příloha č. 2

TECHNICKÝ POPIS

k veřejné zakázce

„Kybernetická bezpečnost Technologického centra města Dvůr Králové nad Labem"

Obsah

1 Účel dokumentu 4
2 První fáze projektu – dodávka HW a vybraného SW 5
2.1 Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení 5
2.1.1 Hardware 5
2.1.2 Software 8
2.1.3 Implementační práce 8
2.2 Pravidelné testování zranitelnosti prvků infrastruktury 10
2.3 Řešení centrálního ukládání a analýzy logů a reportů 11
2.4 Aktivní přístupové prvky, řízení přístupu do vnitřní sítě, 802.1X, detekce síťového provozu, monitoring provozu 15
2.4.1 Hardware 15
2.4.2 Monitoring provozu 26
3 Druhá fáze projektu – implementace 27
4 Třetí fáze projektu – optimalizace a dokumentace 27
4.1 Implementační dokumentace 27
4.1.1 Popis fyzické infrastruktury 27
4.1.2 Instalace serverů, virtuálního prostředí, systémů a aplikací 27
4.1.3 Monitorování a dohled 27
4.1.4 Zapracování konkrétních vstupů od Zadavatele 28
4.1.5 Časový harmonogram projektu 28
4.1.6 Zálohovací strategie 28
4.1.7 Zapracovaní legislativních požadavků a doporučení z GAP analýzy 29
4.1.8 Ošetření nálezů z penetračních testů 29
4.2 Dokumentace skutečného provedení 29
5 Obecné podmínky 30
6 Harmonogram projektu 32
6.1 Časový přehled plnění projektu 32
7 Akceptační testy 33
7.1 Akceptační protokol aktivních prvků 34
7.2 Akceptační protokol implementace ověřování 802.1X 36
7.3 Akceptační protokol virtualizace datového centra 37
7.4 Akceptační protokol diskových polí a SAN infrastruktury 38
7.5 Akceptační protokol virtualizace produkčního a VDI datového centra 39
7.6 Akceptační protokol doménových serverů 40

7.7 Akceptační protokol aplikačních serverů 42
7.8 Akceptační protokol monitoringu síťového provozu 43
7.9 Akceptační protokol testování zranitelností 44
7.10 Akceptační protokol centrálního systému logování 45
7.11 Akceptační protokol provozního monitoringu 46
7.12 Akceptační protokol dokumentace 47

1 Účel dokumentu

Účelem tohoto dokumentu je poskytnout detailní přehled o postupu implementace systému kybernetické bezpečnosti dle připravované změny zákona 181/2014 Sb. Zákon o kybernetické bezpečnosti a prováděcí dokumentace. Obsahuje popis realizace technických požadavků, hardwarových a softwarových technologiích, které jsou součástí projektu s názvem "Kybernetická bezpečnost Technologického centra města Dvůr Králové nad Labem". Zároveň se dokument zaměřuje na popis veškerých implementačních prací, které zahrnují nejen oživení a konfiguraci hardwaru, ale také všechny potřebné migrační činnosti. Tyto činnosti jsou rozděleny do tří hlavních etap, které odpovídají harmonogramu projektu. Každá etapa je podrobně popsána, aby bylo zajištěno, že všechny kroky budou realizovány systematicky a v souladu s plánem a požadovanými výstupy projektu.

2 První fáze projektu – dodávka HW a vybraného SW

První fáze projektu počítá s implementací následujících opatření:

- Dokumentace – v této fázi zpracování Implementační dokumentace – specifikace viz. kap. 4. Dokumentace.
- Doplnění Hardware datacentra a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení.
- Testování zranitelností prvků infrastruktury.
- Aktivní přístupové prvky, řízení přístupu do vnitřní sítě 802.1x, detekce síťového provozu, monitoring provozu.
- Řešení centrálního ukládání a analýzy logů a reportů.

2.1 Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení

Dodávka počítá s testováním hardware, zahoření a základní konfigurací - nových serverů, diskového pole a systému pro zálohu napájení. Součástí jsou též dodané licence a pomocný materiál nutný pro zapojení do stávajícího datového centra. **Datacentrové servery pro produkci, VDI a diskové pole budou od jednoho výrobce z důvodu centralizace správy a sjednocení servisního střediska pro hlášení závad.**

2.1.1 Hardware

2x Servery pro produkční prostředí datového centra

- Určeno pro virtualizaci serverů,
- TPM 2.0 v3,
- výsuvné ližiny a rameno pro vyvázání kabelů pro montáž do 19" racku,
- redundantní napájecí zdroje,
- 2x procesor o výkonu každého procesoru alespoň 22 000 bodů v testu passmark, max. 8 jader z licenčních důvodů, frekvence alespoň 2.9Ghz, cache alespoň 22MB,
- rychlost paměti alespoň 5600MT/s,
- RAM modul o kapacitě alespoň 64GB,
- celkem osazeno 512GB RAM,
- interní řadič pro 2x M.2 SSD karty sloužící pro instalaci hypervisoru o kapacitě 480GB v RAID1,
- min. 2x 10/25Gbps SFP28+ porty pro LAN,
- min. 4x 10/25Gbps SFP28+ porty pro iSCSI,
- min. 2x 1Gbps RJ-45 porty pro LAN,
- čelní kryt serveru včetně LCD displeje,
- redundantní napájecí zdroje o výkonu alespoň 1100W,
- 4x Twinax kabely SFP28 to SFP28, 25 Gbps, alespoň 3 metry dlouhé.
- Server musí podporovat možnost ověření, že po sestavení v továrně nedošlo cestou k nežádoucí změně komponent.
- Modul pro vzdálený management, přístup přes web. prohlížeč s podporou SSL, Telnet/SSH a IPMI nástroje; podpora virtuálních médií, plná podpora pro integraci do prostředí VMware vSphere a vCenter. 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.
- Technická podpora a servis minimálně na 5 let (24x7x365), oprava do 24 hodin od identifikace problému v pracovní dny a jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW v místě instalace HW. Zdarma možnost on-line 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.

2x Servery pro virtuální desktopy (VDI)
- Určeno pro virtualizaci stanic,
- TPM 2.0 v3,
- výsuvné ližiny a rameno pro vyvázání kabelů pro montáž do 19" racku,
- redundantní napájecí zdroje,
- 2x procesor o výkonu každého procesoru alespoň 55 000 bodů v testu passmark, alespoň 28 jader, frekvence alespoň 2.0Ghz, L3 cache alespoň 52MB,
- rychlost paměti alespoň 5600MT/s,
- RAM modul o kapacitě alespoň 64GB,
- celkem osazeno 512GB RAM,
- interní řadič pro 2x M.2 SSD karty sloužící pro instalaci hypervisoru o kapacitě 480GB v RAID1,
- min. 2x 10/25Gbps SFP28+ porty pro LAN,
- min. 4x 10/25Gbps SFP28+ porty pro iSCSI,
- min. 2x 1Gbps RJ-45 porty pro LAN,
- čelní kryt serveru včetně LCD displeje,
- redundantní napájecí zdroje o výkonu alespoň 1100W,
- 4x Twinax kabely SFP28 to SFP28, 25Gbps, alespoň 3 metry dlouhé.
- Server musí podporovat možnost ověření, že po sestavení v továrně nedošlo cestou k nežádoucí změně komponent.
- Modul pro vzdálený management, přístup přes web. prohlížeč s podporou SSL, Telnet/SSH a IPMI nástroje; podpora virtuálních médií, plná podpora pro integraci do prostředí VMware vSphere a vCenter. 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.
- Technická podpora a servis minimálně na 5 let (24x7x365), oprava do 24 hodin od identifikace problému v pracovní dny a jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW v místě instalace HW. Zdarma možnost on-line 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.

