnost definovat maximální počet MAC adres na portu	ANO	
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ANO	
DHCP snooping	ANO	
Dynamic ARP inspection (DAI)	ANO	
Verifikace mapování IP-MAC (např. IP source guard)	ANO	
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ANO	
Šifrování na L2 dle IEEE 802.1AE	ANO	
Šifrování na L2 dle IEEE 802.1AE, AES s délkou klíče 256 bitů	ANO	
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ANO	
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ANO	
konfiguorvatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ANO	
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ANO	
Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní)	ANO	
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	
Podpora koncových zařízení		

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ANO	
Podpora určování polohy klienta, rozšíření WiFi systému pro určování polohy klienta i v pevné LAN síti (například Network Mobility Service Protocol - NMSP)	ANO	
EEE (IEEE 802.3az)	ANO	
Inzerce služeb pomocí Apple Bonjour protokolu i mezi VLANy	ANO	
Management		
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	
CLI rozhraní	ANO	
SSHv2	ANO	
SSHv2 over IPv6	ANO	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO	
SNMPv2	ANO	
SNMPv3	ANO	
Netconf a YANG	ANO	
USB konzolová linka	ANO	
Sériová konzolová linka	ANO	
10/100 management out-of-band port	ANO	
DNS klient	ANO	
NTP klient s MD5 autentizací	ANO	
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ANO	
Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače	ANO	
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ANO	
Statistiky určovány z každého paketu daného "flow"	ANO	
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ANO	
Návaznost skriptů interpretovaných přepínačem po detekci daných parametrů "flow"	ANO	
Zobrazení sbíraných infromací o "flow" přímo v přepínači. I včetně "TopN" pohledu.	ANO	
Export statistik "flow" selektivně na více kolektorů	ANO	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
TACACS+ klient	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Port mirroring (SPAN)	ANO	
port mirroring 1 -> 1	ANO	
port mirroring N -> 1	ANO	
port mirroring ACL (mirroruje pouze definované toky)	ANO	
Vzdálený port mirroring (RSPAN)	ANO	
Vzdálený port mirroring přes L3 síť/WAN (např. ERSPAN nebo ekvivalentní)	ANO	
Syslog	ANO	
Měření zakončení a délky metalického kabelu (TDR)	ANO	
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ANO	
Interpret jazyka Python přímo v zařízení	ANO	
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ANO	
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ANO	
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ANO	
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ANO	
Prvek tvoří součást architektury, která zajistí velkou a funkční L2 doménu rozprostřenu libovolně kdekoli po celé LAN síti	ANO	
Prvek tvoří součást architektury, která zajistí IP subnet rozprostřený libovolně po celé síti	ANO	
Služby		
NTP server	ANO	
DHCP server	ANO	

4.6 Access switche

4.6.1 Minimální požadavky pro mělké LAN access switche

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Základní vlastnosti		
Počet	27ks	
Třída zařízení	L2 switch	
Formát zařízení	fixní konfigurací, rozšiřitelný na stohování, 1RU	
Maximální hloubka	28 cm	
Stohovatelný bez snížení počtu ethernet portů	ANO, dedikovaným modulem	
Stohování pomocí dedikovaného modulu požadováno součástí ceny a konfigurace switche	ANO	
Přepínač musí být sestohovatelný s již v síti provozovanými přepínači Catalyst 2960X	ANO	
Počet portů 10/100/1000	48	
Počet portů 10 Gbit/s a jejich typ	2x SFP+	
možnost volby 1Gbit/s nebo 10Gbit/s rychlosti uplink portu vhodným rozšiřujícím modulem a transcieverem	ANO, transcieverem	
Možnost připojit externí redundantní zdroj	ANO	
Výkonnostní parametry		
Minimální propustnost přepínacího subsystému	200 Gbit/s	
Minimální paketový výkon přepínače	120 milionu paketů/vteřinu	
Rychlost stohovacího propojení	alespoň 80 Gbit/s	
Minimální počet MAC adres	15000	
Vlastnosti stohování		
vzájemné stohování všech modelů 10/100/1000 s 1Gbit/s uplinky s 10Gbit/s uplinky	ANO	
minimální počet přepínačů ve stohu	8	
automatická kontrola a sjednocení verze software přepínačů ve stohu	ANO	
možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením	ANO	
seskupení portů (IEEE 802.3ad) mezi různými prvky stohu	ANO	
kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance)	ANO	
Protokoly fyzické vrstvy		
IEEE 802.3-2005	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
IEEE 802.3ad	ANO	
Podpora "jumbo rámců"	ANO	
Protokoly 2. vrstvy		
IEEE 802.1D	ANO	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN	1000	
Tunelování 802.1Q v 802.1Q	ANO	
IEEE 802.1X - Port Based Network Access Control	ANO	
IEEE 802.1s - multiple spanning trees	ANO	
IEEE 802.1w - Rapid Tree Spanning Protocol	ANO	
IEEE 802.1p - Minimální počet vnitřních front	4	
Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní	ANO	
Detekce protilehlého zařízení (např. CDP, LLDP)	ANO	
Detekce parametrů protilehlého zařízení (např. LLDP-MED)	ANO	
Protokol pro definici šířených VLAN (IEEE 802.1ak nebo VTP)	ANO	
Detekce jednosměrnosti optické linky (např. UDLD)	ANO	
STP root guard	ANO	
STP loop guard	ANO	
Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard)	ANO	
Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech	ANO	
Protokol IP		
IP alias (více IP sítí na jednom rozhraní)	ANO	
QoS	ANO	
QoS i na stohovacím propoji	ANO	
DHCP relay	ANO	
Protokol IPv6		
Certifikace IPv6 ready logo – Phase II	ANO	
IPv6 ACL	ANO	
IPv6 QoS	ANO	
HTTP, SNMP over IPv6	ANO	
RADIUS, TACACS+ over IPv6	ANO	
OSPFv3	ANO	
IPv6 MLDv2 snooping	ANO	
IPv6 Port ACL	ANO	
IPv6 First Hop Security RA guard	ANO	
IPv6 First Hop Security DHCPv6 guard	ANO	
IPv6 First Hop Security IPv6 Binding Integrity Guard	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Směrovací protokoly		
OSPFv2, OSPFv3	ANO	
RIPv2	ANO	
statické směrování	ANO	
Policy-based routing podle ACL	ANO	
Směrování multicastu		
PIM	ANO	
IGMPv2 snooping	ANO	
IGMPv3 snooping	ANO	
IPv6 MLDv1 & v2 snooping	ANO	
Bezpečnost		
Access switche musí být podporovány všemi funkcionalitami, které v síti již provozovaný policy server Identity Services Engine umožňuje	ANO	
ACL na rozhraní IN/OUT	ANO	
ACL pro IP	ANO	
ACL pro ethernetové rámce	ANO	
IPv6 ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
Možnost definovat maximální počet MAC adres na portu	ANO	
Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy)	ANO	
DHCP snooping	ANO	
Dynamic ARP inspection (DAI)	ANO	
Verifikace mapování IP-MAC (např. IP source guard)	ANO	
Ochrana centrálního procesoru (control plane) před útoky typu DoS	ANO	
IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu	ANO	
IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači, sdílení ověření koncových stanic	ANO	
konfiguorvatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x)	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-06 nebo funkčně ekvivalentní).	ANO	
Detekce parametrů připojovaného koncového zařízení a jejich sdílení s policy serverem	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
Podpora koncových zařízení		
Měření a ovládání spotřeby energie připojených koncových zařízení a infrastruktury	ANO	
Podpora určování polohy klienta, rozšíření WiFi systému pro určování polohy klienta i v pevné LAN síti (například Network Mobility Service Protocol - NMSP)	ANO	
EEE (IEEE 802.3az)	ANO	
Management		
Aktivní prvek musí být spravovatelný již v síti provozovaným nástrojem Prime Infrastructure v celém rozsahu dostupných funkcionalit bez omezení	ANO	
CLI rozhraní	ANO	
SSHv2	ANO	
SSHv2 over IPv6	ANO	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ANO	
SNMPv2	ANO	
SNMPv3	ANO	
USB konzolová linka	ANO	
Sériová konzolová linka	ANO	
10/100 management out-of-band port	ANO	
DNS klient	ANO	
NTP klient s MD5 autentizací	ANO	
NetFlow v9 (nebo IPFIX RFC 3917, RFC 3955)	ANO	
Sběr dat pro NetFlow nebo IPFIX export z každého portu přepínače	ANO	
Detailní flexibilní definice "flow" dle L2, L3 i L4 parametrů	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Statistiky určovány z každého paketu daného "flow"	ANO, povýšením software	
Sběr a export TCP příznaků pro monitoring bezpečnostních hrozeb	ANO	
RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
TACACS+ klient	ANO	
Port mirroring (SPAN)	ANO	
port mirroring 1 -> 1	ANO	
port mirroring N -> 1	ANO	
port mirroring ACL (mirroruje pouze definované toky)	ANO	
Vzdálený port mirroring (RSPAN)	ANO	
Syslog	ANO	
Měření zakončení a délky metalického kabelu (TDR)	ANO	
Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů)	ANO	
Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute)	ANO	
Přepínač si může automaticky zazálohovat a obnovit firmware včetně konfigurace z nadřazeného směrovače nebo přepínače	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ANO	
Služby		
DHCP server	ANO	

4.6.2 Minimální požadavky pro LAN a WLAN PoE access switche

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Počet	185ks	
PoE (IEEE 802.3af)	ANO	
PoE+ (IEEE 802.3at, 30W/port)	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Dostupný výkon pro napájení PoE portů s redundantním zdrojem	Min. 1500W	
Typ přepínače - L2/L3 přepínač	ANO	
Formát přepínače - Stohovatelný	ANO	
Počet dedikovaných stohovacích portů - 2	ANO	
Minimální počet zařízení ve stohu - 8	ANO	
Minimální kapacita sběrnice stohu - 400 Gb/s	ANO	
Sdílení výkonu napájecích zdrojů napříč celým stohem	ANO	
Stateful Switch Over v rámci stohu	ANO	
Non-stop Forwarding	ANO	
Možnost instalovat interní redundantní napájecí zdroj	ANO	
Interní redundantní napájecí zdroj 1100W požadován	ANO	
Datový stohovací kabel požadován	ANO	
Napájecí stohovací kabel požadován	ANO	
Počet portů 10/100/1000 s UPoE napájením - 48	ANO	
Podpora mGig 1/2.5/5/10G na min. 12 portech	ANO	
Uplink porty - 8x 10Gb s volitelným optickým rozhraním	ANO	
Min. velikost sdíleného systémového bufferu – 16MB	ANO	
Min. velikost MAC address tabulky - 30000	ANO	
Min. počet IPv4 routes - 32000	ANO	
Min. počet IPv6 routes - 16000	ANO	
Min. počet konfigurovatelných security ACL - 5000	ANO	
IEEE 802.3ad (Link Aggregation)	ANO	
IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis	ANO	
Minimálně 8 linek jako součást Link Aggregation Group trunku	ANO	
Minimální počet konfigurovatelných Link Aggregation Group trunků - 128	ANO	
IEEE 802.1Q	ANO	
Minimální počet aktivních VLAN - 1000	ANO	
IEEE 802.1x	ANO	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací)	ANO	
Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication)	ANO	
Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů	ANO	
RADIUS CoA	ANO	
Podpora instance spanning-tree protokolu per VLAN	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
IEEE 802.1w - Rapid Spanning Tree Protocol	ANO	
Protokol MVRP nebo VTP pro definici a správu VLAN sítí	ANO	
Podpora jumbo rámců (min. 9198 bytes)	ANO	
Detekce protilehlého zařízení (např. CDP nebo LLDP)	ANO	
Směrování protokolů IPv4 a IPv6 v hardware	ANO	
OSPFv2	ANO	
OSPFv3	ANO	
ISIS	ANO	
BGPv4	ANO	
Graceful Insertion and Removal	ANO	
IP Multicast (PIM SSM, PIM SM)	ANO	
Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)	ANO	
MPLS VPN	ANO	
MPLS VPN - 6VPE	ANO	
First Hop Redundancy Protokol (např. VRRP, HSRP)	ANO	
Reverse path check (uRPF) pro IPv4 i IPv6	ANO	
IGMPv2, IGMPv3	ANO	
IGMP snooping	ANO	
MLD snooping	ANO	
DHCP relay	ANO	
Minimální počet HW QoS front - 8	ANO	
QoS classification – ACL, DSCP, CoS based	ANO	
QoS marking - DSCP, CoS	ANO	
QoS - Strict Priority Queue	ANO	
Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní)	ANO	
QoS Policing	ANO	
QoS-Per Flow policing	ANO	
QoS-Hierarchical QoS – min. 2 úrovně	ANO	
First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP)	ANO	
IPv6 services (Telnet, SSH, Syslog, DHCP)	ANO	
IPv6 QoS	ANO	
IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard)	ANO	
IPv6 Port ACL, VLAN ACL	ANO	
Možnost definovat povolené MAC adresy na portu	ANO	
PACL, VACL	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny	ANO	
IEEE 802.1ae na uplink portech	ANO	
IEEE 802.1ae (AES-GCM-256) na uplink portech	ANO	
Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy	ANO	
Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru	ANO	
Bezpečnostní funkce umožňující inspekci provozu protokolu ARP	ANO	
Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů	ANO	
HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů	ANO	
Podpora SUDI (IEEE 802.1AR) autentizace	ANO	
IEEE 802.3af	ANO	
IEEE 802.3at	ANO	
IEEE 802.3az	ANO	
Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu	ANO	
Multicast DNS (mDNS) gateway	ANO	
Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení	ANO	
Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur)	ANO	
Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní	ANO	
Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type	ANO	
Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX	ANO	
SSHv2	ANO	
CLI rozhraní	ANO	
Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu	ANO	
Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG	ANO	
Python scripting	ANO	
Linux shell	ANO	
Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení	ANO	
Application hosting	ANO	
Aplikace softwarových záplat, nikoli povyšování celého firmware	ANO	
Streaming telemetrie prostřednictvím NETCONF/XML	ANO	
SNMPv2/v3	ANO	
Podpora network boot (iPXE) pres IPv4 i IPv6	ANO	
Inventarizovatelnost komponent integrovanou RFID identifikací	ANO	
TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)	ANO	
Vzdálený port mirroring (ERSPAN)	ANO	
NTPv3 server	ANO	

4.7 Identity Services Engine

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
HW appliance/ fyzický server pro používaný systém Identity Services Engine	**2 ks**	
Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.)	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup	ANO	
Poskytuje AAA funkce (viz níže)	ANO	
Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control)	ANO	
Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování kapacity	ANO	
Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace	ANO	
Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem)	ANO	
Je dostupné ve formě Virtuálního stroje na platformách ESX nebo ESXi	ANO	
AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)		
Podporované protokoly		
RADIUS pro autentizaci, autorizaci, zaznamenávání	ANO	
proxy funkce pro externí RADIUS	ANO	
PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST	ANO	
podpora TACACS+ pro administraci zařízení	ANO	
Podporované databáze uživatelů (s možností definovat pořadí průchodu)		
Interní (pro uživatele i koncová zařízení)	ANO	
Active Directory	ANO	
LDAP (RFC 2251)	ANO	
RADIUS Token indentity source (RFC 2865)	ANO	
RSA RADIUS token server	ANO	
Certificate authentication profile	ANO	
Ověřování uživatelů a zařízení		
Ověření uživatelů heslem nebo certifikátem	ANO	
Ověření MAC adresou připojovaného zařízení	ANO	
Autorizace: pružný systém pro definici pravidel pro přístup k síti		
Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:	ANO	
· stavu a typu koncového zařízení (viz níže),	ANO	

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
· uživatele (role, skupiny),	ANO	
· místa připojení,	ANO	
· historie připojení	ANO	
Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě	ANO	
Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě	ANO	
Využívání Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“	ANO	
Řízení přístupu i možným zapojením do trasy komunikace autorizovaných zařízení	ANO	
Podpora přidělení značek prvkům přístupové infrastruktury podle klientské identity/skupiny, pro škálovatelné filtrování přístupů	ANO	
Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti	ANO	
Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat	ANO	
Accounting		
Zaznamenávání aktivity uživatelů a zařízení připojených k síti	ANO	
Dotazovací systém, korelace záznamů, centralizované výkazy	ANO	
Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)	ANO	
Funkce GUEST serveru		
Vytváření casově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi	ANO	
Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů	ANO	
Samoobslužný portál pro uživatele	ANO	
Ověření přes HTTP a HTTPS	ANO	
Rozpoznávání typukoncových zařízení		
Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, SymbiANOS, Apple, Blackberry, HTC)	ANO	
Předdefinované profily pro síťová zařízení NAD od různých vendorů	ANO	
Podpora pro IPv6 koncová zařízení	ANO	
Podpora BYOD		
Onboarding (registrace, provisioning, nastavení klientských zařízení)	ANO	
Onboarding/provisioning proces formou samoobsluhu	ANO	
Specifické politiky pro BYOD zařízení	ANO	
Možnost nastavení limitu BYOD zařízení pro jednoho uživatele	ANO	
Interní CA, pro vydávání certifikátů BYOD zařízením	ANO	
Interní CA lze řetězit jako subordinate pod firemní CA	ANO	
Další vlastnosti		
Možnost autentizace oproti více AD domén, i když nejsou v trust režimu	ANO	
Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují)	ANO	
Podpora Multi-Domain integrace s AD	ANO	
Podpora SXP (Exchange Protocol) dle IETF	ANO	
Funkce pro správu ověřovacího systému		
Centralizovaná správa	ANO	
Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému	ANO	
Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení	ANO	
Grafické rozhraní pro definici pravidel přístupu k síti	ANO	
Grafické rozhraní pro monitorování, definici výkazů, řešení problémů	ANO	
Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture)	ANO	
Zaznamenávání událostí na externí syslog server	ANO	
Podpora SNMPv3	ANO	
NTP pro synchronizaci času	ANO	
SMTP pro zasílání zpráv a výstrah přes e-mail	ANO	
Licence pro Terminal Access Controller Access Control System	ANO	
Technické parametry		

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Centralizované nasazení s podporou vysoké dostupnosti	ANO	
Minimální parametry fyzického serveru – 1x CPU, 64GB RAM, 4x 600GB SAS 10K RPM HDD v RAID 10	ANO	

4.8 Přístupové body

V návaznosti na vybudování nových síťových tras (viz kap. 3 - část b) instalace a zprovoznění nových metalických tras pro infrastrukturu bezdrátové sítě WiFi) je požadováno dodání a instalace přístupových bodů (access pointů) dle specifikace níže

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
WiFi Access Point	**675 ks**	
Access Point určený pro instalaci na strop/podhled	ANO	
Typ antén	Integrované pro obě pásma	
Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu	ANO	
Třetí monitorovací rádio sledující obě pásma 2,4 a 5 GHz	ANO	
Podpora standardů 802.11a/b/g/n a 802.11ac wave 2	ANO	
Podpora 4x4 MIMO, podpora MU-MIMO, až 160 MHz kanál pro 802.11ac	ANO	
Minimální počet inzerovaných SSID (BSSID) per radio	8	
Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 a/g/n/ac klientům (Beam Forming)	ANO	
Podpora mechanismů pro přepojení klientů z 2,4GHz do 5GHz pásma a optimalizovaného roamingu	ANO	
Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI	ANO	
Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům	ANO	
Hardwarová podpora šifrování řídících i uživatelských dat přenášených mezi AP a kontrolerem, šifrování nemá vliv na propustnost AP	ANO	

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**	**Doplní účastník dle nabízeného zařízení**
Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark)	ANO	
AP uzavřené konstrukce, bez větracích otvorů a ventilátoru	ANO	
Access Pointy jsou fyzicky zabezpečitelné/zamknutelné k okolním pevným částem	ANO	
Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 a IPv6 pomocí Telnet a SSH	ANO	
Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference)	ANO	
Hardwarová podpora rozpoznání zdroje rušivého signálu podle signatur	ANO	
Access Point obsahuje Bluetooth low-energy (BLE) 4.1 radio, RX/TX	ANO	
1x MultiGigabit interface s podporou 1/2,5/5 Gb/s (dle 802.3bz) a 1x 10/100/1000 Ethernet rozhraní, podpora 802.3ad	ANO	
Napájení AP pomocí PoE dle standardů 802.3at/802.3bt nebo lokálním zdrojem	ANO	
Plná podpora AP na stávajících bezdrátových kontrolerech zadavatele (CT5520)	ANO	
Součástí dodávky a ceny každého nového AP musí být licence s 5 letou podporou pro • jeho přípojení ke kontroleru bezdrátové sítě, • jeho přiřazení pod existující používaný WLAN management Prime Infrastructure, • aplikační platformu bezdrátové sítě, 15 koncových klientů pro existující používaný Identity Services Engine v rozsahu funkcionalit popsaných kapitole Identity Services Engine	ANO	
• **Aplikační platforma bezdrátové sítě**		
Požadovaný formát zařízení	Virtuální server pro prostředí VMware	
Licence pro stávajících 673ks AP	ANO	
Modul pro rozšířené funkce spektrální analýzy, korelace informací o rušení z jednotlivých AP, lokalizace zdrojů rušení a vizualizace zóny vlivu zdroje rušení	ANO	
REST API rozhraní pro integraci s 3rd party řešeními	ANO	
CLI rozhraní, SSHv2, dohled a konfigurace pomocí https web GUI	ANO	

4.9 Transceivery

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplní účastník dle nabízeného zařízení
Všechny transceivery musí být originální od stejného výrobce jako poptávané aktivní prvky a transceivery musí být dohledatelné pomocí sériového čísla u výrobce aktivních prvků. Nepřipouští se OEM.		
10GBASE-LR SFP Module, Enterprise-Class	690 ks	
1000BASE-BX SFP, 1490NM	4 ks	
1000BASE-BX SFP, 1310NM	4 ks	
1000BASE-T SFP transceiver module for Category 5 copper wire	10 ks	
QSFP 40GBASE-LR4 Trnscvr Mod, LC, 10km, Enterprise-Class	50 ks	
40GBASE-CR4 Passive Copper Cable, 5m	4 ks	
40GBASE Active Optical Cable, 10m	4 ks	
10GBASE-CU SFP+ Cable 5 Meter	35 ks	
10GBASE-CU SFP+ Cable 5 Meter	50 ks	
40GBASE Active Optical QSFP to 4SFP breakout Cable, 3m	10 ks	
SFP+ Bidirectional for 10km, downstream	14 ks	
SFP+ Bidirectional for 10km, upstream	14 ks	
10GBASE-LRM SFP Module	32 ks	
10GBASE Active Optical SFP+ Cable, 10M	40 ks	

5 Rozšíření stávající infrastruktury

5.1 Nové servery

Pořízení serverů pro stávající virtualizační platformu za účelem vytvoření výkonové rezervy pro případ havárie datového centra. Rozšíření serverové farmy o 6 ks serverů 100% kompatibilních se stávajícími servery Fujitsu RX2540 ve virtualizačním prostředí VMware.

Specifikace minimálních parametrů serverů – minimální požadované plnění

Parametr	Minimální požadavky	Způsob plnění - parametry nabízené účastníkem
Počet kusů:	6 ks.	
Provedení serverů:	- do 19" racku, max. 2U - nedělené chassis, - Ližiny do racku (rack mount kit) a rameno pro kabeláž (Cable arm) součástí dodávky.	
Počet procesorových patic na server:	Min. 2., min. 2 osazené procesory nejnovější dostupné generace.	
Počet jader na fyzický procesor:	Min. 20.	
Požadovaný výkon každého procesorů:	Každý CPU min. 20 jader, 2.4GHz, 27.5MB L3 cache, TDP 150W - SPECrate2017_int_base alespoň 210. - SPECrate2017_fp_base alespoň 199. Ke všem výsledkům dostupné oficiální dokumenty od výrobce.	
Operační paměť (osazení) na server:	Osazena min. 12 x 64GB DDR4 2666MHz RDIMM (moduly rovnoměrně rozložené přes všechny paměťové kanály), s rozšiřitelností až na 3TB DDR4 2666MHz, minimálně 24 DIMM slotů.	
Pozice pro HDD – interní storage:	Server obsahuje pozice pro min. 16x 2.5" disk. Všechny disky připojeny na jeden RAID řadič. Rozšiřitelnost na 28x 2.5" HDD. Všechny HDD hot-plug. Možnost interní DVD-RW mechaniky. Interní storage zařízeni o kapacitě min. 150GB pro virtualizační SW. Osazeno: - 4x 1.92TB SSD mixed use, DWPD 3, - 2x SAS 12G 800GB SSD write intensive, DWPD 10, - SSD M.2 SATA 150 GB úložiště s předinstalovaným VMware vSphere ESXi.	
RAID řadič:	HW SAS HBA řadič podporující RAID 0,1. Certifikovaný pro VMware VSAN.	
SAN řadič:	- 2x 1-port FC HBA 16Gb včetně MM optického modulu.	

Ethernet konektivita na server:	- 2x 2-port 10Gbit SFP+ LAN karta, - Min. 2x 1Gbit RJ45 port onboard,	
Napájení - chlazení:	Redundantní hot-plug napájecí zdroje, každý s výkonem 800W a účinností alespoň Platinum – 94%. 2ks napájecích kabelů. Redundantní hotswapové ventilátory - Hot plug redundantní chlazení.	
Management:	HW management, zapnutí, vypnutí, restart serveru, přesměrování KVM nezávislé na OS, vzdálené připojení médií, časově neomezena licence.	
Management port:	Dedikovaný LAN port pro management.	
Rozšiřující sloty:	- Až 8x PCIe3.0 slot + 1x PCIe slot dedikovaný pro ethernet kartu typu LoM (LAN on Motherboard) + 1x min. 2-port RJ45 1Gbit LAN onboard. - VGA port min. 1x zadní - Volitelně sériový port nezabírající PCIe slot.	
USB porty:	Minimálně USB 3.0 – Min. 1 přední, min. 2 zadní + 1 interní.	
Záruka	60 měsíců On-Site, 24x7, garance opravy do 24 hodin od nahlášení s možností rozšíření.	

5.2 Rozšíření HorizonView

Doplnění licencí Academic pro systém, který zvyšuje dostupnost pro obsluhu systémů tím, že zjednodušuje a zkracuje náhradu porouchaného zařízení na pouhou výměnu bez nutnosti konfigurace a instalace nového zařízení. Současně se tímto řeší i provoz z druhého datového centra v případě výpadku. V rámci projektu bude pořízeno 500 licencí.

5.3 vSAN

Doplnění stávajících provozovaných licencí zadavatele Academic VMware vSAN Enterprise o 24 CPU licencí Academic VMware vSAN Enterprise per CPU s originální zárukou/podporou výrobce v úrovni Production Support na standardní dobu 5 let. Záruka/podpora musí být přímo od výrobce virtualizační platformy, nesmí být poskytována třetí stranou (např. na bázi OEM kontraktu).

