Příloha č. 2: Technická specifikace

Obsah

1 Popis projektu a společná kritéria

Projekt je koncipován jako ucelené řešení bezpečnosti Zadavatele, nikoliv jako dodávka technologií. Skládá se z následujících provázaných celků:

1. Analýza a procesní bezpečnost – definice postupů, procesu, směrnic a dalších opatření pro naplnění bezpečnostních potřeb Zadavatele dle analýzy prostředí a požadované kompatibility s definovanými regulacemi.
2. Technologie – souhrn řešení pro jednotlivé oblasti bezpečnosti, jež je tvořena konkrétními produkty s výkonnostními parametry.
3. Integrace – způsob kooperace a míra provázanosti technologií tak, aby tvořily funkční celek s maximální přidanou hodnotou pro bezpečnost daného prostředí.
4. Automatizace – scénáře pro abstrakci práce s technologiemi formou snadno použitelných předpřipravených akcí pro operátory bez nutnosti manuálního zásahu do konfigurace jednotlivých technologií.

V rámci analýzy bude definována bezpečnostní politika v návaznosti na potřeby zadavatele včetně kvantifikovatelných parametrů typu Recovery Time Objective (RTO), Recovery Point Objective (RPO), přičemž hodnoty těchto parametrů budou definovány v rámci projektu v části Analytické práce v oblasti bezpečnosti a dalších, které vycházejí z vyžadované metodiky. Na základě těchto parametrů musí být nastaveny a integrovány dodané technologie, včetně tvorby automatizačních scénářů tak, aby bylo možné splnit mezní limity těchto parametrů. Požadavky na kapacitu, interoperabilitu se známými technologiemi a otevřenost protokolů vychází z předběžné analýzy prostředí a zohledňuje požadavky na míru integrace a automatizace, která je očekávána v rámci projektu.

Ke každé technologii (aktivitě) bude vypracován Cílový koncept (Solution Design dokument), který popíše přesné zapojení do stávající infrastruktury, popis systémové konfigurace a provozní konfigurace, včetně integrací a veškeré interoperability s dalšími technologiemi. Nastavení konfigurace a uvedení do ostrého provozu musí být rozplánováno s ohledem na kapacitní možnosti Zadavatele, případně servisní okna daného prostředí dle dopadů na funkcionalitu. Solution Design musí být vzájemně odsouhlasen.

Konfigurační parametry dané definicí procesů a opatření musí být následně aplikovány na všechny technologie v rámci dodávky projektu a dále na existující technologie, které to dovolují (např. komunikační protokoly včetně úrovně zabezpečení, síla hesla atp.).

DR (Disaster Recovery) plán jakožto jeden z poptávaných výstupů v rámci analytických prací definuje participaci jednotlivých technologií při obnově primárních procesů organizace a určuje formu a rychlost obnovy chodu technologie. Toto musí být reflektováno v popisu obnov technologií a jejich návazností formou detailní provozní dokumentace. Pro účely DR je dále požadováno, aby měly všechny dotčené systémy nastaven adekvátní plán zálohování dat a systémové konfigurace, přičemž bude podle připravených scénářů docházet k pravidelným testům obnovy. Podle typu řešení lze využít formu snapshotu ve virtuálním prostředí, automatického provisioning procesu skrze automatizační scripty a šablony, případně rekonfigurace HW zařízení přes OOB (out of band) rozhraní.

Schopnost dané technologie zajistit konzistenci systémové konfigurace a procesovaných dat při zálohování a obnově je společným požadovaným kritériem pro všechny technologie v rámci dodávky.

Všechny technologie využívající certifikáty musí používat Public Key Infrastructure (PKI) definovanou v rámci projektu, přičemž je vyžadován standard TLS 1.2 či vyšší.

Všechny nově pořizované technologie projektu musí být pokryty podporou od výrobce po dobu minimálně 60 měsíců, a to v režimu NBD 5x9; preferovány jsou trvalé (perpetual) licence, v případě, že trvalá licence není k dispozici, pak subscription s plnou funkcionalitou na dobu minimálně 60 měsíců.

V případě potřeby pořízení dodatečných licencí po dobu nezbytně nutnou pro účely implementace/testování, musí být tyto součástí nabídky dodavatele a řádně naceněny v rámci položkového rozpočtu na separátním řádku jako samostatná položka.

2 Aktivita č. 1 - Realizace perimetrového a centrálních firewallů

Řešení pro ochranu uživatelského a síťového provozu. Zajištění ochrany pomocí realizace parametrového a centrálních firewall technologie v režimu active-active **a** active-passive s odpovídajícími funkcionalitami a požadavky pro ochranu provozu dle specifikace. Ochranu před zero-day malware zajišťuje dedikovaná HW appliance, jenž je s firewall řešením integrována pro kontrolu webového a e-mailového provozu. Řešení musí být homogenní, tj. všechny komponenty jsou od stejného výrobce a společně tvoří funkční celek požadovaných parametrů, včetně jednotné administrátorské konzole.

2.1 Firewall technologie

NG FW č.1		
Obecné požadavky na NGFW platformu	ANO/NE	Popis splnění požadavku
HW appliance o maximální velikosti 1U		
Podpora režimu vysoké dostupnosti active/active a active/passive		
Podpora duálního napájení (dva zdroje a přívodní kabeláž je součástí každého dodaného zařízení)		
Minimálně 2x 10 GbE SFP+		
Minimálně 8x 1 GbE RJ45 síťová rozhraní		
Integrované TPM řešení nebo jeho ekvivalent		
Výkonové požadavky	ANO/NE	Popis splnění požadavku
Minimální propustnost NGFW pro IPv4 provoz je 25 Gbps (UDP komunikace a paket velikosti 512B)		
Kapacita současně navázaných spojení NGFW je alespoň 3 000 000 a kapacita nově sestavených spojení za sekundu je alespoň 120 000		
Propustnost NGFW pro IPSEC VPN je alespoň 25 Gbps bez licenčního omezení počtu sestavených spojení		
Propustnost NGFW při zapnuté funkci SSL inspekce využívající IPS inspekci je alespoň 2,5 Gbps		
Propustnost NGFW při zapnuté funkci aplikační kontroly je alespoň 6,5 Gbps		
Propustnost NGFW při zapnuté funkci IPS inspekce a současném logování provozu je alespoň 4 Gbps		
Propustnost NGFW při paralelně provozovaných funkcích stavového FW, IPS, aplikační kontrole a logovaní (obecně popisovaná kombinace funkcí pro NGFW zařízení) je alespoň 2 Gbps		
Maximální udávaná latence NGFW (pro udp provoz nebo průměrná hodnota) je 9 µs		
Funkční požadavky	ANO/NE	Popis splnění požadavku
Jedná se o řešení dnes označované jako NGFW s integrovanou grafickou a CLI správou umožňující kompletní obsluhu zařízení		
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46		

Podpora režimů explicitní a transparentní proxy		
Podpora ověřování identity uživatelů pomocí externích zdrojů s možností napojení na adresářové služby (například Microsoft Active Directory, OpenLDAP apod.), LDAP, Radius, Kerberos a práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On		
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů		
Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu		
Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek		
Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup.		
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3		
Možnost logické segmentace zařízení s použitím tzv. virtuálních kontextů v minimálním počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty.		
Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků		
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.		
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací		

výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace		
Možnost definice zakázaných slov pro vyhledávání na internetu		
Schopnost inspekce protokolu QUIC		
Možnost využít výrobcem udržovanou databázi internetových služeb při definici bezpečnostní politiky		
Podpora kategorizace streamovaných videí a kanálů jako například YouTube		
Podpora konceptu ZTNA (Zero Trust Network Access) nezávisle na konkrétní architektuře výrobce		
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů		
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času		
Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být alespoň jeden testovací HW/mobilní token a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN		
Podpora směrování provozu prostřednictvím otevřených standardů (např. WCCP v2).		
Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy		
Podpora ICAP rozhraní pro obousměrnou integraci s externími servery		
Podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP)		
Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP ve verzí IPv4 a IPv6		
Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)		
Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení		
Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí		
funkce ochrany proti DDoS útoku na zařízení alespoň v podobě nastavení limitu objemu a typu provozu, který bude zařízení aktivně spracovávat před jeho zahozením		
Analýza a zabezpečení DNS dotazů (ochrana před DNS posoningem), filtrování DNS dotazů na základě kategorizace		
Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu		

NGFW může volitelně obsahovat funkci bezdrátového kontroleru s podporou standardních protokolů pro řízení přístupových bodů		
Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz		
Další požadavky	ANO/NE	Popis splnění požadavku
Součástí každého dodaného zařízení je podpora výrobce s možností kontaktovat podporu 24/7, vyměnit zařízení v režimu 8x5, licence pro spuštění požadovaných funkcí a výrobce umožňuje zdarma stáhnout VPN klienta kompatibilního se standardními protokoly IPsec/SSL. Vše s platností 5 let.		

NG FW č.2		
specifikace FW	ANO/NE	Popis splnění požadavku
min. 4x 10 GbE SFP+ port		
min. 8x 1 GbE SFP port		
min. 16x 1 GbE RJ45 port		
samostatné RJ45 porty pro mgmt, HA a připojení konzoly		
HW appliance (VM app. ani software řešení není akceptovatelné)		
podpora režimu vysoké dostupnosti min. active/active a active/passive, cluster o dvou fyzických zařízeních		
duální napájení		
montáž do 19" RACK, výška max. 1U		
výkonové požadavky	ANO/NE	Popis splnění požadavku
min. 25 Gbps propustnost pro IPv4 provoz (UDP komunikace s pakety s velikostí 512B)		
min. 3 000 000 současně navázaných spojení		
min. 250 000 nových spojení za sekundu		
max. 5µs latence pro pakety o velikosti 64B		
min. 12 Gbps celková propustnost IPSEC VPN (paket 512B a šifrování AES256-SHA256)		
min. 2 Gbps propustnost SSL VPN		
min. 4 Gbps propustnost funkce SSL inspekce		
min. 10 Gbps propustnost při využití aplikační inspekce		
min. 3500 CPS u spojení kontrolovaných pomocí SSL inspekce		
min. 5 Gbps propustnost funkce IPS		
min. 3 Gbps propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací)		
min. 3 Gbps propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem)		
min. 500 současně připojených uživatelů SSL VPN		
min. 2000 souběžně navázaných site-to-site IPSEC tunelů		
funkční požadavky	ANO/NE	Popis splnění požadavku

integrované konfigurační rozhraní pro plnou administraci (grafické i CLI), bez licenčního omezení na počet administrátorů		
logická segmentace HW s použitím tzv. virtuálních kontextů v min. počtu deseti současně běžících kontextů v ceně zařízení, každý kontext musí pracovat izolovaně, možnost interně propojit jednotlivé kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty		
podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46		
možnost nasazení ve všech z následujících režimů: L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)		
ověřování identity uživatelů (MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On		
podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů		
ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu		
funkce QoS, traffic shaping a SD-WAN min. v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek		
funkce VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran), SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy, podpora portálového režimu pro bezklientský přístup		
podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3		
antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků		
funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (mobile malware)		
detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén)		
ochrana před rychle se šířícími kampaněmi škodlivého kódu (virus outbreak)		
sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby)		
funkce rozpoznávání min. 4000 populárních sítových aplikací na základě jejich charakteristiky provozu na apl.vrstvě, pravidelná aktualizace signatur aplikací, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace		

možnost definice zakázaných slov pro vyhledávání na internetu		
podpora funkce Safe Search pro populární vyhledavače		
funkce kategorizace webových stránek (web filtering) s podporou kategorizace na skupiny (pracovní zájmy, osobní zájmy, hazard, pornografie, sdílená uložiště, stránky se škodlivým kódem, nově registrované domény atd.), výrobcem aktualizovaná databáze s pokrytím českého internetu, definice časových kvót pro uživatele a kategorie webu, akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii		
kategorizace streamovaných videí a kanálů min. pro platformu Youtube a Vimeo		
funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů		
možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času		
funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslání/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.		
podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být 2 testovací HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN		
Podpora směrování provozu prostřednictvím otevřených standardů (např. WCCP v2).		
podpora konfig. PAC souborů pro režim nasazení explicitní proxy		
podpora ICAP rozhraní pro obousměrnou integraci s ext.servery		
podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP)		
podpora statického a dynamického směrování min. OSPF a BGP		
podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)		
podpora IPAM funkcionality pro správu přidělených IP adres		
podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí		
analýza a zabezpečení DNS dotazů (ochrana před DNS posoningem), filtrování DNS dotazů na základě kategorizace		
možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu		
volitelná funkce bezdrátového kontroleru s podporou standardních komunikačních protokolů		
schopnost integrace s centrální platformou pro správu síťových prvků		

funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí		
funkce ssl offloading a ssl inspekce pro rozkládaný provoz		
další požadavky	ANO/NE	Popis splnění požadavku
podpora výrobce v režimu 24/7 na dobu 5 let		
všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu 5 let musí být také součástí dodávky		