1x Diskové pole pro virtualizační infrastrukturu

- Diskové pole plně kompatibilní se servery uvedenými výše,
- diskové pole typu rack o velikosti maximálně 2U,
- ližiny pro montáž do 19"racku,
- redundantní napájecí zdroje,
- multikontrolerové řešení s redundantní, vysoce dostupnou architekturou bez SPOF (Single Point of Failure), umožňující upgrade FW za provozu, řadiče v režimu Active-Active,
- redundantní diskové řadiče, každý řadič minimálně 16GB cache,
- podpora RAID 1,5,6,10 a distribuovaný erasure coding odpovídající RAID6,
- back-end SAS 3.0 12Gb/s, vyžadovány jsou minimálně dva SAS 3.0f, 12Gb/s porty na každý řadič,
- konektivita řadiče alespoň 4x 25Gbps SFP28,
- interní backplane pro 24x 2,5" disky s rozhraním 12Gb SAS,
- diskové pole osazeno alespoň 10x 3,84TB SSD disky typu SAS, read intensive,
- diskové pole osazeno alespoň 11x 2.4TB SAS HDD, 10 000 ot/min,
- možnost připojení rozšiřovací jednotky o dalších 48 disků,
- podpora minimálně 1024 snapshotů na diskovém poli,
- 8x Twinax kabely SFP28 to SFP28, 25Gbps, alespoň 3 metry dlouhé,
- podpora asynchronní replikace skrze FibreChannel nebo iSCSI v režimu one-to-many nebo many-to-one včetně možnosti kopie diskového svazku,
- management diskové pole skrze web. prohlížeč s podporou SSL, Telnet / SSH a IPMI nástroje,
- podpora technologií VMware vSphere 8, Windows Server 2025 Citrix XenServer8, podpora VMware API – VAAI. Plugin ke správě diskového pole z VMware vCenter management konzole.
- Vzdálená správa diskového pole: min 1ks GE Management port, grafické uživatelské rozhraní včetně licence pro lokální správu diskového pole a příkazové řádky (CLI), mapování jednotlivých interních rolí a oprávnění na uživatelské skupiny v adresářové službě LDAP.
- 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 do 4 hodin od identifikace problému včetně víkendů a svátků. 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.

1x Třífázová UPS

- Třífázová UPS typu Tower s battery pack,
- UPS s dvojitou konverzí,
- účinnost normálního režimu min. 95%,
- efektivita bateriového provozu min. 95%,
- kompatibilní s PFC,
- možnost rozšíření o další min. 3 jednotky bateriového modulu pro prodloužení výdrže,

- minimálně 2 napájecí vstupy,
- podpora napájení z motorgenerátoru,
- vstupní účiník min. 0.99,
- vstupní proud min. 28A,
- výstupní výkon min. 18kW,
- přepěťová ochrana a filtrování EMI a RFI,
- průběh napětí při napájení z baterie je čistá sinusoida,
- variabilní nastavení výstupního napětí a frekvence,
- výstupní účiník min. 0,9,
- ochrana proti přetížení interního proudu v režimech Line, Baterie a Bypass,
- maximální harmonické zkreslení při lineární zátěži THD 1%,
- maximální harmonické zkreslení při nelineární zátěži THD 5,5%,
- možnost automatického či manuálního Bypass,
- rychlost přechodu do 0ms,
- provoz na baterie při zatížení 9kW minimálně 1 hodina,
- nastavitelný proud nabíjení baterie,
- inteligentní správa nabíjení baterií.
- Management skrze dedikovanou management kartou kompatibilní s datovým cluster uvedeným výše. S podporou SNMPv1 a SNMPv3/http/https/FTP/telnet/ssh přístupu, odesílání emailových notifikací, SNMP trap, Syslog. Karta podporuje autentizaci do UPS s využitím RADIUS, LDAP, LDAPS.
- UPS software s licencí podporující používané technologiemi VMware vSphere s možností řízeného vypínání a monitoringu s možností integrace do VMware vCenter, podpora agentů pro Microsoft Windows od verze 2016 a Linux distribuce Red Hat, Ubuntu Server, Citrix. Licence na dobu min. 5 let - musí být součástí dodávky.
- Možnost lokální konfigurace základních parametrů jako IP adresace, manuální Bypass a další skrze LCD panel.
- Certifikace UPS CE, IEC62040-1, IEC62040-2.
- Záruka na UPS minimálně 2 roky, profylaxe každý rok po dobu udržitelnosti projektu.

2.1.2 Software

Zadavatel požaduje nákup nových licencí, dodaných přes autorizovaného distributora pro Českou republiku. Smlouva včetně licencí a stažení instalačních souborů musí být dostupná on-line.

- 2x Windows Server 2025 Datacenter, 16CORE.
- 160x Windows Server 2025 User CAL.
- 2x Microsoft SQL Server 2025 core – 2 Core License Pack + Software Assurance po dobu min. 5 let.

2.1.3 Implementační práce

Veškeré implementační práce zahrnují:

- Dopravu zařízení na místo objednatele a instalace do racku.
- Dokumentaci provedených prací.
- Zaškolení administrátorů na správu nového HW zařízení a SW vybavení.
- Veškeré implementační práce popsané níže včetně konfigurací s ohledem na bezpečnost, vysokou dostupnost a redundanci.

2.1.3.1 Servery produkční a VDI servery

Veškeré instalační práce na zařízení a souvisejících technologiích musí provádět výrobcem certifikovaný a školený odborník, který disponuje platným certifikátem pro danou technologii. Dodavatel je povinen doložit odpovídající certifikace před podpisem smlouvy.

- Instalace a konfigurace serverů: zahoření hardware a provedení testu pevných disků, RAM a redundance komponent.
- Vybalení zařízení v datovém centru objednatele a fyzická instalace zařízení do racku.
- Připojení elektrických a datových management portů do sítě datového centra dle Best Practices tedy křížové redundantní zapojení a v případě elektrických zapojení do UPS.
- Aktualizace Firmware jednotlivých komponent jako jsou disky, síťové karty, aktualizace BIOS.
- Oživení management portu, nastavení bezpečného hesla dle ZKB a konfigurace MGMT přístupu, IP, časového zdroje, názvu, SNMP, uživatelských účtů, emailové notifikace a další.
- Konfigurace sítě, konfigurace RAID, vzdáleného přístupu, emailových notifikací, odesílání do centrálního Syslog.
- Instalace a konfigurace interního diskového pole: základní nastavení dle Best Practices výrobce, konfigurace RAID svazku nad pevnými disky. Nastavení síťových adaptérů, konfigurace RAID řadičů diskového pole dle Best Practices výrobce serveru pro danou technologii připojení.

2.1.3.2 Diskové pole

Veškeré instalační práce na zařízení a souvisejících technologiích musí provádět výrobcem certifikovaný a školený odborník, který disponuje platným certifikátem pro danou technologii. Dodavatel je povinen doložit odpovídající certifikace před podpisem smlouvy.

- Vybalení zařízení v datovém centru objednatele a fyzická instalace zařízení do racku.
- Připojení elektrických a datových management portů do sítě datového centra dle Best Practices tedy křížové redundantní zapojení a v případě elektrických zapojení do UPS.
- Konfigurace management portů a konfigurace iSCSI portů dle Best Practices výrobce síťových prvků a diskového pole.
- Připojení diskového pole do iSCSI sítě a test komunikace.
- Zapnutí diskového pole, oživení management portu, nastavení bezpečného hesla dle ZKB a konfigurace MGMT přístupu, IP, časového zdroje, názvu, SNMP, uživatelských účtů, emailové notifikace a další.
- Kontrola všech komponent diskového pole a provedení interních testů.
- Provedení upgrade Firmware diskového pole a interních disků.
- Konfigurace diskového pole na RAID s možností výpadku jednoho disku.
- Tvorba čtyřech diskových svazků rozdělených na 50-50 % kapacity SSD disků a rozdělení 30-70 % kapacity SAS disků.
- Nastavení připojení hostitelů virtualizační platformy pomocí konfiguračního rozhraní diskového pole a připojení svazků a povolení multipathing.