5.4 Windows Server a SQL server DC

5.4.1 Windows Server Datacenter

Systémový SW musí zajistit virtualizaci minimálně 12 serverů (celkem 480 jader) včetně správného licencování.

Požadavek	Splňuje (ano/ne)
Virtualizační SW pro dodané virtualizační servery	
Dynamické alokování kapacity	
Možnost replikace serverů po LAN do jiného úložiště	
Možnost zálohování po LAN	
Možnost migrace virtuálního stroje na jiný HW v rámci clusteru bez výpadku	
Vysoká dostupnost – automatický start virtuálního systému na jiném HW po výpadku	
Plná podpora správy pomocí MS System Center Datacenter	
Licence produktu MS Windows Server v aktuální verzi pro virtualizační servery (24 serverů /celkem 480 jader), umožňující provozovat neomezený počet virtuálních serverů na každém fyzickém serveru.	

5.4.2 Microsoft SQL Server 2017 Enterprise Edition

V rámci virtualizované infrastruktury a počtu uživatelů je zvolena databázová licence bez omezení počtu uživatelů – licenční model per core. V rámci virtuálního serveru je možno instalovat databázový server s dostatečný výkon zajišťující 12 core virtuálního CPU. Databázový software bude využit napříč IS, které pro svojí nativní funkci potřebují databázový server.

5.5 Rozšíření stávajících serverů o HDD

Upgrade stávajících serverů o 100% kompatibilní disky a řadiče pro dosažení redundance ukládaných dat.

Rozšíření 12 ks stávajících serverů Fujitsu RX2540 o následující hardware pro rozšíření již provozovaného systému Software – Defined – Storage VMware vSAN. Z důvodů kompatibility řešení s již provozovanou technologií vSAN požaduje zadavatel přesně uvedené P/N nebo jejich výrobcem doporučené ekvivalentní. Uvedená zařízení musí být nová, nepoužitá a určená pro český trh, z důvodu udržení celkové záruky na servery.

Ks	SKU	Popis
24	S26361-F5608-L800	SSD SAS 12G 800GB Write-Int. 2.5" H-P EP
48	S26361-F5588-L192	SSD SATA 6G 1.92TB Mixed-Use 2.5' H-P EP
12	S26361-F3842-L502	PSAS CP400i FH/LP

5.6 Datastore Cluster mode

Popis komponent stávajícího řešení

Zadavatel v současnosti provozuje MetroCluster řešení od společnosti NetApp. Jedná se o 2-nodový MetroCluster, kde v každé lokalitě je jeden kontroler NetApp FAS8040. Použitá verze ONTAP je 8.2.4 7-mode

Zadavatel předpokládá, tam kde je to smysluplné využít stávajících shelfů a/nebo disků v novém upgradovaném řešení. Zbytek stávajícího řešení (kontroléry a některé shelfy) bude provozováno jako vývojové/testovací úložiště.

Storage systémy zadavatele jsou připojeny k fyzickým i virtualizačním serverům prostřednictvím redundantní FC a iSCSI blokové SAN infrastruktury. Souborová data jsou zpřístupňována aplikacím a klientským pracovištím přímo souborovými systémy CIFS a NFS. Zadavatel také používá softwarovou funkcionalitu, která je u úložiště k dispozici – jedná se o funkcionalitu MetroClusteru, asynchronní replikace, vytváření konzistentních aplikačních snapshotů (SnapManager). Minimálně stejná funkcionalita je také požadována pro upgradované úložiště. V rámci aktuálních potřeb na zvýšení kapacity a výkonu provozovaných storage systémů je nutné navrhnout a zprovoznit datové úložiště, které by odpovídalo dnešním i výhledovým kapacitním výkonovým i funkčním požadavkům (alespoň 5 let).

Požadované řešení musí akceptovat požadavek na využití doposud vložených investic a to formou začlenění komponent stávajícího storage systému.

Za tímto účelem v novém systému musí být minimálně volné pozice pro disky a SSD.

- Celkem 140 volných pozic pro 2,5'' SAS
- Celkem 44 volných pozic pro 3,5'' disky
- Celkem 72 volných pozic pro 2,5'' SSD disky

Dále do každé lokality musí být možno doplnit další diskové police a to minimálně jednu pro SSD disky a současně jednu pro SAS nebo NL-SAS disky bez nutnosti doplňovat jiné prvky infrastruktury např bridge nebo switche.

Dodaný upgrade primárního úložiště musí splňovat požadavek na maximální odolnost proti poruše a bez výpadkový provoz, a to jak v rámci lokality, tak i v případě havárie celé lokality. Takovýmto řešením bude možné při zachování redundance a bez přerušení provozu poskytovat příslušné IT služby i za situace, že dojde k výpadku nodu či k odstavení nodu v případě údržby nebo upgradu a podobně. V těchto vyjmenovaných případech je přípustný failover mezi lokalitami, který nesmí mít dopad na aplikace. Diskové pole tedy musí být plně redundantní a v případě odstavení kontroléru (nodu) musí umožnit pro aplikace transparentní failover.

Informace ke kompatibilitě

Veškeré poptávané plnění musí být kompatibilní a implementovatelné se stávající systémovou infrastrukturou a komponentami, které zadavatel požaduje zachovat. Součástí požadavků na kompatibilitu je dále minimálně zajištění provozu a plné funkcionality stávajících aplikací, operačních systému a hypervizorů.

Nové úložiště musí podporovat snapshot integraci s produktem Veeam Availability Suite verze 9.x a to včetně podpory replikace snapshotů na záložní pole Netapp FAS8020, které zákazník pro tyto účely používá.

Architektura

Upgradované diskové pole musí být modulární, minimálně dvouřadičové pole založené na 12Gbit SAS architektuře. Řešení musí být koncipováno jako HW, SW a FW 100% kompatibilní entita, s blokovým a souborovým přístupem k datům (FC, FCoE, iSCSI, NFS, CIFS současně). Řešení pomocí externích např. NAS „head" není přípustné. Řešení musí minimálně splňovat stávající funkcionalitu NetApp MetroClusteru. Toto řešení musí poskytovat samotné kontroléry diskového pole (řešení pomocí externího zařízení není přípustné).

Řešení musí umožňovat rozšíření storage clusteru nejprve na 2 nody v každé lokalitě, tedy 4 celkem a následně až na 4 nody (kontroléry) v každé lokalitě celkem tedy 8x kontrolér. Požadavkem je také to, aby v případě rozšíření ze 4 na 8 nodů, případné další 4 kontroléry nemusely být stejného typu jako budou první 4.

Obecný popis požadovaného řešení

Předmětem návrhu je upgrade a rozšíření stávajícího řešení pro ukládání dat v páteřní IT infrastruktuře s ohledem na již existující datová úložiště zadavatele. Součástí navrhovaného řešení bude zajištění vysoké dostupnosti dat uložených v primárních úložištích, odolnosti systému proti haváriím, a to nejen v jedné lokalitě, ale i výpadku celé lokality. Jakýkoliv takový výpadek musí být pro připojené hosty (aplikace) plně transparentní, a to i v případě výpadku celé lokality. Výsledné řešení musí splňovat aktuální výkonnostní a funkční požadavky, ale musí také počítat s rezervou pro pokrytí předpokládaného růstu požadavků na interní IT v budoucnu cca 5 let.

Účelem realizace zakázky je upgrade a rozšíření primárních datových úložišť tak, aby byla zajištěná vysoká dostupnost dat, zvýšení výkonu a rozšíření diskové kapacity, a to s plnou podporou výrobce na další období. Jedním z nejdůležitějších požadavků je plná kompatibilita se stávajícím prostředím, se kterým bude integrováno a musí také maximálně využít komponenty současného řešení, tam kde je to vhodné a ekonomicky výhodné. Jedná se tedy o využití stávajících diskových shelfů, disků a dalších vhodných komponent. Komponenty stávajícího úložiště, které nebudou použity v nové konfiguraci primárního úložiště bude zadavatel používat jako vývojové/testovací úložiště. Z toho také vyplývá požadavek funkcionality vzdálené replikace mezi upgradovaných úložištěm a úložištěm původním.

Zadavatel požaduje upgrade stávajícího řešení následovně

- Upgrade stávajících kontrolérů na nové, výkonnější.
- Zachování MetroCluster řešení jako vysoce dostupného řešení s RPO (Recovery Point Objective) nula a RTO (Recovery Time Objective) maximálně několik minut .
- Minimální požadované parametry pro nové kontroléry jsou specifikovány v následující části – technická příloha

- Funkcionalita MetroClusteru musí být řešena přímo pomocí kontrolérů diskového úložiště, řešení pomocí virtualizačních nebo jiných externích appliancí není přípustné
- Rozšíření kapacity o následující shelfy s daným počtem disků.
    - 10x DS224C diskový shelf s 124x 1.2 SAS 10k RPM 2.5" HDDs celkem
    - 4x DS4246 diskový shelf s 52x 4TB NL-SAS 7.2k RPM 3.5" HDDs celkem
    - 2x DS2224C diskový shelfy s 24x 960GB SSD celkem
- Zbylé volné sloty v shelfech budou využity na přesunutí disků ze stávajícího úložiště
- Další nezbytné komponenty pro fungování celého řešení (Bridge, SAN switche,atd.)
- Týdenní zaškolení administrátora
- 4x Brocade G620 každý s 48 x zalicencovanými porty 32Gbps včetně SFP+ modulů pro připojení hostů
- Včetně zapojení, instalace a konfigurace upgrade stávajícího řešení včetně případných migrací

Požadované parametry diskového úložiště

- Diskové pole musí obsahovat minimálně dva diskové kontrolery, dostupné v režimu active-active with controller failover and multipath HA storage
- Redundantní napájení pro každý modul včetně řídící jednotky
- Min. 512GB RAM, 36 CPU core per kontrolér
- Rozšiřitelnost pole až na maximálně 1440 disků
- Možnost využití SSD jako dodatečnou cache až do velikosti 144TiB
- Podpora RAID konfigurace odolné proti výpadku až 3 HDD současně
- Minimálně 20x IO expansion slotů per dvojici kontrolérů lokalitu
- Minimálně 4x10GbE Base-T portů v každém kontroleru pro komunikaci mezi clustery a replikaci dat na záložní pole
- Minimálně 4x16Gbps FC porty v každém kontroléru pro připojení host serverů (frontend SAN switchů)
- Minimálně 4x16Gbps FC porty v každém kontroléru pro připojení storage shelfů (backend SAN switchů). Backend SAN switche jsou nutnou součástí dodávky s dostatečným počtem portů pro připojení dodatečných nových FC/SAS bridgů a diskových polic. Minimálně požadujeme 24 licencovaných portů včetně 16Gbps SFP+ v každém SAN switchi.
- Minimálně 1TB NVMe onboard Flash Cache per kontroler rozšiřitelnou až na 8TB

Součásti dodávky také musí být veškeré další komponenty výše nezmíněné, ale nutné pro provoz řešení. Tedy veškeré další nutné IO karty, FC/SAS bridge a veškerá kabeláž pro připojení switchů a diskových polic. Dále je požadována veškerá napájecí kabeláž zakončená koncovkami do lišt v racku C14

Minimální podpora protokolů:

- FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB

Požadované (softwarové) funkcionality diskového řešení a licence zahrnuté v ceně celého řešení. Veškeré funkcionality musí být licencované na celkovou nabízenou kapacitu

Další obecné požadavky

- Blokový přístup k datům FC, FcoE a iSCSI
- Komprese, deduplikace na veškerou nabízenou kapacitu
- Licence na neomezené vytváření snapshotů
- Thin Provisioning technologie včetně zero detect space reclamation:
- Pro vytváření virtuálních disků s použitím Thin Provisioning technologie
- Pro vytváření snapshotů s použitím Thin provisioning technologie
- QoS (Quality of Service)
- Remote Service (call home)
- Microsoft VSS support
- MetroCluster funkcionalita s RPO 0 a RTO v řádu několika minut – naprosto transparentní pro připojené hosty a aplikace, tato vlastonst je vyžadována jako nativní funkcionalita kontrolérů
- Plná VAAI podpora (vStorage API for Array Integration)
- Transparentní migrace dat mezi diskovými prostory
- Upgrade software a hardware u řadičů musí být proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datům
- Řešení musí obsahovat licence na neomezený počet připojení hostitelských serverů a operačních systémů
- Enkrypce pro celou dodávanou kapacitu
- Licence na neomezené vytváření snapshotů a klonů v následujících režimech:
    - inkrementální snapshoty, tzn., kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu
    - reverzní snapshoty - lze provést zpětné přesunutí dat z klonu do původního originálního Volume
    - snapshoty pouze pro čtení
    - vytváření konzistentních snapshotů z databází a aplikací Interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle

Požadovaná záruka na zařízení je 60 měsíců, NBD on-site replacement

Nově dodaná zařízení musí být nová, originální přímo od výrobce diskového pole, nepoužitá a určená pro český trh.

5.7 Datastore – navýšení kapacit

Pořízení kapacity do upgradeovaného diskového pole pro dosažení možnosti synchronní replikace mezi datacentry pro kompletní data významných systémů – navýšení kapacity o 30TB čisté kapacity v SAS HDD a 20TB čisté kapacity v SSD vůči stávajícímu stavu.

Požadováno je rozšíření systému Netapp následujícím způsobem:

• 2 ks shelf DS2224C včetně 48 ks SSD 960GB 2,5" celkem

• 4 ks shelf DS2224Cvčetně 72 ks HDD 1,2 TB SAS 10k RPM 2,5" celkem

Včetně příslušných kabelů, licencí a záruky v délce 60 měsíců

Nově dodaná zařízení musí být nová, originální přímo od výrobce diskového pole, nepoužitá a určená pro český trh.

5.8 Zálohování

5.8.1 Rozšíření systému pro zálohování kritických dat

Rozšíření stávajících provozovaných licencí zadavatele VEEAM Veeam Availability Suite Enterprise Plus o 12 ks stejných licencí Veeam Availability Suite Enterprise Plus s originální zárukou/podporou výrobce na standardní dobu 5 let. Záruka/podpora musí být přímo od výrobce zálohovacího SW, nesmí být poskytována třetí stranou (např. na bázi OEM kontraktu).

5.8.2 HW pro zálohy

Navýšení kapacity stávajícího diskového pole Netapp FAS8020 určeného pro zálohy o 50TB čisté kapacity. Kapacita jednotlivých HDD je požadována stejná jako stávajících disků 4TB, NL-SAS, 7.2k/min otáček. Předpokládá se dodávka disků včetně nových diskových polic – stávající police jsou plně osazené disky. Dodané disky a shelfy musí být nové, originální přímo od výrobce diskového pole, nepoužité a určené pro český trh.

Požadovaná záruka je 60 měsíců, 4hr on-site replacement.

6 Rozšíření kamerového systému

Za účelem pokrytí některých „slepých míst" v areálu a v interiérech FNB [Jihlavská 20 (PMDV)] je třeba rozšířit stávající kamerový systém (CCTV). Požadováno je rozšíření (dodávka, montáž, zprovoznění) IP kamerového systému o kamery s vysokým rozlišením a integrovanou logikou bezpečnostních funkcí. Předpokládá se instalace kamer s vysokou citlivostí na zbytkové světlo, kombinované s technologií přísvitu. Instalovány by měly být výhradně HDR kamery s integrovanou zvýšenou odolností proti oslepení a detekcí poruchy, útoku nebo sabotáže na kameru; podle uspořádání chráněného prostoru a směru s pevným, nebo vzdáleně proměnným ohniskem.

Kamery budou připojeny na centrální správu a centrální úložiště záznamu. Součástí kamerového systému bude vybavení pro centrální správu kamer, záznamu a analýzy obrazu. Kamery a centrální systém budou podporovat detekci a alertování definovaných událostí. Klíčovou rolí systému bude monitoring pohybu osob na určených komunikačních trasách a vstupech do budov nebo jejich částí, ve kterých jsou umístěna datová centra nemocnice a klíčové prvky informační infrastruktury.

Pro rozšíření systému CCTV bude použito celkem 29ks kamer. Jako jádro kamerového systému je požadováno softwarové řešení v rozsahu 29 licencí pro kamery, umožňující monitorování, nahrávání a ovládání IP kamer.

Rozšíření kamerového systému musí být navrženo a dodáno tak, aby bylo kompatibilní se stávajícím systémem. Z tohoto důvodu je technická specifikace následující:

A. Technická specifikace pro kamery:

Kategorie	Specifikace	Počet
Typ A	4 Mpx PTZ kamera IP exteriérová, Day/Night s mechanickým IR filtrem, Smart IR LED dosvit 100 m, 1/3" Color CMOS, rozlišení 2592 x 1520 px @ 25 fps, citlivost 0,05 lx / F1.6, B/W 0,005 lx / F1.6, motor zoom objektiv 4,5–135,0 mm / F1.6–F4 .4, 30x optický zoom, úhel záběru 60°–2,4°, horizontální natáčení 360°, vertikální náklon od -15° do +90°, ATW, BLC, HLC, AWB, AGC, WDR, 3DNR, inteligentní funkce, komprese H.265 / H.264 / MJPEG, ONVIF kompatibilní, alarm I/O 2/1, audio I/O 1/1, slot na MicroSD kartu max. 128GB, napájení 24 V AC, 958 mA, PoE+, pracovní teplota od -40 °C do +70 °C, IP 66, rozměry orientačně ø 186 x 309 mm, hmotnost orientačně 3,5 kg, součástí balení by měl být zdroj a držák na zeď	11 ks
Typ B	4 Mpx kompaktní kamera IP exteriérová antivandal, Day/Night s mechanickým IR filtrem, Smart IR LED dosvit 50 m, 1/3" 4 Megapixel progressive scan CMOS, rozlišení 2688 x 1520 px @ 25 fps, citlivost 0,03 lx / F1.4 (Color, 1/3 s, 30 IRE), 0,3 lx / F1.4 (Color, 1/30 s, 30 IRE), 0 lx / F1.4 (IR ON), motor zoom objektiv 2,7–13,5 mm / F1.4, 5x optický zoom, úhel záběru 106°–31°, BLC, HLC, AWB, AGC, WDR (120 dB), 3DNR, inteligentní funkce, komprese H.265+ / H.265 / H.264+ / H.264, ONVIF kompatibilní,	7 ks

	alarm I/O 2/1, audio I/O 1/1, 1x video výstup, slot na MicroSD kartu max. 128 GB, napájení 12 V DC, 1079 mA, ePoE, pracovní teplota od -30 °C do +60 °C, IP 67, IK 10, rozměry orientačně 273 × 95 × 95 mm, hmotnost orientačně 1 kg	
Typ C	4 Mpx kompaktní kamera IP exteriérová antivandal, Day/Night s mechanickým IR filtrem, Smart IR LED dosvit 50 m, 1/3" 4Megapixel progressive scan CMOS, rozlišení 2688 x 1520 px @ 25 fps, citlivost 0,03 lx / F1.4 (Color, 1/3 s, 30 IRE), 0,3 lx / F1.4 (Color, 1/30 s, 30 IRE), 0 lx / F1.4 (IR ON), motor zoom objektiv 2,7–13,5 mm / F1.4, 5x optický zoom, úhel záběru 106°–31°, BLC, HLC, AWB, AGC, WDR (120 dB), 3DNR, inteligentní funkce, komprese H.265+ / H.265 / H.264+ / H.264, ONVIF kompatibilní, alarm I/O 2/1, audio I/O 1/1, 1x video výstup, slot na MicroSD kartu max. 128 GB, napájení 12 V DC, 1079 mA, ePoE, pracovní teplota od -30 °C do +60 °C, IP 67, IK 10, rozměry orientačně 273 × 95 × 95 mm, hmotnost orientačně 1 kg.	11 ks

Jednotlivé kamery by měly být svedeny a zapojeny do stávajících rack-skříní místně příslušným k jednotlivým budovám. U všech kamer musí být provedeny kamerové zkoušky a nasměrování dle požadavků uživatele. Konkrétní rozmístění prvků a jejich propojení **dle dokumentace pro provedení stavby *„Dokumentace datových rozvodů pro zvýšení kybernetické bezpečnosti“* (samostatná příloha v režimu důvěrných informací).**

B. Technická specifikace pro Systém

Kamerový server by měl být provozován na stávajících serverech FNB ve virtuálním prostředí. Uložiště pro záznam kamer pro server by mělo být řešeno dodaným diskovým polem rackového provedení kompatibilním s virtuální platformou VMWare. Pro záznam kamer musí být velikost uložiště min. 24TB (například 8*4TB HDD, RAID5+Spare).

Jako jádro kamerového systému je požadováno softwarové řešení v rozsahu 29 licencí pro kamery, umožňující monitorování, nahrávání a ovládání IP kamer. Je požadováno rozšíření licenci pro záznamový software, který umožňuje nahrávat až 300 IP kamer nebo webserverů na jeden server a jehož pomocí, se na server připojí současně neomezený počet online klientů. Systém musí podporovat ONVIF kamery, High Definition Stream Management (HDSM)™, záznam Profi řady kamer, ukládání pohledů, POS transakce, eMapy a rychlé vyhledávání pomocí náhledů.

Na záznamový software by měl být instalován nadstavbový systém pro pokročilou videoanalýzu. Systém umožňující velmi krátké znázornění dlouhého časového období se zachováním všech aktivit v obraze. Rozlišování objektů podle velikosti, barvy, směru, trajektorie, rychlosti, oblasti a délky výskytu v obraze, nastavení pravděpodobnosti. Výsledná analýza exportovatelná do krátkého videa. Provoz nadstavby rovněž na stávajících serverech FNB ve virtuálním prostředí. Úložiště společné s dodaným diskovým polem pro záznam kamer.

Je požadováno rozšíření licencí v rozsahu 29 kamer s podporou systému na 5 let. Zkušební provoz (po provedení výchozí revize) po dobu min. 14 dní. Kabelové rozvody, napájení a zálohování, jakož i provozní značení **dle dokumentace pro provedení stavby *„Dokumentace datových rozvodů pro zvýšení kybernetické bezpečnosti“* (samostatná příloha v režimu důvěrných informací)**.

Pro zpracování analýzy obrazu je očekáván server s následujícími parametry:

- Pro Server type: Rack mount
- OS: Windows 10 Professional or Windows Server 2016
- CPU: 1 x Intel Xeon Gold 6134 3.2GHz, 3.7GHz
- GPU: 2 x Quadro P4000 / 2 x Tesla T4
- OS drive: 512 GB SSD
- RAM: 128 GB
- Diskové úložiště: 14 TB

Pro Systém jsou dále požadovány následující parametry:

- nízké nároky na síť v architektuře klient-server (přenos pouze toho, co je vidět na obrazovce)
- možnost nahrávat kamery do rozlišení 30MPx
- možnost zobrazit obraz na iOS, Android zařízeních s využíváním digitálního zoomování
- možnost nahrávat 30fps v duálním kodeku
- možnost přemazávat záznam na ½ resp. ¼ snímků
- 256 bitová zašifrovaná komunikace mezi kamerou a serverem
- podpora kodeků MJPEG, H.264, JPEG2000
- možnost spojení neomezeného počtu kamer přes klient-server architekturu
- možnost vytvořit virtuální matici z neomezeného počtu monitorů, ovladatelných pomocí jedné klávesnice a myši
- možnost nahrávat v max. rozlišení a současně v CIF rozlišení kamery při použití kodeku H264
- možnost přemazání max. rozlišení a nahrazení záznamů CIF záznamem při použití kodeku H264
- možnost zahájení spolupráce mezi klientskými stanicemi – odevzdání digitálního zoom kamery jinému operátorovi
- pomoc při vyhledávání událostí na vzdálené ploše, kooperace mezi přihlášenými uživateli
- možnost posunout automaticky alarm na dalšího uživatele v případě nečinnosti
- možnost zablokování optického zoom pro jednotlivé uživatele /skupiny
- plná podpora českého jazyka
- automatický upgrade firmwaru na kamerách a klientských PC
- možnost připojení neomezeného počtu klientů

- možnost spravovat neomezený počet serverů současně z jednoho klienta
- možnost přihlásit se jako klient na neomezený počet server současně
- možnost zvolit si libovolnou kameru z libovolného server současně na jednom klientském PC
- možnost automatického záložního nahrávání kamer na druhý a třetí server při výpadku spojení se serverem nebo při poruše serveru
- možnost připojení neomezeného počtu kamer do jednoho systému
- možnost exportu záznamu v následujících formátech: AVI, JPEG, TIFF, PNG, PDF, WAV
- možnost editace alarmových zpráv s následným odesláním na emailové adresy
- možnost vytvoření vlastních zvukových zpráv, které se při vyvolání alarmu automaticky spustí
- možnost ovládat relé výstupy na kamerách pomocí klientského software
- možnost přepojit systém s Active Directory existující sítě
- možnost změnit datový tok ze serveru přímo na klientovi
- možnost ukládání nadefinovaných pohledů u každého uživatele zvlášť
- možnost označení části záznamu a znemožnění vymazání daného záznamu
- možnost vyhledávání na základě změny v obraze
- možnost vytvoření virtuální PTZ z vícero megapixelových kamer
- vyhledávání v záznamu na základně změny pixelů
- možnost nastavit až 10 sekund před alarmový čas
- možnost úplně vypnout PTZ ovládání na kamerách
- možnost zobrazit webovou stránku přímo v softwaru
- možnost editování velikosti oken na klientské stanici
- systém odolný vůči posunu na letní čas

7 Upgrade firmware telefonní ústředny

Fakultní nemocnice Brno využívá pro zajištění telefonního provozu síť moderních telefonních digitálních ústředen Alcatel Lucent řady OmniPCX Enterprise. Stávající konfigurace zahrnuje tři hlavní samostatné jednotky instalované v areálu Bohunice – Jihlavská 20, Dětská nemocnice – Černopolní 9 a Porodnice – Obilní trh 11 o celkové kapacitě cca 3800 vnitřních linek.

Veškeré požadované sw nástroje musí být pro zajištění ochrany stávajících investic 100% kompatibilní s již provazovanými systémy.