2.2 Implementace

NGFW, Analýza a ukládání logů – implementace		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
fyzická montáž zařízení a propojení do stávající síťové infrastruktury		
upgrade firmware na aktuální stabilní verzi doporučenou výrobcem		
analýza stavu topologie a současné konfigurace		
zapojení do clusteru, včetně možnosti rozložení zátěže na jednotlivé boxy		
úprava konfigurace firewallu dle doporučení vyplívající z analýzy		
optimalizace bezpečnostních profilů		
migrace konfigurace všech funkcionalit implementovaných na stávajících firewallech včetně WiFi kontroléru		
konfigurace hloubkové SSL inspekce		
akceptační testy a testovací provoz		
školení administrátorů v rozsahu 4 hodin		
dokumentace skutečného provedení		
rekonfigurace RDS, která byla pozdržena do doby upgrade centrálních firewallů		
návrh topologie SD-WAN		
konfigurace SD-WAN, dynamic routing (BGP, OSPF) v centru		
konfigurace SD-WAN, dynamic routing (BGP, OSPF) vzdálených lokalit, rekonfigurace fw pravidel		
implementace management nástroje a napojení všech prvků do managementu		
implementace nástroje pro bezpečnostní analýzu logů z NGFW zařízení se schopností jejich korelace včetně možnosti ukládání logů		

3 Aktivita č. 2 - Realizace nástroje pro detekci a prevenci pokročilých hrozeb

Sandbox appliance zpracovává dokumenty poskytnuté firewall řešením a není zapojena inline v cestě datového toku infrastruktury. Appliance musí provádět kontrolu připojených datových uložišť na přítomnost malware v obsažených souborech.

3.1 Sandbox

Sandbox		
Obecný požadavek	ANO/NE	Popis splnění požadavku
Požadováno je řešení ochrany před zero-day hrozbami, škodlivým kódem a malwarem s využitím technologie sandbox, formou samostatného zařízení (fyzického nebo virtuálního). Řešení musí umožnit obousměrnou integraci s NG firewally a bezpečnostními bránami pomocí standardních nebo výrobcem dokumentovaných rozhraní (např. API, ICAP, log forwarding), s technickou podporou výrobce. Součástí dodávky musí být technická podpora a předplatné všech požadovaných funkcí na dobu minimálně 5 let s dostupností 24x7.		
HW požadavky	ANO/NE	Popis splnění požadavku
HW nebo SW appliance s operačním systémem navrženým pro bezpečnostní analýzu pro analýzu zkoumaných vzorků		
Minimálně 3 paralelní instance sandboxu s operačním systémem Windows včetně licencí (součástí dodávky).		
Minimálně 1 instance pro analýzu dokumentů Microsoft Office.		
Funkční požadavky	ANO/NE	Popis splnění požadavku
- Podpora sandboxingu různých OS: Windows 7–11, macOS, Linux, Android, systémy průmyslového řízení.		
Plnohodnotná, výrobcem podporovaná a obousměrná integrace s nabízeným modelem firewallu a dalšími nabízenými bezpečnostními prvky		
Možnost integrace s interními systémy pomocí dokumentovaného API, podpora funkce API musí být součástí nabídky		
Odchozí komunikace ze sandboxovacích image musí do internetu odcházet přes dedikované síťové rozhraní		
Podpora režimu clusterování s cílem dosažení vysoké dostupnosti a navyšování výkonosti v budoucnu		
Inspekce vzorků založená na vícevrstvá ochrana před škodlivým kódem – kombinace antivirové kontroly za pomoci signatur, emulace kódu a plnohodnotný sandboxing (spuštění v reálném operačním systému) a umělé inteligence (AI)/strojového učení (ML). Všechny tyto úrovně musí být integrovány do jednoho zařízení a vzájemně spolupracovat.		

Možnost vytvořit, spustit a pro sandboxing používat vlastní konfiguraci operačního systému, včetně konkrétních aplikací odpovídajících konfiguraci v chráněné síti, který bude naimportován do platformy Sandbox a využíván pro inspekci		
Detailní konfigurace politiky pro kontrolu, kontrola v různých typech OS, možnost kontroly jednoho souboru v různých operačních systémech zároveň, možnost definice vybraných aplikaci v různých typech OS.		
Ochrana proti zjištění běhu v sandbox prostředí (anti evasion techniky)		
Všechny prvky ochrany musí být poskytovány lokálně, nikoliv jako cloud služba (s výjimkou těch, u kterých to nedovoluje legislativa)		
Detekce komunikace s C&C centry		
Podpora detekce přístupu na kompromitované URL		
Funkce reportingu nalezených problémů (Součástí výsledné informace nesmí být pouze status čistý/škodlivý kód, ale kompletní informací včetně detailního popisu chování, packet capture, a v případě projevu malware v GUI také screenshoty či video záznam), podpora reportingu v MITRE ATT&CK formátu pro analýzu SoC, podpora STIX 2.0 formátu		
Podpora kontroly minimálně následujících typů souborů a aplikací: MS Office, Adobe Acrobat Reader, Adobe Flash Player, MS Internet Explorer, Mozilla Firefox, Google Chrome, Java, MS .NET Framework, Visual C++, Python; spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např. .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh,Mach, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip		
Podpora sandboxingu průmyslových řídících protokolů a aplikací: tftp, modbus, s7comm, http, snmp, bacnet, ipmi		
Podpora reportování ve standardních formátech (HTML, CSV, PDF, XML, …)		
Automatická aktualizace signaturových databází odhalených hrozeb včetně funkce sdílení těchto signatur na nabízenou platformu firewallů a dalších bezpečnostních komponent		
Přímé obousměrné propojení s nabízenou platformou firewallů a dalších bezpečnostních komponent		
Podpora logování na externí nástroje a SIEM		
Podporované režimy nasazení minimálně: napojení na bezpečnostní prvky pomocí otevřených a dokumentovaných rozhraní, sniffer režim (odposlech a rekonstrukce sítového provozu min. pro protokoly http, smtp, pop3, imap, ftp, mapi, im, smb), sanboxing souborů uložených na		

dostupných sítových discích, příjem souborů k sandboxingu pomocí API, podpora rozhraní typu ICAP.		
Výkonové požadavky	ANO/NE	Popis splnění požadavku
Kapacita inspekce neznámého kódu pomocí paralelního běhu s využitím až 14 skenovacích image operačního systému Windows na jedna sandbox appliance		
Výrobcem udávaná propustnost min. 10000 souborů za hodinu při aplikaci pre-filteringu před samotným sandboxingem a využití plné kapacity sandboxu		

3.2 Integrace

Řešení musí podporovat dynamické seznamy objektů z komponent, které definují virtuální koncová zařízení a uživatele, nejméně z prostředí Microsoft AD a VMware tak, aby tyto objekty mohly být využity pro tvorbu bezpečnostních politik bez nutnosti manuální rekonfigurace pravidel při změně jednotlivých položek dynamického objektu.

Automatizační procesy, jež jsou požadovány a budou součástí Solution Designu musí zahrnovat změny bezpečnostní politiky firewall formou změn bez nutnosti manuálního zásahu správce. Řešení musí být takto konfigurovatelné i přes API rozhraní. Minimální množina automatizačních postupů pro firewall:

1. Změna filtračních pravidel reflektujících riziko koncového zařízení či síťového segmentu (zablokování, restrikce na administrátorský prostup, povolení do původního stavu),
2. konfigurace IPS profilu,
3. založení VPN prostupu či jeho zablokování,
4. nastavení nového uživatele pro SSL VPN či jeho zrušení,
5. schopnost záchytu síťové komunikace ve formě PCAP pro požadované rozhraní,
6. odpojení síťových rozhraní či skupin rozhraní při kritickém scénáři.

3.3 Implementace

Součástí dodávky je nasazení řešení jako součásti perimetrové ochrany, včetně oddělení IT/OT infrastruktury, ochrany uživatelského provozu a zabezpečení interních segmentů, zejména datových center. Řešení musí být implementováno tak, aby podporovalo požadovanou funkcionalitu dle této specifikace.

4 Aktivita č. 13 – Analytické práce v oblasti bezpečnosti

4.1 Bezpečnostní dokumentace

Zadavatel požaduje v této části kompletní dodávku bezpečnostní politiky a bezpečnostní dokumentace. Očekává se po formální stránce plná shoda se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), včetně všech prováděcích vyhlášek, resp. s právní úpravou, která uvedený právní rámec v době plnění nahradí a zajištění shody s přílohou č. 5 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

Před vytvářením bezpečnostní dokumentace bude provedeno zmapování současného stavu a sběr informací o zaběhlých procesech a pravidlech nemocnice tak, aby bylo možné vytvořit harmonogram tvorby bezpečnostní dokumentace. Při tvorbě bezpečnostní dokumentace musí být brány v potaz již existující dokumenty nemocnice.

Pro všechny výstupy je požadována vysoká připravenost na novou legislativu NIS2. V případě, že v průběhu plnění smlouvy o dílo před dokončením a akceptací této aktivity bude platná a účinná nová legislativa NIS2, požaduje se plná shoda výstupů této části s novou legislativou.

Pro naplnění celé řady zákonných požadavků je nutné vytvořit bezpečnostní politiky a další bezpečnostní dokumentaci, minimálně v rozsahu požadavků (viz příloha č. 5 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti):

1. Politika systému řízení bezpečnosti informací
2. Politika řízení aktiv
3. Politika organizační bezpečnosti
4. Politika řízení dodavatelů
5. Politika bezpečnosti lidských zdrojů
6. Politika řízení provozu a komunikací
7. Politika řízení přístupu
8. Politika bezpečného chování uživatelů
9. Politika zálohování a obnovy a dlouhodobého ukládání
10. Politika bezpečného předávání a výměny informací
11. Politika řízení technických zranitelností
12. Politika bezpečného používání mobilních zařízení
13. Politika akvizice, vývoje a údržby
14. Politika ochrany osobních údajů
15. Politika fyzické bezpečnosti
16. Politika bezpečnosti komunikační sítě
17. Politika ochrany před škodlivým kódem
18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
20. Politika bezpečného používání kryptografické ochrany
21. Politika řízení změn
22. Politika zvládání kybernetických bezpečnostních incidentů
23. Politika řízení kontinuity činností

24. Zpráva z auditu kybernetické bezpečnosti
25. Zpráva z přezkoumání systému řízení bezpečnosti informací
26. Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik
27. Zpráva o hodnocení aktiv a rizik
28. Prohlášení o aplikovatelnosti
29. Plán zvládání rizik
30. Plán rozvoje bezpečnostního povědomí
31. Evidence změn
32. Hlášené kontaktní údaje
33. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků
34. Další doporučená dokumentace (doporučí dodavatel dle best practise)

4.2 Analýza rizik

Nezbytnou součástí plnění je provedení identifikace a hodnocení aktiv a rizik v souladu s požadavky § 4 řízení aktiv a § 5 řízení rizik vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.