- Kontrola redundantního zapojení diskového pole fyzický odpojením jedné z cest.
- Výkonnostní testy připravených svazků.
- Kontrola korektního připojení do datového centra.

2.1.3.3 UPS

Veškeré instalační práce na zařízení a souvisejících technologiích musí provádět školený odborník, který disponuje platným certifikátem pro danou technologii. Dodavatel je povinen doložit odpovídající certifikace před podpisem smlouvy.

- Vybalení zařízení a instalace všech dodatečných komponent jako management karty a senzorů.
- Fyzická instalace do serverovny zadavatele.
- Napojení na stávající elektrické rozvody serverovny.
- Zapojení management karty, napojení na monitorovací systémy zákazníka.
- Konfigurace notifikací o událostech napájení.
- Konfigurace pravidel pro řízené vypínání a náběh.
- Konfigurace pravidla, které zapne připojené zařízení až v případě nabití baterie nad 20 %.
- Zapojení zařízení v racku do PDU, případně přímo výstupů UPS podle důležitosti.
- Nastavení odesílání logů zařízení do centrálního Syslogu.
- Otestování UPS na funkčnosti veškerých pravidel pro vypnutí/zapnutí napojených zařízení.

2.2 Pravidelné testování zranitelnosti prvků infrastruktury

Veškeré instalační práce na zařízení a souvisejících technologiích musí provádět výrobcem certifikovaný a školený odborník, který disponuje platným certifikátem pro danou technologii. Dodavatel je povinen doložit odpovídající certifikace před podpisem smlouvy.

1x Produkt pro testování a vyhodnocování zranitelností prvků infrastruktury

- Způsoby detekce budou zahrnovat skenování portů, kontrolu dostupných služeb a identifikaci verzí obsahující známé zranitelnosti, konfigurační chyby a další.
- Ke sledování zranitelností a nálezů bude sloužit interaktivní dashboard s náhledem na reálná data.
- Bude generována zpráva, která shrne nalezené problémy včetně možností jejich řešení.
- Nebude se pokoušet o aktivní použití nalezených zranitelností, ale pouze na jejich detekci a reportování.
- Testovaná zařízení budou všechna zařízení připojená k síti, ať jde o síťový prvek, server, koncovou stanici, tiskárnu nebo jiné zařízení.
- Umožní opakované testování.
- Produkt umožňuje provádění testů zranitelnosti průběžně během provozu infrastruktury.
- Požadované funkcionality, SW záruka a podpora výrobce po dobu 5 let s aktivním centrem pro hlášení problémů telefonní nebo emailovou cestou.

2.3 Řešení centrálního ukládání a analýzy logů a reportů

1x Centrální úložiště logů

Veškeré instalační práce na zařízení a souvisejících technologiích musí provádět výrobcem certifikovaný a školený odborník, který disponuje platným certifikátem pro danou technologii. Dodavatel je povinen doložit odpovídající certifikace před podpisem smlouvy.

- Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware.
- Integrovaná appliance (HW se specializovaným Firmware/Software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávislé na infrastruktuře zadavatele.
- Určené pro montáž do stávajícího serverového datového rozvaděče 19", včetně výsuvných kolejnic a ramene pro vedení kabelů.
- Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení.
- Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze.
- Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem, zdroji dat a jednotlivým ovládacím částem systému.
- Je požadován bezagentový sběr logů pro protokoly UDP/TCP 514 (Syslog), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Pro systémy Windows je umožněn agentový i bezagentový sběr v rámci licence.
- Příjem a zpracování logů, událostí a dalších strojově generovaných dat - minimálně protokoly UDP/TCP 514 (Syslog), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně), RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows Event Log.
- Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Windows Event Logů (včetně rozšířených), šifrovaná komunikace, SW agent obsahuje buffer pro případ ztráty komunikace a umožní zpětné nahrání dat při obnově spojení.
- Překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem.
- Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv.
- Systém umožňuje filtrování událostí (včetně událostí z textových souborů) na straně Windows před samotným odesláním logu z daného endpointu, čímž snižuje objem přenášených a zpracovávaných dat.
- Systém umožňuje filtrování událostí (včetně událostí z textových souborů) na straně Windows před samotným odesláním logu z daného endpointu, čímž snižuje objem přenášených a zpracovávaných dat.
- Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy.
- Nemožnost mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci.

- Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace – změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období.
- Předpřipravené pohledy výrobce (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání.
- Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti, notifikace správce systému při riziku zaplnění vyrovnávací paměti.
- Integrovaná podpora doplňování logů dalšími údaji – zejména umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům zejména dat, aplikacím, zařízením, IP rozsahům.
- Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce podle MAC adresy.
- Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, sloužící jako výchozí časový údaj pro systém.
- Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení.
- Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování).
- Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran.
- Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (zejména SQL dotazů). Průběžná aktualizace přednastavených reportů výrobcem.
- Integrované REST API rozhraní pro napojené systémy, musí umožnit autorizovaný přístup ke strukturované databázi logů v rámci licence.
- Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění – okamžitého zobrazení rozparsovaných testovacích dat včetně případných chyb.
- Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Hyper-V, VMware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortigate, Cisco, Dell servery, Synology, Linux, Apache, M365 a další.
- Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min. SMTP, Syslog.
- Min. 5000EPS (events per second), krátkodobá (min. 10 min) přetížitelnost systému až 200%.
- Využitelná diskové kapacita pro ukládání dat min. 40TB, disky musí být chráněny min. RAID5.
- Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis i čtení) o kapacitě min. 8GB.
- Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat.
- Systém musí mít redundantní napájení - min. 2 nezávislé zdroje.

- Min. 2x LAN 1Gb Base-T a 2x LAN 10Gb SFP+ 1x 1Gb Base-T nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem.
- Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade, aktualizace parsovacích pravidel a podpory výrobců zdrojových zařízení.
- Integrované zálohování a obnova konfigurace.
- Možnost archivace logů na externí úložiště včetně zajištění integrity archivů.
- Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako cluster.
- Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce.
- Záruka min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze Firmware/software, konzultační činnosti, softwarová podpora a aktualizace řešení pro ukládání logů.
- Za účelem uchovávání logů je řešení doplněno o archivační úložiště pro ukládání logů.
- Systém logmanagementu musí zajistit integritu archivu. Dodávané řešení musí být standardní Log/Event Management, který musí umožnit budoucí rozšíření o systémy třetích stran (např. systém SIEM) nebo napojení na služby SOC (Security operations center). Řešení musí umožnit sofistikovanou, transparentní a opakovatelnou pokročilou analýzu, spojenou s řešením běžných provozních i bezpečnostních událostí/incidentů a upozorňováním na ně, a to z kritických i nekritických a podpůrných systémů a aplikací. Řešení musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, primárně v českém jazyce a dále variantně v jazyce anglickém, bez nutnosti používat SQL (či obdobnou „programátorskou“) syntaxi pro definici či úpravu reportů. Řešení musí zachovávat originál logů za účelem bezpečnostního auditu, a to v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. Řešení musí umožnit snadné a rychlé multikriteriální vyhledávání pro účely analýz, auditů, a podporu běžného provozu komplexního řešení ICT infrastruktury. Pro zajištění požadavků bezpečnosti musí řešení Log/Event Management disponovat konfigurovatelným uživatelským oddělením rolí a ochranou centralizovaných logů před neoprávněným přístupem k citlivým datům. Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace. Řešení musí umožnit správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Ukládání všech informací bude prováděno do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých systémů. Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně Firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy).