A. Upgrade SW telefonní ústředny Centrálního Velína a tím sjednocení SW ústředen FNB na jednotnou poslední vydanou verzi

Z důvodu garance maximální spolehlivosti síťového řešení telefonních ústředen Fakultní nemocnice Brno platformy Alcatel Lucent, je nutné z důvodů kompatibility zajistit sjednocení SW verze všech digitálních ústředen na poslední SW verzi vydanou výrobcem. Tuto podmínku nyní nesplňuje dedikovaná ústředna Centrálního Velína FNB. Vzhledem k tomu, že se jedná o stávající ústřednu, není možné toto realizovat jinak, než je dáno specifikací níže:

Popis	PN	ks
User software licenses (CC40)		
OmniPCX Enterprise major software upgrade - 1 user	3BA09835JA	50
Alcatel-Lucent OmniPCX Enterprise R12.1 software license	3BA09959JA	1
Software Support Services (NN02)		
ENTERPRISE SPS restart 1 year	3EY10002TA	1
Montáž, naprogramování, zaškolení obsluhy		1

B. Nová telefonní ústředna FNB Netroufalky

Stávající ústředna nezapadá do konceptu telefonní sítě FNB, vzhledem ke svému stáří je nespolehlivá, dochází k výpadkům, neumožňuje dálkovou správu, monitoring, správu tarifních dat a nelze ji příčkou spojit s ostatními ústřednami zadavatele. Vzhledem k plánovanému dalšímu využití objektu je požadována instalace nové digitální telefonní ústředny začleněné do síťového konceptu telekomunikační sítě nemocnice a 100% kompatibilní s ostatními ústřednami zadavatele, tedy Alcatel Lucent řady OmniPCX Enterprise.

Požadovaná kapacita je 16 digitálních portů, 48 analogových portů, 30 IP licencí, 8 systémových telefonů, záložní baterie.

Součástí dodávky musí být také:

- Montáž, naprogramování, zaškolení obsluhy, doprava.
- RACK, Patch panel, patch cord, organizer

C. Výměna záložních baterií hlavních ústředen Fakultní nemocnice Brno

Telefonní ústředny jsou z pohledu napájení připojeny do elektrické sítě Fakultní nemocnice Brno na okruhy zálohované dieselagregáty. Pro garanci funkčnosti telefonních ústředen v době výpadku napájení je nutné zajistit záložní zdroj (baterie) k překlenutí náběhu diesel agregátu. Baterie je nutné dle doporučení výrobce telefonních ústředen měnit v cyklu 5 let. Baterie byly dodány v r 2014, nutná výměna nejpozději v roce 2019.

- Hlavní lokalita: 4 x baterie FWL 12-12
- Vedlejší lokality: 8 x baterie CT12-24
- Práce, doprava, drobný materiál

8 Rozšíření přístupového systému

8.1 Přístupový systém pro rozvaděče

Fyzické zabezpečení 125 ks racků a jejich monitoring

Fyzické zabezpečení racků a jejich monitoring	
Minimální požadavky	**Splňuje (ano/ne)**
Řešení pro přístupový systém (vyklápěcí klika, RFID čtečka pro standard Mifare DESFire 1K,4K)	
Řízení přístupu (dva elektronické zámky pro otevírání předních a zadních dveří rozvaděče)	
Možnost osadit magnetické čidlo pro druhé dveře v racku	
Komunikační rozhraní – Ethernet/IP, email, SNMP	
Centrální správa všech 125ks zařízení	
Podpora skupin racků a skupin uživatelů	
Podpora minimálně 100 interních účtů	
Synchronizace lokálních účtů a oprávnění s centrální databází	
Podpora statistik, logování přístupu ke každému racku, alarm každého otevření dveří	
Možnost budoucího rozšíření pro monitoring teploty a vlhkosti v racku, předávání informací protokolem SNMP	
Schopnost pracovat offline i bez konektivity k centrální správě	

8.2 Čipové karty

V rámci řešení vícefaktorové identifikace uživatelů zadavatel požaduje dodat **6500** ks multifunkčních identifikačních karet.

8.2.1 ID karty s podporou PKI, EMV pure a Mifare

Požadovaná podpora minimálně těchto certifikačních autorit:

Poskytovatelé	Kvalifikované služby
Česká pošta, s. p. IČO: 47114983, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek. Vydávání prostředků pro bezpečné vytváření elektronických podpisů.
eIdentity a. s. IČO: 27112489, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.

8.2.2 Hybridní karta: contact PKI/contactless EMV

Je požadována dodávka typu hybridních QSCD čipových karet s podporou bezkontaktního čipu a kontaktním čipem s personalizovanou PKI aplikací. Formát čipové karty ID-1. Bezkontaktní čip zároveň musí sloužit pro identifikaci držitele v rámci bezkontaktních systémů organizace.

Zařízení musí podporovat vytváření kvalifikovaného elektronického podpisu dle nařízení eIDAS a disponuje platnou QSCD certifikací. Současně dovoluje v kontaktním čipu hostovat certifikáty z jiných certifikačních autorit než akreditovaných, zejména jde o podporu uložení doménových certifikátů.

Vlastnosti kontaktního čipu:

Všechny operace s privátním klíčem musí probíhat uvnitř čipu – klíč neopustí prostředí karty. Privátní klíč uložený na kartě nelze z karty vyexportovat. Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu. Karta musí podporovat ověření původu klíče prostřednictvím výpočtu kryptogramů na kartě a jeho komparaci s výpočtem na serveru. Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány (např. ze souborů PkcS#12). Podpora importu klíčů musí být integrována v ovládacím software ke kartě a nevyžaduje tak pořízení jiné aplikace. Zejména se jedná o proces bezpečné zálohy šifrovacích klíčů. Ke klíčovým párům lze na kartu uložit i příslušné certifikáty.

Mimo kvalifikované podepisování karta musí podporovat vytváření kvalifikované pečeti podle náležitostí nařízení eIDAS. Karta je v souladu se standardem CC EAL5+.

Čipová karta musí být v souladu se standardem EN 419 211 a profily:

Požadavek	Splňuje (ano/ne)
BSI-CC-PP-0059	
BSI-CC-PP-0075	
BSI-CC-PP-0071	
BSI-CC-PP-0072	
BSI-CC-PP-0076	

Soulad s technologickými standardy:

- ISO 7816 4, 5, 6, 8, 9, 15

a. PC/SC (interoperabilita čteček)

b. CCID

- Javacard, GlobalPlatform (platforma čipu)
- Smart card minidriver Specification
- MS cryptoaPi (caPi)/ (caPi2), cryptography next Generation (cnG)
- Microsoft Base Smart card crypto Provider/microsoft Smart card key Storage Provider
- PKCS#11
- MS Xenroll / certenroll (generování žádostí o certifikáty)

Kontaktní čip musí splňovat specifikaci a formáty běžných pro toto zařízení:

Požadavek	Splňuje (ano/ne)
PKCS#7 (formát zabezpečení dat)	
PKCS#12 (import klíčů)	
PKCS#10 (žádosti o certifikáty)	
X.509 (certifikáty)	
S/mime (zabezpečení e-mailových zpráv)	
EN 419212 (former EN 14890) (formát el. podpisu)	

Podporované budou minimálně kryptografické algoritmy:

Požadavek	Splňuje (ano/ne)
Symetrické: 3DES, AES 128, 192, 256	
Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
RSA: 1024, 2048 bitů (generování i import), 3072, 4096 bitů (pouze import, nelze generovat)	
Eliptické křivky: NIST P-224, P-256, P-384, P-521	

PKI aplikace musí podporovat:

Vytváření elektronického podpisu na bázi certifikátů ve formě:

Požadavek	**Splňuje (ano/ne)**
kvalifikovaného elektronického podpisu	
zaručeného elektronického podpisu	
uznávaného elektronického podpisu	
Podpora pro vytváření kvalifikované elektronické pečetě	
jiné formy elektronického podpisu	

Dvoufaktorovou autentizaci na bázi certifikátů X.509 do PC (prostředí Microsoft AD/Smartcard Logon, webových služeb, VPN, aplikací), možnost uložení certifikátů třetích stran, zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů), archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů, generování a práce s RSA a ECC klíči v čipu, podpora PUK pro odblokování PIN a QPIN, zablokování PIN a QPIN resp. PUK po opakovaném chybném zadání PIN/QPIN, resp. PUK (konfigurovatelný počet pokusů), podpora změny PIN pomocí standardního logon desktopu MS Windows, od verze Win7.

Čipová karta musí podporovat získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů. Tato služba předpokládá napojení na akreditovaného poskytovatele kvalifikovaných služeb.

Ověření původu klíče pro kvalifikovaný podpis musí karta podporovat na bázi principu kryptogramu vygenerovaného kartou a jeho ověření na serveru akceptované více akreditovanými CA v ČR.

Dodaná karta musí min. podporovat následující počet míst pro uložení klíčů a rozložení paměti karty:

- Minimální počet pro uložení klíčů je 16 kontejnerů.

- Přičemž do kontejnerů je možné uložit různé délky klíčů příslušného algoritmu, a to v podporované délce:

a. RSA / kvalifikovaný: 4x

b. RSA / komerční: 6x

c. ECC / kvalifikovaný: 3x

d. ECC / komerční: 3x

Karta musí podporovat dvě oblasti pro uložení kvalifikovaných a nekvalifikovaných certifikátů, přičemž každá oblast má svůj PIN s ohledem na rozlišení pinové politiky:

- PIN (komerční):

a. rozsah 4 - 16 číslic
b. nastavena 4-místná konstantní hodnota
c. počet neúspěšných pokusů před zablokováním: 3
d. není vyžadována změna před prvním použitím PIN
e. PIN je možné pro operaci s komerčními certifikáty cachovat
f. lze odblokovat pomocí PUK
- QPIN (kvalifikované):
a. rozsah 5 - 16 číslic
b. nastavena 5-místná konstantní hodnota
c. počet neúspěšných pokusů před zablokováním: 3
d. je vyžadována změna před prvním použitím QPIN
e. lze odblokovat pomocí PUK
- PUK:
a. rozsah 8 - 16 číslic
b. nastavena 8-místná konstantní hodnota
c. počet neúspěšných pokusů před zablokováním: 5
d. není vyžadována změna před prvním použitím QPIN
e. nelze odblokovat

Vlastnosti bezkontaktního čipu:

Do těla karty jsou integrovány dva typy bezkontaktních čipů:

technologie Unique 125kHz
technologii 13,56 MHz Mifare DESFire 4K.

Příprava/stav dodané karty:

Inicializovaná PKI aplikace s PIN, QPIN a PUK. Konstantní QPIN s vynucením změny na novou hodnotu. PIN a PUK dynamická hodnota vytištěná v diskrétní zóně přiloženého PIN formuláře a zalepena do distribuční obálky. Základní design těla karty podle požadavků Zadavatele. Personalizace karty zaměstnaneckými údaji bude probíhat v rámci organizace. Předání seznamu personalizovaných karet, pro import do evidence. U každé karty bude uvedena hodnota UID bezkontaktního čipu, číslo kontaktního čipu.

Bezkontaktní čip je dodán v tovární konfiguraci (bez zápisu dat či klíčů).

Ovládací software pro karty:

Čipové karty budou dodány s ovládacím software pro integraci kontaktního čipu karty do operačního systému. Použití ovládacího software nebude vyžadovat dokoupení servisní podpory nebo další aplikace k licenci karty. Vlastnosti ovládacího software:

Ovládací software musí podporovat přenos veřejných dat z aplikace karty do centrální evidence. Jedná se zejména o obsah čipu, změny PIN, QPIN, PUK a kdo změny na kartě provádí. Získána data budou sloužit pro sestavení kompletního obrazu karty v organizaci v průběhu jejího života. Tato součást bude součástí každé pracovní stanice, kde se karta používá.

Odpovídá specifikaci Microsoft Smart Card minidriver for Windows Base CSP V7.07 anebo novější.

Podpora Microsoft CryptoAPI, Microsoft CNG i PKCS#11.

Použití na OS:

MS Windows 7 anebo vyšších verzích; verze pro 32-bitové i 64-bitové systémy.

Linux – LTS (Long Term Support) verze pro Ubuntu a RHEL (PKCS#11).

OS X (PKCS#11).

Mobilní zařízení s OS Android a iOS – implementována je podpora minimálně 2 výrobců BT čteček.

8.2.3 Aplikace pro správu čipových karet

Základním předmětem dodávky je dodat SW aplikace pro správu hybridních karet a certifikátů s licencí na dobu neurčitou. Vybudovat hierarchii doménových certifikačních autorit. Certifikační autority postavené na platformě MS Windows Server a umožnit z nich výdej požadovaných infrastrukturních a uživatelských certifikátů.

Pro podporu práce s kartami a certifikáty dodá dodavatel aplikace, které budou podporovat níže popsané funkce:

Registrační pracoviště pro doménovou autoritu, správa a potisk karet

Pro správu karet bude dodána aplikace (subsystém), která:

- Implementuje centrální evidenci provozovaných karet, jejich držitelů, stavů a historie.
- Obsahuje auditní informace o bezpečnostně citlivých operacích, které byly prováděny s provozovanými kartami. (Např. vydání / odebrání / ztráta / nalezení karty, apod.). Auditní údaje musí obsahovat také čas provedené operace a informaci o uživateli, který danou operaci provedl či autorizoval.
- Obsahuje informace o certifikátech, vydaných na provozované čipové karty. V jednom systému jsou evidovány jak certifikáty vydané akreditovaným poskytovatelem, tak interní doménovou certifikační autoritou.
- Opírá oprávnění přístupu k informacím v evidenci o uživatelské oprávnění v Active Directory. (Oprávnění přístupu do evidence karet jsou řízena na základě členství uživatelů v definovaných doménových skupinách.)

- Umožňuje vyhledávat a prohlížet informace v evidenci karet.
- Podporuje vydávání certifikátů z interní certifikační autority, v doméně MS Windows. Certifikáty jsou vydávány na základě definovaných šablon (certificate template). Podporovány musí být obvyklé mechanismy vydávání certifikátů v doméně, vč. archivace šifrovacích klíčů, certifikáty pro Smartcard Logon, automatické doplňování údajů do certifikátů z Active Directory, apod…
- Podporuje funkce pro import informací o nově dodaných kartách. (Soubory s informacemi o kartách bude dodavatel dodávat spolu s každou množinou nově dodaných karet.)
- Podporuje dotisk osobních údajů na karty, jako součást procesu přidělení karty držiteli. Alespoň část informací o držiteli karet bude aplikace čerpat přímo z Active Directory. (Držitelé karet budou mít účet v Active Directory.) Provedení dotisku proběhne na pracovišti správy karet, v prostorách nemocnice. Dotisk bude zahrnovat pouze osobní údaje držitele, popř. pracovní zařazení apod.
- Vhodným způsobem podporuje navržené stavy životního cyklu karet a usnadňuje tím úkony pro správu karet.
- Běží na operačním systému MS Windows 7 nebo vyšších verzích; verze pro 32-bitové i 64-bitové systémy
- Je lokalizována do češtiny.

8.3 Čtečky karet

V rámci řešení vícefaktorové identifikace uživatelů zadavatel požaduje dodat 2500 ks čtecích zařízení karet integrovaných do plnohodnotné PC klávesnice (připojení k PC přes USB port, délka kabelu 180 cm, odpovídající vestavěná čtečka čipových karet, česká lokalizace, numerická klávesnice).

8.4 Dvou faktorová autentizace

Zadavatel hodlá do své infrastruktury doplnit bezpečnostní vrstvu, vybudovanou na bázi PKI.

Implementace PKI by měla doplnit bezpečnostní funkce, jako jsou např.:

- Zabezpečení komunikace (SSL apod…)
- Autentizace serverů vůči počítačům a uživatelům

Část PKI je určena pro vydávání uživatelských certifikátů na čipové karty a následné zavedení 2-faktorové autentizace (náhrada autentizace jménem / heslem).

Pro implementaci PKI je zvolena technologie, které je nativně podporována v prostředí Active Directory: certifikační služba na platformě MS Windows Server. Díky této technologii bude dosaženo podstatného navýšení bezpečnosti s minimálními náklady na integraci.

V rámci prostředí bude vybudována hierarchie certifikačních autorit. Vybudované certifikační autority budou podřízeny pod jedinou kořenovou CA.

- V prostředí budou provozovány 2 vydávající CA:
  - jedna pro vydávání uživatelských certifikátů,
  - druhá pro vydávání certifikátů serverům, počítačům a infrastruktuře
- K certifikačním autoritám bude existovat provozní i bezpečnostní dokumentace.

Pro zvýšení úrovně zabezpečení budou do prostředí implementovány 2 vydávající certifikační autority na platformě MS Windows Server:.

- „technologická" CA pro vydávání certifikátů pro počítače, servery a infrastrukturu
- „uživatelská" CA, pro vydávaní uživatelských certifikátů na čipové karty

Díky vydaným certifikátům bude moci infrastruktura využívat kryptografické zabezpečení při komunikaci počítač – počítač, a také při komunikaci uživatel – systém.

Vybudování „uživatelské" CA umožní vydat uživatelské certifikáty na čipové karty a zavést 2-faktorovou autentizaci uživatelů do informačních systémů zadavatele. Uživatelská CA rovněž umožní vydávat šifrovací uživatelské certifikáty.

Všechny vydávající CA budou mít vydán certifikát z kořenové CA, která bude offline a nebude chráněna HW prostředky.

8.4.1 Provozní a bezpečnostní koncept PKI zadavatele

Bude zpracován dokument cílového konceptu PKI v prostředí zadavatele. V rámci konceptu budou navrženy jednotlivé aspekty PKI:

- Hierarchie CA
- Infrastruktura PKI
- Bezpečností perimetry a jejich separace
- Vlastnosti a parametry jednotlivých CA
- Bezpečnostní koncept PKI, role, oprávnění, ochrana aktiv, využití HSM
- Typy vydávaných certifikátů a vlastnosti příslušných šablon certifikátů
- Parametry certifikačních autorit (1 CA kořenová, 1 CA pro vydávání uživatelských certifikátů a 1 CA pro vydávání certifikátů pro počítače, servery, infrastrukturu)
- Definice distribučních bodů CRL a certifikátu CA
- Návrh konceptu zálohování CA

Koncept PKI bude v souladu s bezpečnostními politikami zadavatele. Podle navrženého konceptu PKI budou následně implementovány PKI subsystémy do prostředí zadavatele.

8.4.2 Instalace, konfigurace a zprovoznění certifikačních autorit

Do prostředí budou implementovány 2 certifikační autority: 1 CA pro vydávání uživatelských certifikátů a 1 CA pro vydávání certifikátů pro počítače, servery, infrastrukturu.

- Instalace hostitelského operačního systému MS Windows Server

(Licenci operačního systému zajistí zadavatel)

- Instalace certifikačních služeb
- Vydání certifikátu CA z kořenové CA
- Konfigurace certifikačních služeb podle schváleného konceptu PKI
- Implementace distribučních bodů CRL a certifikátů CA
- Vytvoření vztahu důvěry, propagace certifikátů CA v rámci forestu
- Definice šablon certifikátů a jejich oprávnění
- Uvedení certifikačních autorit do rutinního provozu, ověření fungování

Certifikační autority budou implementovány v módu issuing entrprise CA na platformě MS Windows Server.

CA budou pravidelně zálohovány. Technologii zálohování zajistí zadavatel.

8.4.3 Dokumentace k CA

Schválený koncept PKI bude rozpracován do provozních a bezpečnostních dokumentů, určených specificky pro prostředí zadavatele:

- Provozní dokumentace a havarijní plány. Návod pro správce certifikační autority, uvádí informace: jak udržet CA v chodu, jaké profylaktické a provozní operace provádět, co dělat, když se CA porouchá či havaruje, jaké nouzové postupy použít.
- Certifikační politiky. Formální dokument v souladu s RFC 3647, uvádí informace o typech vydávaných certifikátů, pravidla pro vydávání, participující subjekty, atd. V jednom dokumentu certifikační politiky budou uvedeny všechny typy certifikátů, vydávaných z dané CA. Celkem tedy budou dodány 2 dokumenty s certifikačními politikami (uživatelská CA a CA pro infrastrukturu).
- Certifikační prováděcí směrnice. Formální dokument v souladu s RFC 3647, uvádí informace o provozu CA, typech certifikátů, zabezpečení, atd… V jednom dokumentu certifikační prováděcí směrnice budou uvedeny všechny typy certifikátů, vydávaných z dané CA. Celkem tedy budou dodány 2 dokumenty s certifikačními prováděcími směrnicemi (uživatelská CA a CA pro infrastrukturu). Certifikační prováděcí směrnice bude podrobnější než certifikační politika.

8.4.4 Online zálohování dat certifikační autority

Pomocí systému budou data CA zálohována do MS SQL databáze. Součástí systému je mechanismus pro obnovu chybějících dat z MS SQL do CA. Do stejné DB budou zálohována data obou CA (pro uživatele a pro infrastrukturu). Součástí systému je publikační modul, který exportuje data z CA.

8.4.5 Kořenová CA

Kořenová CA bude offline a ochrana soukromého klíče probíhat SW prostředky. Ke kořenové CA budou také doplněny *Certifikační politiky* a *Certifikační prováděcí směrnice* tak, aby i v dokumentační bázi bylo dosaženo stejné kvalitativní úrovně jako u podřízených CA. Kořenová CA bude vydávat certifikáty pro podřízené CA.

9 Virtualizace sítě, mikrosegmentace

Dodávka systému virtualizace sítě za účelem zajištění jednak segmentace sítě až do úrovně izolace jednotlivých virtuálních strojů do vlastních segmentů sítě a dále zajištění řízení komunikace pomocí politik (a také tagů, příslušností do skupin atd.) s integrací na perimetrový Next Generation Firewall s uplatněním bezpečnostních politik a kontroly komunikace i uvnitř datového centra nejen pouze na perimetru.

Požadavky na systém virtualizace sítě na úrovni stávající virtualizační platformy VMware:

Požadavek	**Splňuje (ano/ne)**
Licence pro 48 CPU.	
Musí umožnit sběr informací z operačních systémů virtuálních strojů	
Možnost sledovat spuštěné procesy uvnitř virtuálních strojů a jejich vlastníka	
Rozpoznání aplikace na sedmé vrstvě	
Možnost nastavení firewall pravidel pro konkrétního uživatele Remote desktop spojení dle jména nebo příslušnosti ke skupině, nikoliv pouze IP adresy serveru	
Monitoring a sběr informací o toku dat v ceně řešení	
Vizualizace toku dat mezi virtuálními stroji včetně informace o použitých FW pravidlech, routovacích informací, průchozích bodech apod.	
Analýza toku dat a návrh FW pravidel s možností exportu do souboru	
V ceně řešení nástroj pro migraci mezi DC a automatizovaného převodu VMtools, sítí apod. (adaptace na nové prostředí)	
Distribuovaný L4 load balancing	
V ceně řešení WAN optimalizace s možností inteligentního balancování zátěže přes několik linek	

10 Rozšíření Work Space One

Bezpečná centrální distribuce aplikací na koncová zařízení bez možnosti uživatelských změn s řízením přístupů k aplikacím. Doplnění stávající licence VMware WSP One o 1200 uživatelů.

11 Nástroj pro zobrazení a vyhodnocení toků na virtualizované síťové infrastruktuře

Za účelem dosažení plné viditelnosti na síťové úrovni včetně možností statistik i vyhodnocování a reakci na bezpečnostní události a neobvyklý provoz je požadován nástroj pro správu a vizualizaci provozu na síťové vrstvě v Software Defined Datacenter při využití Software Defined Networking ve spolupráci se stávající nasazenou virtualizační technologií VMware.

Nabízený produkt musí zajistit plnou kompatibilitu s nástrojem pro virtualizaci a mikrosegmentaci sítě (viz. **Error! Reference source not found.**).

12 Nástroj pro správu IP adresních prostorů

IP Adress Management Systém bude sloužit pro zajištění správy adresního prostoru v datové komunikační síti a pro zajištění kompletní viditelnosti na síti. Jedná se tedy o kompletní centrální přehledový a kontrolní nástroj pro správu IP adresních prostorů v úplném síťovém prostředí FN Brno.

Požadované vlastnosti nástroje jsou:

Požadavek	**Splňuje (ano/ne)**
Správa IP adresního prostroru FN Brno	
Automatické sledování ip adres	
Integrace na WindowsAD, DHCP, DNS - Microsoft, Cisco, BIND	
Integrace na vmware	
Podpora pro REST api	
Držení historie IP adres	
Dokumentace a mapování síťové infrastruktury;	
Vyhodnocení a kontrola stavu síťových protokolů a technologií;	
Kontrola provozního záměru a odhalování skrytých rizik;	
Automatické diagramy a vizualizace síťové infrastruktury;	
Dynamická vizualizace směrovacích protokolů a přepínaných instancí;	
Vyhodnocení změn a sledování historického vývoje sítě;	
Identifikace zdrojů výkonnostních nedostatků a ztrátu produktivity;	
Usnadnění celkové správu přenosové infrastruktury;	
Minimální počet zařízení v sítí pro licencování je 5000	

13 Analytické práce v oblasti bezpečnosti

Účastník zpracuje Analýzu rizik, která bude zahrnovat revizi dosud identifikovaných a identifikaci nových aktiv, hrozeb a zranitelností, z nichž bude určena míra bezpečnostních rizik, a na jejich základě budou doporučena vhodná bezpečnostní opatření. Analýza rizik bude realizována nejen v rozsahu identifikovaných a nahlášených informačních systémů základních služeb (dále rovněž jen ISZS), ale v rámci celého informačního systému FN Brno, a to vzhledem k návaznostem ISZS a celkovou efektivitu řešení. Součástí zakázky je vytvoření nebo aktualizace obsahu bezpečnostní dokumentace tak, aby byla v souladu s požadavky zákona č. 181/2014 Sb., Zákon o kybernetické bezpečnosti (dále rovněž jen ZoKB), vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále rovněž jen VyKB), Varováním Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17.12.2018 před použitím technických nebo programových prostředků následujících společností, včetně jejich dceřinných společností Huawei Technologies Co., Ltd., a ZTE Corporation a souvisejících dokumentů a zároveň umožnila přípravu na certifikaci ISO 27000.

Dodavatel v prostředí zadavatele naimplementuje Systém managementu bezpečnosti informací (dále jen ISMS).

Dodavatel se zavazuje, že implementovaný systém bude připraven na získání certifikace dle ISO 27001.

Zadavatel požaduje provedení implementačních kroků v následujícím rozsahu:

Implementační požadavky ISMS
Analýza rizik a jejich dokumentace
Ustanovení, definice a zdokumentování systému ISMS
Implementace vybraných opatření
Příprava na certifikaci
Proces certifikace

13.1 Analýza rizik a jejich dokumentace

Dodavatel realizuje analýzu rizik v rozsahu a dle požadavků ISO/IEC 27001.

Dodavatel provedená analýza rizik bude rozdělena dle následující struktury:

- Identifikace a hodnocení aktiv
- Identifikace a hodnocení hrozeb
- Identifikace a hodnocení zranitelností
- Stanovení hodnoty rizika pro jednotlivá aktiva

Požadavek	Splnění (ano/ne)
Dodavatel se zavazuje, že provedená analýza rizik bude založena na principech norem ISO/IEC 27001, ISO/IEC 27005 a ISO/IEC 31000 a bude v souladu s požadavky ZoKB a VyKB a Varováním Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17.12.2018	
Dodavatel se zavazuje ohodnotit aktiva z hlediska jejich důvěrnosti, dostupnosti a integrity.	
Dodavatel se zavazuje na identifikovaná rizika vytvořit plán zvládání rizik, který bude obsahovat podrobný plán zavádění opatření do prostředí zadavatele.	