4.3 Řízení kontinuity činností

Součástí dodávky je také provedení analýzy dopadů (BIA – Business Impact Analysis), na kterou navazuje tvorba plánů kontinuity (BCP) a plánů obnovy (DRP) v souladu s § 15 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (Řízení kontinuity činností).

5 Aktivita č. 4 – Realizace nástroje pro řízení přístupu na síti

Cílem je, aby se k interní síti mohli připojit pouze autorizovaní uživatelé a zařízení, a aby se tak zamezilo nežádoucím připojením k síti. Cílem je zajistit co možná nejsnazší, ale dostatečně robustní, politikou řízený a prosazovaný přístup k síti a jejím zdrojům s ohledem na aktuální stav přistupujícího i již připojeného zařízení.

Centrálně definované politiky budou určovat způsob, typ, místo a rozsah přístupu pro konkrétní skupiny uživatelů a zařízení (případně v kombinaci). 802.1x politika bude řídit nejen přístup pro adekvátně ověřené skupiny uživatelů a kategorie zařízení, ale má být dalším stupněm kybernetické ochrany. Jejím sekundárním úkolem proto bude dohlížet momentální stav již připojených zařízení a bezprostředně reagovat na jeho nežádoucí změnu (např. vypnutí AV ochrany, nebo projev jiné hrozby).

5.1 NAC technologie

Realizace nástroje pro řízení přístupu na síti		
OBECNÉ POŽADAVKY NA PLATFORMU	ANO/NE	Popis splnění požadavku
Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM (HW alternativa není poptávána)		
Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance		
Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami		
Autentizační brány musí být nasazené mimo samotný datový tok (tzv. inline řešení není akceptovatelné)		
Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem		
Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky		
Schopnost NAC řešení komunikovat se síťovými prvky, drátovými i bezdrátovými, jiných výrobců pomocí SNMP a CLI a vymáhat na nich definované bezpečnostní politiky bez nutnosti využití 802.1x nebo MAB		
Možnost instalace samostatného NAC řešení v podobě pouze enforcement brány bez nutnosti nákupu dalších prvků, jako například centrální management. Pokud je další prvek nutný, musí být součástí nabídky.		
Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě		
Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting		
Všechny požadované funkce pokrývá jeden typ licence a je možné dostatečně zvýšit počet licencí v systému		
Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů		

POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ	ANO/NE	Popis splnění požadavku
Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN)		
Možnost detailní profilace připojeného zařízení a klienta, a to buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externími systémy a to bez nutnosti dodatečného licencování této funkcionality		
Podpora politik pro automatickou profilaci zařízení (minimálně na základě: SNMP, RADIUS, SYSLOG, DHCP, API, SSH, NMAP, DHCP fingerprinting, HTTP(s), IP range, telnet, expect scripty, vyhodnocení TCP/UDP portů, VENDOR OUI/MAC, WMI profil, pollování firewallu a vyhodnocování síťové komunikace, perl skripty) a to bez nutnosti dodatečného licencování této funkcionality		
Periodická kontrola připojeného zařízení, zda odpovídá profilu, na základě kterého bylo zařízeno vpuštěno do sítě a možnost odpojit zařízení v případě, kdy nesplňuje podmínky původního profilu		
Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS		
Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí standardních Radius atributů		
Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL		
Podpora 802.1x		
Podpora MAB autentizace		
Podpora tvorby lokálních účtů a lokální autentizace		
Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě		
Podpora funkce RADIUS proxy		
Možnost integrace se stávající CA (certifikační autorita)		
Podpora agentů pro operační systémy: Windows, MacOS, Linux (agent dodává detailní informace o počítači, informace o login/logout, umožňuji spouštění skriptů a zajišťuje notifikace pro uživatele) a licence pro tyto agenty je součástí dodané licence		
Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP		
Podpora captive portál v rámci autentizační brány s plně editovatelným prostředí		
Minimálně 5 různých captive portálů		
Podpora tzv. sponzorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email		
NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovní přístupové vrstvy v případě zjištění bezpečnostního incidentu		

Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty		
Podpora integrace s NGFW řešením dodávaným v rámci plnění této zakázky, včetně podpory analytických nástrojů daného výrobce		
Podpora RSSO nebo obdobného mechanismu pro jednotné řízení přístupu ve spolupráci s nasazeným NGFW řešením		
Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele		
POŽADAVKY NA ENDPOINT COMPLIANCE	ANO/NE	Popis splnění požadavku
Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici		
Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě)		
Kontrola stavu AV na stanici		
Kontrola stavu registrů		
Kontrola existence konkrétních souborů v lokálním filesystému		
Ověření domény		
Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name, …		
Ověření verze a patch na úrovni operačního systému		
Podpora sběru informací o instalovaných aplikacích na endpointech		
Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál		
Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance		
REPORTING	ANO/NE	Popis splnění požadavku
Možnost tvorby reportů o stavu platformy a stavu připojených zařízení v reálném čase a alespoň zpětně o jeden týden. Reporting je nativní funkce dostupná v GUI bez nutnosti dodatečného licencování		
NOTIFIKACE ADMINISTRÁTORŮ A UŽIVATELŮ	ANO/NE	Popis splnění požadavku
Možnost napojení autentizační brány na systémy pro notifikaci (např. SMS nebo e-mail gateway) s podporou přímého konektoru		
POŽADAVKY NA LICENCE A PODPORU VÝROBCE	ANO/NE	Popis splnění požadavku
Licence pro min. 500 endpointů		
Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let		

6 Aktivita č. 5 – Zajištění vysoké dostupnosti sítě

Cílem je modernizace počítačové sítě náhradou zastaralých prvků a zvýšení její kapacity doplněním nových prvků. Současně bude pro zvýšení úrovně zabezpečení počítačové sítě implementován systém řízení přístupu k síti NAC na bázi protokolu IEEE 802.1X s napojením na centrální databázi identit Active Directory. NAC bude implementován jako jednotný pro drátovou i bezdrátovou část sítě a dynamické zařazování koncových zařízení do VLAN na základě ověření, typu zařízení apod.

6.1 Technologie

Zajištění vysoké dostupnosti sítě		
WiFi přístupový bod		
MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 30		
Požadavky na řízení a správu přístupových bodů	ANO/NE	Popis splnění požadavku
Přístupové body musí být centrálně řízeny a spravovány řešením v podobě on-premise nástroje nebo cloud platformy		
Ideálně nástroj centrální správy umožňuje terminovat provoz SSID, v tunelovém režimu, s ohledem na možnou potřebu segmentace drátového a bezdrátového provozu		
On-premise varianta řešení centrální správy může být součástí jiného, v tomto projektu nabízeného, produktu stejného výrobce		
řešení musí splňovat:		
automatická nebo manuální autorizace přístupových bodů na základě auto discovery mechanismu		
jednotné management rozhraní, ze kterého lze spravovat přístupové body a případně i další produkty stejného výrobce		
jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID		
jednotné management rozhraní pro zobrazení stavu všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujících SSID včetně síly signálu interferujícího SSID vůči konkrétnímu přístupovému bodu		
možnost vyhledávání, v jednotném management rozhraní, konkrétních připojených zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno		
možnost automatické aktualizace operačního sytému přístupového bude po jeho připojení do sítě		
možnost automaticky registrovat přístupový bude na servisní portál výrobce		
možnost automatické karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti		
možnost hromadného upgrade firmware z jednotného management rozhraní		

Konkrétní technické požadavky na bezdrátový přístupový bod	ANO/NE	Popis splnění požadavku
Formát zařízení: indoor s interními anténami		
Příslušenství k montáži na zeď/strop/T-Rail		
Počet rádií: minimálně 3 pro přenos v pásmech 2,4, 5 a 6GHz		
Podpora kanálů o šířce 160MHz v 6GHz pásmu		
Podpora BSS Coloring		
Minimálně 2x2 MIMO		
Dedikované Bleutooth/ZigBee rádio pro lokalizační služby		
Možnost provozu dvou rádií v pásmu 5GHz		
Alespoň 1x 10/100/1000 a 1x 1x 100/1000/2500 Base-T RJ45 Base-T RJ45 uplink porty s možností sestavení LAG		
1x USB port 3.0 a 1x konzolový port RJ45		
Možnost souběžně provozovat až 16 SSID		
Podpora Cellular Co-existence, TWT (Target Wake Time)		
Možnost spektrální analýzy přímo na AP		
Možnost zachytávání paketů na zařízení pro jejich analýzu		
Podpora napájení pomocí 802.3af		
Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az		
Kensigton lock na samotném AP		
Obecné požadavky na podporu všech druhů AP výrobcem	ANO/NE	Popis splnění požadavku
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		
L2 přepínače - 48p, POE		
MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 6		
Obecné technické požadavky na poptávané L2 přepínače	ANO/NE	Popis splnění požadavku
L2 přepínač		
Podpora IEEE 802.3ad, IEEE 802.1q, IEEE 802.1ab		
Možnost propojení s prvkem podporující IEEE 802.1s		
Podpora IEEE 802.1w		
Podpora ACL IPv4		
Podpora QoS pro IPv4 včetně 802.1p		
Podpora 802.1x		
Podpora MAB		
Podpora Radius CoA		
Podpora Radius Accounting		
Podpora ARP inspekce		

Podpora IGMP a DHCP snooping		
Podpora SPAN		
Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS		
Podpora REST API pro konfiguraci a monitoring prvku		
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů		
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN		
Specifické technické požadavky na poptávané přístupové přepínače s 48 porty s PoE	ANO/NE	Popis splnění požadavku
Minimálně 48x10/100/1000 RJ-45, 4x 10GE SFP+		
PoE budget až 740W a podpora 802.3aft/at na všech access RJ-45 portech		
Samostatný konzolový port		
Velikost maximálně 1RU		
Minimální přepínací kapacita 175 Gbps		
Propustnost minimálně 250 Mpps		
Velikost bufferu pro zpracování paketů je alespoň 2MB per port		
Minimální velikost MAC tabulky alespoň 32000 záznamů		
Minimální počet podporovaných VLAN alespoň 4000		
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač		
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		
L2 přepínače – 48p		
MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 6		
Obecné technické požadavky na poptávané L2 přepínače	ANO/NE	Popis splnění požadavku
L2 přepínač		
Podpora IEEE 802.3ad, IEEE 802.1q, IEEE 802.1ab		
Možnost propojení s prvkem podporující IEEE 802.1s		
Podpora IEEE 802.1w		
Podpora ACL IPv4		
Podpora QoS pro IPv4 včetně 802.1p		
Podpora 802.1x		
Podpora MAB		
Podpora Radius CoA		
Podpora Radius Accounting		
Podpora ARP inspekce		
Podpora IGMP a DHCP snooping		