- Řešení musí umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.

1x Archivační úložiště pro centrální ukládání logů

- NAS s 4 HDD SATA 3,5" pozicemi s redukcí pro 2,5" disky a 2 pozice pro NVME disky,
- disky vyměnitelné za provozu,
- možnost připojení expanzní diskové jednotky,
- CPU o výkonu alespoň 3000 bodů dle passmark, alespoň 2 výpočetní jádra, L3 cache alespoň 3MB,
- min. 4GB RAM s možností rozšíření až na 32GB,
- min. 2x 1GbE RJ-45,
- podpora hardwarového šifrování,
- podpora Jumbo Frame,
- 2x min. 16TB HDD, 7200ot/min kompatibilních s NAS s možností vyčítání SMART a podporou aktualizace Firmware,
- záruka 5 let na NAS i HDD.

Systém pro archivaci logů je k dispozici na jednom místě, záznamy budou ve sjednoceném formátu při zachování jejich dostupnosti, důvěrnosti a integrity. Systém zajistí uložení dat k okamžitému prohlížení a prohledávání minimálně po dobu 12 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby po dobu dalších 2 let.

1x Analytický nástroj k Firewallu pro metropolitní síť

- Nástroj pro bezpečnostní analýzu logů z NGFW Fortigate zařízení se schopností jejich korelace včetně možnosti ukládání logů.
- Podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení.
- Virtuální appliance pro platformu VMWare, Microsoft Hyper-V, KVM (fyzické zařízení není přípustná alternativa).
- Možnost nativní integrace se stávajícím zařízením typu NGFW Fortigate, které bude sloužit jako zdroj dat pro analýzu.
- Možnost provozovat poptávané řešení jako prosté uložiště logů z dalších zařízení zákazníka bez jejich další analýzy.
- Možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje.
- Možnost generovat reporty na základě specifikace dotazů do databáze logů poptávaného řešení.

- HTML/CSV/XML/PDF formát generovaných reportů s možností plánování pravidelné automatické tvorby reportů.
- Možnost logické segmentace s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat.
- Musí obsahovat předdefinované vzory reportů a umožňovat úpravu vzhledu generovaných reportů prvky zákazníka (loga, hlavička, …).
- Možnost zobrazení aktuálních logů z jednotlivých integrovaných NGFW zařízení v reálném čase.
- Možnost zpětného zobrazení a analýzy logů z důvodu možnosti zpětné analýzy provozu a možných uskutečněných bezpečnostních hrozeb.
- Plnohodnotná správa pomocí grafického rozhraní a CLI.
- Podpora SNMPv2 a SNMPv3 a REST API.
- Samostatná sekce v grafickém rozhraní pro zobrazení zjištěných hrozeb.
- Podpora přijímání Syslogů ze zařízení třetích stran.
- Možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením.
- Minimálně 4x vNIC.
- Alespoň 5TB alokovatelná kapacita dlouhodobého úložiště logů a alespoň 5GB minimální limit pro množství přijatých logů k analýze za jeden den (možnost navýšení limitů pomocí dodatečné licence).
- Podpora výrobce v režimu 24/7 na dobu min. 5 let.
- Všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu min. 5 let - musí být součástí dodávky.

2.4 Aktivní přístupové prvky, řízení přístupu do vnitřní sítě, 802.1X, detekce síťového provozu, monitoring provozu

2.4.1 Hardware

SAN přepínače budou zajišťovat přístup serverové infrastruktury k diskovému poli.

2x SAN přepínač

- Formát zařízení: 1U,
- Typ přepínače: L2/L3 přepínač,
- Formát přepínače: stohovatelný,
- Počet dedikovaných stohovacích portů spolu s propojovacím modulem: 2,
- Minimální počet zařízení ve stohu: 8,
- Minimální kapacita sběrnice stohu: 1 000Gb/s,
- Stateful Switch Over v rámci stohu,
- Min. přepínací kapacita: 1Tbps,
- Min. paketový výkon přepínače: 744Mpps,
- Min. velikost sdíleného systémového bufferu: 16MB,
- Redundantní ventilátory vyměnitelné za chodu zařízení,
- Non-stop Forwarding,
- Sdílení výkonu napájecích zdrojů napříč celým stohem,
- Možnost instalovat interní redundantní napájecí zdroj,

- Interní redundantní napájecí zdroj: vyžadován,
- Možnost redundance zdrojů v režimu N+1,
- Stohovací zdrojový kabel: vyžadován 0.3m,
- Možnost stohování přes dedikované porty - bez snížení počtu použitelných ethernetových portů,
- Stohovací datový kabel: vyžadován 0.5m,
- Počet portů 1/10/25G SFP28: 12,
- Možnost přepínač rozšířit o modul s volitelným fyzickým rozhraním: vyžadován,
- Velikost MAC address tabulky: 32000,
- Min. počet IPv4 routes: 39000,
- Min. počet IPv6 routes: 19500,
- Min. počet konfigurovatelných security ACL: 5000,
- IEEE 802.3ad (Link Aggregation),
- IEEE 802.3ad přes více přepínačů,
- Minimálně 8 linek jako součást Link Aggregation Group trunku,
- Minimální počet konfigurovatelných Link Aggregation Group trunků: 128,
- IEEE 802.1Q, minimální počet aktivních VLAN: 1000,
- IEEE 802.1x,
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací),
- Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication),
- Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů,
- RADIUS CoA,
- Podpora instance spanning-tree protokolu per VLAN a IEEE 802.1w – Rapid Spanning Tree Protocol,
- Protokol MVRP nebo VTP pro definici a správu VLAN sítí,
- Podpora jumbo rámců (min. 9198 bytes),
- Detekce protilehlého zařízení (např. CDP nebo LLDP),
- Směrování protokolů IPv4 a IPv6 v hardware,
- OSPFv2 a OSPFv3,
- Podporované protokoly: EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868), ISIS, BGPv4,VXLAN s BGP EVPN, Policy based routing uvnitř VRF, IP Multicast (PIM SSM, PIM SM), Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF), MPLS VPN, MPLS VPN přes GRE tunely, MPLS VPN - 6VPE,
- First Hop Redundancy Protokol (např. VRRP, HSRP),
- Reverse path check (uRPF) pro IPv4 i IPv6,
- IGMPv2, IGMPv3,
- IGMP snooping,
- MLD snooping,
- DHCP relay,
- Minimální počet HW QoS front: 8,
- QoS classification – ACL, DSCP, CoS based,
- QoS marking - DSCP, CoS,
- QoS - Strict Priority Queue,

- Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní),
- QoS Policing,
- QoS-Per Flow policing,
- QoS-Hierarchical QoS., min. 2 úrovně,
- First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP),
- IPv6 services (Telnet, SSH, Syslog, DHCP),
- IPv6 QoS,
- IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard),
- IPv6 Port ACL, VLAN ACL,
- Možnost definovat povolené MAC adresy na portu,
- PACL, VACL,
- IEEE 802.1ae (AES-GCM-128) na uplink portech,
- IEEE 802.1ae (AES-GCM-256) na uplink portech,
- Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy,
- Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru,
- Bezpečnostní funkce umožňující inspekci provozu protokolu ARP,
- Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce Secure Boot, která ověřuje autentičnost a integritu jak Bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. Trusted modulů,
- HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů,
- Podpora SUDI (IEEE 802.1AR) autentizace,
- IEEE 802.3az,
- Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu,
- Multicast DNS (mDNS) gateway,
- Application Visibility – pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) - povýšením Firmware,
- Application Visibility – monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní,
- Application Visibility - možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type,
- Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX,
- Full Flexible Netflow,
- SSHv2 a CLI rozhraní,
- Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení v prostředí Python scripting, Linux shell,
- Aplikace softwarových záplat, nikoli povyšování celého Firmware,
- Streaming telemetrie prostřednictvím NETCONF/XML,
- SNMPv2/v3,
- Podpora network boot (iPXE) pres IPv4 i IPv6,
- TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting),
- AVC (NBAR2) - povýšením Firmware,

- Vzdálený port mirroring (ERSPAN) - povýšením Firmware,
- NTPv3 server,
- Záruka a podpora výrobce na HW/SW po dobu 5 let (režim minimálně 8x5xNBD).