Ustanovení, definice a zdokumentování systému ISMS

Dodavatel vypracuje pro podmínky zadavatele dokumentaci, která bude specifikovat a definovat systém ISMS zadavatele a bude připravena pro certifikaci dle normy ISO/IEC 27001.

Dodavatel zpracuje dokumentaci v následujícím rozsahu:

Požadavek	Splňuje (ano/ne)
Politika bezpečnosti informací	
Organizace bezpečnosti práce	
Bezpečnost lidských zdrojů	
Řízení aktiv	
Řízení přístupu	
Kryptografie	
Fyzická bezpečnsot a bezpečnsot prostředí	
Bezpečnost provozu	
Bezpečnost komunikací	
Akvizice, vývoj a údržba systému	
Vztahy s dodavateli	
Řízení incident bezpečnosti informací	
Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací (Hvavrijní plan a plan obnovy	
Souhlas s požadavky	
Prohlášení o aplikovatelnosti	
Bezpečnostní příručka pro uživatele	
Bezpčenostní příručka pro administrátora	
Formuláře pro vedení nezbytných evidence a záznamů (registry bezpečnostních incident, registry neshod, registry rizik apod.	

Dokumenty a postupy pro řízení ISMS (řízení dokumentů a záznamů, provádění interních auditů, řízení náprvných a preventivních opatření, řezení neshod, pravidla pro přezkoumání systému)	
Další dokumenty a postupy nezbytné pro efektivní fungování a certifikování systému ISMS	

Implementace vybraných opatření

Požadavek	**Splňuje (ano/ne)**
Dodavatel se zavazuje realizovat bezpečnostní školení uživatelů v rozsahu 5 člověkodní pro vybrané osoby a v souladu s požadavky § 9 VyKB.	
Dodavatelem realizované školení bude provedeno lektorem, který je pro tuto činnost dostatečně kompetentní. Tuto kompetenci doloží dodavatel referencí z realizovaných školení.	
Dodavatel se v rámci implementace vybraných opatření zavazuje, poskytnout zadavateli konzultace při jejich zavádění (např. v podobě konzultace konfigurace a nastavení systému, změny v infrastruktuře, konzultace při výběru nových technických řešení apod.	
Jako jedno z nutných opatření bude implementace klasifikace informaci. Požadujeme implementovat SW pro klasifikaci informací formou doplňku pro aplikace MS Office, který jednoduchou formou umožní doplnit klasifikaci do dokumentu.	

Požadavky na poptávaný SW, který umožní realizovat směrnici o klasifikaci informací organizace:

Požadavek	**Splňuje (ano/ne)**
Požadujeme doplněk do všech aplikací sw Office včetně poštovních kientů.	
Možnost konfigurace tříd klasifikace dle interní dokumentace.	
Vkládání viditelné značky do dokumentu a současné uložení klasifikačních informací do metadat souboru.	
Možnosti nastavení formátu klasifikační značky (velikost, font, umístění, barva apod.).	
Vynucování klasifikace (uživatel nemůže dokument uložit bez klasifikace).	
Manuální i automatická klasifikace dle obsahu.	
Možnosti efektivní a snadné klasifikace již existujících dokumentů.	
Vynucení ochrany klasifikovaných informací. SW musí umět spolupracovat s případným SW na ochranu informací (DLP řešení, šifrovací nástroje, RMS apod.).	
Reportovací nástroje.	

Integrace s Windows Explorer a kontextovým menu.	
Logování klasifikace včetně informací o uživateli, který klasifikaci provedl. Možnost napojení na SIEM řešení nebo centrální logování.	
Integrace s AD.	

V rámci nasazení produktu pro klasifikaci informací požadujeme nasazení v následujícím rozsahu:

Požadavek	**Splňuje (ano/ne)**
Analýza prostředí a návrh nasazení.	
Dodávka licencí SW pro kasifikaci informací pro klasifikaci dat pro celkově 8000 stanic.	
Instalace v testovacím prostředí pro pilotní provoz.	
Školení administrátorů a obsluhy.	
Dodávka dokumentace	
Podpora plošného nasazení.	
Servisní podpora v českém jazyce v rámci pilotního provozu i v produkci.	
Integrace s navazujícími systémy (SIEM/centrální logování, DLP atd.).	

Příprava na certifikaci

Dodavatel se zavazuje realizovat v prostředí zadavatele systémový (interní) audit.

Dodavatel zpracuje auditní zprávu z interního auditu, která bude sloužit certifikační autoritě jako jeden z podkladů.

Proces certifikace

Dodavatel se zavazuje být přítomen v průběhu certifikačního auditu zadavatele a poskytnou maximální možnou součinnost zadavateli.

Dodavatel se zavazuje poskytnout následnou pomoct při odstraňování případných neshod z certifikačního auditu.

13.2 Návrh bezpečnostních politik pro BYOD a mobilní zařízení

Požadavek	**Splňuje (ano/ne)**
Dodavatel vytvoří politiku pro mobilní zařízení. Tato politika musí být v souladu s interními politikami, směrnicemi a nařízeními.	
Dodavatel v rámci politiky definuje:	

○ Typy zadavatelem používaných mobilních prostředků, včetně speciálních mobilních zařízení, pro které bude platit zvláštní režim používání ○ Kategorie vlastnictví mobilních prostředků ○ Práci s mobilními prostředky ○ Práce se speciální kategorií mobilních zařízení ○ Ochranu dat na mobilních prostředcích ○ Zálohování mobilních zařízení ○ Vzdálený přístup a zabezpečení vzdáleného přístupu	
Dodavatel jako součást politiky mobilních zařízení definuje pravidla a povinnosti pro případ použití vlastního zařízení pro pracovní účely (dále jen BYOD).	
Dodavatel pro speciální kategorii mobilních prostředků definuje zabezpečení v podobě: ○ Geolokační politiky definující: ▪ povolený pohyb s daným zařízením ▪ implementace a monitorování geolokační politiky ○ Speciální politiky pro práci s tímto typem mobilních zařízení	
Dodaným výstupem bude: textový editor ve formátu .doc/.pdf, ve kterém bude definována politika mobilních zařízení obsahující výše uvedené.	
Dodavatel se zavazuje, že veškeré navržené politiky budou použitelné při implementaci technologických řešení pro správu mobilních zařízení.	

13.3 Tvorba procesu pro řízení bezpečnostních incidentů

Dodavatel vytvoří na proces pro řízení bezpečnostních incidentů dle potřeb a pro podmínky zadavatele. Proces řízení incidentů poskytne obecný postup řešení bezpečnostních incidentů. Tento proces bude následně dodržován v jednotlivých příručkách pro řešení incidentů.

Požadavek	**Splnění (ano/ne)**
Dodavatel garantuje soulad procesu s mezinárodními standardy pro danou oblast. Zejména se standardy: ○ ISO/IEC 27035 ○ ITIL ○ NIST ○ OWASP ○ a doporučeními organizace SANS	
Dodavatel garantuje, že jím vytvořený proces bude v souladu s interními politikami, směrnicemi a nařízeními, které se na tuto oblast váží.	

Dodavatel v rámci tvorby procesu identifikuje slabá místa, která by mohla funkčnost procesu řízení bezpečnostních incidentů ohrozit. Dodavatel zejména posoudí: ○ Smluvní vztahy organizace se třetími stranami, které by mohly mít vliv na funkčnost procesu řízení bezpečnostních incidentů. Zejména dodavatel posoudí smluvně definované reakční časy uvedené v jednotlivých smlouvách. ○ Vazby mezi jednotlivými odděleními zadavatele s ohledem na reakční kroky procesu řízení bezpečnosti incidentů.	
V případě identifikace slabých míst dodavatel vytvoří návrh vedoucí k optimalizaci a zefektivnění procesu řízení bezpečnostních incidentů.	
Dodavatel pro proces řízení bezpečnostních incidentů vytvoří v souladu kategorie bezpečnostních událostí a incidentů, na základě, kterých bude stanovena kritičnost jednotlivých incidentů.	
Dodavatel vytvoří metriky pro klasifikaci bezpečnostních incidentů a tyto metriky naimplementuje do SIEM řešení	
Dodavatel v kooperaci se zadavatelem navrhne podobu dohody o úrovni poskytování služeb (dále jen SLA) pro jednotlivé zadavateli poskytované služby. SLA budou stanoveny na úrovni kategorií bezpečnostních incidentů.	
Dodavatel v kooperaci se zadavatelem navrhne podobu dohody o úrovni provozních služeb (dále jen OLA), která bude v souladu se stanovenými SLA.	
Dodavatel v kooperaci se zadavatelem navrhne podobu dohody o úrovni provozních služeb (dále jen OLA), která bude v souladu se stanovenými SLA.	
Dodavatel v kooperaci se zadavatelem navrhne podobu podpůrných smluv (dále jen UC) pro jednotlivé externí dodavatele služeb, která rovněž bude obsahovat dohodu o dodávkách.	
Dodavatel v kooperaci se zadavatelem vytvoří metriky pro hodnocení kvality dodávané služby. Tyto metriky pak dodavatel implementuje do příslušného řešení (SIEM případně Service Desk).	
Dodavatel se zavazuje vytvořit proces pro obohacování analýzy rizik pro případ identifikace rizika plynoucího z poskytování služeb.	
Dodavatel proces pro obohacování analýzy rizik zautomatizuje prostřednictvím nástroje pro správu a vyhodnocení rizik, dle specifikací uvedených dále v textu.	
Dodavatel jako součást procesu řízení bezpečnostních incidentů navrhne komunikační proces. Dodavatel jako součást tohoto procesu vytvoří: ○ komunikační matice obsahující veškeré potřebné informace o jednotlivých členech, kteří jsou do procesu řízení bezpečnostních incidentů zainteresováni;	

○ eskalační proces, ve kterém budou stanoveny přesné kroky, jak v případě eskalace postupovat, včetně časových intervalů, kdy k eskalacím musí dojít; ○ podobu a obsah reportů pro jednotlivé úrovně managementu.	
Dodavatel garantuje funkčnost veškerých navržených procesů.	
Dodavatel vytvoří na implementované Use case uživatelské příručky k řešení daných incidentů (dále jen příručky nebo také guidelines). Tyto příručky budou v souladu s vytvořený procesem řízení bezpečnostních incidentů a politiky, směrnice a nařízení zadavatele. Dodavatel se zavazuje zpracovat guidelines v rozsahu: ○ Na každý vytvořený Use case bude existovat jedna příručka popisující jeho řešení. ○ Guidelines budou respektovat a dodržovat vytvoření proces pro řízení bezpečnostních incidentů a všechny jeho pod části. ○ Dodavatel vytvořené guidelines importuje do databáze (Service Desk), kde k těmto guidelines budou přistupovat jednotlivý operátoři. ○ Dodavatel vytvoří obecnou strukturu guidelines (šablonu), která bude obecně aplikovatelná na veškeré dále vznikající. ○ Dodavatel pro jednotlivé guidelines vytvoří identifikátory, které budou stanovovat situace, kdy je nezbytná komunikace s 3. stranami (např. ÚOOÚ, NBÚ, apod.)	
Dodaným výstupem bude: textový editor ve formátu .doc/.pdf, ve kterém budou popsány veškeré výše uvedené body jako samostatné kapitoly.	

14 Perimetrový Next Generation Firewall a Interní firewall

Předmětem poptávky je NGFW řešení skládající se z centrálního managementu, perimetrového firewallu, interního firewallu, ochrany před zero-day malware. Nabízené řešení musí být od jednoho výrobce a realizované v režimu vysoké dostupnosti. Součástí dodávky musí být veškeré licence potřebné pro instalaci a provoz řešení. V rámci dodávky bude požadována instalace a konfigurace dodaného hardwaru a softwaru, dále poskytnutí záruky a podpory na 5 let od výrobce. Nabídková cena musí obsahovat veškeré náklady dodavatele nezbytné k realizaci zakázky.

2x Perimetrový firewall v HA
FW rozhraní: 4x10GBASE-T / SFP+, 8x 1 GBASE-T RJ45
Přibližná propustnost firewallu (Enterprise Mix / Real-World Protocol Mix): 40 Gbps
Min. propustnost firewallu s NGFW – FW, AppControl, IPS, URL filtering, Antivirus, AntiBot, ZeroDay (Enterprise Mix / Real-World Protocol Mix): 8 Gbps
Počet současných spojení: 6 000 000
INFO - průměrná velikost packetu v současném prostředí: 1100 B

Virtuální Interní Firewall s podporou mikro-segmentace
Přímé napojení na vmware NSX 48 CPU

Onpremise Sandbox v HA
FW rozhraní: 2x 10 GBASE-T / SFP+ a možnost rozšíření, 6x 1 GBASE-T RJ45
Přibližná propustnost (Enterprise Mix / Real-World Protocol Mix): 2 Gbps
Počet souborů za hodinu: 2500
INFO - průměrná velikost packetu v současném prostředí: 1100 B

14.1.1 Perimetrový firewall

Požadavek	**Splňuje (ano/ne)**
Požadované funkcionality: • firewall, • IPS, • aplikační kontrola, • URL filtrování, • antivirová a botnet ochrana, • sandbox	
Možnost příchozí a odchozí HTTPS inspekce	
Možnost získávání identit uživatelů z AD bez nutnosti instalace klientů na koncové stanice	

Podpora software agenta na koncové stanice pro přesné získavaní identit, min. pro systémy Windows a Mac	
Automatické vypnutí IPS ochrany v případě přetížení HW (využití CPU nebo fyzické paměti) nad definovanou prahovou hodnotu.	
Detekce a řízení síťových aplikací. Minimální počet rozpoznávaných aplikací, minimálně 8000	
Detekce a řízení síťových aplikací. Minimální počet aplikací/pluginů pro sociální sítě, minimálně 300000	
Podpora URL filteringu na základě kategorizace. Poskytované řešení musí pokrývat min. 85% Alexa top milion sites	
Zablokování již prvního pokusu o stažení zero-day malware (dosud neznámy soubor) přes HTTP/HTTPs komunikaci. Zařízení vykoná akci (povolí nebo zablokuje soubor) až na základě výsledku emulace v sandboxing, ne dřív/detekce (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	
Zablokování již provního výskytu zero-day malware v mailové komunikaci	
Nasazení zero-day ochrany pro mailový provoz v režimu MTA (Mail Transfer Agent)	
Řešení musí detekovat zero-day útok ve fázi exploitace (zneužití zranitelnosti) – ještě přes spuštěním shell kódu a stažením/spuštěním malwaru.	
Řešení musí detekovat ROP a jiné exploitační techniky monitorováním CPU flow	
Řešení musí emulovat soubory vložené v dokumentech .	
Ochrana proti neznámým hrozbám pomocí extrakce zneužitelných komponent z dokumentů ve formě příloh emailové komunikace.	
Propustnost Firewallu, minimálně 40 Gbps (RFC 3511, 2544, 2647, 1242)	
Propustnost IPS, minimálně 20 Gbps	
Propustnost NGFW (Firewall, IPS, Aplikační kontrola), minimálně 12 Gbps	
Propustnost Threat ochrana (Firewall, IPS/IDS, Aplikační kontrola, Antivir, Botnet, URL filtr), minimálně 8 Gbps	
Počet nových spojení za vteřinu (CPS) minimálně 250.000	
Počet současných spojení, min. 6.000.000	
Počet požadovaných fyzických síťových rozhraní, min. 8x 10/100/1000baseT	
Počet požadovaných fyzických síťových rozhraní, min. 4x 10Gb SFP+ rozhraní včetne transceiverů (SR)	
Firewall platforma ve formě samostatné hardware appliance	
Instalace do standardního 19" kabinetu	
Podpora redundance dvou a více zařízení v režimech Active-Active/Active-Standby s automatickou synchronizací Podpora agregace fyzických portů LACP	

Předefinované IPS/IDS politiky	
Out of band management/ILO/LOM	
Redundantní zdroj	
Lokální HDD, min 240GB, v případě výpadku centrálního management log serveru	
Centrální jednotná správa politik z GUI aplikace	
Centrální ukládaní logů, indexování a filtrování logů ze všech bezpečnostních zařízení (firewall, endpoint, ddos)	
Jednotný centrální management: správa politik a analýza logů na stejné VM appliance od výrobce	
Kontrola politik proti chybám a duplicitám	
Podpora administrátorských profilů pro delegaci oprávnění (čtení, zápis)	
Možnost přidělení práv administrátorům jen pro definovaný seznam firewall pravidel v rámci politiky	
Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).	
Práce s bezpečnostními logy – možnost prohledávaních všech typů logů (fw, ips, urlf) v jedné záložce s definováním vlastních permanentních filtrů.	
Možnost rekonfigurace a ladění IPS engine přímo z log výstupů firewallu	
Podpora korelace bezpečnostních logů a incidentů	
Možnost vytváření vlastních pravidel pro vzájemnou korelaci bezpečnostních událostí	
Musí graficky zobrazovat jednotlivé kategorie událostí ve formě interaktivních koláčových a časových grafů	
Musí umožnit definici a uložení vlastního Dashboard panelu pro jednotlivé uživatele	
Musí podporovat automatické reakce na definované bezpečnostní události – minimální akce: poslat email, blokovat zdroj útoku, SNMP trap do interního systému, spustit vlastní skript	
Musí podporovat nástroj pro definici a ruční/automatizované generování reportů	
Minimální počet zpracovaných korelovaných událostí (jeli omezeno licencí, licence pro požadovaný počet korelovaných log záznamů musí být součástí nabídky) – min. 4 miliony událostí za den	
Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní log/event záznamů a indexů (je-li disková kapacita omezena licencí, licence pro požadovanou velikost musí být součástí nabídky) - min. 16 TB	
Management server musí být realizován formou malé lehce přenositelné virtuálky	
Retence logů minimálně 6 měsíců	

Centrální jednotná správa politik z grafické aplikace	
Management musí být fyzicky oddělený od firewall platformy – samostatný HW nebo jako SW licence na virtuálním serveru.	
Konsolidovaný centrální management: správa politik a analýza logů na jedné VM	
Funkcionalita ukládaní, filtrování a korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy Možnost vytváření uživatelsky definovatelných reportů a přehledů a jejich automatické zasílání emailem ve formátu PDF	
Možnost propojení se systémem SIEM třetí strany	
Automatická verifikace politiky (např. proti redundanci, překryvu a inkonzistenci pravidel)	
Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů.	
Podpora administrátorských profilů s možností přidělování práv (read only, red-write, none) pro jednotlivé skupiny administračních funkcí	
Konzistentní modifikace politiky více administrátory najednou, konzistence politik na základě uzamykání pravidel, politik a objektů	
Podpora vnořených politik (sub-politiky)	
Možnost přidělení práv administrátorům jen pro definovoanou skupinu pravidel (sub-politiku) v rámci politiky	
Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky	
Automatická verifikace politiky proti redundanci nebo překryvu pravidel	
Fulltext prohledávaní logů, vráteně technologií indexace pro účinné a rychlé prohledávání logů/záznamů v milionech	
Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).	
Interní certifikační autorita za účelem vydávaní a správy PKI certifikatů pro jednotlivé firewall a VPN (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	
Compliance modul za účelem ověření nastavení firewall politiky proti standardům, min. ISO27001, ISO27002, GDRP (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	
Podpora uchovávaní, zpracování a korelace log záznamů zařízení třetích stran, syslog, snmp (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	
Management log server musí zpracovat min. 20.000 logů/sek	
Minimální historie uložených stavových informací (logů a eventů) 36 měsíců. Minimální podporovaná velikost diskové kapacity pro dlouhodobé ukládaní	

log záznamůa eventů na management serveru (jeli disková kapacita omezena licencí, licence pro požadovanou velikost musí být součástí nabídky), min. 16 TB	
Požadována licence pro centrální správu a dedikovaný reporting, min. 10 firewallů	
Podpora revizí bezpečnostních politik, jejich verzování.	
Podpora auditních informací u změn bezpečnostní politiky (číslo požadavku, kdo provedl změnu)	

14.1.2 Onpremise Sandbox v HA

Požadavek	**Splňuje (ano/ne)**
Zablokování již prvního pokusu o stažení „zero-day" malware (dosud neznámy soubor) přes HTTP/HTTPs komunikaci. Zařízení vykoná akci (povolí nebo zablokuje soubor) až na základě výsledku emulace v sandboxing, ne dřív než detekce (může být zabezpečeno produktem třetí strany, musí být součástí nabídky)	
Zablokování již provního výskytu zero-day malware v mailové komunikaci	
Nasazení zero-day ochrany pro mailový provoz v režimu MTA (Mail Transfer Agent)	
Řešení musí detekovat zero-day útok ve fázi exploitace (zneužití zranitelnosti) – ještě přes spuštěním shell kódu a stažením/spuštěním malwaru	
Řešení musí detekovat ROP a jiné exploitační techniky monitorováním CPU flow	
Řešení musí emulovat soubory vložené v dokumentech	
Ochrana proti neznámým hrozbám pomocí extrakce zneužitelných komponent z dokumentů ve formě příloh emailové komunikace	
Přímá integrace na EndPoint řešení v bodu **Error! Reference source not found. Error! Reference source not found.**	

14.1.3 Interní Firewall ve VMware NSX

Požadavek	**Splňuje (ano/ne)**
Oficialni podpora/certifikace VMware NSX-T	
Oficialni podpora/certifikace VMware NetX API NSX 6.4.3 a vyssi	
Oficialni podpora/certifikace VMware ESXi 6.7 U1 a vyssi	
Zabezpečení komunikací v rámci SDN (Software Defined Networking) na platformě VMware NSX Hypervisor Mode	
Řešení certifikované přímo ze strany výrobce SDN (VMware)	

Dynamická aktualizace objektů bezpečnostních politik na základě automatické importu z prostředí VMware NSX a VMware vCenter	
Podpora importu NSX security groups z vCenter do bezpečnostní politik bez manuálního zásahu v konfiguraci vCenter nebo NSX	
Podpora importu NSX security groups z vCenter do bezpečnostní politik bez manuálního zásahu v konfiguraci vCenter nebo NSX	
Identické označení objektů v rámci NSX (nejen IP adresy jednotlivých VM) a stavových informacích a reportech bezpečnostního řešení (logy, události)	
Integrace do centrální jednotné správy bezpečnosti spolu s ochranou perimetru (fyzickými bezpečnostními branami)	
Jednotná bezpečnostní politika pro fyzické a virtualizované objekty bran s využitím objektů VMware NSX a VMware vCenter	
Podpora pro nastavení virtálních objektů v globální bezpečnostní politice „north-south" appliance bez přesměrování provozu v NSX	
Podpora pro deployment dvou a více bezpečnostních bran na tom stejném esxi nodu	
Řešení musí podporovat fail-open a fail-close pro každou instanci v případě, že je ztracena konektivita do vCenter nebo NSX	
Podpora orchestračních a automatizačních platforem s granulárními profily práv až na úroveň jednotlivých pravidel	
Podpora připojení k více instancím VMware NSX/vCenter současně	
Podpora vMotion & DRS a garantovaná plná stavová inspekce během procesu vMotion	
Podpora vMotion & DRS a garantovaná plná stavová inspekce během procesu vMotion	
Bezpečnostní politiku lze nasadit do prostředí bez nutnosti předchozího přesměrování provozu do NSX	
Sdílení aktuálního bezpečnostního stavu VM formou tagování s platformou NSX pro možnost automatizované reakce (umístění do karantény apod.)	
Řešení poskytne dedikovanou podpolitiku pro mikrosegmentaci s granulárními administrátorskými privilegii	
Možnost o rozšíření i o veřejné Cloud služby (MS Azure, AWS nebo Google Cloud) s jednotným managmentem a jednotnou politikou	
Řešení umožní zobrazení parametrů virtuálního stroje – IP, lokace v datacentru, OS v bezpečnostní politice	
Propustnost NGFW (IPS, APPC) min. 5 Gbps pro jedno CPU	
Nabízené řešení musí licenčně podporovat ESX prostředí pro 48 CPU soketů	

Požadované implementační práce:

- Provedení analýzy nasazení – analýzu stávajícího provozu a následné vytvoření návrhu nových filtračních pravidel pro jednotlivé segmenty sítě dle aktuálních potřeb, technický a procesní návrh
- Příprava
- instalace a základní konfigurace komponent;
    - instalace a konfigurace HW, SW, napojení komponent na management
    - implementace a konfigurace auditního logování a napojení na SIEM a na provozní monitoring
    - vytvoření pravidel, migrace pravidel, nastavení aplikační kontroly a dalších bezpečnostních funkcí v monitorovacím režimu pro první dva měsíce;
    - převedení stávajících ACL do nového řešení
    - Test konfigurovaných komponent;
    - Failover a Failback test dle testovacích navržených DR scénářů;
    - Dokumentace s popisem zapojení, konfigurace, DR plánů, zálohování apod.;
- Provozní nasazení – migrace provozu, ladění a vytvoření politik pro NGFW a Sandbox
    - Nastavení https inspekce
    - Podpora produktivního režimu po dobu 2 měsíců s SLA (Kritický incident 30 minut doba odezvy, 2 hodiny doba vyřešení)
- Post-implementační úpravy
    - Ladění, optimalizace, tuning

15 Ochrana proti DDoS

Ochrana proti DDoS útokům
Rozhraní: 2x 10 GBASE-T / SFP+, 6x 1 GBASE-T RJ 45 - internal fail-open minimálně pro metalické porty
Max kapacita pro mitigaci (propustnost zařízení) 6 Gbps
Maximální ochrana před Flood útokem: 5.5 mil. pps
Počet současných spojení: 3 000 000
Latence: < 60 mikrosekund
INFO - průměrná velikost packetu v současném prostředí: 1100 B

Síťová podpora

Požadavek	**Splňuje (ano/ne)**
Podpora IPv4	
Podpora IPv6 VLAN (802.1Q)	
Podpora agregace portů do bond rozhraní	
Podpora enkapsulace (pro bezpečnostní inspekci) VLAN, MPLS, L2TP, GRE, IP-in-IP	
Plně transparetní na bezpečnostních portech	
Podpora Jumbo rámců	

Metody ochrany proti DoS/DDoS útokům – přehled

Požadavek	**Splňuje (ano/ne)**
Behaviorální analýza síťového provozu s automatickou detekcí útoku a automatickým blokováním pomocí signatur vytvořených na základě této analýzy	
Blokování síťového útoku musí být automaticky zahájeno v řádech desítek sekund (max. do 30 sekund)	
Blokování minimálně těchto útoků pomocí behaviorální analýzy síťového provozu a automatického generování signatur: ○ TCP Flood (FIN, RESET, SYN+ACK and TCP fragment floods) ○ UDP Flood (včetně DNS, RTP, SIP a jiných UDP-based flood útoků) ○ ICMP Flood ○ IGMP Flood	
Podpora SYN-cookies mechanismu Blokování Synflood útoků v asymetrickém prostředí	