Podpora SPAN		
Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS		
Podpora REST API pro konfiguraci a monitoring prvku		
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů		
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN		
Specifické technické požadavky na poptávaný L2 přepínač s 48 porty bez PoE	ANO/NE	Popis splnění požadavku
Minimálně 48x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+ síťové porty		
Samostatný konzolový port		
Velikost maximálně 1RU		
Minimální přepínací kapacita 170 Gbps		
Propustnost minimálně 260 Mpps		
Minimální počet podporovaných VLAN alespoň 4000		
Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky		
Proudění vzduchu ze strany do zadní částí přepínače		
Bez nutnosti aktivního chlazení přepínače		
Podpora duálního firmwaru		
Podpora sFlow pro IPv4		
Integrovaný nástroj pro packet capture		
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů, a to až pět let po ohlášení konce možnosti objednat nabízený přepínač		
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		
L2/L3 přepínače – 48p		
MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 2		
Obecné technické požadavky na poptávané přístupové L2/L3 přepínače	ANO/NE	Popis splnění požadavku
L2/L3 přepínač		
Podpora IEEE 802.3ad, IEEE 802.1q, IEEE 802.1ab		
Možnost propojení s prvkem podporující IEEE 802.1s		
Podpora IEEE 802.1w		
Podpora IPv4 a IPv6		
Podpora ACL IPv4 a IPv6		
Podpora 802.1x		
Podpora MAB		
Podpora Radius CoA		
Podpora Radius Accounting		

Podpora ARP inspekce		
Podpora QoS pro IPv4 a IPv6 včetně 802.1p, prioritních front, WRED, čítačů QoS statistik		
Alespoň osm prioritních QoS front per port		
Podpora IGMP a DHCP snooping		
Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN a RSPAN		
Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS		
Podpora REST API pro konfiguraci a monitoring prvku		
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů		
Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6		
Možnost definovat alespoň 64 VRF domén		
Podpora BFD pro protokoly RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6		
Podpora multicast PIM-SM protokolu		
Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN, RSPAN a ERSPAN		
Podpora Multi-Chassis Link Aggregeation protokolu		
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN		
Podpora kontroly validity instalovaného firmware z pohledu shody s oficiálním vydáním dané verze firmware výrobcem		
Podpora uložení až dvou verzi firmware na zařízení a volby, který načíst při startu zařízení		
Podpora sFlow pro IPv4		
Minimální počet LAG skupin odpovídá celkovému počtu portů přepínače (bez konzolového, mgmt a USB portu)		
Integrovaný nástroj pro packet capture		
Specifické technické požadavky na poptávané přístupové přepínače s 48 porty bez PoE	ANO/NE	Popis splnění požadavku
Minimálně 48x10/100/1000 RJ-45, 4x10GE SFP/SFP+ a 2x QSFP+ portů		
Samostatný konzolový port, L3 mgmt port a USB port		
Velikost maximálně 1RU		
Minimální přepínací kapacita 330 Gbps		
Propustnost minimálně 500 Mpps		
Velikost bufferu pro zpracování paketů je alespoň 4MB per port		
Minimální velikost MAC tabulky alespoň 32000 záznamů		
Minimální počet podporovaných VLAN alespoň 4000		
Dva napájecí zdroje a přívodní elektrický kabel pro CZ jsou součástí dodávky		
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů, a to až pět let po ohlášení konce možnosti objednat nabízený přepínač		

Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		
L2/L3 přepínače – 48p POE		
MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 1		
Obecné technické požadavky na poptávané přístupové L2/L3 přepínače	ANO/NE	Popis splnění požadavku
L2/L3 přepínač		
Podpora IEEE 802.3ad, IEEE 802.1q, IEEE 802.1ab		
Možnost propojení s prvkem podporující IEEE 802.1s		
Podpora IEEE 802.1w		
Podpora IPv4 a IPv6		
Podpora ACL IPv4 a IPv6		
Podpora 802.1x		
Podpora MAB		
Podpora Radius CoA		
Podpora Radius Accounting		
Podpora ARP inspekce		
Podpora QoS pro IPv4 a IPv6 včetně 802.1p, prioritních front, WRED, čítačů QoS statistik		
Alespoň osm prioritních QoS front per port		
Podpora IGMP a DHCP snooping		
Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN a RSPAN		
Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS		
Podpora REST API pro konfiguraci a monitoring prvku		
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů		
Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6		
Možnost definovat alespoň 64 VRF domén		
Podpora BFD pro protokoly RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6		
Podpora multicast PIM-SM protokolu		
Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN, RSPAN a ERSPAN		
Podpora Multi-Chassis Link Aggregeation protokolu		
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN		
Podpora kontroly validity instalovaného firmware z pohledu shody s oficiálním vydáním dané verze firmware výrobcem		
Podpora uložení až dvou verzi firmware na zařízení a volby, který načíst při startu zařízení		
Podpora sFlow pro IPv4		

Minimální počet LAG skupin odpovídá celkovému počtu portů přepínače (bez konzolového, mgmt a USB portu)		
Integrovaný nástroj pro packet capture		
Specifické technické požadavky na poptávané přístupové přepínače s 48 porty s PoE	ANO/NE	Popis splnění požadavku
Minimálně 48x10/100/1000 RJ-45, 4x10GE SFP/SFP+ a 2x QSFP+ portů		
PoE budget až 1440W a podpora 802.3aft/at na všech access RJ-45 portech		
Samostatný konzolový port, L3 mgmt port a USB port		
Velikost maximálně 1RU		
Minimální přepínací kapacita 330 Gbps		
Propustnost minimálně 500 Mpps		
Velikost bufferu pro zpracování paketů je alespoň 4MB per port		
Minimální velikost MAC tabulky alespoň 32000 záznamů		
Minimální počet podporovaných VLAN alespoň 4000		
Dva napájecí zdroje a přívodní elektrický kabel pro CZ jsou součástí dodávky		
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů, a to až pět let po ohlášení konce možnosti objednat nabízený přepínač		
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		
L2/L3 přepínače - 24p Fiber		
MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 2		
Obecné technické požadavky na poptávané přístupové L2/L3 přepínače	ANO/NE	Popis splnění požadavku
L2/L3 přepínač		
Podpora IEEE 802.3ad, IEEE 802.1q, IEEE 802.1ab		
Možnost propojení s prvkem podporující IEEE 802.1s		
Podpora IEEE 802.1w		
Podpora IPv4 a IPv6		
Podpora ACL IPv4 a IPv6		
Podpora 802.1x		
Podpora MAB		
Podpora Radius CoA		
Podpora Radius Accounting		
Podpora ARP inspekce		
Podpora QoS pro IPv4 a IPv6 včetně 802.1p, prioritních front, WRED, čítačů QoS statistik		
Alespoň osm prioritních QoS front per port		
Podpora IGMP a DHCP snooping		

Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN a RSPAN		
Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS		
Podpora REST API pro konfiguraci a monitoring prvku		
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů		
Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6		
Možnost definovat alespoň 64 VRF domén		
Podpora BFD pro protokoly RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6		
Podpora multicast PIM-SM protokolu		
Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN, RSPAN a ERSPAN		
Podpora Multi-Chassis Link Aggregeation protokolu		
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN		
Podpora kontroly validity instalovaného firmware z pohledu shody s oficiálním vydáním dané verze firmware výrobcem		
Podpora uložení až dvou verzi firmware na zařízení a volby, který načíst při startu zařízení		
Podpora sFlow pro IPv4		
Minimální počet LAG skupin odpovídá celkovému počtu portů přepínače (bez konzolového, mgmt a USB portu)		
Integrovaný nástroj pro packet capture		
Specifické technické požadavky na poptávané optické přepínače s 24 porty	ANO/NE	Popis splnění požadavku
Minimálně 24x10/100/1000 SFP a 4x10GE SFP/SFP+ portů		
Samostatný konzolový port, L3 mgmt port a USB port		
Velikost maximálně 1RU		
Minimální přepínací kapacita 128 Gbps		
Propustnost minimálně 180 Mpps		
Velikost bufferu pro zpracování paketů je alespoň 4MB per port		
Minimální velikost MAC tabulky alespoň 32000 záznamů		
Minimální počet podporovaných VLAN alespoň 4000		
Dva napájecí zdroje a přívodní elektrický kabel pro CZ jsou součástí dodávky		
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů, a to až pět let po ohlášení konce možnosti objednat nabízený přepínač		
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		
L2 přepínače - 24p		

MINIMÁLNÍ POŽADAVKY	ANO/NE	Popis splnění požadavku
Požadovaný počet: 2		
Obecné technické požadavky na poptávané L2 přepínače	ANO/NE	Popis splnění požadavku
L2 přepínač		
Podpora IEEE 802.3ad		
Podpora IEEE 802.1q		
Podpora IEEE 802.1ab		
Možnost propojení s prvkem podporující IEEE 802.1s		
Podpora IEEE 802.1w		
Podpora ACL IPv4		
Podpora QoS pro IPv4 včetně 802.1p		
Podpora 802.1x		
Podpora MAB		
Podpora Radius CoA		
Podpora Radius Accounting		
Podpora ARP inspekce		
Podpora IGMP a DHCP snooping		
Podpora Jumbo Frame o velikosti alespoň 9000B		
Podpora SPAN		
Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS		
Podpora REST API pro konfiguraci a monitoring prvku		
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů		
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN		
Specifické technické požadavky na poptávaný L2 přepínač s 24 porty bez PoE	ANO/NE	Popis splnění požadavku
Minimálně 24x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+ síťové porty		
Samostatný RJ-45 konzolový a USB port		
Velikost maximálně 1RU		
Minimální přepínací kapacita 120 Gbps		
Propustnost minimálně 180 Mpps		
Minimální počet podporovaných VLAN alespoň 4000		
Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky		
Proudění vzduchu ze strany do zadní částí přepínače		
Bez nutnosti aktivního chlazení přepínače		
Podpora duálního firmwaru		
Podpora sFlow pro IPv4		
Integrovaný nástroj pro packet capture		
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů, a to až pět let po ohlášení konce možnosti objednat nabízený přepínač		

Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.		

6.2 Implementace

Aktivní prvky		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
fyzická montáž zařízení a propojení do stávající síťové infrastruktury		
upgrade firmware na aktuální stabilní verzi doporučenou výrobcem		
analýza stavu topologie a současné konfigurace		
akceptační testy a testovací provoz		
školení administrátorů v rozsahu 2 hodin		
dokumentace skutečného provedení		

7 Aktivita č. 7 – Nástroj pro správu privilegovaných účtů

Nasazení systému, který zajistí správu privilegovaných účtů a monitoring privilegovaných relací. Tento systém zajistí logování všech relací, logování aktivit administrátorů, možnost dohledání zadaných a vykonávaných příkazů a možnost pozastavit, uzamknout nebo terminovat relaci. Dodávané řešení pro správu privilegovaných uživatelských účtů musí splňovat alespoň následující funkce a parametry.