1x Přepínač pro metropolitní síť

Přepínač pro metropolitní síť zajišťuje připojení podřízených institucí k metropolitní síti a prostředkům městského úřadu. Přepínač musí disponovat dostatečným počtem rozhraní s podporou 1/10/25Gb ethernetu.

- Formát zařízení: 1U,
- Typ přepínače: L2/L3 přepínač,
- Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28: 48,
- Minimální počet neblokovaných portů 40GE s volitelným fyzickým rozhraním typu QSFP28: 4,
- Možnost volby rychlosti 40/100GE na rozhraních typu QSFP28: min. 4 rozhraní,
- Redundantní napájecí zdroj,
- Min. velikost sdíleného systémového bufferu: 36MB,
- Velikost MAC address tabulky: 80000,
- Min. počet IPv4 routes: 212000,
- Min. počet IPv6 routes: 212000,
- Min. počet konfigurovatelných security ACL: 27000,
- Min. přepínací kapacita: 3.2Tbps,
- Min. paketový výkon přepínače: 1Bpps,
- Flexibilní alokace SRAM a TCAM zdrojů,
- StackWise Virtual,
- IEEE 802.3ad (Link Aggregation - LAG),
- IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis,
- Podpora ISSU,
- Minimální počet aktivních VLAN: 4000,
- IEEE 802.1w - Rapid Spanning Tree Protocol,
- Podpora instance spanning-tree protokolu per VLAN,
- Podpora jumbo rámců (min. 9216 bytes),
- Detekce protilehlého zařízení (např. CDP nebo LLDP),
- Protokol MVRP nebo VTP pro definici a správu VLAN sítí,
- Podpora routovacích protokolů OSPFv2, OSPFv3,
- Podpora routovacího protokolu EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868),
- Podpora routovacího protokolu ISIS,
- Podpora routovacího protokolu BGPv4,
- Podpora VXLAN s BGP EVPN,
- Policy based routing uvnitř VRF,
- Graceful Insertion and Removal,
- IP Multicast (PIM SSM, PIM SM),
- Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF),
- MPLS VPN,

- MPLS VPN přes GRE tunely,
- MPLS VPN - 6VPE,
- First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6,
- Reverse path check (uRPF),
- Minimální počet HW QoS front: 8
- QoS - Strict Priority Queue,
- QoS classification – ACL, DSCP, CoS based,
- QoS marking - DSCP, CoS,
- QoS Policing,
- QoS-Per Flow policing,
- QoS-Hierarchical QoS. min. 2 úrovně,
- Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní),
- First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP),
- IPv6 services (Telnet, SSH, Syslog, DHCP),
- IPv6 QoS,
- IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard),
- Port ACL, VLAN ACL,
- Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny.
- Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce Secure Boot, která ověřuje autentičnost a integritu jak Bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. Trusted modulů,
- HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů,
- Podpora SUDI (IEEE 802.1AR) autentizace,
- IPv6 Port ACL, VLAN ACL,
- IEEE 802.1AE na všech portech,
- IEEE 802.1ae (AES-GCM-256) na všech portech,
- Source-Group Tag Exchange Protocol nebo ekvivalentní,
- IGMPv2/v3 snooping,
- MLD snooping,
- Multicast DNS (mDNS) gateway,
- Application Visibility - pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur),
- Application Visibility - monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní,
- Application Visibility - možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type,
- Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX,
- Podpora Full Flexible Netflow,
- SSHv2 a CLI rozhraní,
- Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG,
- Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení v prostředí Python scripting, Linux shell,
- Application hosting,
- Aplikace softwarových záplat, nikoli povyšování celého Firmware,

- Streaming telemetrie prostřednictvím NETCONF/XML,
- SNMPv2/v3,
- Inventarizovatelnost komponent integrovanou RFID identifikací,
- TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting),
- Vzdálený port mirroring (ERSPAN),
- NTPv3 server,
- 40x SFP BiDi modul, TX:1550, RX:1310, 1Gbps, 20km,
- 8x SFP RJ45 modul, 1Gbps,
- 4x redukční modul z QSFP na SFP+,
- Záruka a podpora výrobce na HW/SW po dobu 5 let (režim minimálně 8x5xNBD).

1x L2 přepínače pro rozšíření LAN

L2 přepínač rozšiřuje stávající přístupovou vrstvu uživatelů o dalších 48 portů s podporou POE.

- Formát zařízení: 1U,
- Typ přepínače: L2/L3 přepínač,
- Formát přepínače: stohovatelný,
- Počet dedikovaných stohovacích portů spolu s propojovacím modulem: 2,
- Minimální kapacita sběrnice stohu: 80Gb/s,
- Minimální kapacita přepínání: 176Gb/s,
- Minimální paketová kapacita: 130Mp/s,
- Stateful Switch Over v rámci stohu,
- Min. velikost sdíleného systémového bufferu: 6MB,
- Redundatní větráky,
- Možnost instalovat interní redundantní napájecí zdroj,
- Minimální počet zařízení ve stohu: 8,
- Počet dedikovaných stohovacích portů: 2,
- Možnost stohování přes dedikované porty, bez snížení počtu použitelných ethernetových portů,
- Stohovací datový kabel: vyžadován 0.5m,
- Počet portů 10/100/1000 Base-TX s PoE+ napájením: 48,
- Minimální PoE budget: 740W,
- IEEE 802.3af,
- IEEE 802.3at,
- Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače,
- Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení,
- Uplinkové porty s volitelným rozhraním SFP+: 4x 1/10Gbps,
- Velikost MAC address tabulky: 16000,
- Min. počet IPv4 routes: 3000,
- Min. počet IPv6 routes: 1500,
- Min. počet konfigurovatelných security ACL: 1500,
- IEEE 802.3ad (Link Aggregation),
- IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis,
- Minimálně 8 linek jako součást Link Aggregation Group trunku,