Behaviorální analýza DNS provozu pro automatizovanou ochranu před útoky na DNS servery s možností autpomaticky blokovat nelegitimní DNS provoz na úrovni parametrů Doménových jmen, velikosti paketů, destination IP. Nabízené řešení můsí podprovat automatizované vytváření signatur na základě behaviorální analýzy.	
Nabízené řešení musí podprovat blokování Denial Of Services útoků bez degradace prospustnosti legitimního provozu	
Možnost zvolit mezi pouze "monitorováním" a "monitorováním a blokováním"	
Podpora manuálního nastavení Blacklisiting a Whitelisting s definicí minimálně těchto parametrů: Source IP/network, Destination IP/Network, Source Port group, Destination Port group, fyzická skupina portů, VLAN tag a protokol.	
Nabízené řešení musí podporovat detekce útoků s využitím Challenge response technik pro přesnou detekci s nízkým poměrem false positives. Podporované techniky zahrnují minimálně 302 web challenge, JavaScript challenge a DNS challenge.	
Podpora detekce a ochrany proti DoS/DDoS útokům typu "Low and Slow" pomocí speciálních nástrojů.	
Rozpoznávání a blokování horizontálního i vertikálního skenování.	
Rozpoznávání a blokování neznámých DoS útoků pomocí behaviorální analýzy.	
Průběžné sledování útoků a automatická úprava dynamicky generovaných řetězců při změně útoku.	
Rozpoznávání a blokování anomálií podle předdefinovaných řetězců (signatur)	
Rozpoznávání a blokování na základě protokolových anomálií	
Rozpoznávání a blokování na základě anomálií provozu (rate based)	
Možnost definovat vlastní řetězce (signatury) pro rozpoznávání a blokování útoků	

Možnosti nasazení

- transparentně v cestě provozu (L2 inline)
- TAP, SPAN porty jen pro monitoring
- Mimo cestu (Out of path)
- Možnost zvolit mezi pouze "monitorováním" a "monitorováním a blokováním"
- Možnost definovat různá pravidla pro různé části sítě i různé uživatele

Hardware

Požadavek	**Splňuje (ano/ne)**
Minimálně 6x 1Gbps metalické rozhraní	
Minimálně 2x 10Gbps SFP+ rozhraní	
Propustnost zařízení při DDoS útoku, min. 1 Gbps	
Prevence pro útoky do intenzity 5.5 milionů paketů za vteřinu	
Počet současně navázaných spojení, min. 3 mil	
Možnost licenčního navýšení výkonu propustnosti až na 2 Gbps	
Latence, max. 60 microseconds	
Redundantní hot-swap napájení	
Obnova systému ze záložního média	
Možnost nasazení páru zařízení (aktivní – záložní)	
Ochrana před přetížením	
Integrovaná Fail Open síťová rozhraní v případě výpadku zařízení, minimálně pro metalické porty	

Požadované implementační práce:

Požadavek	**Splňuje (ano/ne)**
Provedení analýzy nasazení – analýzu stávajícího provozu a následné vytvoření návrhu nových filtračních pravidel pro jednotlivé segmenty sítě dle aktuálních potřeb, technický a procesní návrh.	
Příprava	
Instalace a základní konfigurace komponent;	
▪ instalace a konfigurace HW, SW, napojení komponent na management	
▪ implementace a konfigurace auditního logování a napojení na SIEM a na provozní monitoring	
▪ vytvoření pravidel	
▪ Test konfigurovaných komponent;	
▪ Failover a Failback test dle testovacích navržených DR scénářů;	
▪ Dokumentace s popisem zapojení, konfigurace, DR plánů, zálohování apod.;	

16 Web aplikační firewall

Technická specifikace obsahuje závazné technické parametry požadované zadavatelem pro jednotlivé části poptávaného řešení.

Požadovaná minimální funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
PLATFORMA	
Nasazení páru nezávislých HW zařízení ve funkci load-balancer a SSL akcelerátoru	
Možnost připojení 4 x 10Gbps SFP (SFP SR moduly součástí dodávky) a 4 x 1Gbps SFP	
RAM: 32 GB	
Datová propustnost zařízení alespoň 20Gbps L4, L7 či více	
Minimální propustnost HTTP požadavků: 1M za sekundu	
Minimální počet nových L4 spojeni: 200k za sekundu	
Počet současných L4 spojení: 20M	
Počet SSL transakcí za sekundu min. 8k (při použití 2K klíče)	
Počet SSL transakcí za sekundu min. 6k (při použití ECDSA P-256 klíče)	
Minimální propustnost SSL 10Gbps	
Nezávislé rozhraní pro management, umožňující provádět vzdáleně veškeré operace jako z lokální konzole (ILOM)	
Zdvojené napájení	
K dispozici jako autonomní box nebo ve formě šasi	
Management: sériový port, GUI, příkazový řádek, ILOM	
OPERAČNÍ SYSTÉM	
Plnohodnotná proxy architektura na všech OSI vrstvách	
Identický OS napříč všemi platformami (HW, Virtual)	
Plnohodnotná podpora IPv6	
Podpora HSM modulu	
Podpora validace intermediate certifikatu	
Podpora Spanning Tree Protokolu (STP)	
Možnost přidat vlastní funkce pomocí skriptování	
Podpora HTTP/2	
Podpora IPSec IKEv2	
Podpora konfigurace a správu zařízení přes REST API	
Plná podpora IPv6, IPv4/IPv6 gateway	
V souladu s certifikací UC-APL	
Dostupné také ve formě virtuální edice	

Požadovaná minimální funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Supports SNMP (v1/v2c/v3)	
Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall - ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall	
Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu	
Podpora Active-Active a Active-Pasive módu	
Podpora transparentního nasazení (TAP/SPAN)	
WEB Aplikační firewall	
Integrace s nástrojem na detekci zranitelností webových aplikací	
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10	
Možnost doprogramovat si filtrovací pravidla pro aplikace	
Automatická korelace zranitelností do jednoho bezpečnostního incidentu	
Ochrana AJAX a JSON aplikací	
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	
Podpora Captcha metody	
Automatické odlišení skutečných uživatelů od robotů	
Integrovaný XML a XML/SOAP firewall	
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění, vlastní Regulární výrazy atd.	
Automatické nahrávání a aplikování nových signatur	
Podpora pozitivního a negativního bezpečnostního modelu	
Blokování útočníků na základě geolokace	
Podpora ICAP pro antivirovou kontrolu – pro HTML, SOAP a SMTP	
Ochrana SMTP a FTP na aplikační úrovni	
Podpora SSL (šifrování a dešifrování)	
Podpora různých typů reportů – PCI, geolokační reporty	
Podpora standardů PCI DSS, HIPAA, Basel II a SOX	
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint	
Podpora application visibility a reportingu – monitorování URI	

Požadovaná minimální funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: • Cenzic Hailstorm • WhiteHat Sentinel • IBM Rational AppScan • QualysGuard Web Application Scanning	
Podpora aplikačního firewallu v cloudu	
Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu	
Ochrana proti Session Highjacking pomocí Browser Fingerprintingu	
Detekce a ochrana „Heavy URL" (stránky vykazující různé chování v čase)	
Validace log-on parametrů a aplikačních flows	
Automatická korelace útoků do jednoho incidentu	
Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI	
Filtrování WebSocket provozu & policy enforcement	
Blacklistování IP adres, které opakovaně snaží překonat „challenge" nebo se vyznačují vysokou mírou blokování	
Možnost vytvoření bezpečnostních politik způsobem hierarchie – nadřízené a podřízené politiky.	
Podpora aplikační ochrany na úrovni jednotlivých stránek (URL)	
Podpora více DoS profilů per VIP	
ŘÍZENÍ PROVOZU	
Možnost aktivovat L4-7 LoadBalancing, ICSA certifikovaný webový aplikační firewall, SSL VPN na jedné platformě HW	
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API	
Možnost přidat vlastní funkce pomocí skriptování	
Podpora REST API	
Autentikace klientů přes LDAP/Radius	
Podpora Active-Active, Active-Passive módů	
Povolení/zakázání ICMP pro VIP	
Podpora HTTP 2.0	
Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení	
Podpora alespoň pro 10 různých metod rozvažování zátěže	

Požadovaná minimální funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Možnost filtrace paketů	
Podpora ToS, QoS (marking/preservation/mimic)	
Podpora SNMP (v1/v2c/v3)	
Plná podpora IPv6, IPv4/IPv6 gateway	
Podpora rozvažování zátěže založené na poměrech (ratio based) s CARP perzistencí	
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	
Podpora práce s 4096-bit klíči	
Soucasna podpora ECC a RSA certifikatu	
Podpora Camellia cipher pro SSL	
Podpora pro TLS 1.2	
Podpora ECC a DH ciphers v HW	
Podpora SSL Forward proxy	
Statefull paketový filtr	
Podpora monitoringu per specifická služba	
Monitoring služeb – možnost přizpůsobení skriptováním	
Monitoring služeb založený na výkonnosti konkrétního hosta	
TCP optimalizace síťových flows	
Komprese a caching per specifická služba	
SSL Session a SSL Connection mirroring napříč celým ADC clusterem	
TCP optimalizace – dynamický TCP Tuning	
Podpora TLS Dynamic record sizing	
ŘÍZENÍ UŽIVATELSKÝCH PŘÍSTUPŮ	

Požadovaná minimální funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Autentizace: - HTTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SerurID - OAM - Tacacs+ - Local DB	
Import uživatelských identit IF-MAP	
Podpora pro External logon page	
AAA-server autentizace a vysoká dostupnost	
OTP (generování a ověření)	
Podpora CAPTCHA	
Podpora Google recaptcha v2	
Autorizace: - Radius - LDAP - Active Directory	
SAML: - SP - IdP	
Modifikace SAML atributů	
Podpora SAML 2.0	
SSO: - HTTP basic - HTML form - NTLM v1/v2 - Kerberos - SAML	
Cachování uživatelských identit a SSO proxy	

Požadovaná minimální funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS)	
Podpora for Kerberos ticketingu	
PCoIP proxy	
RDP proxy	
Patching: - HTML - JavaScript - CSS - Flash - Java	
Jednotný URL portál	
Uživatelský portál, kde se zobrazují aplikace podle přístupových práv	
Podpora L7 ACL	
Dynamický import ACL	
Dynamická kontrola přístupů	
Podpora ochrany a enkrypce „pracovniho“ prostoru („workspace“)	
Network SSL VPN DTLS	
Separátní SSL VPN tunel pro každou přístupnou aplikaci	
Přístup pomocí Client-less	
OS support: - Windows - MAC - Linux - iOS - Android	
Podpora nativní MDM	
Podpora Oauth 2.0	
Podpora IPSEC IKE v2	
Kontrola zabezpečení koncových bodů a posture kontrol	
Podpora L7 ACL pro uživatelský přístup	
Grafický editor pro správu řízení uživatelských přístupů	
Podpora Microsoft ActiveSync a Outlook Anywhere s client-side NTLM	
Zjednodušený řízení uživatelských přístupů pro Citrix XenApp a XenDesktop	
Step-up autentizace	

Požadovaná minimální funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Podpora Ping Identity's Policy Agent protocol	
Podpora forward proxy chaining	
Podpora ADFS proxy a ADFS-PIP protokolu	

Požadované implementační práce:

- Fyzická montáž zařízení
- Konfigurace síťového prostředí (VLAN, IP, route)
- Nastavení parametrů HA
- Základní konfigurace virtuálních server (až 50)
    - Nastavení profilů
    - Terminace SSL
    - Nastavení loadbalancingu
    - Případné komprese a cashování
- K sestavení pokročilejších kontrol modulem WAF musí využito Learning modu až 20 aplikací
- Základní vytvoření bezpečnostních politik
    - Konfigurace základních parametrů negativního bezpečnostního modelu dle využitých platforem
    - Základní konfigurace pozitivního modelu a aplikace nastavení na filetypes a uri metacharter validation
- Konfigurace anomaly detection
- Konfigurace/import wsdl schémat
- Nastavení parametrů learning modu (po uplynutí 1 měsíce aktivního learning modu)
- Vyhodnocení událostí a incidentů learning modu
    - Úprava hodnot learning modu
    - Úprava blocking settings pro jednotlivé položky
    - Zapnutí blocking modu
- Připojení k autentizačním prvkům a nastavení SSO
- Nastavení ochrany proti volumentrickým útokům DDoS
- Nastavení ochrany proti bruteforce
- Integrace s VMware Horizon
- Napojeni na SIEM řešení a provozní monitorng

17 Kompletní ochrana koncových stanic

Dodané řešení musí pokrýt minimálně 2000 uživatelů, a to včetně záruky výrobce na 5 let. Řešení musí splňovat následující parametry:

Administrace

Požadavek	Splňuje (ano/ne)
Nabízené řešení musí nabízet více administrativních rolí pro uživatele za účelem rozdělení pravomocí a zodpovědnosti mezi jednotlivé uživatele. Role musí obsahovat minimálně: • administrátor (systémová konfigurace), • administrátor (konfigurace politik), • helpdesk (support), • read-only role.	
Nabízené řešení musí umožnit administrátorovi vytvářet a spravovat logické skupiny zařízení nezávisle na rozdělení zařízení v Active Directory.	
Administrátor musí být schopný spravovat politiky na úrovni skupin uživatelů i jednotlivých uživatelů.	
Nabízené řešení musí být schopno využít uživatele a skupiny definované v Active Directory.	

Restrikce na úrovni uživatelů

Požadavek	Splňuje (ano/ne)
Nabízené řešení nesmí vyžadovat instalaci programů nebo nástrojů na koncové stanici s administrátorskými funkcemi. Jinými slovy, uživatel nesmí mít možnost spravovat nebo měnit nastavení bezpečnostních politik na koncové stanici.	
Software instalovaný na koncové stanici nesmí vyžadovat administrátorská oprávnění ke svému běhu.	
Koncový uživatel nesmí být schopný obejít nastavené politiky ani v případě, když disponuje administrátorským oprávněním.	
Řešení musí mít zabudované kontrolní mechanizmy, aby bylo zabráněno uživateli vykonávat: • smazání/odinstalace koncového klienta, • vypnutí/zapnutí služeb koncového klienta nebo souvisejících služeb, • zabránění správné funkčnosti koncového klienta, • modifikace koncového klienta a jeho souborů.	

Komunikace agent–server

Požadavek	Splňuje (ano/ne)
Bezpečnostní politiky přenášené mezi serverem a klientem musí být během přenosu šifrované.	
Citlivé informace přenášené mezi serverem a klientem musí být během přenosu šifrované.	

Auditing

Požadavek	Splňuje (ano/ne)
Auditní log musí podporovat soulad s detailní uživatelskou a systémovou úrovní logování. Logované informace musí obsahovat detaily o zařízení, časové razítko a další data pro správný audit.	
Auditní logy uložené na serveru musí být chráněny před neoprávněnou modifikací nebo smazáním.	
Auditní logy uložené na koncové stanici budou chráněny před neoprávněnou modifikací nebo smazáním.	

Firewall na koncové stanici

Požadavek	Splňuje (ano/ne)
Nabízené řešení musí být schopné zabránit neoprávněné síťové komunikaci koncové stanice v obou směrech (směrem od stanice i na stanici).	
Řešení musí umožňovat vynucování základních firewallových politik.	
Řešení musí umět detekovat a filtrovat příchozí i odchozí provoz. Dále musí být možnost povolit, blokovat či zalogovat a ohlásit příchozí i odchozí spojení dle nastavených firewallových politik.	
Nabízené řešení musí umožnit povolit nebo zablokovat síťový provoz v závislosti na oblasti, odkud je spojeni inicializováno nebo kam je realizováno (důvěryhodná zóna, blokovaná zóna a internetová zóna).	
Nabízené řešení musí být schopno ochránit sdílené adresáře před zneužitím k infikování dalších stanic.	
Nabízené řešení musí mít schopnost zakázat, povolit nebo si vyžádat zásah od uživatele pro příchozí i odchozí spojení. Tato schopnost musí být realizována na základě aplikace, která spojení inicializovala, využitého protokolu, portu, cílové a zdrojové IP adresy.	

Nabízené řešení musí disponovat funkcí pro blokování běžných síťových útoků, zejména pak útoků typu denial-of-service. Musí být prokázána spolehlivost a robustnost proti takovým útokům.	
Nabízené řešení musí disponovat funkcí pro skrytí všech nevyužívaných portů a povolit pouze legitimní aplikace a síťový provoz pro příchozí i odchozí spojení.	
Řešení musí umožňovat aplikovat různé politiky dle umístění koncové stanice (minimálně uvnitř a vně firemní sítě).	
Navrhované řešení musí umožňovat automatické nastavení politik v závislosti na stavu zařízení. V případě porušení nastavených politik znemožnit síťovou komunikaci.	
Navrhované řešení musí disponovat možností vytvářet seznamy aplikací, které mohou komunikovat ze stanice do sítě, a naopak aplikací, které nebudou mít možnost komunikovat do sítě.	
Navrhované řešení musí být schopné provozu na Windows 7 (32-bit a 64-bit), Windows 7 SP1 (32-bit a 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows 10 (32-bit a 64-bit), Windows Server 2012, Windows Server 2012 R2, MacOS X.	

Klient pro vzdálený přístup (VPN)

Požadavek	**Splňuje (ano/ne)**
Navrhované řešení musí mít integrovanou IPSec VPN funkcionalitu.	
Řešení musí umožňovat rozdělení komunikace (například přístup do internetu směřovat mimo VPN tunel a přístup do interní sítě směřovat přes VPN tunel).	
Řešení musí disponovat funkcí automatického přihlášení.	
Podporovaný typ autentizace musí být minimálně pomocí uživatelského jména a hesla a pomocí klientského certifikátu.	
Musí být podporována vícefaktorová autentizace.	
Nabízené řešení musí umožňovat využití funkce jednorázového hesla zaslaného formou SMS ve spojení se standardním uživatelským heslem.	
Nabízené řešení musí podporovat přechody mezi různými typy sítí bez ukončení spojení (například z kabelového na Wi-Fi, 3G, 4G apod.)	
Řešení musí podporovat VPN funkci v prostředí za NAT systémem a za firewallem, který nepodporuje IPSec provoz (možnost tunelovat VPN spojení přeš HTTPS).	

17.1 Šifrování pevných disků a přenosných disků

Požadavek	Splňuje (ano/ne)
Šifrování přenosných disků musí být aplikovatelné na USB flash disky, externí pevné disky, paměťové karty atd.	
Šifrování pevných disků nemůže uživateli umožnit rozhodnout se, zda daný soubor bude šifrovaný nebo ne.	

Šifrování pevných disků

Požadavek	Splňuje (ano/ne)
Nabízené řešení musí zašifrovat celý pevný disk sektor po sektoru včetně oblasti s bootovacími záznamy, operačním systémem, metadaty souborového systému, SWAP oddílem, dočasnými soubory a Windows registry.	
Nabízené řešení musí zajistit, že celý pevný disk včetně hibernačních souborů zůstane zašifrovaný i v případě, když počítač přejde do hibernačního módu.	
Nabízené řešení musí být schopno ochránit data a obnovit šifrování při spuštění po výpadku napájení nebo vypnutí systému.	
Nabízené řešení musí podporovat různé typy pevných disků, například IDE, SATA, SSD.	
Nabízené řešení musí umožnit autentizaci uživatele nebo koncové stanice při spuštění PC pomocí autentizace heslem a vícefaktorové autentizace pomocí smart karet, hardwarových tokenů, softwarových tokenů apod.	
Řešení musí podporovat Single-Sign-On přihlášení do systému Windows bez nutnosti zadávat heslo po předchozí preboot autentizaci.	
Celý proces Single-Sign-On přihlášení nesmí být znatelně pomalejší oproti klasickému přihlášení do Windows (maximální povolené zpoždění jsou 2 sekundy).	
Preboot prostředí musí být přizpůsobitelné (například vložit logo nebo číslo na helpdesk).	
Šifrování pevných disků musí být transparentní pro uživatele a nesmí mít znatelný dopad na výkon stanice.	
Nabízené řešení musí být jednoduché na používání pro koncové uživatele a nesmí vyžadovat žádné dodatečné zaškolování uživatelů.	
Nabízené řešení musí podporovat více uživatelů i administrátorů na jedné stanici.	
Nabízené řešení musí umožňovat přihlášení uživatele na více koncových stanic.	

Řešení musí disponovat funkcí pro vzdálené vymazání dat a/nebo uzamčení počítače.	
Nabízené řešení musí být kompatibilní s nástrojem EnCase.	
Nabízené řešení musí být možno provozovat na Windows 7 (32-bit a 64-bit), Windows 7 SP1 (32-bit a 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows 10 (32-bit a 64-bit), Windows Server 2012, Windows Server 2012 R2, MacOS X, Linux.	

Šifrování přenosných disků

Požadavek	**Splňuje (ano/ne)**
Nabízené řešení musí podporovat šifrování následujících přenosných zařízení: ▪ USB, ▪ paměťové karty, ▪ CD/DVD	
Nabízené řešení musí být schopno vynucovat šifrovací politiky na přenosných zařízeních bez nutnosti zásahu uživatele.	
Řešení musí být schopno umožňovat následující šifrovací politiky: ▪ šifrování všech souborů uložených na přenosném zařízení, ▪ automatické šifrování pouze nových souborů uložených na přenosném zařízení z chráněné stanice.	
Nabízené řešení musí umožnit výměnu šifrovaných dat na přenosných zařízeních prostřednictvím definovaných skupin uživatelů (výměna dat v rámci skupiny) nebo ochranu heslem (pro výměnu dat s externími uživateli).	
Nabízené řešení musí umožnit autorizovaným systémům dešifrovat přenosné zařízení.	
Koncový uživatel musí mít možnost specifikovat data, která chce sdílet s definovanou skupinou nebo pomocí ochrany heslem.	
Nabízené řešení musí být možno provozovat na Windows 7 (32-bit a 64-bit), Windows 7 SP1 (32-bit a 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows 10 (32-bit a 64-bit), Windows Server 2012, Windows Server 2012 R2, MacOS X, Linux.	

Kryptografie

Požadavek	**Splňuje (ano/ne)**
Nabízené řešení musí využívat pouze dobře známé kryptografické standardy, konkrétně AES a RSA.	

Délka kryptografického klíče pro symetrické algoritmy musí být alespoň 256 bitů.	
Nabízený šifrovací modul musí splňovat FIPS 140-2 standard a certifikaci Common Criteria EAL4.	
Šifrování pevných disků musí zašifrovat každou stanici s využitím unikátního šifrovacího klíče.	
Pokud je šifrovací klíč pro šifrování pevných disků uložen na stanici, musí být chráněn před přístupem bez preboot autentizace.	
Nabízené řešení nesmí zobrazovat šifrovací klíč v čitelné podobě v konzoli pro správu řešení.	
Nabízené řešení musí podporovat integraci s hardwarovým bezpečnostním modulem pro bezpečnou správu klíčů (například TPM čip).	

Enforcement

Požadavek	**Splnění (ano/ne)**
Nabízené řešení musí poskytovat preboot autentizaci ve všech případech: vypnutý PC, zapnutý PC, režim spánku, režim hybernace, offline a online.	
Nabízené řešení musí být odolné v průběhu prvotního šifrování vůči výpadku proudu nebo vypnutí počítače. V tomto případě musí při opětovném zapnutí počítače obnovit proces šifrování.	
Prvotní proces šifrování musí běžet na pozadí tak, aby uživatel mohl stále používat počítač k pracovnímu výkonu. Proces musí mít minimální dopad na výkon.	
Jakmile je pevný disk kompletně zašifrován, další šifrování a dešifrování musí probíhat transparentně pro uživatele a na pozadí.	
Nabízené řešení musí zajistit, že disk image zůstane zašifrován i při použití forenzních nebo zálohovacích nástrojů, které vytvoří image disku. V případě, že je zapnuté šifrování pevných disků, nesmí řešení žádným způsobem ovlivnit operační systém, aplikace, souborový systém nebo jiný bezpečnostní software. Aplikace a soubory musí být přístupné stejně jako normálně.	
Řešení musí poskytovat funkci pro obnovení zašifrovacích dat bez nutnosti autentizace v preboot prostředí. K tomuto může využít různých obnovovacích postupů.	
Nabízené řešení musí poskytovat informace o stavu šifrování na každé koncové stanici a prokázat, že zařízení bylo šifrování v době jeho ztráty nebo krádeže.	

Management hesel

Požadavek	Splňuje (ano/ne)
Hesla nesmí být uložena v čitelné podobě.	
Hesla nesmí být přenášena v čitelné podobě.	
Nabízené řešení musí disponovat funkcí proti útokům hrubou silou na prebootovací prostředí. Možné protiopatření mohou být:	
• Zamknout účet po předem nastaveném počtu neúspěšných pokusů, takovýto účet může být resetován pouze administrátorem.	
• Dočasné uzamčení účtu a automatické odemčení po určité době. Tato doba se zvyšuje po každém neúspěšném pokusu o autentizaci.	
• Nabízené řešení musí umožňovat jednoduchý, ale bezpečný přístup ke koncové stanici v případě, že uživatel zapomene heslo.	
Postup pro obnovení hesla musí splňovat následující kritéria:	
• Nevyžaduje, aby uživatel nosil disk se šifrovacím klíčem pro obnovení.	
• Nevyžaduje výměnu šifrovacího klíče nebo hesla během obnovovacího procesu.	
• Nevyžaduje síťové připojení.	
• Řešení nesmí zobrazovat heslo v čitelné podobě v konzoli pro centrální správu.	

17.2 Anti-malware

Obecné požadavky

Požadavek	Splňuje (ano/ne)
Nabízené řešení musí být schopno detekovat a odstranit viry, spyware a další malware za využití kombinace technik signaturní detekce, behaviorální analýzy a heuristické analýzy.	
Nabízené řešení musí být možno provozovat na Windows 7 (32-bit a 64-bit), Windows 7 SP1 (32-bit a 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2008 R2 SP1 (64-bit), Windows 10 (32-bit a 64-bit), Windows Server 2012, Windows Server 2012 R2, MacOS X.	

Enforcement

Požadavek	Splňuje (ano/ne)
Nabízené řešení musí být schopno detekovat přítomnost viru v systémové paměti, boot sektorech a ve všech formách uložených dat na pevných a přenosných discích.	