7.1 Technologie

Správa privilegovaných účtů		
OBECNÉ POŽADAVKY NA PLATFORMU	ANO/NE	Popis splnění požadavku
Podpora virtualizační plaformy Vmware a HyperV		
Podpoda vTPM		
Podpora minimálně 5 privilegovaných účtů		
Podpora HA režimu active-pasive (pro případ pozdějšího rozšíření, nyní HA není předmětem poptávky)		
Podpora integrace se SIEM/SYSLOG v podobě možnosti exportu logů		
Správa řešení z jednotné webové konzole		
Podpora importu certifikátů pro potřeby přístupu k management rozhraní – import ze souboru a protokolem SCEP		
Podpora import CA certifikátu interní CA		
Podpora automatické zálohy konfigurace v případě změny konfigurace nebo periodicky – nahrání konfigurace na FTP, SFTP nebo HTTP/S server		
Možnost zachytávat packety s definovanými filtry a následky exportu do nástroje typy Wireshark		
Podpora protokolu SNMPv3		
Podpora 2FA autentizace – mobilní aplikace, hardwarový token nebo email		
Podpora ověřování přes protokol LDAP		
Podpora ověřování přes protokol Radius		
Podpora ověřování přes protokol SAML		
Podpora reportingu – statistiky využíváni systému		
Podpora zasílání upozornění na email při změně konfigurace, kritických systémových událostech atd.		
Podpora přístupové proxy pro protokoly SSH, RDP, VNC, SFTP, SMB a HTTP		
Podpora SSH filtru – filtrování SSH příkazů		
Podpora nahrávání relace ve formě videa a uložení záznamu		
Možnost umožnit přístup k cílovému systému bez znalosti skutečného hesla		
Podpora periodické změny a verifikace hesla na cílovém systému		
Podpora DLP – definice vlastních pravidel		

Podpora spouštění nativních aplikací při přístupu k cílovému systému (Putty, Windows RDP atd.)		
Podpora schedulingu – časových oken, kdy je přístup umožněn nebo zakázán		
Podpora schvalování přístupů (minimálně 2 schvalovatelé)		
Agent pro koncovou stanici (pokud je vyžadován) musí být poskytován zdarma nebo musí být zahrnut v ceně řešení		
Podpora výrobce na nabízené řešení funguje v režimu 24/7 a je součástí dodávky s platností po dobu 60 měsíců		

7.2 Implementace

Nástroj pro správu privilegovaných účtů		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu agentů (bude-li použito), akceptačních testů, pilotního testování.		
Návrh politiky způsobu řízení privilegovaných účtů. Konzultace se Zadavatelem a finalizace politiky.		
Instalace centrální správy.		
Instalace dalších komponent (například skenery nebo další potřebné servery).		
Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.		
Vytvoření skenovacích úloh (host Discovery a privilegovaných účtů, otestování funkčnosti na pilotním vzorku, vyladění autentizace v rámci privilegovaných skenů).		
Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení.		
Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting.		
Realizace akceptačních testů.		
Seznámení s obsluhou pro 2 administrátory řešení v rozsahu 1 dne.		

8 Aktivita č. 3 - Vybudování PKI a aktivita č. 9 – Zavedení systému jednotného přihlašování a dvou faktorové autentizace

Vybudování interní certifikační autority PKI (public key infrastructure – architektura veřejných klíčů), která bude ve správě žadatele. Zaměstnanci se tak budou moci jednoznačně a bezpečně identifikovat například při přístupu do sítě nebo do významných aplikací.

Zavedení SSO (Single Sign-On, systém jednotného přihlašování), který zajistí jednotné přihlašování uživatele. Uživatel se tak přihlásí například do operačního systému, a již nebude nutné se hlásit samostatně do dalších aplikací, ale bude do nich již přihlášen. Zavedení 2FA (dvoufaktorové autentizace), tedy autentizace pomocí dvou faktorů – například push notifikace. Dvoufaktorová autentizace by měla být používána při přihlašování do významných systémů a pro privilegované účty

Vybudování PKI a zavedení SSO		
Služby, funkce systému	ANO/NE	Popis splnění požadavku
Ověření zaměstnance (uživatele, administrátora) druhým faktorem při přihlašování k – OS Windows (lokálně, přes doménu AD), – OS Linux (lokálně, přes IdM, příp. doménu AD), – aplikacím, IS (lokálně, přes AD, příp. IdM), – datovým úložištím (přes doménu AD, příp. IdM), – cloud službám a kancelářským nástrojům s podporou 2FA, – síťovým a dalším infrastrukturním zřízením s podporou 2FA, – VPN přes VPN bránu s podporou 2FA pomocí X.509 certifikátu vystaveného pro účely ověření identity uživatele uloženého na čipové kartě (Smart Card), – nebo digitálního klíče (passkey) uloženého na klíčence (Security Key) splňující standard FIDO.		
On-line napojení na interní certifikační autorita (CA), příp. zavedení PKI organizace s využitím interní CA (AD CS).		
Online napojení min. na dvě veřejné, akreditované certifikační autority.		
Integrace s identitními, autentizačními systémy AD a IdM (NetIQ).		
Monitorování činností systému a interní CA.		
Záloha systému a interní CA, včetně kontinuální záloh s průběžným zaznamenáváním změn CA v reálném čase.		
Bezpečná správa čipových karet, klíčenek, certifikátů a přístupových klíčů.		
Využití čipových karet a klíčenek i pro účely: – šifrování komunikace, dokumentů,		

– podepisování dokumentů kvalifikovaným elektronickým podpisem, pečetí, – ověření pracovníka stávajícím elektronickým přístupovým systémem při fyzickém vstupu do budovy, místnosti nebo vjezdu na parkoviště.		
Vytváření sumarizačních a přehledových reportů o používání čipových karet, klíčenek, certifikátech a provozu systému.		
Vytváření záznamů o vzniklých událostí a činnostech administrátorů během správy životního cyklu certifikátu, čipové karty a klíčenky, s možností jejich poskytovaní systémům třetích stran, jako je LM systém, SIEM, SOC.		
Správa a konfigurace systému přes web GUI, případně GUI nebo CLI.		
Čipová karta	ANO/NE	Popis splnění požadavku
Formát ID-1 s QSCD čipem.		
Soulad se Security Target.		
Certifikace Common Criteria.		
Kvalifikovaný prostředek (QSCD) dle Evropského nařízení eIDAS zapsaný na seznamu kvalifikovaných zařízení (QSCD) EU.		
Kryptografický obsah čipové karty lze logicky dělit na dvě nezávislé části: část pro uložení komerčních certifikátů a část pro uložení kvalifikovaných certifikátů, a to včetně jim příslušným šifrovacích klíčů.		
Nastavení hodnot PUK pro kvalifikovanou a nekvalifikovanou část samostatně.		
Podpora bezheslového a bezdotykového přihlašování.		
Kompatibilita s oficiálními ovladači bez nutnosti instalovat vlastní		
Klíčenka	ANO/NE	Popis splnění požadavku
USB klíč s QSCD čipem.		
Možnost bezdrátového ověření.		
Certifikace FIDO2.		
Certifikace Microsoft.		
Kvalifikované zařízení (QSCD) dle Evropského nařízení eIDAS zapsaného na seznamu kvalifikovaných zařízení (QSCD) EU.		
Kompatibilita s oficiálními ovladači bez nutnosti instalovat vlastní.		
Podpora bezhlesového a bezdotykového přihlašování.		
Podpora ověření pomocí TouchID, FaceID nebo PIN přes mobilní aplikaci.		
Podpora samo registrace a obnovy zapomenutých nebo ztracených přihlašovací údajů.		
Správa čipových karet a klíčenek	ANO/NE	Popis splnění požadavku
Správa celého životního cyklu (vydávání, zneplatnění) čipové karty (kvalifikovaného prostředku) uživatele.		

Resetování PIN karty jejím uživatelem bez nutnosti asistence osoby s vyšším delegovaným oprávněním.		
Odemčení čipu karty, klíčenky jejím uživatelem pomocí šifrovaného PUKU bez nutnosti asistence osoby s vyšším delegovaným oprávněním.		
Zamezí změny PIN nebo přístupu k obsahu karty neoprávněné osobě pomocí externí aplikace.		
Zneplatnění, recyklace (revokace a vymazání uložených certifikátů a ostatních datových typů a nastavení defaultního PIN, PUK) karty uživatele.		
Poskytování informací o uživateli a jeho čipové kartě integrovaným systémům třetích stran.		
Správa certifikátů	ANO/NE	Popis splnění požadavku
Správa celého životního cyklu (podání žádosti o vydávání, vydávání, obnova a revokace) certifikátu uživatele.		
Obnova certifikátu na zařízení (PC stanice) uživatele po schválení žádosti o obnovu osoby s vyšším delegovaným oprávněním.		
Automatická obnova certifikátu na zařízení (PC stanice) uživatele bez zásahu osoby s vyšším delegovaným oprávněním.		
Zneplatnění interních a kvalifikovaných, komerčních certifikátů.		
On-line vydávání kvalifikovaných, komerčních certifikátů CA.		
Monitorování platnosti a zasílání notifikací o expiraci aplikačních, serverových a dalších infrastrukturních certifikátů.		
Zasílání notifikace vypršení platnosti nebo vystavení nového certifikátu uživatele.		
Ověření platnosti vystavených certifikátů přes univerzální rozhraní		
Způsob provedení	ANO/NE	Popis splnění požadavku
Virtuální zařízení (VMware, Hyper-V).		
Časově neomezená nebo dlouhodobá (min. na 5 let) licence pro zajištění provozu všech požadovaných komponent a funkcí zařízení.		
Způsob nasazení	ANO/NE	Popis splnění požadavku
Analýza stávajícího stavu.		
Stanovení rozsahu nasazení systému.		
Vypracování detailního návrhu řešení zahrnující – propojení systému na AD, AD CS, příp. IdM (NetIQ), – nastavení technických aktiv (počítačů, serverů, aplikací a infrastrukturních systémů a zařízení), – harmonogram prací včetně času a kapacit zdrojů pro fázi přípravy, realizace, testování, pilotního provozu a předání,		

– seznam požadavků na součinnost, – dokumentace skutečného provedení, – bezpečnostní dokumentace.		
Provedení implementace (instalace a integrace, nastavení dotčených technických aktiv) systému dle odsouhlaseného návrhu řešení.		
Zajištění proaktivního monitoringu prostředí a provádění korekcí během implementace.		
Zaškolení uživatelů a předání příručky pro uživatele systému.		
Zaškolení správy (administrace) systému a předání dokumentace skutečného provedení, instalační, provozní a bezpečnostní dokumentace a příručky pro administrátory systému.		
Zajištění podpory během pilotního provozu.		
Rozšiřitelnost, škálovatelnost	ANO/NE	Popis splnění požadavku
HA řešení (cluster).		
Konektivita	ANO/NE	Popis splnění požadavku
Min. 1x Virtual Network Interface (VIF).		
Kapacita, výkon, parametry	ANO/NE	Popis splnění požadavku
Min. počet uživatelů: 300.		
Počet čipových karet: 250 ks		
Počet čteček karet: 200 ks		
Počet klíčenek: 50ks		
Bezpečnostní parametry	ANO/NE	Popis splnění požadavku
Bezpečné ukládání dat.		
Bezpečný přístup (šifrovaná komunikace a AAA) ke správě systému.		
V případě web GUI použití HTML5 bez technologie JavaScript.		
Bezpečnostní parametry	ANO/NE	Popis splnění požadavku
Proces bezpečného vývoje aplikací (DevSecOps).		
Podpora systému a aktualizace služeb a funkcí min. po dobu 5 let v rozsahu: – udržování aktuálnosti systému (bezpečnostní a funkční hrozby, aplikace aktualizací) – oprava chyb – údržba systému – bezpečnost systému a reakce na bezpečnostní hrozby – právní soulad (eIDAS, certifikační poltiky CA) – implementace změn certifikační politiky		
Systémová podpora: - zajištění funkčnosti a chodu systému - provoz, dostupnost a funkčnost služeb certifikační autority - zpracování změnových pořadavků - zajištění telefonické podpory		

9 Aktivita č. 8 – Zajištění fyzického zabezpečení datového centra, Aktivita č. 10 – Realizace systému pro řízení fyzického přístupu

Zajištění vyššího fyzického zabezpečení datacenter/serveroven. Nainstalování alarmu, teplotních a požárních čidel, zajištění bezpečného přístupového systému do místností, instalace bezpečnostních dveří atd.