- Minimální počet konfigurovatelných Link Aggregation Group trunků: 48,
- IEEE 802.1Q,
- Minimální počet aktivních VLAN: 512,
- IEEE 802.1x,
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací),
- Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication),
- Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů,
- RADIUS CoA,
- Podpora instance spanning-tree protokolu per VLAN,
- IEEE 802.1w - Rapid Spanning Tree Protocol,
- Protokol MVRP nebo VTP pro definici a správu VLAN sítí,
- Podpora jumbo rámců (min. 9198 bytes),
- Detekce protilehlého zařízení (např. CDP nebo LLDP),
- Směrování protokolů IPv4 a IPv6 v hardware,
- RIP, EIGRP Stub, OSPFv2; OSPFv3 - minimálně 1000 routes,
- OSPFv2; OSPFv3 - povýšením Firmware
- EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868) - povýšením Firmware
- ISIS - povýšením Firmware,
- IP Multicast (PIM SSM, PIM SM) - povýšením Firmware,
- Virtualizace směrovacích tabulek - např. Virtual Routing and For Warding (VRF) - povýšením Firmware,
- HSRP, VRRP,
- Reverse path check (uRPF) pro IPv4 i IPv6,
- IGMPv2, IGMPv3,
- IGMP snooping,
- MLD snooping,
- Minimální počet HW QoS front: 8,
- QoS classification – ACL, DSCP, CoS based,
- QoS marking - DSCP, CoS,
- Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní),
- QoS Policing,
- QoS-Hierarchical QoS., min. 2 úrovně,
- IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard),
- Možnost definovat povolené MAC adresy na portu,
- PACL, VACL,
- Paketové filtry (ACL) jsou stále aplikovány a filtrují v případě, že jsou na nich prováděny změny,
- IEEE 802.1ae na uplink portech,
- Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy,
- Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru,
- Bezpečnostní funkce umožňující inspekci provozu protokolu ARP,
- Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce Secure Boot, která ověřuje autentičnost a integritu jak Bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. Trusted modulů.
- HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů,

- IEEE 802.3az,
- Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu,
- Application Visibility - pokročilá detekce a klasifikace jednotlivých přenášených aplikaci (DPI na7.vrstvě OSI modelu dle aplikačních signatur) - povýšením Firmware,
- Application Visibility - monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní,
- Application Visibility - možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type,
- Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX,
- Podpora Full Flexible Netflow,
- SSHv2 a CLI rozhraní,
- Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG,
- Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení,
- Aplikace softwarových záplat, nikoli povyšování celého Firmware,
- Streaming telemetrie prostřednictvím NETCONF/XML,
- SNMPv2/v3,
- Podpora network boot (iPXE),
- Inventarizovatelnost komponent integrovanou RFID identifikací,
- TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting),
- AVC (NBAR2) - povýšením Firmware,
- NTPv3 server,
- Záruka a podpora výrobce na HW/SW po dobu 5 let (režim minimálně 8x5xNBD).

100lic. Ověřování 802.1X – NAC server

V síti zákazníka je již nasazeno NAC řešení od společnosti MACMON, kdy je již využíváno 400ks licencí**.** Tento počet licencí již není dostačující vzhledem k růstu a přibývání zařízení v LAN síti.

Macmon premium bundle

- 100 ks licence
- perpetuální licence pro koncová zařízení – podpora min. 5 let

1x detekce síťového provozu s aktivním zásahem

- určeno pro software pro detekci síťového provozu,
- TPM 2.0 v3,
- výsuvné ližiny a rameno pro vyvázání kabelů pro montáž do 19" racku,
- redundantní napájecí zdroje,
- procesor o výkonu alespoň 22 000 bodů v testu passmark, max. 12 jader z licenčních důvodů, frekvence alespoň 2.0Ghz, cache alespoň 30MB,
- rychlost paměti alespoň 5600MT/s,
- RAM modul o kapacitě alespoň 32GB,
- celkem osazeno 64GB RAM,
- interní řadič pro NVME disky s podporou RAID 0, 1, 5, 6, 10, 50, 60,
- 2x 3.84TB SSD NVME Read Intensive,

- min. 4x 1/10Gbps Base-T porty pro SPAN,
- min. 2x 1Gbps RJ-45 porty pro LAN,
- čelní kryt serveru včetně LCD displeje.
- Modul pro vzdálený management, přístup přes web. prohlížeč s podporou SSL, Telnet / SSH a IPMI nástroje; podpora virtuálních médií, plná podpora pro integraci do prostředí VMware vSphere a vCenter. 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.
- Hardware plně kompatibilní se software monitoring síťového provozu s aktivním zásahem.
- Technická podpora a servis minimálně na 5 let (24x7x365), oprava do 24 hodin od identifikace problému v pracovní dny a jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW v místě instalace HW. Zdarma možnost on-line 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.

Software pro detekci a monitoring síťového provozu

Veškeré instalační práce na zařízení a souvisejících technologiích musí provádět výrobcem certifikovaný a školený odborník, který disponuje platným certifikátem pro danou technologii. Dodavatel je povinen doložit odpovídající certifikace před podpisem smlouvy.

Systém pro analýzu síťového provozu složený z hardwarového zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. Systém je plně napojitelný na centrální LDAP zdroj identit.

Systém zajišťuje detailní viditelnost do síťové komunikace s drill down prokliky na veškerá uložená data. Všechny komponenty systému musí být instalované v interním prostředí zadavatele (On Premise) a použití externích komponent nebo cloudových služeb se nepřipouští.

Analýza plného síťového provozu

Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. Systém musí být schopen získávat data zrcadlené komunikace ze SPAN portů a síťových TAPů. Systém je zcela pasivní vzhledem k monitorovanému provozu, monitorovaný provoz přes něj neprochází.

Analýza protokolů typu NetFlow

Dodaný systém musí analyzovat síť na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.

Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.

Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, SSL/TLS zapouzdření.

Je požadováno vysokorychlostní úložiště pro uchování datových toků na dobu minimálně 12 měsíců. Dále je požadováno, aby uživatel mohl v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků, dat a agregovaných síťových statistik na základě minimálně těchto parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (klient nebo server), číslo portu, VLAN, země, ASN.

Je požadována automatická detekce přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod.

Systém musí být schopen upozornit na vznik nových služeb v interní síti a sledovat jejich změny, a to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Direktory služby, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, CIFS, POP3S, IMAPS, MSSQL, TELNET, FTP, TFTP, a to i v případě, že nebudou využívat standardních „well known" portů.

Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:

- změna IP/MAC adresy hosta,
- duplicitní IP/MAC adresa,
- změna VLAN,
- vytvoření nové podsítě,
- připojení nového zařízení,
- použití nové služby,
- nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení,
- přístup nového zařízení ke službě či zařízení.

Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.

Systém musí být schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu.

Samostatné učení behaviorálních aktivit a detekce anomálií
Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.

Detekce na základě databáze známých hrozeb (signaturní detekce)
Systém musí být schopen identifikovat a reportovat události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a Best Practices a dalších rizik. Tato databáze musí být aktualizovaná minimálně na hodinové bázi. Nesmí se jednat

o volně dostupnou/open-source databázi, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.

Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).

Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu.

Systém musí být schopen v monitorovaném provozu porovnávat hash zachycených souborů s databázemi známých hashů škodlivých souborů.

Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.

Kontrola platnosti certifikátů
Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.

Asistované učení (eliminace falešně pozitivních detekcí v rámci síťového provozu s možností manuálního zásahu a opravy). Falešně pozitivní detekci musí být možno uživatelsky eliminovat na základě minimálně všech následujících parametrů: IP adresa, MAC adresa, hostname, segment sítě / podsíť, lokalita – ASN, země apod., směr komunikace – určení klienta, nebo serveru, detekovaná událost – kategorie, název apod., použité službě, protokolu, portu a libovolné kombinaci výše popsaných.

Systém musí být schopen hodnotit reputaci níže uvedených parametrů na základě pravidelně se aktualizující databáze. Jedná se o ověření: reputace TLS certifikátů, reputace DNS/Hostname záznamů, reputace URL adres, reputace HASH přenášených souborů.
Systém musí být schopen okamžitého vyhledávání a vizualizace pro forenzní analýzu a podporu Threat Hunting bez zvláštního dotazovacího jazyka a bez hlubokých znalostí konkrétních komunikačních protokolů.

Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech zpracovávaných dat, tj. bezpečnostních událostí a zaznamenaných síťových toků, a to minimálně podle parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.