Uživatel musí mít možnost provést skenování konkrétních disků, adresářů nebo souborů.	
Antivirová ochrana musí běžet v reálném čase a musí být možnost spustit skenování na vyžádání. Toto skenování musí mít minimální dopad na výkon koncové stanice.	
Nabízené řešení musí být schopno detekovat a zastavit všechny pokusy o infekci známým malwarem.	
akmile je detekován malware, musí být možnost informovat o této situaci uživatele. Řešení musí být schopno provést nápravné kroky k odstranění škodlivého kódu.	
Řešení musí umožnit přesunutí škodlivého souboru, který nelze žádným způsobem vyčistit, do bezpečného prostředí na lokálním pevném disku.	
Nabízené řešení musí být schopno proskenovat nejčastější komprimační a archivační formáty souborů – například Microsoft Office dokumenty, ZIP a RAR archivy, JPG, GIF.	
Nabízené řešení musí mít sebeobranné mechanizmy, které chrání jeho procesy před škodlivými kódy a exploity.	
Řešení musí mít možnost ověřit konzistenci signaturní databáze.	
Nabízené řešení musí umožňovat při aktualizaci signaturní databáze stáhnout pouze přírůstky oproti aktuálnímu stavu.	
Řešení musí umožňovat stažení aktuální signaturní databáze z centrálního serveru nebo z internetu, pokud to je potřebné.	
Nabízené řešení musí umožňovat nastavit maximální rychlost komunikace mezi stanicí a serverem.	
Nabízené řešení musí ochránit systém a běžně používané aplikace před přetečením zásobníku.	
Výrobce řešení musí vydávat aktualizace signaturní databáze alespoň na denní bázi.	
Nabízené řešení musí být schopno detekovat přítomnost nechtěného škodlivého kódu v reálném čase a odstranit ho. Jedná se například o: ▪ spyware, ▪ adware, ▪ trojské koně, ▪ rootkity, ▪ diallery, ▪ ransomware, ▪ další potenciálně škodlivé nebo nechtěné aplikace. ▪ Nabízené řešení musí chránit před instalací potenciálně nechtěných aplikací.	

17.3 Pokročilé zabezpečení koncové stanice

Obecné požadavky

Požadavek	Splňuje (ano/ne)
Řešení musí být plně integrovatelné s dalším bezpečnostním softwarem na koncových stanicích (například anti-malwarová ochrana).	
Možnost spuštění automatické analýzy vyvolané bezpečnostním produktem třetí strany.	
Agent na koncové stanici musí zabírat méně než 500 MB v operační paměti za účelem minimalizace dopadu na výkon stanice.	
Nabízené řešení musí ukládat data na koncové stanici bez nutnosti dalšího přídavného hardwaru.	
Nabízené řešení musí být schopno izolovat infikovanou koncovou stanici.	
Nabízené řešení musí být schopno izolovat infikovaný soubor.	
Nabízené řešení musí umět zablokovat další šíření malwaru.	
Řešení musí být schopné provozu na operačních systémech Windows.	

Pokročilá ochrana

Požadavek	Splňuje (ano/ne)
Nabízené řešení musí automaticky identifikovat vstupní bod při infekci malwarem a identifikovat škody napáchané malwarem.	
Nabízené řešení musí odhalit zero-day a neznámé útoky.	
Řešení musí umět detekovat komunikaci na C&C server (po infekci).	
Řešení musí umět detekovat exploity.	
Nabízené řešení musí umět blokovat útoky bez ohledu na to, zda jsou webové, e-mailové nebo z přenosných zařízení.	
Nabízené řešení musí umět využívat IOC (indikátory kompromitace) a musí umožňovat tyto indikátory na všech koncových stanicích.	
Řešení musí poskytovat funkci roll-back, tedy vzít zpátky změny registrů a systému.	
Nabízené řešení musí umožňovat vložení doplňku do webového prohlížeče (Google Chrome, Firefox, Safari) za účelem detekce zero-day hrozeb a extrakce dat ze stahovaných souborů.	

Sandbox

Požadavek	Splňuje (ano/ne)

Řešení musí umožňovat detekci zero-day malwaru odesláním podezřelého souboru do sandboxu (on-premise nebo cloud).	
Soubory, které jsou staženy nebo zkopírovány na koncovou stanici musí být odeslány do sandboxu k analýze vůči zero-day útokům.	
Řešení musí umožňovat paralelní extrakci dat ze souboru, který je ve stejném okamžiku analyzován v sandboxu.	
Nabízené řešení musí proaktivně předcházet infikovaní koncové stanice způsobem, kdy je originální soubor analyzován v sandboxu, zatímco jsou uživateli vyextrahována data do bezpečného formátu souboru.	

Forenzní analýza

Požadavek	**Splňuje (ano/ne)**
Řešení musí nabízet funkci forenzní analýzy	
Nabízené řešení musí disponovat funkcí analýzy incidentu, která poskytuje kompletní přehled o vektoru útoku, vstupním bodu, hlavních akcích útočníka nebo malwaru a identifikaci škod.	
Data forenzní analýzy uložená na koncové stanici mohou využívat pouze předem definovanou velikost souborového systému. Jakmile je tato velikost dat dosažena, začnou se postupně přepisovat data od nejstarších.	
Data forenzní analýzy musí být uložena na koncové stanici a musí být zabráněno neoprávněnému přístupu.	

Reporting

Požadavek	**Splňuje (ano/ne)**
Řešení musí umět vytvořit kompletní přehledný report o průběhu útoku.	
Nabízené řešení musí umět podat administrátorovi reporty s obsahem: • aktivity malwaru na koncové stanici, • forenzního reportu, • kompletního přehledu útoku, • přehledu o všech procesech, které byly malwarem spuštěny	
Řešení musí zobrazit reputaci souboru ve forenzním reportu.	
Nabízené řešení musí identifikovat uživatele, který stáhl daný infikovaný soubor z internetu.	
Nabízené řešení musí identifikovat uživatele, který stáhl daný infikovaný soubor z internetu.	
Řešení musí umět korelovat více událostí mezi sebou.	

18 Management zranitelností a bezpečnostní politiky

18.1 Management zranitelností

Dodané řešení musí pokrýt minimálně 4000 IP adres, a to včetně záruky výrobce na 60 měsíců a musí mít následující funkce a parametry:

Architektura řešení

Požadavek	Splňuje (ano/ne)
On-premise – řešení musí být implementováno v síti Zadavatele a musí být schopno sbírat data a vyhodnocovat zranitelnosti bez nutnosti využití cloudových služeb.	
Řešení musí být schopno běžet na virtualizované platformě a na operačních systémech RHEL7/CentOS7, aby se nezvyšovaly licenční náklady na OS.	
Možnost distribuovaného nasazení skenovacích agentů do podsítí Zadavatele s napojením na centrální správu	
Možnost skenování ze skenovacích agentů umístěných v externí síti (Internetu).	

Centrální správa

Požadavek	Splňuje (ano/ne)
Podpora zabezpečeného přístup do management konzole pomocí využití protokolu https ze standardních webových prohlížečů.	
Možnost řízení přístupu podle sledovaných systémů (např. administrátoři z jedné pobočky nebudou mít přístup k systémům z druhé pobočky).	
Možnost řízení přístupu uživatelů dle předdefinovaných rolí. Možnost nastavení vlastních rolí.	
Podpora autentizace vůči Microsoft Active Directory.	
Automatické aktualizace databáze zranitelností.	
Centrální správa musí disponovat přehledovou obrazovkou, kterou si může uživatel přizpůsobit. V rámci přizpůsobení je požadováno alespoň: • možnost zobrazit nejzranitelnější stroje v síti; • zobrazení nejčetnějších zranitelností v síti; • zobrazení počtu zranitelností uvedených v OWASP Top Ten;	

Seznam skenovaných aktiv

Požadavek	Splňuje (ano/ne)

Možnost rychlé identifikace technických aktiv za využití discovery skenování.	
Možnost kategorizace aktiv na základě operačního systému, IP adres a dalších atributů.	
Možnost dynamické kategorizace aktiv na základě počtu zranitelností, typu zranitelností, přítomnosti konkrétní zranitelností a dalších atributů	

Skenování zranitelností

Požadavek	**Splňuje (ano/ne)**
Možnost definovat šablony skenů pro jednoduché vytváření více stejných skenů pro různé systémy.	
Možnost definovat skenovaný systém pomocí statické a dynamické kategorizace aktiv.	
Skenování za pomoci časového harmonogramu.	
Možnost autentizovaného skenu:	
• OS Microsoft Windows;	
• OS Linux;	
• pomocí SSH.	
Řešení musí obsahovat předdefinované šablony pro jednoduché spuštění skenů zranitelností bez nutnosti složité konfigurace.	
Možnost definovat vlastní sken bez nutnosti využít předdefinované šablony.	

Kontrola souladu s bezpečnostní politikou

Požadavek	**Splňuje (ano/ne)**
Řešení musí být schopno zkontrolovat konfiguraci skenovaného systému vůči standardizovaným bezpečnostním politikám (např. CIS).	
Řešení musí umožňovat kontrolu konfigurace vůči vlastním bezpečnostním politikám Zadavatele.	

Vyhodnocení výsledků

Řešení musí umožňovat analýzu detekovaných zranitelností a poskytovat minimálně následující informace o zranitelnosti:

Požadavek	**Splňuje (ano/ne)**
IP adresa a DNS stroje, na němž byla zranitelnost detekována;	
operační systém stroje, na němž byla zranitelnost detekována	
závažnost zranitelnosti	

CVE zranitelnosti;	
CVSS skóre	
datum zveřejnění zranitelnosti	
datum první identifikace v síti Zadavatele;	
datum zveřejnění záplaty (v případě, že byla zveřejněna)	
možnost exploitace a náročnost exploitace	
popis zranitelnosti	
návod na odstranění zranitelnosti	
Řešení musí umožnit filtrovat zranitelnosti dle výše uvedených parametrů	
Řešení musí poskytovat obrazovku s přehledem: • všech detekovaných zranitelností; • zranitelností detekovaných konkrétním skenováním; • zranitelných strojů specifikovaných IP adresou nebo DNS názvem s počtem zranitelností jednotlivých závažností; • zranitelností seskupených dle portu	
Řešení musí být schopno oddělit zranitelnosti od položek konfigurace, které nejsou ve shodě s bezpečnostní politikou.	
Řešení musí umožnit vytvoření výjimky pro konkrétní zranitelnost případně snížení její závažnosti.	
Řešení musí disponovat vlastním ticketovacím systémem s možností vytvořit ticket na konkrétní zranitelnost a přiřadit definovanému uživateli.	

Reporting

Požadavek	**Splňuje (ano/ne)**
Řešení musí poskytovat reporting ve formátu PDF a CSV.	
Možnost využít předdefinovaných šablon.	
Možnost vytvoření vlastního reportu bez využití šablon.	
Řešení musí umožňovat vytvořit vlastní report s možností filtrování zranitelností dle parametrů uvedených v prvním bodě kapitoly „Vyhodnocení výsledků“.	
Řešení musí umožňovat přidání vlastních komponent do reportu (tabulky, grafy, texty), aby si mohl Zadavatel přizpůsobit reporty svým požadavkům a vytvářet reporty pro různé úrovně managementu.	
Možnost automatického reportování po vykonání skenu a odeslání na specifikované emailové adresy.	
Možnost pravidelného reportování za pomoci časového harmonogramu.	

Integrace

Požadavek	Splňuje (ano/ne)
Řešení musí být schopno integrace na systémy SIEM.	
Řešení musí být schopno integrace na systémy správy privilegovaných účtů za účelem poskytnutí přihlašovacích údajů pro autentizované skeny.	
Řešení musí disponovat rozhraním API pro integraci s interními systémy zákazníka.	

18.2 Dodávka bezpečnostních politik

V rámci dodávaného řešení požaduje Zadavatel vytvoření bezpečnostních politik:

- textový popis politik ve formátu docx, ve kterém jsou obsaženy všechny položky konfigurace, které je nutné dodržovat a které se kontrolují auditním souborem.
- vypracování checklistů ve formátu XLS – pro každou konfigurační položku politiky
- auditní soubory – importovatelný soubor pro automatizovanou kontrolu konfigurace

Pro platformy uvedené níže, skripty pro automatizovanou kontrolu konfigurace těchto platforem a reporty, které budou vyhodnocovat soulad nebo nesoulad jednotlivých bodů konfigurace s bezpečnostní politikou rozdělených do kategorií (např. kategorie politika hesel, nastavení služeb atd.)

Bezpečnostní politiky jsou vyžadovány pro následující platformy:

Požadavek	Splňuje (ano/ne)
Red Hat Enterprise Linux 5, 6 a 7	
CentOS 7	
Microsoft Windows Server 2008, 2008 R2, 2016	
Microsoft Windows Server 2012 DC , 2012 R2 DC, 2019 DC	
Microsoft Exchange.	
Microsoft ISS 8.5	
Tomcat	
VMware esxi, vcenter, vSAN, NSX ve verzi 6.7	
Cisco IOS verze 15	
Apache HTTPD	
CheckPoint NGFW	
F5	
Oracle DB 11g	
Microsoft SQL Server 2008 R2, 2012 ,2014 ,2016	

19 Nástroj pro sběr a korelaci událostí a logů (SIEM), Systém pro správu rizik

19.1 SIEM

Tato část dokumentu stručně shrnuje požadavky na řešení jednotného systému bezpečnostního monitoringu v prostředí zadavatele (dále jen SIEM). Specifikace vychází zejména z platných legislativních požadavků, interních politik, směrnic a nařízení a z praktických zkušeností provozu ICT prostředí zadavatele.

Hlavním požadavkem je vybudování centralizovaného sběru, uchování a vyhodnocení zdrojů (logů) z aktivních prvků sítě, serverů, aplikací, bezpečnostních řešení a dalších. SIEM řešení má zajistit nástrojovou podporu při analýze událostí a logů a poskytnout tak přístup k datům.

Zadavatel požaduje po dodavateli splnění níže uvedených požadavků. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele se jedná o nesplnění zadávacích podmínek.

Dodavatel ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek (s dalším nezbytným popisem pro jednoznačnou identifikaci zařízení/prvku ze strany zadavatele). Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí výslovně prokazovat, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

Dodavatel do tabulky povinných parametrů uvede odkaz na část nabídky, kde je možné ověřit naplnění parametru, tzn. na část nabídky s detailním popisem. Vyplněné tabulky z tohoto oddílu technické specifikace učiní dodavatel součástí své nabídky.

Nástroj pro sběr a korelaci událostí a logů (SIEM)			
Požadavky na funkcionalitu	**Minimální požadavky**	Způsob naplnění tohoto parametru – tzn. uvedení výrobce, obch. označení, příp. uvedení konkrétních parametrů	Odkaz na přiloženou část nabídky, kde je případně možné ověřit naplnění parametru
Obecné požadavky	SIEM nástroj zajišťuje automatické monitorování bezpečnostního prostředí podnikové sítě v reálném čase. SIEM nástroj integruje		

	bezpečnostní technologie (řešení), síťové routery a switche, Windows a Unix / Linux systémy, aplikačních servery, databázové servery, úložná řešení a další komponenty do jednoho centrálního bodu prostřednictvím standardizovaných auditních záznamů (dále také logů). Nástroj musí být schopen integrace i nestandartního zdroje logů.		
	Řešení musí být schopno identifikovat více skrytých a sofistikovaných útoků v průběhu sběru dat a tyto jednotlivé útoky vzájemně provázat a spojit (dále také korelovat) do jednoho upozornění (dále také alert).		
	Informace o (bezpečnostních) událostech se používají k detekci hrozeb, škodlivých akcí, fraudů a anomálií a na základě této detekce usnadňují následné činnosti v rámci řízení bezpečnostních událostí a incidentů.		
	Řešení musí podporovat certifikaci alespoň CC EAL 2+.		
Požadavky na architekturu	Součástí řešení musí být veškerý potřebný hardware, software a licence.		
	Řešení musí umožňovat šifrování komunikace mezi jednotlivými komponentami.		
	Řešení musí zajistit integritu všech sbíraných informací.		
	Řešení musí být dostatečně škálovatelné, aby vyhovovalo malému nebo distribuovanému prostředí. Řešení musí mít možnost přidávat další komponenty bez nutnosti výměny hardwaru, softwaru a licencí.		

	Řešení musí zachytit nejméně **5000 trvalých EPS** a 25000 maximálních EPS.		
	Řešení musí zachytit alespoň **150000** FPM trvalého síťového provozu.		
	Řešení musí být schopno provádět vyhledávání a detekci anomálií v reálném čase.		
	Kompletní řešení musí mít možnosti virtualizace ve VMware prostředí.		
	Řešení musí podporovat nasazení v cloudu i on-premise.		
	Řešení musí podporovat potřebné operační systémy třetích stran a požadavky na softwarové licence.		
	Řešení musí podporovat standardizované úložiště třetích stran, pro uložení záloh dat.		
Minimální požadavky	Řešení musí poskytovat jednotné webové rozhraní pro správu všech komponent, analýzu událostí, netflow a síťové komunikace, vytváření reportů, nastavení korelací, správu incidentů atd. dle níže uvedených požadavků.		
	Webové grafické uživatelské rozhraní (dále také GUI) musí podporovat drill down zobrazení detailu pro účely analýzy v minimálním rozsahu: dotaz na konkrétní informaci, filtr a vyhledávání.		
	Řešení musí umět maskovat (dále také obfuskovat) data, která umožní pověřenému pracovníkovi (např. v podobě administrátora) identifikovat a omezit přístup k osobním údajům prostřednictvím segregace rolí a oprávnění. Systém musí umožnit vybrat data (na úrovni metadat), označit je jako citlivá a zamaskovat je.		

	Schopnost zamaskování dat musí být k dispozici v celém systému.		
	Řešení musí bezplatně poskytovat alespoň základní forenzní analýzu malware na end-point zařízeních (dále také EDR) prostřednictvím agentů, které se na koncové zařízení naimplementují. Řešení musí mít možnost rozšíření licence na plnou verzi a to tak, aby se jednalo o plnohodnotné řešení v podobě Endpoint Detection and Reaction (dále také EDR).		
	Řízení EDR agentů musí být umožněno přímo z webového GUI řešení.		
	Řešení musí umět monitorovat funkčnost všech součástí systémů včetně možnosti zasílání upozornění (dále také alertů) o sledovaném stavu minimálně prostřednictvím e-mailu.		
	Řešení musí umožňovat vytvoření různých profilů pro zobrazení logů a pro účely šetření, definovaného na úrovni oprávnění profilu.		
	Řešení musí poskytovat alespoň následující časové intervaly pro analýzu/šetření: posledních 5 minut, posledních 10 minut, posledních 15 minut, posledních 30 minut, poslední hodinu, posledních 24 hodin, poslední 2 dny, posledních 5 dní, celý den, všechna data a volitelný časový interval.		
	Řešení musí podporovat volitelné rozšíření (On-Demand Enrichment) – přidání dalšího kontextu během fáze analýzy.		
	Systém musí podporovat zadávání regulárních výrazů během analýzy / šetření.		

	Řešení musí umožňovat analýzu událostí u metadat i u surových (raw) logovaných dat.		
	Řešení musí mít před vytvořený (dále také out-of-the-box) profil a skupiny pro jednotlivé úrovně procesu řešení bezpečnostních událostí (např. pro účely detekce, vyšetřování a reakce).		
	Řešení musí mít v rámci analýzy možnosti kopírování.		
	Řešení musí podporovat úplnou rekonstrukci událostí a možnost reprezentovat rekonstruovanou událost ve formátu metadat nebo formou prostého logu.		
	Generátor pravidel v GUI pro reporty, grafy, alerty a korelace musí být dostatečně flexibilní a bez nutnosti používání komplexního skriptovacího jazyka pro jejich tvorbu.		
	Systém musí podporovat stahování a instalaci softwarových aktualizací přímo prostřednictvím webového GUI nebo v rozhraní příkazového řádku.		
	Systém musí umožňovat centrální monitorování stavu všech komponent systému prostřednictvím webového GUI. Monitorovány musí být alespoň následující parametry - CPU, systémová paměť, paměť alokovaná procesy systému, stav a rychlost zachycení události/logu, disk (fyzický, logický), agregované informace, uptime, OS, využití souborového systému. Veškeré statistiky musí být zobrazeny v grafickém formátu s možností filtrování.		
	Systém musí umožňovat konfiguraci parametrů monitorování jednotlivých komponent včetně možnosti zasílání alertů alespoň prostřednictvím e-mailu.		

	Systém musí mít schopnost alespoň monitorovat zdroj událostí v případě, kdy tento zdroj událostí neposílá logy.		
	Řešení musí umět importovat automaticky nebo manuálně doplňující informace z externích zdrojů pro rozšíření sbíraných logů (například: umístění zdroje logů událostí, vlastník zdroje logu, oddělení, klasifikované informací apod.).		
	Řešení musí podporovat princip víceúrovňové indexace (Multi-Index Feeds), která umožní sloučení záznamů z různých zdrojů na základě AND nebo OR logiky, předtím než budou tyto záznamy obohaceny.		
	Řešení musí poskytovat offline nápovědu (dále také tooltips) a online nápovědu s kontextovým vyhledáváním.		
	Řešení musí obsahovat před vytvořené reporty (např. v podobě grafů) v reálném čase formou dashboardů jako např. celkový přehled událostí, identity, provozní logy, síťový provoz, indikátory hrozeb, průnik hrozeb atd.		
	Řešení musí umožňovat vytváření grafů a jejich použití ve vlastních vytvořených dashboardech.		
	Systém musí podporovat dashboard pro řízení incidentů.		
	Systém musí podporovat přístup založený na rolích (dále také RBAC).		
	Řešení musí poskytovat vymezenou roli pro Data Privacy officera / manažera, který má přístup k originálním a vybraným obfuskovaným datům.		
	Řešení musí poskytovat vymezenou roli analytika, který má přístup k obfuskovaným datům a vybraným originálním datům.		

	Systém musí podporovat HTML5 webové GUI.		
	Systém musí podporovat alespoň tyto webové prohlížeče - Chrome, Internet Explorer a Mozilla Firefox.		
	Seznam nejnovějších podporovaných zdrojů událostí musí být připojen k požadavkům.		
	Řešení musí disponovat možností provádět centrální audit a audit přihlašování do řešení.		
	Řešení musí podporovat vytvoření vlastního parseru alespoň ve formátu XML nebo v jazyce LUA.		
	Řešení musí podporovat připojení ke cloudovým službám pro stahování informací jako jsou: pokročilé přetrvávající hrozby (dále také APT), informace o botnetech, informace o škodlivých sítích, indikátory kompromitace a útoků typu Zero-day, doplňující reporty, nově dostupné parsery, reportovací pravidla a grafy.		
	Řešení musí zahrnovat informaci o geografické lokalizaci IP adres (dále také GeoIP) pro účely vyšetřování.		
	Systém musí umět exportovat sbírané logy z webového GUI do formátu Text, XML, JSON a CSV.		
	Řešení musí umožňovat konfiguraci přihlašovacího banneru.		
	Řešení musí mít možnost provádět analýzu maskovaných (obfuskovaných) dat.		
	Řešení musí podporovat jednotné webové rozhraní pro správu systému (reporty, notifikace, incidenty, správa konfigurace atd.).		
	Řešení musí podporovat analýzu všech shromážděných dat (logů, paketů, netflow a dat koncových zařízení)		

	prostřednictvím jednoho přehledu v rozhraní (aniž by se při vyšetřování shromážděných dat musel měnit pohled nebo obrazovka v rozhraní).		
	Řešení musí podporovat sběr všech shromažďovaných dat v reálném čase (logy, pakety, netflow a data koncových zařízení).		
	Řešení musí podporovat reporty nad alerty a incidenty.		
	Řešení musí podporovat vlastní přizpůsobení předvytvořených šablon pro reporty.		
	Řešení musí podporovat vytváření uživatelsky definovaných šablon pro reporty a grafy.		
	Řešení musí podporovat korelaci veškerých sbíraných dat (logů, paketů, netflow a dat koncových zařízení) v reálném čase.		
	Systém musí mít podporu nativní integrace s řešeními na koncovém zařízení (EDR).		
	Systém musí sbírat informace o aktivech z řešení na koncových zařízeních pro rozšíření shromážděných dat.		
	Řešení musí nabízet možnost kontextového zobrazení (incidenty, varování, seznamy, koncové stanice, a další relevantní pro danou bezpečnostní události) v průběhu šetření.		
	Všechny komponenty systému musí mít možnost připojení prostřednictvím IPv4 nebo IPv6 adresy.		
	Řešení musí mít zálohovací a obnovovací postupy pro všechny součásti systému		

Požadavky na zabezpečení	Systém musí mít možnost volitelně zvolit STIG Hardeningový profil pro všechny systémy.		
	Systém musí podporovat zabezpečenou komunikaci mezi všemi komponentami systému.		
	Minimální délka hesla: - Minimální počet velkých písmen - Minimální počet malých písmen - Minimální počet číslic - Minimální počet speciálních znaků - Minimální počet znaků ne-latinské abecedy (zahrnuje znaky Unicode z asijských jazyků) - Zda heslo může, nebo nemůže obsahovat uživatelské jméno Uživatel si může při prvním přihlášení změnit své heslo		
	Systém musí umožňovat změnu defaultních hesel systémových uživatelů (admin, root atd.).		
	Systém musí podporovat alespoň následující systémová bezpečnostní nastavení: • Doba po, které dojde k uzamčení • Povolená doby nečinnosti • Časový limit pro relace • Uživatelské jméno nezávislé na velikosti písmen • Maximální povolený počet chybných přihlášení • Doba pro vypršení platnosti výchozího hesla uživatele Upozornit uživatele <n> dní před uplynutím platnosti hesla		
	Systém musí podporovat vytvoření vlastního banneru, který požádá		

	uživatele, aby před přihlášením souhlasil s podmínkami.		
Požadavky na sběr dat	Řešení musí být dostatečně výkonné, aby bylo schopné provádět sběr všech logů současně s analýzou v reálném čase.		
	Řešení musí podporovat statické (XML) a dynamické (regex) parsování logovaných událostí.		
	Řešení musí podporovat sběr NetFlow v9 komunikace bez dodatečných licencí nebo požadavků na hardware.		
	Řešení musí podporovat sběr dat ve formátu CEF (Common Event Format).		
	V případě potřeby musí řešení podporovat CEF filtraci nebo mít funkci pro sběr událostí ze specifických zařízení.		
	Systém musí být schopen přijímat logy ze Syslog Relay.		
	Řešení musí být schopno přeposílat syslog zprávy jinému příjemci syslogu.		
	Řešení musí mít schopnost filtrování událostí pro všechny podporované metody sběru zdrojových dat.		
	Řešení musí umožnit vytváření vlastních parserů zdrojových událostí pro systémy nebo aplikace, které nejsou řešením standardně podporovány.		
	Řešení musí poskytovat metodu sběru logů bez agentů.		
	Řešení musí mít schopnost mapovat parser(y) na konkrétní IP adresu nebo FQDN.		