Minimální požadavky:

- Autonomní přístupový a zabezpečovací systém do serveroven
- Požadovaná kompatibilita karet (viz bod 15 – Přístupový systém karty)

Technologická část – PZTS+EKV:

Nemocnice Hustopeče, serverovny, zabezpečení			
PZTS+EKV			
Technický popis	**MJ**	**Počet MJ**	**ANO/NE**
Poplachový, zabezpečovací a tísňový systém – PZTS			
Ústředna až 96 zón a 16 grup v krytu bez klávesnice s komunikátorem a zdrojem	ks	1	
Akumulátor 12V / 18Ah se šroubovými svorkami M5 a životností až 3 roky	ks	1	
TCP/IP komunikátor bez krytu pro GALAXYGD, verze dle EN norem. ISOM protokol	ks	1	
Systémový GSM modul v kovovém krytu pro posílání SMS a volání uživateli	ks	1	
Koncentrátor v kovovém krytu pro 8 zón se 4 PGM výstupy	ks	1	
LCD klávesnice	ks	2	
MG kontakt čtyřdrátoý polarizovaný s pracovní mezerou 22mm, kabel 3m	ks	2	
Duální detektor digitální s držákem, vějíř 15m, montážní výška 1,8 - 2,4m, EOL	ks	2	
Konvenční komb. (optickokouřový a teplotní - tř. A1R) hlásič, bez patice	ks	2	
Std. patice pro hlásiče, reléová samoresetovací 12 V	ks	2	
Kabel SYKFY 3x2x0,5	m	150	
Kabel F/UTP kat.5e	m	120	
CYKY-O 2x1,5	m	60	
Programování ústředny, oživení systému PZTS	kpl	1	
Funkční zkouška, uvedení do provozu, školení obsluhy	kpl	1	
Instalační materiál a práce			
Žlab PVC 40x20	m	40	
trubka ohebná, d=25 mm	m	120	

Nespecifikované instalační a stavební práce	kpl	1	
Podružný instalační materiál	kpl	1	
Elektronická kontrola vstupu – EKV			
Řídící modul pro dvě čtečky se zdrojem a 8-mi zónami	ks	2	
Řídící modul pro připojení dvou bezkontaktních čteček	ks	4	
Bezkontaktní multitechnol. čtečka (podpora SIO) 13.56 MHz a 125 kHz, úzká	ks	11	
Akumulátor 12V / 18Ah se šroubovými svorkami M5 a životností až 3 roky	ks	2	
Elektromechanický hluboký samozamykací panikový zámek, komplet včetně syst. kabelu, dveřní průchodky, protiplechu	ks	11	
Bezpečnostní kování, nerez/mat, madlo/klika, čtyřhran	ks	11	
Úprava dveří pro osazení samozamykacího panikového zámku	ks	11	
Kabel F/UTP kat.5e	m	560	
CYKY-O 2x1,5	m	230	
Nastavení systému EKV	kpl	1	
Funkční zkouška, uvedení do provozu, školení obsluhy	kpl	1	
Instalační materiál a práce			
Žlab PVC 40x20	m	200	
trubka ohebná, d=25mm	m	50	
Nespecifikované instalační a stavební práce	kpl	1	
Podružný instalační materiál	kpl	1	
Ostatní			
Montážní a stavební práce	kpl	1	
Doprava	kpl	1	
Projektová dokumentace DPS+DSPS	kpl	1	

standardní out-of-band management řešení (např. IPMI, Redfish nebo ekvivalentní)

Požadavek vSAN
Jedná se o infrastrukturní prvky, které jsou nezbytné pro provoz systémů: • Virtualizační server • Licence operačního systému včetně klientských licencí • Licence pro virtualizaci Součástí dodávky implementace jsou veškeré nezbytné práce a jejich smyslem je zprovoznění dodávaných prvků infrastruktury včetně zapojení do stávajícího prostředí tak, aby je zadavatel mohl užívat obvyklým způsobem. Dodavatel infrastruktury poskytne součinnost dodavatelům informačních systémů v nezbytném rozsahu, maximálně však 5 člověkodní. Zadavatel si po vyhodnocení VŘ, a tedy nejvýhodnějšího řešení vyhrazuje právo na praktickou ukázku od zvoleného Dodavatele požadovaných vlastností na testovacím nebo demo vzorku zařízení výrobce, jako je předmětem nabídky Dodavatele.

Virtualizační server – 3ks
Technická specifikace, minimální požadavky pro Virtualizační server: Požadovaným cílovým stavem je vytvořit prostředí serverové virtualizace využívající hyperkonvergované infrastruktury. Ta bude provozována jako single clusteru na primární lokalitě se zajištěním služeb v případě výpadku některého z nodu clusteru. Vzhledem k zajištění kontinuity provozu a zachování znalostní báze požaduje Zadavatel dodání řešení postaveného na technologiích VMware. Dodavatel dodá veškeré potřebné licence pro zajištění on-premise provozu nabízeného řešení pokrývající celou dodanou serverovou hyperkonvergovanou infrastrukturu (HCI). **Obecné požadavky na fyzické servery** • Součástí dodávky jsou i veškeré propojovací kabely a zásuvné moduly (SFP, GBIC) do všech dodaných zařízení i do všech aktivních prvků zadavatele potřebné pro realizaci komunikačních spojení podle výše uvedených parametrů. • Veškeré prvky řešení musí podporovat IPv4 a IPv6 až na úroveň administrace. • Každý prvek musí být dodán se dvěma napájecími zdroji zajišťujícími funkcionalitu při výpadku libovolného z nich. Napájecí kabel IEC-320 C13-C14 pro propojení do PDU datového rozvaděče

bude takové délky, aby při manipulaci mohl být prvek případně za provozu vysunut, přičemž PDU v datovém rozvaděči jsou na výšku vzadu vlevo a vpravo od serveru.

- Servery budou kompatibilní pro montáž do 19“ datových rozvaděčů 42U.
- Pokud Dodavatel, spolu s výrobcem, z nějakého důvodu nemůže zajistit garanci bezchybné funkčnosti systémů po všech update/upgrade firmwarů jednotlivých komponent dle HCI, musí na své náklady zřídit testovací prostředí, kde ověří funkčnost nových firmwarů s totožnou konfigurací jako obsahuje prostředí produkční. Každé budoucí rozšíření infrastruktury bude znamenat totožné rozšíření testovacího prostředí o tuto změnu, opět na náklady Dodavatele. Zadavatel k tomu poskytne místo v racku.

vSAN		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	ANO/NE	Popis splnění požadavku
Dodávka virtualizačního SW pro on-premise provoz pro všechny dodávané servery a disková úložiště, včetně všech licencí pro dodávanou konfiguraci, pro splnění funkcí a vlastností uvedených ve všech bodech této zadávací dokumentace.		
Virtualizace musí umožnit bezvýpadkový chod virtuálních systémů automatickou migrací mezi hosty.		
Virtualizace musí umožnit virtualizovat diskový subsystém.		
Podpora management klienta v HTML5.		
Umožnění prioritizace síťového a datového provozu dynamickou alokací dostupností zdrojů.		
Pokročilý monitoring a alerting virtuální vrstvy, včetně storage.		
Pokročilé kapacitní plánování.		
Virtualizace storage součástí licence.		
Technická podpora a servis na 5 let, centrální kontaktní místo pro hlášení poruch napříč všemi komponentami řešení pro všechny HW i SW komponenty dodávaného systému od výrobce		
Technická podpora a servis je poskytován výrobcem řešení nebo jeho autorizovaným partnerem		
Zahájení servisních prací do 4 hodin od identifikace problému		
Servis probíhá v místě instalace HW		
Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení		

ovladačů a Firmware je požadována po dobu životního cyklu daného HW.		
Celá infrastruktura musí být koncipována na budoucí rozvoj s jednoduchou škálovatelností na úrovni jednotlivých komponent nodů anebo celých nodů v clusteru.		
Architektura bude postavená na standardní x64 architektuře, včetně souvisejících SW licencí.		
Infrastruktura nesmí obsahovat SPOF (Single-Point-Of-Failure). Požadujeme kompletní redundanci včetně odolnosti systému proti výpadku jednoho nebo několika disků, serverů nebo skupiny serverů, instalovaných do racku.		
Automatizace aktualizace životního cyklu (update/upgrade) jednotlivých vrstev a komponent softwarově definované storage.		
Řešení musí být schopno efektivně škálovat v každé části životního cyklu řešení, nákladově efektivně, bez negativního dopadu na provoz produkčního prostředí, v každém případě bez nutnosti vypnout nebo restartovat cluster a omezit tak dostupnost produkčního prostředí.		
Řešení musí být možno v budoucnu rozšířit o nody, které budou konfiguračně rozdílné od iniciálních nebo budou technologicky odpovídat nejnovějším generacím procesorů, řadičů, diskových kapacit, síťových karet dostupných v daný čas. Tyto nody bude možno připojit do stávajícího clusteru a vytvořit tak heterogenní cluster a zároveň spravovat jejich životní cyklus automatizovaně na všech vrstvách řešení.		
Integrace managementu softwarově definované storage s virtualizační infrastrukturou pro zjednodušení obsluhy.		
Softwarově definovaná storage musí umožňovat QoS minimálně na úrovni omezení IOPS s granularitou per virtuální disk.		
Řešení musí zajistit redundanci na úrovni síťové infrastruktury.		
Řešení musí být vytvořeno jako jeden produkt sestávající z hyperkonvergovaných uzlů, hardwarové virtualizace, SDS, řídícího systému a podpory.		
Výrobce řešení musí poskytnout jediné kontaktní místo pro přímou telefonickou podporu a poskytovat ji pro řešení všech problémů spojených jak s hardwarovými, storage tak virtualizačními komponentami řešení.		

Řešení musí umožňovat správu integrovanou v rámci GUI hypervizoru a musí umožňovat veškeré funkce související s hardwarem, jako je přidávání/odebírání nových nodů, upgrady systémových záplat, dohled stavu systémů a vypnutí systémů.		
Komponenty řešení musí být nově vyrobeny pro toto řešení. A v řešení nebudou použity žádné repasované nebo opravené součásti.		
Softwarově definovaná storage clusteru v primární lokalitě musí mít výkon minimálně 63k IOPS pro 4 KB blok s latencí do 1 ms. Jedná se o OLTP workload, poměr čtecích a zápisových operací 70/30, 100% náhodný pattern.		
Jednoduchá a automatizovaná instalace a upgrade výrobcem otestovaných verzí software a firmware, včetně automatizované aktualizace BIOS FW a FW řadičů úložiště, bez nutnosti odstávky/výpadku SDDC.		
Nástroj musí podporovat automatizovanou kontrolu aktuální kompatibility klíčových komponent HCI řešení (HW, SDS, hypervizor) vůči online certifikační matici výrobce řešení a automatizovanou bez výpadkovou, postupnou instalaci nových verzí firmwaru/sw jednotlivých komponent.		
Rozšiřitelnost storage clusteru v primární lokalitě musí být minimálně na 20 nodů.		
SW řešení HCI s kontrolou dostupných patche a upgrade balíčků podle certifikační HCL výrobce, tak, aby nemohlo dojít k instalaci necertifikovaného balíčku.		
Součástí dodávky jsou licence potřebné pro plnohodnotný provoz SDS a neomezený počet VM v rozsahu zmiňovaném v tomto dokumentu.		
SDS musí umožňovat granulární změnu atributů pro redundanci a efektivitu uložení dat na jednotlivých objektech uložených v rámci SDS File Systemu minimálně pro následující objekty: virtuální stroj, virtuální disk, snapshot, home directory. Změna atributů musí být dynamická bez omezení přístupu k datům/objektům.		
Model použitého serveru bude uveden na seznamu kompatibility hypervizoru (např. VMware HCL) (Hardware Compatibility List) dle dokumentu vydávaného společností VMware. U serveru generačně vyššího, Dodavatel musí doložit		