Požadavek na podporu metod sběru	Syslog		
	TCP/UDP multiline syslog		
	TLS syslog		
	ODBC		
	CheckPoint události (OPSEC LEA)		
	HTTP Receiver		
	Cisco NSEL		
	VMware události		
	Oracle		
	SDEE		
	SMB Tail		
	Log File		
	SNMP (v2c, v3)		
	Microsoft Event Log (Windows události)		
	MS SQL		
	NetFlow (v.9)		
	SDEE		

	IPFIX		
Požadavek na schopnost shromažďování událostí, a to minimálně ze zde uvedených typů zařízení a aplikací	CheckPoint		
	Cisco IOS routery a switche		
	Cisco firewally		
	Cisco management systémy		
	Cisco Nexus zařízení		
	Cisco ISA		
	Cisco Wifi controler		
	F5 LoadBalancer		
	F5 WAF		
	VMS		
	Windows a Windows Server		
	Databáze MS SQL		
	MS Exchange		
	Databáze Oracle		
	VMware		
	MS SharePoint		

	NIS, RIS, TIS, FARMIS, MPA, MIS, NAV		
	AD		
Threat Intelligence	Řešení musí obsahovat Threat Intelligence funkcionalitu bez nutnosti dokupování další licence.		
	Řešení musí podporovat integraci Threat intelligence systémů třetích stran jako je STIX, TAXII a další.		
	Řešení musí podporovat sdílení hrozeb (možnost oboustranného sdílení informací o hrozbě). Oboustranné sdílení hrozeb musí zahrnovat minimálně poznatky o hrozbě a analytické chování.		
	Řešení musí podporovat obsahovou funkci spoustitelných balíčků, kde lze stáhnout různý obsah jako je například Hunting and Investigation Pack.		
	Řešení musí podporovat obsahovou kategorizaci pro analýzu a šetření založenou na osvědčených detekčních metodách pro pokročilou detekci hrozeb. Kombinací kategorizace a označení mohou analytici při analýze bezpečnostních událostí provádět konkrétněji cílené odhalování a inspekci.		
Korelace	Řešení musí podporovat korelace v reálném čase.		
	Webové GUI musí poskytovat grafické shrnutí korelovaných událostí.		
	Řešení musí umožňovat otestovat pravidla pro korelaci před jejich nasazením.		
	Řešení musí podporovat UBA (User Behavior Analytics) k detekci útoků typu C2 (Command and Control), Lateral Movement a další anomálie /		

	útoky na pakety (L2 - L7) a logovaná data.		
	Řešení musí podporovat UBA (User Behavior Analytics) pro zjišťování anomálií v chování uživatelů, i v kombinaci s EDR na koncových stanicích.		
	Nástroj pro analýzu chování uživatelů musí mít možnost analyzovat chování sledované entity / zařízení, uživatelů a procesů za účelem detekce anomálií, malware, beaconing a dalších škodlivých aktivit.		
	Řešení musí disponovat možností nastavení učící doby pro analýzu chování uživatelů prostřednictvím GUI.		
	Řešení musí mít možnost použít obfuskace dat během korelace a tyto data zobrazit až ve výstupu.		
	Řešení musí umožňovat dril-down zobrazení pro další šetření / analýzu přímo ze souhrnné stránky pro korelace událostí.		
	Korelační pravidla musí být vytvářena a spravována v rámci webového rozhraní systému, bez nutnosti instalace dalších nástrojů třetích stran.		
	Systém musí obsahovat předem definovaná korelační pravidla. Předdefinovaná korelační pravidla musí být možné uživatelsky upravovat.		
	Korelační pravidla musí umět vyvolat aletry alespoň přes SMTP, SNMP, Syslog a skriptů.		
	Korelační pravidla musí umožnit rozšíření korelačních alertů o údaje z externích databázových zdrojů (Mongo, Oracle, Postgresql atd.), GeoIP, In-Memory tabulky.		
	Korelační pravidla musí jít importovat a exportovat do a ze systému.		

	Korelační pravidla musí být k dispozici v prostém textu pro snadné kopírování a úpravy prostřednictvím webového GUI.		
	Systém musí poskytovat alespoň následující úrovně závažnosti pro korelační pravidla - kritická, vysoká, střední a nízká. Úroveň závažnosti musí být nastavitelná pro všechna korelační pravidla.		
	Korelační pravidla musí být možné povolit nebo zakázat v webovém GUI.		
	Systém musí podporovat vzájemnou korelaci mezi lokalitami, kde korelované události z různých lokalit mohou být korelovány v jednom (hlavním) korelačním nástroji.		
Autentizace	Řešení musí podporovat AD / LDAP, Kerberos, Radius, PKI nebo dvoufaktorovou autentizaci (tokeny).		
Archivace	Řešení musí poskytovat externí archivační platformu pro dlouhodobé uchovávání dat a pro účely prokazování souladu (compliance účely).		
	Řešení archivace musí poskytovat kompresní poměr alespoň 3:1 a umožňovat export dat do zálohovacích / archivačních systémů třetích stran (např.NAS).		
	Řešení archivace musí podporovat selektivní požadavky na uchovávání záznamů s možností vytvářet různé datové filtry a časová kritéria pro archivaci, například ponechat Windows event log číslo "4625" po dobu 6 měsíců a všechny další události po dobu 3 měsíců. Klíčovými požadavky na selektivní uchování logů je rozdělení logů dle různých retenčních dob.		

	Řešení musí podporovat agregaci do skupin pro sdílení agregačních úloh mezi více archivačních zařízení.		
	Řešení musí mít jednoduché možnosti obnovy dat ze záloh.		
	Řešení archivace musí umožňovat provádět analýzu / šetření a používat reportovací funkce přímo z webového GUI.		
	Řešení musí umožňovat systémový monitoring archivační platformy.		
	Řešení archivace musí podporovat minimálně sha256, sha1 a md5 hašovací funkce.		
	Archivační řešení musí podporovat alespoň gzip kompresní algoritmus.		
	Řešení musí podporovat přesun dat alespoň dle zvoleného času nebo intervalu.		
Řízení bezpečnostních incidentů	Součástí řešení musí být i funkcionalita pro řízení incidentů bez nutnosti dokupování dodatečných licencí.		
	Řízení incidentů musí umožnit orchestraci a automatizaci prostřednictvím předdefinovaných postupů pro různé druhy hrozeb.		
	Řešení musí umět znázornit jednotlivé incidenty graficky a mít možnost zobrazit detaily incidentů pomocí drill down funkce.		
	Jednotlivé incidenty musí být možné rozšířit o informace z různých zdrojů, jako jsou: AD, seznamy (statické nebo dynamické), Threat Intelligence, informace z koncových zařízení, GRC řešení, jiné události a incidenty.		
	Řízení incidentů musí umožnit zobrazení přehledu incidentů, alertů a nápravných opatření. Všechny přehledy musí umožňovat hloubkovou		

	analýzu, možnost přidávání dalších komentářů / poznámek, změnu stavu incidentu, zvládání a ošetření incidentu a podobně.		
	Řízení incidentů musí umožňovat filtrování.		
	Řízení incidentů musí umožnit prohlížení záznamů s alerty, které incident vyvolaly.		
	Šetření incidentů musí být možné přímo z modulu řízení incidentů.		
	Správa incidentů musí umožnit sběr alertů přinejmenším z varování dle korelačních pravidel, varování na výskyt malwaru a reportingu.		
	Pravidla pro řízení incidentů musí být konfigurovatelná přes webové GUI.		
	Řízení incidentů musí podporovat alespoň nastavení e-mailových upozornění a notifikací.		
	Řešení musí mít schopnost integrovat se na řešení webové detekce hrozeb a zobrazovat všechny vlastní incidenty, i incidenty z webové detekce hrozeb v jednotném webovém rozhraní.		
Reporting	Součástí řešení musí být i funkcionalita pro řízení incidentů bez nutnosti dokupování dodatečných licencí.		
	Řízení incidentů musí umožnit orchestraci a automatizaci prostřednictvím předdefinovaných postupů pro různé druhy hrozeb.		
	Řešení musí umět znázornit jednotlivé incidenty graficky a mít možnost zobrazit detaily incidentů pomocí drill down funkce.		
	Jednotlivé incidenty musí být možné rozšířit o informace z různých zdrojů, jako jsou: AD, seznamy (statické nebo dynamické), Threat Intelligence,		

	informace z koncových zařízení, GRC řešení, jiné události a incidenty.		
	Řízení incidentů musí umožnit zobrazení přehledu incidentů, alertů a nápravných opatření. Všechny přehledy musí umožňovat hloubkovou analýzu, možnost přidávání dalších komentářů / poznámek, změnu stavu incidentu, zvládání a ošetření incidentu a podobně.		
	Řízení incidentů musí umožňovat filtrování.		
	Řízení incidentů musí umožnit prohlížení záznamů s alerty, které incident vyvolaly.		
	Šetření incidentů musí být možné přímo z modulu řízení incidentů.		
	Správa incidentů musí umožnit sběr alertů přinejmenším z varování dle korelačních pravidel, varování na výskyt malwaru a reportingu.		
	Pravidla pro řízení incidentů musí být konfigurovatelná přes webové GUI.		
	Řízení incidentů musí podporovat alespoň nastavení e-mailových upozornění a notifikací.		
	Řešení musí mít schopnost integrovat se na řešení webové detekce hrozeb a zobrazovat všechny vlastní incidenty, i incidenty z webové detekce hrozeb v jednotném webovém rozhraní.		
Obecné požadavky	Řešení musí podporovat vizuální znázornění různých parametrů jako je zdrojová IP adresa, cílová IP adresa, typ zařízení, hostname, typ protokolu, doména, uživatelské jméno.		
	Řešení musí mít schopnost používat technologii CEP (Complex Event Processing) v korelačním nástroji.		

	Řešení musí bez dalších licencí poskytovat konfigurace Indentity Feed tak, aby se mohly přidat k paketům (logům) Active Directory domény, pracovní stanice a uživatelská jména a ne-Windowsové relace.		
	Řešení pro správu incidentů by mělo být schopno integrace s používaným Help Desk řešením.		
	Řešení musí podporovat vytváření vlastních akcí v kontextovém menu (možnosti po kliknutí pravým tlačítkem myši) pro rychlejší šetření a analýzu, například: • Drill down detaily v nové záložce. • Otevření externí webové stránky pro zobrazení doplňujících informací. Spuštění skenu pro analýzu malwaru.		
	Řešení by mělo umožňovat integraci s jinými systémy pro řešení bezpečnosti: • Data Loss Prevention (DLP) • Nástroje pro analýzu malware na koncových zařízeních • Identity Management • NGFW (Next Genration Firewall) • WAF (Web Application Firewall) • EDR (Endpoint Detection and Reaction) VMS (Vulnerability Management Scanner)		
	Řešení musí mít přístupné REST API UI pro účely automatizace.		
	Řešení musí umožňovat budoucí rozšíření o Data Science, kde lze využít technologii Hadoop.		

	Systém musí poskytovat možnost rozšíření o sběr logů s vysokou dostupností – mód s umístěním zařízení pro sběr logů do vzdálené lokality.		
	Systém musí mít možnost budoucího rozšíření o externí úložiště pro zajištění delší retence dat.		
	Systém by měl mít možnost budoucího rozšíření o úložiště pro dlouhodobou archivaci dat.		

Požadavky na síťovou forenzní analýzu

Požadavek	Splňuje (ano/ne)
Řešení musí pro všechny konkrétní události/alerty zajistit zobrazení všech relevantních informací sloučením informací z paketů a logů.	
Řešení musí provádět sběr a analýzu plného síťového provozu (na vrstvách v rozsahu L2 - L7).	
Řešení musí podporovat nativní dešifrování SSL příchozího provozu.	
Řešení musí poskytovat ENTROPY analýzu síťového provozu bez jakékoliv dešifrovací technologie.	
Řešení musí podporovat sběr síťového provozu z virtuálních prostředí prostřednictvím řešení třetích stran	
Parsování síťového provozu musí být prováděno v reálném čase (v paměti) a poté zapsáno na disk.	
Řešení musí mít možnost povolit síťový parser v režimu "Enable", "Disable" nebo "Transient". Transient režim znamená, že analyzované informace se používají během procesu parsování, ale nejsou zapsány na disk.	
Řešení musí umět generovat a indexovat metadata (typ služby, hostname, zdrojová IP adresa, cílová IP adresa, e-mailový účet, uživatelský účet, přílohy, názvy souborů, operační systém, cílové porty, cílová země, cílové město, zdrojová země, zdrojové město, URL) extrahovaná ze síťového provozu a zpřístupňovat je pro dotazy a analýzu v reálném čase a zároveň umožňovat reporting a alerty.	

Systém musí umět filtrovat síťový provoz (BPF - Barkley Packet Filter) před zápisem na disk, aby se zabránilo ukládání zbytečného síťovému provozu jako například: • Důvěryhodné zálohy aplikace / sítě. • Filtrování specifické komunikace mezi segmenty sítě. • Filtrování komunikace pro konkrétní zařízení. • Filtrování komunikace na specifickém portu.	
Systém musí poskytovat možnosti korelace síťové komunikace a logovaných událostí v jednotném korelačním nástroji.	
Systém musí umět exportovat síťovou komunikaci ve formátu PCAP z webového GUI.	
Řešení musí umožňovat analýzu a šetření síťových incidentů pomocí drill down přístupu k určení jejich příčin a odstranění dopadu v analyzované komunikaci.	
Řešení musí podporovat detekci útoků DDoS nebo podobnou analýzu síťové komunikace.	
Řešení musí podporovat detekci interních útoků prostřednictvím stanovení základního chování sítě a neustálým porovnáváním sledované komunikace s tímto základním chováním sítě v reálném čase.	
Řešení musí podporovat automatický alerting na výskyt událostí, které nespadají do sledovaných modelů komunikace.	
Systém musí umět identifikovat služby botnet sítě na základě Threat Intelligence monitorování síťové komunikace pro známé C&C (command and control) servery.	
Řešení musí umět detekovat šifrované aplikace v rámci sledované síťové komunikace.	
Systém musí umožňovat identifikaci a / nebo evidenci použitých aplikací založených na přednastavených třídách jako Peer-to-Peer, Business, Social Media, Streaming, Instant Messaging, Tunneling, Gaming atd.	
Systém musí umožnit generování reportů ke sledování trendů ve využívání síťových zdrojů a plánování jejich kapacit.	
Řešení musí podporovat sběr síťové komunikace prostřednictvím TAP SPAN a / nebo Mirror portů.	
Řešení musí podporovat rekonstrukci síťové komunikace (web, e-maily, dokumenty atd.) z vrstev L2 - L7.	
Řešení musí umět rekonstruovat kompletní relace nejen pakety.	

Řešení musí umět kombinovat fragmentované relace a být schopno je zrekonstruovat.	
Řešení musí podporovat různé možnosti rekonstrukce událostí, jako jsou Meta, Hex, Packets, Text, Web, Mail a Files.	
Řešení musí podporovat plnou obnovu souborů a možnosti jejich exportu.	

Požadavky na výkon

Architektura pro sběr logů musí být distribuována napříč primární i vzdálenou lokalitou. Všechny logy ze vzdálených lokalit musí být přesunuty do primární lokality, logy mohou být uloženy na vzdáleném místě pouze na krátkou dobu v případě potíží s připojením mezi primární a vzdálenou lokalitou nebo při výpadku systému v primární lokalitě.

Požadavek	**Splněno (ano/ne)**
Počet zařízení (zdroje událostí): Bez omezení (omezeno pouze výkonem hardwaru)	
Maximální EPS: Řešení musí být schopno sbírat až 50 000 EPS z primární a vzdálené lokality	
Trvalý EPS: Řešení musí být schopno trvale sbírat 5 000 EPS z primární a vzdálené lokality	
Korelační nástroj: musí být škálovatelný až do 100 000 EPS	
Síťové karty: 4x 10/100/1000 RJ 45	
Datové úložiště: 1. Minimální kapacita 46 TB v primární lokalitě 2. Minimální kapacita 46 TB ve vzdálené lokalitě	**1.** **2.**
Možnosti archivace: Vyhrazená appliance s minimálně 46 TB externího úložiště pro účely archivace logů v každé lokalitě	
Zařízení umístitelné do racku s redundantním zdrojem napájením	
Systém musí podporovat RAID	
Doba uchování (data retention) pro online data (bez komprese - RAW logy) pro 5 000 EPS musí být 1 rok	
Doba uchování (data retention) offline dat (archivační účely) musí být nejméně 1 rok	

Síť:

Požadavek	**Splňuje (ano/ne)**
Řešení musí být schopno zachytit až 500 Mbps trvalé síťové komunikace	

Retence online síťové komunikace musí být alespoň 7 dní (500 Mbps) nebo 30 dní (100 Mbps)	
Datové úložiště: • Minimální kapacita 30 TB v primární lokalitě	
Síťové karty: 4x 10/100/1000 RJ 45 • Řešení musí mít možnost upgradovat na 10G rozhraní	
Zařízení umístitelné do racku s redundantním napájecím zdrojem	
Systém musí podporovat RAID	

Požadavky na instalaci

Požadavek	Splněno (ano/ne)
Implementace systému musí být provedena školenými /certifikovanými techniky (viz technické kvalifikační požadavky).	

Požadavky na záruku

Požadavek	Splněno (ano/ne)
60 měsíců pro celý systém	

Další požadavky

Požadavek	Splněno (ano/ne)
Kompletní řešení musí být od jediného výrobce, aby bylo používáno pouze jedno rozhraní, a tím usnadněno řízení a správa.	

19.1.1 Implementační požadavky

Zadavatel požaduje od dodavatele poskytnutí následujících činností v rámci implementace:

Implementační požadavky
Analýza nasazení SIEM v prostředí zadavatele
Implementace technologie SIEM do prostředí zadavatele
Tvorba procesu pro řízení bezpečnostních incidentů
Konfigurace technologie SIEM (SW, OS)
Nastavení logování a sběru bezpečnostních záznamů
Integrace technologie SIEM do infrastruktury zadavatele
Implementace Use case – zavedení korelací, reportů, vizualizace
Zkušební provoz a proškolení operátorů technologie SIEM (zkušební provoz v rozsahu 1 měsíc, v průběhu kterého budou provedeny školení operátorů) předání provozní dokumentace
Předání do plného provozu

19.1.2 Analýza nasazení SIEM

Předpokládá se, že SIEM bude přímo napojen na systém pro analýzu rizik a na ticketovací systém, a to tak že:

- Logy a události a incidenty budou obohaceny o rizika, assety ze systému pro analýzu rizik
- Na SIEM bude prioritizovat incidenty na základě velikosti rizika
- Systém pro analýzu rizik bude v reálném čase propočítávat rizika z potvrzených incidentů v SIEMu
- SIEM bude automaticky zakládat incidenty v ticketovacím systému a také si vyzdvihne stav řešení incidentu.

Záměrem zadavatele je zpracovat analýzu nasazení Security Incident and Event Managementu (dále jen SIEM), který se následně bude implementovat do zadavatelovy infrastruktury. Zadavatel požaduje od dodavatele poskytnutí následujících činností v rámci analýzy:

Implementační požadavky analýzy nasazení SIEM
Analýza aktuálního stavu infrastruktury zadavatele z pohledu bezpečnostního architekta
Identifikace a hodnocení aktiv (zdrojů logů)
Aktualizace analýzy rizik
Rozšíření katalogu hrozeb
Tvorba Use Case dle identifikovaných hrozeb

Analýza nasazení SIEM má za cíl posoudit aktuální stav infrastruktury, do které bude SIEM implementován, identifikovat aktiva, která budou SIEM řešením monitorována (dále také zdroje logů) včetně identifikace těch zdrojů, u kterých není možné nativní zasílání logů (dále také custom zdroje). Požadované povinné kroky, formální požadavky a dokumentace, které musí být v rámci dodávky dodány:

Analýza aktuálního stavu infrastruktury zadavatele z pohledu bezpečnostního architekta s cílem zhodnocení současného stavu infrastruktury, topologie a nastavení implementovaných technologií, identifikace nedostatků a návrh kroků vedoucích k jejich odstranění, které povedou ke zvýšení bezpečnosti napříč infrastrukturou zadavatele. Veškeré navržená úprava infrastruktury musí být navržena tak, aby byla co nejvhodněji uzpůsobena provozování SIEM řešení. V rámci analýzy současného stavu musí být minimálně posouzeno:

V rámci analýzy současného stavu musí být minimálně posouzeno:	**Splněno (ano/ne)**
audit síťové infrastruktury a topologie	
servery, infrastruktura, VMware	
fyzická vrstva	
internetová konektivita	
síťová vrstva	
síťový monitoring	
provozní monitoring	

aplikační monitoring všech systémů spadajících pod základní službu	
logování	
implementované technologie v rámci tohoto projektu a jejich konfigurace	

Identifikace a hodnocení aktiv (zdrojů), která budou připojena a monitorována SIEM řešením s cílem vytvoření registru SIEM aktiv, včetně plánu připojení aktiv pro aktiva, u kterých není možné nativní zasílání logů.

Veškeré identifikovaná aktiva musí být dodavatelem ohodnocena použitím metodiky, kterou dodavatel vytvoří přímo na míru a pro prostředí zadavatele. Tato metodika musí být plně v souladu s interními politikami, směrnicemi a nařízeními zadavatele a zároveň musí respektovat principy uvedené v zákoně č. 181/2014 Sb., Zákon o kybernetické bezpečnosti (dále jen zákon o kybernetické bezpečnosti, nebo také ZoKB) a vyhláškách k němu se vztahujících. Dodavatelem vytvořená metodika musí být v souladu s mezinárodními standardy ISO pro příslušnou oblast.

Registr aktiv musí minimálně obsahovat:	**Splněno (ano/ne)**
seznam všech standardních zdrojů, které budou připojeny do SIEM řešení, včetně plánu a způsobu jejich připojení	
seznam všech nestandardních zdrojů, které by bylo vhodné připojit do SIEM řešení, včetně plánu a způsobu jejich připojení	
identifikaci vazeb mezi jednotlivými zdroji	
vlastníka odpovědného za dané aktivum (zdroj)	
hodnocení zdrojů dle dodavatelem vytvořené metodiky	
způsob připojení zdroje do SIEM řešení	
časovou známku stanovující prioritu připojení do SIEM řešení	

Zdroje musí být identifikovány minimálně v rozsahu:	**Splněno (ano/ne)**
síťové prvky	
servery	
koncové stanice	
aplikace	
data	
bezpečnostní technologie	

Aktualizace analýzy rizik - dodavatel v rámci hodnocení aktiv zhodnotí relevantnost hrozeb definovaných v zadavatelově analýze rizik pro jednotlivá aktiva a tuto analýzu rizik aktualizuje.

Rozšíření katalogu hrozeb - dodavatel doplní katalog identifikovaných hrozeb dodaný dodavatelem s cílem rozšíření existujícího katalogu hrozeb o hrozby, které jsou pro zadavatele a činnost jím vykonávanou relevantní a doposud nebyly zohledněny analýzou rizik.

Tvorba Use Case dle identifikovaných hrozeb

Veškeré analýzou rizik definované hrozby dodavatel spáruje s identifikovanými aktivy, včetně vazeb aktiv a na tyto hrozby vytvoří postupy jejich zvládání (dále také Use Case). Tyto páry aktivum – hrozba dodavatel doplní do analýzy rizik.

Dodavatel se zavazuje navržené Use case implementovat do SIEM řešení zadavatele.

Dodavatel jednotlivým Use case přiřadí úroveň kritičnosti na základě metodiky, kterou dodavatel vytvoří přímo pro podmínky zadavatele. Jednotlivé Use case budou na základě této metodiky kategorizovány a bude jim přiřazena kritičnost v SIEM řešení.

Dodavatel vytvoří pro zadavatele seznam jednotlivých navržených Use case a to v minimálním rozsahu:

Požadavek
identifikátor Use case
popis Use case
doporučenou kritičnost Use case
status Use case
výčet hrozeb, které daný Use case reflektuje
výčet aktiv a jejich vazeb, která jsou daným Use case chráněna
zdrojové data, která jsou pro daný Use case nezbytná

Dodavatel vytvoří a naimplementuje do SIEM řešení Use case, a to se specifikacemi:

- Use case budou vycházet z hrozeb identifikovaných analýzou rizik a budou tyto hrozby reflektovat.
- Use case budou zohledňovat aktuálně implementované bezpečnostní technologie
    - Use case budou zohledňovat nově implementované bezpečnostní technologie, které jsou součástí tohoto RFP.
    - Veškeré vytvořené Use case dodavatel zdokumentuje v textovém editoru a předá zadavateli dokumentaci ve výše uvedeném rozsahu.

Zadavatel dále požaduje po dodavateli vytvoření use case v minimálním rozsahu:

Windows:

- Server Shutdown/ Reboot
- Removable media detected
- Windows abnormal shutdown
- Login attempts with the same account from different source desktops
- Detection of Server shutdown-reboot after office hours
- Administrative Group Membership Changed
- Unauthorized Default Account Logins

- Interactive use of service account
- Remote access login - success & failure
- Windows Service Stop-Restart
- ACL Set on Admin Group members
- Windows Account Enabled Disabled
- Multiple Windows Account Locked out
- Multiple Windows Logins by Same User
- Brute force attempt from same source
- Logins outside normal business hours
- Logins to multiple user accounts from the same source.
- Brute force attempt from same source with successful login
- Windows Account Created Deleted
- Windows Hardware Failure
- Failed Login to Multiple Destination from Same Source
- Administrative Accounts - Multiple Login failure
- Detection of user account added/removed in admin group
- Detection of system time changes (Boot time)
- Detection of use of default product vendor accounts
- User Deleted Within 24hrs of Being Created
- Critical service stopped on Windows Servers
- Windows Security Log is full
- Multiple Password Changes in Short time period
- Windows group type was changed
- Audit Policy change
- Audit Log cleared
- Windows Security Log is full
- Detection of user account added
- Logon Failure-A logon attempt was made using an expired account
- High number of users created/ removed within a short period of time
- Outbound Traffic observed from Severs to internet.
- Failed Logins/Attempt with Disabled/Ex-Employee/Expired Accounts
- Windows File-Folder Delete
- Windows-File Folder Permission Changes
- High number of users created/removed within a short period of time

UNIX:

- Unix FTP File Import and Export Events
- Unix File system full
- Server shutdown
- Users Created /Deleted within short period
- Users Group Created /Removed within short period
- Unix-Login attempts with the same account from different source desktops
- Failed Logins

- Failed Logins with disabled accounts Unix FTP Login Access
- Unix multiple SFTP Connection
- Failed logins from root access
- Unix Multiple SU login failures
- Remote Logon Attempts using Root User on Production Node
- Sudo access from Non sudo users
- Detection of use of default product vendor accounts
- Adding or Removing users to the group "root"
- Critical Service Stop
- Unix-High number of login failure for the same account within a short time
- Password Changed
- Adding, removing and modifying cron jobs
- SU login failures.
- Detection of change in syslog configuration
- Detection of change in network configuration

Firewall:

- Firewall critical alert observed
- VPN configuration change observed
- Administrator Login Failure detected Successful logon between Non - Business Hours
- Successful access from Suspicious Countries
- Checkpoint Service restarts
- Firewall Cluster/Gateway Configuration Change
- CPU Utilization High
- Checkpoint Policy Installed
- High number of denied events
- Smart-Defense Signature Based Alert
- VPN Certificate Verification Failure
- Configuration Change detected
- Firewalls reboot

Exchange:

- Top 10 users sending mails to external domains
- Top 10 Email Receivers/Senders
- Data Leakage Identified through
- Large file send via mail
- Malicious/Suspicious attachments identified
- Email Usage Group IDs
- Monitoring mails going out from the company domain to other domains after Office Hours
- High Email Bandwidth utilization by individual users
- Detection of Undelivered Messages
- Mailbox Access by Another user

- User sending a Message as another user
- User Sending a Message on behalf another user
- Detection of Users login to the Mail Box which is not their Primary Account
- Detection of Auto Redirected Mails
- Top 10 users sending mails internally
- SMTP gateway sudden spike in Incoming mails
- High number of rejected mails from single “from” address
- Detection of Users login to the Mail Box which is not their Primary Account
- Detection of Auto Redirected Mails

Wireless/VPN:

- Rouge Network Traffic Detected.
- Top VPN Account Logged in from Multiple Remote Locations
- Top VPN Account Logged in From VPN and on Local Network
- Wireless unauthorized login attempts
- Wireless authorization server is down.
- Anonymous login from unknown IP address
- VPN Account logged in from multiple locations in short span of time, or from suspicious countries
- Simultaneous Login from Multiple Locations for Single User
- VPN Connection beyond 24 Hour
- VPN Access from Internal IP Address
- VPN access from overseas
- Rogue AP detected.
- Wireless AP rebooted
- Wireless unsecure AP detected
- VPN access from onshore team
- VPN access and Access card on Onshore observed

IPS:

- UNIX Password File Access Attempt
- IPS High Alert
- Possible Exploit of Vulnerability
- Probable Port Scanning in the network
- SQL Injection Attempt
- Virus Traffic in the network
- Signature Based Attacks

Proxy:

- Access attempts on unidentified protocols & port
- Malware Domain Access Report
- Proxy Category based Summary Report
- Malware IP Access Report
- Potentially Unwanted Software access

- Dynamic DNS Host
- Malicious Sources/Malnets
- Malicious Outbound Data/Botnets
- Peer-to-Peer (P2P)
- Proxy Avoidance
- Remote Access Tools
- Access from unusual User Agent
- Post request to uncategorized sites after office hours
- Unwanted Internet Access
- Proxy configuration changes
- Proxy failed login attempt
- Content access violation
- Anonymous proxy access
- Hacker tool website access
- Access attempts by BOTNET identified by HTTP Request header

Oracle/DB:

- Oracle password expired
- Critical command usage
- Critical commands executed on the database during non-business hours
- Oracle - Update or Insert Commands
- Oracle user Created/Deleted
- Multiple login failures observed for database
- Database Schema Creation/Modification
- Top Query Execution Failures.
- Monitoring login attempts on database
- Use of default vendor accounts against policy
- Database access during non-business hours
- Login failures for sys/system or privileged accounts
- Connection to production databases from disallowed network segments

Routers and Switches:

- Emergency router error messages
- BGP Neighbor Relationship Status Change
- Router-Power supply failure
- Configuration Change
- Critical messages observed from the SWITCH
- Alert messages observed from the SWITCH
- Detection of Antispam
- File Dropped due to large size
- Detection of application process proxy
- Detection of land attack
- Detection of Ping of death attack

- Detection of new policy addition
- Detection of policy violation
- Virus traffic
- Content filtering detected
- Authentication failure/success

Antiviruses:

- AV Virus Detected
- AV Detection of Backdoor traffic in the network
- Removable Storage Identified
- AV Malware Infection Identified (Not quarantined/cleaned/deleted/moved)
- Multiple AV Malware Infection Identified from Same Host
- Multiple Sources accessing the same Malware URL
- Multiple Types of AV Malware Infection Identified from Same Host
- Detection failure of Antivirus DAT update in end user machines
- Detection of Worm outbreak in the network
- Detection of Virus Outbreak
- Attempt to stop the Adhoc/daily scan schedules
- Detection of Backdoor traffic in the network
- Attempt to stop the AV Services
- Attempt to stop the critical AV modules
- AV identified the Rogue machines in the network
- Detection of the scan which is stopped before it completes
- Detection of the scheduled scan is stopped/paused (delayed)
- Detection of the computer which is not protected with latest definitions
- Detection of the new client software installed
- Detection of the client software uninstalled
- AV Malware Breakout Identified across multiple machines on same Subnet/ Different Subnet
- Multiple re-occurrence of same Infection identified from same machine (AL and Trend - Historical)
- Multiple re-occurrence of unique Infection identified from same machine (AL and Trend - Historical)
- Blacklist Domain/IP Addresses monitoring of traffic emerging to/from the Infected machine (AL and Trend – Real Time)
- Brute Force/port or host scan/privilege elevation access attempt from the Infected machine (AL and Trend – Real Time)
- Attempt to restart AV service or process, AV modules from Infected machine
- Access to critical file share, network path, SSH or Remote RDP attempt from the Infected Host

Uncategorized:

- Default User Account Usage

- Inactive User Accounts
- After Hour VPN Assess Monitoring
- Firewall Top Talkers
- P2P Traffic
- Distributed Host Port Scan
- Distributed Network Host Scan
- SYN Flood by IDS/Firewall
- High Number of Denied Connections for a Single Host
- Worm/Virus Outbreak Detected
- Outbound/Inbound Network Sweep
- AV Update Failed
- Malware IP Access
- Malware URL Access
- Hacking attempt on web portal
- Data Leakage
- Detection of BOTNET infection in Internal LAN
- Unauthorised access from Third Party or vendor networks
- Infected Host Activities
- Suspicious, Adware, Phishing and Hacking Activities
- Unwanted Software's
- AV Malware Breakout Identified across multiple machines
- Monitor Development team's access to Production systems
- Blacklisted IP
- Blacklisted IP Pass after multiple Firewall Block
- Blacklisted URL
- Data Overview Trend
- Outbound Traffic to Suspicious Countries
- Outbound Traffic to Suspicious port
- Outbound Traffic to Suspicious Services
- Terminated User Activity
- Malicious Traffic to Vulnerable Asset
- Communications to Bad Domains
- Communications to Blacklisted Domains/IP's
- Data Transfer involved on Blacklisted Domains/IP's
- Outbound traffic involving Database
- Cross Site Scripting
- Script Injection
- Malicious Activity
- Detection of FW Interface Status Changes/Failures
- Insecure Protocol Usage - Detection of insecure traffic like FTP, telnet, VNC on critical servers
- VPN Access from Outside Country

- Suspicious VPN Login Attempts
- Detection of service stop on ESX servers
- Detection of multiple user failed logins on ESX servers from the same source
- Detection of ESX server shutdown/restart
- Detection of virtual machine start/stop/resume/reboot
- Detection of addition/removal of a host on vCenter
- Detection of virtual machine creation/removal on vCenter
- Probable XSS attack observed
- Probable Directory Traversal attack observed
- Suspicious HTTP methods observed
- HTTP Request Other Than GET, POST, HEAD and OPTIONS
- Probable SQL Injection attack observed
- Web Attack - Vulnerability scanning using Nessus

Na výše definované a další Use case dodavatel vytvoří a naimplementuje zadavateli minimálně 400 pravidel do SIEM řešení.

19.2 Systém pro správu rizik

Dodavatel pro podmínky zadavatele navrhne systém řízení organizace, správu rizik a dosažení shody s legislativními a normativními požadavky (dále také Governance, Risk and Compliance, nebo také GRC).

Dodavatelem se zavazuje, že jím navržený systém bude v souladu s interními politikami, směrnicemi a nařízeními, které se na tuto oblast váží.

Dodavatelem navržené GRC řešení musí splňovat následující obecné požadavky:

Požadavek	**Splňuje (ano/ne)**
Řešení je modulární a umožňuje budoucí rozšíření nástroje.	
Podporuje standardy a legislativu pro řízení bezpečnosti a procesů (ISO/IEC 27001, PCI DSS, SOX) a poskytuje rámec pro snadnou implementaci specifických požadavků (legislativa ČR, nařízení ČNB a další).	
Lze přizpůsobit procesům a postupům zavedených zadavatelem.	
Poskytuje nástroje pro snadný import dat do definovaných struktur (již existující evidence, reporty atd.).	
Veškeré změny provedené uživateli jsou v nástroji zaznamenávány a ukládány do historie.	
Řešení umožňuje definovat workflow (schvalovací, validační, eskalační, …).	
Řešení obsahuje široké možnosti reportování – desítky přednastavených reportů, snadné vytváření reportů na míru. Každý uživatel musí mít možnost si jednoduchým postupem vytvořit vlastní reporty.	

Zadavatel požaduje od dodavatele poskytnutí následujících činností v rámci implementace nástroje pro správu a vyhodnocení rizik:

Implementační požadavky nástroje pro správu a vyhodnocení rizik
Úvodní analýza a identifikace současného stavu
Instalace SW řešení
Úprava SW řešení pro potřeby organizace
Migrace a integrace dat
Podpora zavedení mezi uživatele

19.2.1 Úvodní analýza a identifikace současného stavu

Dodavatel identifikuje v rámci úvodní analýzy a identifikace současného stavu zejména:

- Stávající hlavní procesy a jejich atributy (vstupy, výstupy, workflow, vlastníci procesů, aj.)
- Vstupní data a jejich zdroje (např. zdrojové databáze, podpůrné aplikace, aj.)
- Metodiky, které mají být zpracovány (např. metodika analýzy rizik, proces řízení bezpečnostních incidentů, aj.)
- Podpůrné procesy, které jsou na hlavní procesy navázány

19.2.2 Instalace SW řešení

Dodavatel provede instalaci SW řešení do infrastruktury zadavatele.

19.2.3 Úprava SW řešení pro potřeby organizace

Dodavatel na základě informací z úvodní analýzy a identifikace současného stavu upraví SW řešení dle potřeb a pro podmínky VŘ.

Dodavatelem navržená úprava musí zohledňovat zadavatelovy hlavní procesy a jejich atributy a tyto procesy musí být dodavatelem implementovány do SW řešení.

Dodavatel v kooperaci se zadavatelem navržené úpravy otestuje. V případě potřeby dodatečných úprav SW řešení se dodavatel zavazuje tyto úpravy realizovat po dobu poskytnuté záruky.

19.2.4 Migrace a integrace dat

Dodavatel naplní databázi GRC řešení iniciačními daty.

V rámci naplnění databází se dodavatel zavazuje k:

- Nahráním dat z datových souborů, obvykle typu CSV, prostřednictvím datových importů
- Nastavením integrací s databázemi

19.2.5 Podpora zavedení mezi uživatele

Dodavatel poskytne zadavateli podporu formou školení v rozsahu 3 člověkodní pro uživatele GRC řešení s tím, že jednotlivým zájmovým skupinám v prostředí zadavatele představí řešení jako celek a jeho jednotlivé části, které budou uživatelé využívat pro svou práci.

Dodavatel poskytne zadavateli podporu formou školení pro administrátory v rozsahu 2 člověkodní a to tak, aby mohly být prováděny zásahy do řešení bez účasti dodavatele.

Požadavky na systém:

Požadavek	**Splňuje (ano/ne)**
Řešení musí nabídnout nástroje pro správu problémů nebo schopnost tento nástroj nastavovat v souladu s neustálým vylepšováním procesu.	
Systém musí automaticky generovat zprávy o nesprávných odpovědích z dotazníkových kampaní.	
Systém musí nabídnout schopnosti vytváření, přidělování a sledování problémů	
Systém musí počítat zbytkové riziko i na základě již provedených nápravných opatření.	
Systém musí nabídnout standardní konsolidované řešení správy problémů napříč organizací.	
Systém musí umožňovat sesbírat a dále poskytovat rizika, problémy a všechny ostatní nálezy, které nejsou v shodě s politikami na nejnižší možné úrovni a také je umět logicky seskupovat.	
Systém musí umožnit manuálně vkládat různé další vstupy, které jsou považovány za problém nebo nález (jako incidenty, hodnocení rizik, audity apod.)	
Systém musí poskytnout schopnost nastavit si frekvenci vytváření a posílání sledovaných problémů.	
Systém musí zadavateli umožnit jasně přidělovat vlastnictví jednotlivých problémů.	
Systém musí přidělovat nálezy zodpovědným řešitelům automatizovaně.	
Systém musí poskytnout schopnost dokumentování, sledování a vyhodnocení správného výstupu / schvalování všech problémů.	
Systém musí umožnit automatizovaně provádět všechna hlášení, aktualizace stavů i nutné eskalace.	
Řešení musí umožnit nejen sledovat a oznamovat problém, ale zároveň dodávat i stavy nápravných opatření.	
Systém musí nabídnout zprávy o kritických nálezech, dílčích stavech problémů a také pokroky v nápravných opatřeních.	

Řešení musí umožnit přidělování závažnosti problému na základě subjektivního pocitu auditora.	
Řešení musí umět omezit přístup k nálezům a pokroku v řešení na konkrétní osoby/role.	
Systém musí umožňovat sběr a skladování odpovědí k jednotlivým problémům od managementu.	
Systém musí mít připravenu strukturu správy předschválených výjimek, ale také musí umožnit tuto strukturu přizpůsobovat potřebám firemního procesu.	
Systém musí umožnit řídit výjimky s odpovídajícímm přijetím rizika.	
Systém musí podporovat vložení časově omezených žádostí o výjimky z politiky, sledovat konce výjimek a předem informovat příslušné strany.	
Systém musí podporovat jasně definovaný proces žádosti o výjimku nebo změnu v politikách společnosti.	
Systém musí mít připravenu strukturu správy nápravných opatření, ale také by měl umožnit tuto strukturu přizpůsobovat potřebám firemního procesu.	
Systém musí přiřazovat nápravná opatření všem nálezům, na které je v opatřeních odkazováno.	
Řešení musí soustředit plány nápravných opatření z různých zdrojů {jako řízení rizik a shody s firemní politikou nebo výstupy z auditů} na jedno místo.	
Řešení musí organizaci umožnit jasné přidělování vlastnictví nápravných opatření, jejich správné přidělování zodpovědným osobám ke správě, sledování a vyhodnocování schvalovacího procesu a výstupů a v případě nutnosti i jejich eskalaci.	
Řešení musí stejně dobře umět sledovat a hlásit problémy i nápravná opatření.	
Řešení musí poskytovat zprávy, o propásnutých nálezech a protahujících se nápravných opatřeních.	
Systém musí poskytovat oznámení, která třídí nálezy podle procesů, oddělení, divizí nebo jiné organizační jednotky.	
Systém zahrnuje základní metodologii analýzy podnikových dopadů (BIA), která může poskytnout společnou strukturu pro organizaci.	
Systém musí obsahovat registr záznamů o procesech a jejich atributy, jako popis, umístění, personál atd.	
Metodologie analýzy dopadů (BIA) musí obsahovat různé druhy kategorií hodnocení závažnosti procesu.	
Metodologie analýzy dopadů (BIA) musí obsahovat standardizované propočty k procesům (cílový čas a objekt obnovy / RTO,RPO) vedoucí k celkovému hodnocení závažnosti jednotlivých aktiv.	
Metodologie analýzy dopadů (BIA) musí podporovat postupnou hloubkovou analýzu dopadů tak, aby procesy dle závažnosti, RTO's a RPO's	

(cílový čas a objekt obnovy) mohly být zděděny podpůrnými zařízeními a aplikacemi.	
Systém musí obsahovat atributy a data o procesech získané na základě ostatních GRC procesů, jako jsou profily rizik, kontinuita, shoda s organizačními politikami, Incidenty apod.	
Systém musí obsahovat vlastnosti pro skupinu lidí zabývající se řízením kontinuity organizací (BCM) tak, aby mohla provádět nebo měnit metodologii analýzy dopadů napříč organizací. Navíc systém musí umožnit sledování metologií procesů, které nejsou správně aktualizované.	
Systém musí zahrnovat pracovní postup pro více účastníků procesu Metodologie analýzy dopadů (BIA), včetně vlastníka procesu a dalších, kteří mohou potřebovat dodávat vstupy. Systém dále musí zahrnovat přezkoumávání ostatních úrovní týmem BCM (řízení kontinuity organizací).	
Systém musí umožnit mapování procesů na jejich podpůrnou infrastrukturu, dodavatele a personál.	
V systému musí být zaznamenávány i závislosti na ostatních procesech.	
Metodologie analýzy dopadů (BIA) musí bý každý rok aktualizována nebo vyrobena zcela nová.	
Systém musí umožňit archivovat a spravovat jednotlivé Metodologie analýzy dopadů (BIA).	
Administrátoři musí mít možnost resetovat uživatelská hesla, nastavovat bezpečnosnostní pravidla a řídit pravidla politiky hesel	
Systém musí poskytovat předkonfigurované uživatelské/adminstrátorské role	
Systém musí bý schopen bezproblémové integrace se systémem Active Directory a LDAP (Lightweight Directory Access Protocol).	
Systém podporuje autentizační protokol SAML 2.0	
Systém musí umožňovat rozšiřirovat implementované a přidávat nové "use cases" (případy užití) za pochodu.	
Jednotlivé Use cases (případy užití) umožňují přidání dalších polí/atributů bez zásahu profesionálních služeb dodavatele. Vzorce nebo kalkulace použité v polích/atributech musí umožnit jednoduše měnit lokálním administrátorem bez zásahu služeb dodavatele.	
Systém musí umožnit uspořádání a přizpůsobení uživatelského rozhraní	
Systém musí umožňit sestavovat vztahy mezi aktivy (např. vztah zařízení k prostředí, ve kterém je instalováno).	
Systém musí dokázat zdokumentovat organizační schéma organizace.	
Systém musí dokázat zmapovat organizační infrastrukturu včetně produktů a služeb, procesy, informační aktiva, budovy, zařízení i personál.	

20 Service desk systém

Předmětem je zajištění nového procesně-analyticko-řídícího nástroje ServiceDesk pro 50ti členný řešitelský tým, který bude plně v souladu s best-practices ITIL V3. Součástí je plná implementace do prostředí zadavatele pro řízení interních procesů, externích dodavatelů a bezpečnostních incidentů pro SOC. Tyto procesy budou definovány během analytických prací definovaných v kapitole 13.

Požadavky na systém:

Požadavek	**Splňuje (ano/ne)**
Certifikace PinkVERIFY, ITIL v3.+	
Založení ticketu	
Přiřazení ticketu řešiteli	
Nastavení termínu vyřešení kritičnosti	
Automatická historie a audit	
Možnost definování procesů	
Reporting	
Definice SLA pro různé projekty	
Definice služeb, přístupů, rolí	
Definice schvalovacích pravidel	
Integrace na AD a email	
Automatické zakládání ticketů z emailů	
Incident, problém change, service management	
Aplikace musí běžen ana systému linux a musí používat opensource databázi	

20.1 Tvorba procesů dle standardu ITIL

Definice procesů podpory podle ITIL (a service desk – při zadani na externí dodavatele)

Požadavek	**Splňuje (ano/ne)**
Dodavatel vytvoří politiku pro systém managementu služeb. Tato politika musí být v souladu s interními politikami, směrnicemi a nařízeními.	
Dodavatel danou politiku vytvoří tak, aby byla v souladu zejména s: o ISO/IEC 20000 – Management služeb o ISO/IEC 9001 – Systémy managementu kvality o ITIL	
Dodavatel danou politiku zpracuje minimálně v rozsahu: o Pochopení a naplňování požadavků na služby pro dosažení spokojenosti zákazníků	

○ Ustanovení politiky a cílů pro management služeb ○ Návrh a dodávka služeb založených na systému managementu služeb přinášejících přidanou hodnotu pro zákazníka ○ Monitorování, měření a přezkoumání výkonnosti systému managementu služeb ○ Neustálé zlepšování systému managementu služeb na základě objektivních měření	
Dodaným výstupem bude: textový editor ve formátu .doc/.pdf, ve kterém bude definována politika systému managementu služeb obsahující výše uvedené.	

21 Bezpečnostní operační centrum SoC

Dodavatel se zavazuje poskytovat zadavateli služby v režimu 24x7 (tj. 24 hodin 7 dní v týdnu)

Dodavatel se zavazuje poskytnout pro výkon služby bezpečnostního operačního centra zadavateli Incident Response tým (CSIRT) a to dle specifikací:

Služba	Splňuje (ano/ne)
Incident response tým (CSIRT)	
Security Awareness	

21.1.1 SOC team

Dodavatel garantuje zadavateli dojezdový čas pro přímý zásah on-site v případě incidentu, který to vyžaduje, a to následovně:

Kategorie incidentu	Dojezdový čas	Splňuje (ano/ne)
Kritický incident	Max 60 minut	

Dodavatel garantuje zadavateli schopnost řešení bezpečnostního incidentu. Tuto schopnost dodavatel potvrdí zadavateli získanými certifikacemi řešitelského týmu pro jednotlivé technologie používané pro řešení bezpečnostního incidentu.

Dodavatel garantuje zadavateli čas odezvy bezpečnostního incidentu (dále jen Incident Response Time nebo také IRT) a to pro jednotlivé kategorie bezpečnostních incidentů následovně:

Kategorie incidentu	IRT	Splňuje (ano/ne)
Kritický	Max 30 minut	
Vysoký	Max 1 hodina	
Střední	Max 1 den	
Nízký	Max 3 dny	

Jednotlivé incidenty budou kategorizovány na základě dodavatelem vytvořené metriky, která vznikla v rámci Procesu pro řízení bezpečnostních incidentů této zadávací dokumentace.

Je požadováno v rámci této služby převzít všechny implementované Use-case, které jsou součástí implementace SIEM řešení.

Zadavatel požaduje, aby v rámci poskytování služby Bezpečnostního operačního centra dodavatel rovněž dodával Security Awareness program, a to minimálně v rozsahu:

21.1.2 Security Awareness

Dodavatel se zavazuje poskytovat zadavateli kontinuální vzdělávání/zvyšování povědomí o kybernetických bezpečnostních hrozbách a k nim vztažené problematice.

Dodavatel se zavazuje realizovat vzdělávání/zvyšování povědomí na dvou rozdílných úrovních a to:

- Uživatelská úroveň
- Administrátorská úroveň

Dodavatel se zavazuje realizovat vzdělávání/zvyšování povědomí pro úrovně v rozdílné míře detailu a složitosti.

Dodavatel se zavazuje realizovat vzdělávání minimálně v oblastech:

- Rozpoznání a reakce na nové hrozby
- Obsluha technologií
- Procesu řízení bezpečnostních incidentů

Dodavatel se zavazuje realizovat školení v minimálním rozsahu 1 školení (8 hodin) kvartálně.

Dodavatel se zavazuje ke zvyšování bezpečnostního povědomí prostřednictvím zasílání novinek v této oblasti prostřednictvím emailu. Tyto novinky dodavatel poskytne zadavateli formou článků v českém nebo anglickém jazyce minimálně 1x týdně.

22 Podmínky technické podpory (SLA)

Dodavatel se zavazuje poskytovat zadavateli služby v režimu 24-7 v minimálním rozsahu:

- telefonická hot-line podpora pro okamžitou komunikaci 24h denně
- diagnostika a odstraňování poruch systému
- profylaxe - preventivní prohlídka systému v rozsahu
- kontrola stavu nainstalovaných updatů a hotfixů
- kontrola a analýza chybových logů systémového SW, stejně tak aplikačního programového vybavení
- kontrola vytíženosti systémových zdrojů
- sběr zpětné vazby od administrátorů systému

Dodavatel garantuje zadavateli čas pro odezvu a čas pro vyřešení provozního incidentu, a to pro jednotlivé kategorie provozních incidentů následovně:

Kategorie incident	Doba odezvy (IRT)	Doba vyřešení (TRT)
Kritický - v případě kritické chyby	60 minut	2 hodiny
Vysoký – v případě závažné chyby	60 minut	8 hodin
Střední – v případě běžné chyby	1 den	3 dny
Nízký – v případě minoritní chyby	3 dny	Best effort

Podpora je poskytovaná v českém jazyce ve formě Help-desk podpory a v případě kritického incidentu telefonické podpory. Jednotlivé úkony/akce dle specifikace podpory jsou definovány následovně.

Doba odezvy (IRT)

Je definovaná jako časový interval měřený od doby, kdy Objednatel ohlásil incident do Helpdeskové aplikacee poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikace po dobu, kdy je zpětně kontaktovaný poskytovatelem nebo je incident přijat do řešení. Doba odezvy může být také označována jako reakční doba.

Doba vyřešení (TRT)

Je definovaná jako časový interval měřený od doby, kdy Objednatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikaci po dobu, kdy poskytovatel vyřešil popsaný incident.

Priority

Zaručená doba odezvy na vzniklé incidenty se dělí dle jejich priority. Priorita je dána kritičností vzniklého incidentu v návaznosti na požadovanou funkčnost produktu:

- **Kritická chyba** – Nefunkčnost způsobená dodanou technologií, Nefunkčnost/nedostupnost řešení
- **Závažná chyba** – Nefunkčnost některé z komponent, která nedovoluje vykonávat požadovanou činnost. Vážné chyby řešení ovlivňující provoz objednatele.
- **Běžná chyba** – Nefunkčnost některé z komponent, která nemá přímý dopad na dostupnost objednatele, vážné konfigurační chyby.
- **Minoritní chyba** – Chyby v konfiguraci, Chyby řešení neovlivňující provoz objednatele, Nefunkčnost komponent minoritního charakteru.

SLA podpora v režimu 24-7 dodavatele je uvažována pro následující body technické specifikace:

- LAN a WiFi instrastruktura
- Service desk systém
- Perimetrový Next Generation Firewall, Interní firewall a ochrana proti DDoS
- Web aplikační firewall
- Kompletní ochrana koncových stanic
- Nástroj pro sběr a korelaci událostí a logů (SIEM)

23 Příloha

Součástí této Technické specifikace je následující příloha:

- Příloha č. 1: Cílový koncept – vzor dokumentu