kompatibilitu s verzemi používaného hypervizoru, např. ESXi v7U3 a v8		
Velikost jednotlivých serverů bude max. 2U.		
Počet serverů musí být nejméně v počtu tří kusů		
Servery musí být identické, všechny součásti stejného typu, stejně osazené.		
Cluster musí disponovat minimálně 48 CPU fyzickými jádry		
Cluster musí disponovat minimálně celkovou CPU frekvencí 134GHz (součet „base frekvencí“ všech fyzických jader).		
Celkový procesorový výkon jednoho serveru měřený při plném osazení socketů musí dosahovat minimálně 333 bodů dle výsledků benchmarku SPECint2017 (např. Rates Result Base) (http://spec.org/cpu2017/results/rint2017.html).		
Celkové množství operační paměti pro celý cluster musí být nejméně 768GB.		
Servery musí být osazeny paměťovými moduly splňující parametry podle doporučení výrobce použitého procesoru (doporučený typ a taktovací frekvence). Všechny moduly musí být totožného typu.		
Každý osazený paměťový modul musí mít hrubou kapacitu nejméně 64GB.		
Při návrhu diskového systému clusteru se dodavatel musí řídit Best Practice pro sizing vSAN SDS OSA/ESA architektury		
Diskový systém každého serveru bude v konfiguraci Hybrid s rozhraním min.NL-SAS/SAS/SSD/NVMe.		
Diskový systém každého serveru musí obsahovat místo pro minimálně 2 diskové skupiny SDS.		
Dostupný užitný diskový prostor clusteru pro data musí být alespoň 33TB (dekadické TB = 10^12 Bajtů) v RAID 1. Kapacita bude dostupná bez použití komprese a deduplikace.		
Užité kapacitní disky musí mít kapacitu alespoň 2.4TB.		
Užité cache disky s minimální kapacitou 1.6TB typu SAS SSD s DWPD3		
Ethernetový adaptér min. 4x 10/25Gbps SFP28 na každý server pro připojení do LAN / SDS podporující protokol RoCEv2 s použitým SDS.		
Servery musí být dodány se samostatným managementem dostupným přes další oddělený port Base-T LAN port, umožňující plnohodnotnou a nezávislou administraci serveru, včetně připojení na vzdálenou IP konzoli.		

Každý server musí být dodán v konfiguraci s nezávislým úložným prostorem o kapacitě nejméně 400GB, alespoň Flash typu s min. 400 TBW pro provozování hypervizoru a případně pomocných VM, a chráněným na HW úrovni proti výpadku jednoho disku		

Licence serverového operačního systému - 3ks		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	ANO/NE	Popis splnění požadavku
Výrobce (prosím uveďte)		
Typ (prosím uveďte)		
Aktuální verze serverového operačního systému Windows, která umožňuje provozování neomezeného množství virtuálních strojů		
Licence vázaná na HW		
Licence pokrývající všechna jádra nabízeného fyzického serveru		

Licence pro virtualizaci		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	ANO/NE	Popis splnění požadavku
Výrobce (prosím uveďte)		
Typ (prosím uveďte)		
Licence virtualizace odpovídající splnění požadavku celého řešení a funkčnosti na platformě VMware		
Virtualizace musí umožnit bezvýpadkový chod virtuálních systémů automatickou migrací mezi hosty		
Virtualizační platforma musí umožnit virtualizovat diskový subsystém		
Součástí licence virtualizace storage		
Kompletní SW pro virtualizaci s podporou na 5 let		

Deduplikační diskové úložiště – 1 ks		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	ANO/ NE	Popis splnění požadavku

Výrobce a obchodní název nabízeného zařízení		
Deduplikační diskové úložiště, provedení RACK – šíře 19”		
Čistá využitelná kapacita (nededuplikovaná kapacita, která je dostupná pro uložení dat a lze ji zkontrolovat prostřednictvím management nástrojů): min. 21TiBu		
Možnost rozšíření kapacity minimálně až na 172TBu čisté kapacity.		
Propustnost pro zápis: min. 21TB/h		
Propustnost pro čtení: min. 1,2TB/h		
Síťové rozhraní 10GbE RJ-45: počet rozhraní min. 4x		
Síťové rozhraní 25GbE SPF+, osazeno 10/25GbE optical multi-mode SR: počet rozhraní min. 2x		
Možnost rozšíření:		
• FC16 (min. 4 porty)		
• 25GbE (min. 2x SFP+ porty)		
• 10GbE (min. 4x SFP+ porty)		
Minimální počet konkurenčních zálohovacích úloh: min. 260		
Úložiště musí při ukládání dat využívat princip in-line deduplikace na cíli na principu variabilní délky bloku.		
Deduplikace musí být prováděna přes celé zálohovací prostředí		
Úložiště musí data před uložením komprimovat (komprimace nesmí mít dopad na výkon úložiště při záloze nebo obnově dat)		
Architektura diskového úložiště musí pro deduplikace využívat procesorový výkon a nesmí být závislá na počtu a typu backendových disků		
Diskové úložiště musí konsolidovat a centralizovat zálohovací prostředí (lokální i vzdálené) – všechna data budou deduplikována v rámci jednoho boxu		
Zařízení musí podporovat minimálně vyjmenované protokoly a musí umožnit jejich současné použití: CIFS, NFS, VTL, FC		
Zařízení musí umožňovat přímou integraci s různými typy zálohovacích SW (minimálně Microfocus Data Protector, Veritas NetBackup, Networker, Avamar, PPDM, Veeam, Quest, Microsoft DPM, Oracle RMAN, MS SQL Studio, SAP Hana)		
Diskové úložiště musí umožňovat přímou integraci se stávajícím zálohovacím software zadavatele – Veeam Backup Veeam Backup & Replication v12. Přímá integrace musí být doložitelná jak výrobcem diskového úložiště, tak výrobcem software, tzn. společností Veeam na veřejně dostupném místě (např. https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120)		
Popište způsob integrace		
Diskové úložiště je univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v		

produkčním prostředí – tzn. soubory, databáze, emaily, VMware, MS Exchange		
Kompatibilita se standardem OpenStorage		
Požadujeme Certifikace podle SEC 17a-4f nebo ekvivalentní evropské nebo české normy, uchazeč uvede jednotlivé certifikace.		
Deduplikace je prováděna přes celé zálohovací prostředí – jak přes všechny aplikace, tak přes cílová úložiště		
Možnost distribuce deduplikačního algoritmu z cílového (deduplikačního úložiště) na zdrojové zařízení (backup klienta nebo backup server)		
Funkce multitenancy (logické dělení diskového prostoru pro různé skupiny uživatelů s právy pouze na tyto logické jednotky s možností definice tenant administrator)		
Diskové úložiště musí obsahovat licenci pro replikaci do záložní lokality		
Diskové úložiště musí posílat do záložní lokality pouze deduplikovaná zkomprimovaná data		
Diskové úložiště musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci		
Replikaci musí být možno spustit ve stejném čase jako zálohu bez dopadu na výkon zálohy		
Diskové úložiště musí umožnit funkcionalitu šifrování replikačního toku data-in-flight		
Interní algoritmus pro neustálou kontrolu zdraví uložených dat a jejich automatickou obnovu v případě poškození tak, aby bylo možno zálohy kdykoliv obnovit k jakémukoliv okamžiku		
Zařízení musí obnovovat data vždy z deduplikovaného a komprimovaného stavu, není přípustný mezikrok (např. externí disková cache),		
Funkcionalita pro šifrování ukládaných data metodou data-at-rest		
Úložiště musí obsahovat HotSpare disky		
Kompletní verifikace dat – okamžitá verifikace záloh a kontrola integrity právě ukládaných dat		
Úložiště musí disponovat mechanismem pro mazání expirovaných dat, který nebude mít dopad na úlohy zálohy, obnovy a replikace (nebude snižovat počty současně běžících úloh, nebude vynucovat maintenance window, atd.) – tento proces musí být možno v případě potřeby spustit, nebo přerušit bez jakéhokoliv dopadu na zdraví a konzistenci uložených dat		
Nabízené zařízení musí umožňovat šifrovat data a musí disponovat i nástroji pro správu klíčů.		
Úložiště musí umožňovat nastavit skartační lhůty uložených dat, granulárně podle definovaných politik řízených zálohovacím SW.		
Retenční zámek úložiště musí ochránit data před změnou, nebo smazáním před vypršením retenční lhůty		
Úložiště musí disponovat mechanismem ochrany dat a samotného úložiště před napadením útočníkem z prostředí zadavatele i mimo toto prostředí (např. hackerský útok, ransomware, apod.).		

Úložiště musí umožnit tzv. HW hardening – tedy takové nastavení, aby nebylo možno jedním uživatelem s dostatečnými právy manipulovat s uloženými daty nebo systémovým nastavením (např. princip čtyř očí). Požadujeme, aby bylo možné data ošetřit tak, aby neexistovala oprávněná osoba, či soubor osob, které by je mohly modifikovat či smazat.		
Správa prostřednictvím jednotného webového rozhraní		
Funkcionalita automatického reportingu, automatický call-home (tato funkce musí mít možnost deaktivace na přání zadavatele)		
Monitoring pomocí MP pro SCOM aktuální verze		
Správu na principu rolí s různými typy oprávnění		
Záruka a podpora výrobce na 5 let s reakční dobou 4 hodiny, 24x7, pro chybu, která znemožňuje chod systému nebo má dopad na fungování systému. Přístup k telefonické podpoře výrobce 24x7x365. Aktualizace systému dostupné min. po dobu záruky zdarma, nabízené v servisním portálu výrobce po zadání sériového čísla.		
Možnost sledování servisních reportů prostřednictvím internetu.		
Vadná datová média, vyměněná v rámci záruky, se nevrací, ale zůstávají v majetku Zadavatele.		

DR SRV		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	Specifikace aplikačního serveru	Popis splnění požadavku
2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.	Form Factor a vnitřní uspořádání	
Dvousocketový systém založený na Intel platformě s využitím čtvrté generace CPU Xeon.	CPU	
Osazený 1x CPU s 16 jádry, o základní frekvenci min. 2.8 GHz. Celkový procesorový výkon měřený při plném osazení socketů musí dosahovat minimálně 333 bodů dle SPECint2017 Rates Result Base (http://spec.org/cpu2017/results/rint2017.html)		
4x 64GB na 5600MHz s možností osazení až 16 slotů.	RAM	
Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server osazený hot-plug disky: 1. 4x 3.84TB SSD SATA Read Intensive, DWPD1 2. Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:	Diskový subsystém	

3. 2x 480GB M.2 SSD NVMe v RAID1		
4. typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory) 5. podpora RAID 0, 1, 5, 6, 10, 50, 60 6. podpora 12Gbps technologie rozhraní disků 7. podpora Online Capacity Expansion (OCE) 8. podpora Online RAID Level Migration (RLM) 9. podpora Auto resume po ztrátě napájení 10. podpora 4K native sector velikosti 11. NVRAM “Wipe” 12. podpora TRIM/UNMAP příkazů pro SSDs v Pass-Thru mode 13. podpora NVRAM “Wipe” 14. podpora End Device Frame Buffering (EDFB) 15. podpora SED disků a SSD disků 16. Fast initialization for quick array setup 17. Configurable stripe size up to 1MB 18. Load balancing 19. podpora až 64 logických disků a 64TB LUN 20. podpora DDF compliant Configuration on Disk (COD) 21. podpora S.M.A.R.T. 22. podpora globálního i dedikovaného hot-spare 23. minimálně 8GB cache typu NV (cache to flash)	Diskový řadič	
2 x 1GbE port Base-T (RJ45) 2 x 10/25 GbE port Ethernet typu SFP28 2x 10 GbE port typu Base-T (RJ45)	Síťové rozhraní	
Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)	Napájení	
1. 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0 2. 2 x VGA (1 vpředu, 1 vzadu)	Interface	
3. Min 3x PCIe Gen4/5 sloty volné pro budoucí použití	Rozšiřující sloty	

4. Zásuvné ližiny s ramenem pro vedení kabelů	Kolejnice	
5. Microsoft® Windows Server® 2019/2022, x64 6. SUSE® Linux® Enterprise Server 7. Red Hat® Enterprise Linux 8. Canonical Ubuntu Server LTS 9. VMware vSphere™	Kompatibilita	
10. Windows Datacenter 2022 – licence na všechna jádra	Operační systém	
11. samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru 12. s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6 13. monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách 14. vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP 15. management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů 16. automatická instalace a obnova SSL certifikátu vestavěného serveru 17. přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE 18. podpora multifaktorové autentizace, podpora MS AD a generického LDAP	Management a vzdálená správa	

19. možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack 20. data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace 21. podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback 22. podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu 23. podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment) 24. management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora 25. management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.		

26. OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině 27. OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home) 28. možnost přístupu přes dedikovaný USB port s emulací síťového připojení 29. vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) 30. management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru 31. licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě 32. management umožňuje monitoring spotřeby el. energie na úrovni serveru 33. identifikace připojeného vzdáleného uživatele 34. vzdálená identifikace serveru		
35. Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli	Bezpečnostní funkce	

36. Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory. 37. Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory. 38. Prodávající se zavazuje, že zařízení a veškeré jeho komponenty: 39. pochází z autorizovaného obchodního kanálu výrobce 40. je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení 41. je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel	Podpora a servis	

Pásková knihovna / Autoloader – 1ks		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	Specifikace aplikačního serveru	Popis splnění požadavku
1. Pásková knihovna o max. velikosti 1U, barevně značené hot-plug vnitřní komponenty	Form Factor a vnitřní uspořádání	
2. min 1x LTO 8 SAS pásková mechanika	Mechaniky	
3. možnost osadit až 9 pásek do zásobníku 4. 10 kusů LTO 8 medií	Média	
5. Ano 6. Min. 200 štítků na pásky	Čtečka čárových kódů	
7. Ano 1ks	Čistící kazeta	

8. redundantní síťové napájecí zdroje, včetně 4 m napájecích kabelů	Napájení	
9. možnost šifrování pro LTO 7 a výše	Šifrování	
10. podpora webové správy 11. min 1x management port 12. vzdálená správa s funkcionalitami kontroly a konfigurace systému, spouštění diagnostiky systému, možnost inventarizace, prohlížení systémových protokolů	Management a vzdálená správa	
13. typ LCD s možností správy systému, kontroly, konfigurace a diagnostiky	Ovládací panel	

Back server		
Minimální požadavky na hardwarovou a softwarovou konfiguraci / vlastnosti	Specifikace aplikačního serveru	Popis splnění požadavku
1U server s uzamykatelným přením panelem. Pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty	Form Factor a vnitřní uspořádání	
Jednoprocesorový systém založený na INTEL platformě a osazený procesorem s těmito parametry: - min. 8 fyzickými jádry při frekvenci min. 3.2Ghz na jádro. Požadovaná cache CPU min. 24M a maximální výkon 95W. Zároveň výkon tohoto CPU potažmo celého systému odpovídá minimálnímu hodnocenému výkonu v kategorii Base 95 bodů dle www.nezávislé testovací skóre dle uznávané metodiky/cpu2017/results/rint2017.html	CPU	
64GB typu DDR5 s možností rozšíření až na 128GB	RAM	
Server musí podporovat minimálně 4x3,5 palcových disků SSD, SAS nebo NLSAS, požadujeme server s hot-plug disky. Server požadujeme osadit do RAID1 konfigurace: 1. 2x 480GB SATA SSD s DWPD3	Diskový subsystém	

2. typu SAS, PCI Express 3 kompatibilní, dvoukanálový (2 konektory) 3. podpora RAID a Pass-Through režimu. Tyto režimy se nastavují na úrovni disků a umožňují kombinovaný provoz řadiče 4. podpora RAID 0, 1, 10 5. podpora 12Gbps technologie rozhraní disků 6. automatická kontrola konsistence dat 7. Online Capacity Expansion (OCE) 8. Online RAID Level Migration (RLM) 9. Auto resume rebuildu po ztrátě napájení 10. podpora 4K native sector velikosti 11. podpora TRIM/UNMAP příkazů pro SSDs v Pass-Thru mode 12. podpora SED disků 13. podpora min 32 logických disků 14. podpora DDF compliant Configuration on Disk (COD) 15. podpora funkcí S.M.A.R.T. 16. podpora globálního hot-spare i dedikovaného hotspare	Diskový řadič	
Min. 2 x gigabit ethernet porty typu Onboard Min. 2x 10/25GbE porty typu SFP28 Min. 4x 12Gbps SAS rozhraní pro připojení páskové mechaniky	Síťové rozhraní	
Redundantní síťové napájecí zdroje min. 700W Titanium, zajišťující maximální výkon serveru i při výpadku jednoho zdroje a s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50%	Napájení	
1. minimálně 3x USB, z toho min. 2x USB 3.2 včetně 1x interní 2. sériový port 3. VGA port 4. systémová LED indikující stav systému	Interface	

5. Microsoft® Windows Server® 2008 R2 SP1, x64 (includes Hyper-V™ v2) 6. Microsoft Windows® HPC Server 2008 7. Microsoft® Windows Server® 2012 (includes Hyper-V™ v3), R2 8. Microsoft Windows Small Business Server 2011 9. SUSE® Linux® Enterprise Server 10. Red Hat® Enterprise Linux	Kompatibilita	
11. Citrix® XenServer™ 12. VMware vSphere™ 13. Red Hat Enterprise Virtualization™	Podpora virtualizace (embedded)	
14. Windows Standart 2022 – licence na všechna jádra	Operační systém	
15. samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru 16. s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6 17. monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách 18. vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP 19. management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů	Management a vzdálená správa	

20. automatická instalace a obnova SSL certifikátu vestavěného serveru 21. přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE 22. podpora multifaktorové autentizace, podpora MS AD a generického LDAP 23. možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack 24. data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace 25. podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback 26. podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu 27. podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment) 28. management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora		

29. management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení. 30. managementová karta pro vzdálenou správu serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině 31. managementová karta pro vzdálenou správu musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home) 32. možnost přístupu přes dedikovaný USB port s emulací síťového připojení 33. vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) 34. management musí umožnit bezpečné smazání dat ze serveru a		

jeho médií pro případ vyřazení nebo přesunu serveru 35. licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě 36. management umožňuje monitoring spotřeby el. energie na úrovni serveru 37. identifikace připojeného vzdáleného uživatele 38. vzdálená identifikace serveru		
39. Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli	Bezpečnostní funkce	
40. Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory. 41. Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory. 42. Prodávající se zavazuje, že zařízení a veškeré jeho komponenty: 43. pochází z autorizovaného obchodního kanálu výrobce	Záruky a servis	

44. je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení 45. je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel		

10 Sx;x;erviceDesk, procesy ITIL

ServiceDesk, procesy ITIL		
OBECNÉ POŽADAVKY NA PLATFORMU		
Asset management:	**ANO/NE**	**Popis splnění požadavku**
Licence řešení pro počet počítačů: min 100		
Možnost evidovat jakékoli další objekty v minimálně 30x násobku počtu licencím řešení pro počet počítačů		
Řešení obsahuje rozsáhlou knihovnu softwarových vzorů – minimálně 25.000.		
Řešení obsahuje rozsáhlá pravidla na rozpoznávání registrů – minimálně 150.000.		
Řešení obsahuje automatický mechanizmus pro odesílání hlaviček nerozpoznaného software bez nutnosti ručního zásahu a následný automatický upgrade aktualizované softwarové knihovny.		
Organizace pracovní plochy vychází z přehledného stromu organizace se začleněným hardware a software.		
Zákazník má plný přístup k databázi a naprosto volnou možnost tvorby reportů od předpřipravených výstupů, přes možnost exportu do Excelu až po možnost přímého SQL dotazu do databáze.		
Řešení obsahuje možnost bezagentové detekce SW a HW.		
Požadavky na funkcionalitu, podpora procesů – řešení pro řízení nákladů spojených s dodávání IT služeb:	**ANO/NE**	**Popis splnění požadavku**
Umožňuje podporu všech procesů, které zadavatel potřebuje pro řízení životního cyklu IT zdrojů souvisejících s provozem IT služeb. Z doporučených procesů ITIL, které musí navržený software podporovat musí být v rámci projektu realizovány procesy a funkce:		
a. Software Asset Management – řízení životního cyklu spojeného se softwarovými aktivy; podpora automatizace zjišťování informací o konfiguračních položkách software; zautomatizovaná podpora operativní práce IT týmu spojená s řešením a udržením softwarové čistoty.		
b. Asset and Configuration Management – podpora správy konfigurační databáze. Je umožněno sledování vazby a vzájemné závislosti mezi konfiguračními položkami a uchovávána historie konfiguračních položek; podpora automatizace zjišťování informací o konfiguračních položkách hardware a software; zautomatizovaná podpora operativní práce IT týmu spojená se změnami konfiguračních položek.		
Uživatelské rozhraní je lokalizováno do češtiny.		
Umožňuje generování a tisk reportů.		

Systém obsahuje znalostní databázi o software, automaticky udržovanou a publikovanou výrobcem a poskytovanou formou služby		
Je vyřešen bezpečný přístup do aplikace (Integrované přihlašování do portálu i konzol, řízení oprávnění přístupu k informacím).		
Portál pro zaměstnance, manažery a IT tým		
Podpora využití čárových kódů při operativní práci spojené s pořizování a zaváděním nových majetků		
Podpora inventarizace IT majetku s využitím podpory čárových kódů		
Podpora vedení návazné dokumentace		
Vlastnosti administrace řešení:	**ANO/NE**	**Popis splnění požadavku**
Pro administrátory je plná oprávnění k systému a tím i možnost nezávisle na dodavateli systém modifikovat podle měnících se potřeb zadavatele (po dokončení implementace) i měnit jeho konfiguraci včetně možnosti:		
• Přidávání a odebírání uživatelů a jejich zařazování do skupin.		
• Přidávání a odebírání skupin, přidávání uživatelských rolí.		
• Nastavení přístupových práv k jednotlivým objektům.		
• Nastavení posílání víceúrovňových notifikací a úprava jejich obsahu.		
• Možnost přidávat vlastní položky do formulářů.		
• Možnost nastavení grafického vzhledu portálu – skinování.		
Integrace s aplikacemi třetích stran:	**ANO/NE**	**Popis splnění požadavku**
• Nativní integrace s Microsoft Active Directory. Automatické načítání vztahu zaměstnance a jeho nadřízeného. Automatické načítaní informací o PC.		
• Integrace s nástroji pro správu pracovních stanic (VNC, RemoteDesktop, apod.).		
• Import a export dat z Microsoft Excel.		
• Export dat do Microsoft Word.		
Technické předpoklady:	**ANO/NE**	**Popis splnění požadavku**
Využití databáze MS SQL pro ukládání dat (dodávka databáze není součástí poptávky).		
Integrace s Active Directory – automatické přihlašování do aplikace (dodávka Active Directory není součástí poptávky).		
Podpora výrobce	**ANO/NE**	**Popis splnění požadavku**
Agent pro koncovou stanici (pokud je vyžadován) musí být poskytován zdarma nebo musí být zahrnut v ceně řešení		
Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let		