Systém musí pro vyhledávání poskytovat již před počítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.

Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.

Systém musí být schopen pro každé zařízení získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace:

- jméno uživatele a další jeho parametry z doménového řadiče (Active Directory), včetně její historie,
- hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu,
- IP geolokace,
- IP reputace, včetně údaje, jestli je IP adresa na blacklistu nebo podezřelá,
- historie použitých MAC adresa a výrobce zařízení,
- operační systém a jeho historie na zařízení,
- uživatelem zadané poznámky a informace k zařízení.

Požadované funkcionality, SW záruka a podpora výrobce po dobu 5 let (režim minimálně 8x5xNBD) s aktivním centrem pro hlášení problémů telefonní nebo emailovou cestou.

2.4.2 Monitoring provozu

Využívá se současný systém pro monitoring provozu systém NetXMS. Dodaná zařízení budou konfigurována pro využití protokolu SNMP v3 a SNMP v2 pro připojení na stávající monitorovací systém.

3 Druhá fáze projektu – implementace

Tato fáze spadá pod NDA (Non-Disclosure Agreement) – popis implementačních prací zahrnuje dokument - Příloha č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.

4 Třetí fáze projektu – optimalizace a dokumentace

Dokumentace bude vytvořena ve formátu PDF pro snadnou distribuci a ve formát DOCX pro snadnou editaci. Dokumentace bude tvořena strukturovaně dle jednotlivých technologických celků uvedených výše s popisem architektury systému, bezpečnostních nastavení. Schéma či topologie zapojení budou ve formátu Visio.

Dokumentace bude dále obsahovat kontakty na zpracovatele dokumentace.

4.1 Implementační dokumentace

4.1.1 Popis fyzické infrastruktury

Detailní specifikace fyzických komponent, včetně serverů, diskových polí, síťových aktivních prvků, záložních napájecích systémů (UPS), zálohovací infrastruktury a dalších aplikovaných technologií.

Rozmístění fyzických zařízení v datacentru (např. racková schémata, propojení kabeláže a napájení).

Požadavky na prostor, chlazení a energetickou náročnost jednotlivých komponent.

4.1.2 Instalace serverů, virtuálního prostředí, systémů a aplikací

Postup instalace operačních systémů a virtualizační platformy, včetně nastavení clusterů, storage a síťových propojení.

Dokumentace systémů pro řízení přístupu do sítě (např. 802.1x) a jejich integrace s dalšími bezpečnostními nástroji.

Konfigurace systémů pro detekci anomálií v síťovém provozu, včetně podrobného popisu používaných pravidel, filtrů a analytických nástrojů.

Implementace a konfigurace systému pro centrální sběr a analýzu logů ze všech relevantních zařízení.

4.1.3 Monitorování a dohled

Popis implementace nástrojů pro sledování síťového provozu (Flow Monitoring) a identifikaci potenciálních problémů nebo hrozeb.

Návrh monitorovacích procesů pro fyzické prvky (např. teplotní čidla, stav napájení) a aplikace nebo služby.

Definice metrik a reportů, které budou z monitorovacích systémů generovány, včetně jejich frekvence a způsobu distribuce.

4.1.4 Zapracování konkrétních vstupů od Zadavatele

Přehled potřebných údajů z prostředí zadavatele, jako jsou IP adresní plány, názvoslovné konvence (Naming Conventions), pravidla pro správu VLAN nebo další specifické požadavky. Týká se to i dokumentace systémů třetích stran, které jsou zainteresované do této zakázky.

Vzory pro integraci s existujícími systémy zadavatele.

4.1.5 Časový harmonogram projektu

Rozpracovaný časový plán přípravných prací, instalačních kroků, testování a školení.

Rozdělení časových bloků podle očekávané náročnosti (0,5–5 MD).

Specifikace kritických milníků, na které budou navázány kontrolní body a případná schvalování.

4.1.6 Zálohovací strategie

Dokumentace zálohování musí být komplexní, přehledná a snadno použitelná při obnově dat. Dokumentace bude obsahovat popis zálohované infrastruktury, strategii zálohování (frekvence, typy záloh), umístění záloh, bezpečnostní opatření a postup pro obnovu dat.

Struktura dokumentace zálohování

- Přehled zálohovaných systémů – Servery, databáze, aplikace, síťové prvky.
- Strategie zálohování
  - Frekvence záloh (denní, týdenní, měsíční).
  - Typy záloh (plná, přírůstková, rozdílová, Snapshoty).
  - Retention Policy (jak dlouho jsou zálohy uchovávány).
- Technologie a nástroje– popis použitých řešení, jak aplikací, tak technologií.
- Umístění záloh – primární úložiště, Offsite/Cloudové lokace, Air-Gapped zálohy.
- Šifrování a ochrana dat – přístupová práva, šifrování dat při přenosu a uložení dat.
- Obnova dat (Disaster Recovery Plan)
  - Postup obnovy jednotlivých systémů.
  - Testovací scénáře pro ověření obnovitelnosti.
  - Definování Recovery Time Objective (RTO) a Recovery Point Objective (RPO).
- Monitorování a notifikace – jak se kontroluje úspěšnost záloh, kdo dostává upozornění, co se děje v případě neúspěšné zálohy.
- Historie a audit – Evidence testů obnovy a změn v zálohovací strategii.

4.1.7 Zapracovaní legislativních požadavků a doporučení z GAP analýzy

V rámci GAP analýzy byla sepsána legislativní doporučení a požadavky na fungování jednotlivých technologií. Tyto požadavky byly zapracovány do popisu implementačních prací u jednotlivých technologií. V dokumentaci bude uvedeno, jak byla doporučení zapracována. V opačném případě budou uvedeny důvody, proč nedošlo k zapracování doporučení.

4.1.8 Ošetření nálezů z penetračních testů

V rámci penetračního testování, které bylo předmětem GAP analýzy byly zjištěny nálezy. Tyto nálezy byly specifikovány v implementační dokumentaci a zároveň popsány oblasti, kterých se nálezy týkají. Součástí této kapitoly dokumentace bude seznam ošetřených nálezů, které vycházejí z penetračních testů. Neošetřené nálezy budou zdůvodněny.

4.2 Dokumentace skutečného provedení

Vychází z implementační dokumentace.

1. **Úvodní shrnutí**
   - Krátký popis projektu, jeho cílů a výsledků.
   - Přehled použitých technologií, zařízení a řešení.
   - Stručné srovnání plánovaného a skutečného průběhu projektu (např. změny oproti původnímu plánu).
2. **Technická dokumentace fyzické infrastruktury**
   - Aktualizované schéma rozmístění fyzických zařízení (servery, disková pole, síťové prvky, UPS, kabeláž).
   - Přehled sériových čísel, modelů a verzí Firmware nainstalovaných zařízení.
   - Fotodokumentace instalace (např. racky, kabeláž, napájení).
3. **Síťová a systémová konfigurace**
   - Detaily aktuální konfigurace všech síťových zařízení (např. switche, routery, firewally).
   - Finální IP adresní plán, VLAN struktura a pravidla pro řízení přístupu.
   - Konfigurace serverů a virtualizačních prostředí, včetně přidělených prostředků (CPU, RAM, storage).
   - Logická topologie sítě, včetně spojení mezi jednotlivými prvky a jejich rolí.
4. **Bezpečnostní a monitorovací systémy**
   - Dokumentace nasazených bezpečnostních systémů (např. Firewall pravidla, 802.1x konfigurace, detekce anomálií).
   - Popis implementace monitorovacích nástrojů a metrik, včetně ukázek reportů.
5. **Zálohování a kontinuita**
   - Konfigurace zálohovacích systémů a nastavení frekvence záloh.
   - Plány obnovy.
6. **Provozní dokumentace**
   - Návody k obsluze a údržbě nasazených zařízení a systémů.
   - Postupy pro běžnou údržbu, aktualizace a řešení potenciálních problémů.
   - Plán údržby pro nasazované technologie – příklad tabulky:

Technologie	Popis zařízení / systému	Poslední aktualizace	Plánovaná aktualizace	Četnost	Popis aktualizace
Firewall	Centrální perimetr	10.4.2025		Čtvrtletně	Aktualizace OS a Firmware
Aktivní prvky	Přístupové switche	10.4.2025		Čtvrtletně	Aktualizace OS a Firmware
Hypervisor	Virtualizační platforma	10.4.2025		Čtvrtletně	Aktualizace OS a Firmware
Diskové pole	Centrální úložiště dat	10.4.2025		Čtvrtletně	Aktualizace OS a Firmware
Log management	Systém pro centrální ukládání logů	10.4.2025		Čtvrtletně	Aktualizace OS a Firmware

    - Kontaktní informace pro technickou podporu dodavatelů jednotlivých zařízení a technologií.
7. **Akceptační testy**
    - Záznam výsledků všech akceptačních testů, včetně případných odchylek a jejich řešení.
    - Potvrzení splnění všech akceptačních kritérií a schválení zadavatelem.
8. **Výstupy z projektu**
    - Seznam všech vytvořených dokumentů, reportů, přístupových údajů a licencí.
    - Přehled přístupových údajů (např. hesla, certifikáty, klíče), které byly předány zadavateli.
    - Stav všech zařízení a systémů k datu předání.
9. **Změnové řízení**
    - Přehled všech změn oproti původnímu plánu a jejich důvody.
    - Záznam schválení změn zadavatelem.
10. **Závěrečné shrnutí a doporučení**
    - Návrhy na budoucí zlepšení a doporučení pro další rozvoj.
    - Přehled potenciálních rizik nebo problémů, které mohou nastat v budoucnu.

5 Obecné podmínky

Zaškolení administrátorů

Nabídková cena obsahuje náklady na školení administrátorů/správců v nezbytně nutném rozsahu. Školení proběhne v prostorách Zadavatele v rozsahu 4 MD pro každou oblast:

- Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení.
- Testování zranitelnosti prvků infrastruktury.

- Řešení centrálního ukládání a analýzy logů a reportů.
- Aktivní přístupové prvky, řízení přístupu do vnitřní sítě, 802.1X, detekce síťového provozu, monitoring provozu.

Stručné shrnutí požadovaných parametrů dodávky

- Dodávka poptávaných komponent včetně odpovídajícího počtu licencí.
- Součástí dodávky bude potřebný instalační a propojovací materiálu (propojovací kabely datové i napájecí, potřebné moduly do switchů, police apod.).
- Instalace/konfigurace/implementace/migrace.
- Zapojení, upgrade a migrace fyzických serverů/storage.
- Zapojení a konfigurace UPS.
- Zapojení a konfigurace NAS.
- Upgrade a migrace VM virtuálních serverů.
- Migrace aplikaci třetích stran na nové VM.
- Instalace a zprovoznění systémů pro monitoring datového provozu a detekci anomálii (ADS).
- Zvýšení dostupnosti síťových služeb.
    - Testy zranitelností v průběhu implementace pro zajištění vysoké míry zabezpečení:
        - zabezpečení ethernetové sítě,
        - topologie sítě,
        - uživatelské stanice,
        - Microsoft Active Directory,
        - ostatní.
    - Práce spojené s mitigací nálezů z testů zranitelnosti během implementace.
    - Konfigurace Firewallu v DC pro nové technologie.
    - Instalace a zprovoznění analytického nástroje k Firewallu.
    - Doplnění licencí 802.1x s NAC server a konfigurace na nových přepínačích.
- Zapojení, instalace, konfigurace switchů.
- Integrace systémů NAC, ADS.
- Instalace a konfigurace dohledového systému, konfigurace politik pro automatické řízení bezpečnosti při zjištěných incidentech, průběžná konfigurace nastavení filtrů a alertování, vytváření vlastních pravidel pro automatizaci.
- Instalace, zprovoznění, otestovaní a vyhodnocení systému na testování zranitelností.
- Zapojení, instalace, zprovoznění a vyladění centrálního úložiště logů a nastavení a otestování archivace logů, průběžná změna konfigurace, nastavení alertování, nastavení tresholdů, konfigurace politik a automatického vyhodnocování potencionálních incidentů.
- Zajištění koordinace všech zúčastněných stran a dodavatelů technologií.
- Školení administrátorů.
- Implementační dokumentace.
- Dokumentace skutečného provedení.

6 Harmonogram projektu

6.1 Časový přehled plnění projektu

Dnem začátku plnění je den podpisu smlouvy, čas T0.

Fáze	Činnosti	Termín
Dodávka HW a SW pro datové centrum a virtualizaci	Kompletace a dodávka HW zadavateli, test hardware, zahoření, základní konfigurace, licence na software pro HW zařízení.	T0 + 45 dní
Dodávka HW a SW pro aktivní prvky, řízení přístupu do sítě, detekce síťového provozu	Kompletace a dodávka HW zadavateli, test hardware, zahoření, základní konfigurace, licence na software pro HW zařízení.	T0 + 45 dní
Předání HW a SW	Předání dodaného HW a SW a Implementační dokumentace.	T0+45 dní
Fakturace (1. část)		
Implementace aktivních prvků, nástroje pro monitoring síťového provozu, provozní monitoring, řízení přístupu do sítě	Konfigurace aktivních prvků a implementace nástroje na sledování síťového provozu. Konfigurace provozního monitoringu. Aplikace licencí do nástroje pro řízení přístupu do sítě.	T0 + 90 dní
Implementace serverů do datového centra	Konfigurace serverů vytvoření cluster řešení, konfigurace diskových polí, instalace hypervisorů, konfigurace operačních systémů.	T0 + 100 dní
Migrace Active directory	Migrace služeb Active Directory, DNS a DHCP služeb na nové servery, revize a zabezpečení domény.	T0 + 110 dní
Implementace centrálního systému logování	Implementace serveru a systému pro centrální log management, konfigurace pravidel, napojení na systémy.	T0 + 110 dní
Migrace aplikačních serverů	Migrace všech aplikačních, databázových a provozních serverů.	T0 + 160 dní
Předání konfiguračních a implementačních prací realizovaných v rámci projektu	Odstranění nedostatků z penetračních testů, akceptace jednotlivých částí projektu.	T0 + 190 dní
Fakturace (2. část)		
Dokumentace a školení	Příprava dokumentace, školení správců.	T0 + 220 dní
Optimalizace infrastruktury	Ladění infrastruktury dle provozních zjištění, optimalizace Workflow, řešení vzniklých problémů.	T0 + 220 dní
Finální akceptace projektu	Akceptace projektu jako celku, dodaných technologií včetně zaškolení administrátorů.	T0+220 dní
Fakturace (3. část)		

Ostrý provoz a ukončení projektu	Spuštění ostrého provozu infrastruktury po akceptaci dílčích částí.	T0+221 dní
Udržitelnost projektu	Udržitelnost projektu 5 let po ukončení realizace.	

7 Akceptační testy

Tato kapitola slouží jako podklad pro akceptační testy pro jednotlivé technologické celky projektu a je podkladem pro finální předání celého projektu.

7.1 Akceptační protokol aktivních prvků

Název testu	Postup ověření	Výsledek	Výhrady
Kontrola fyzického umístění	Vizuální kontrola. Umístění zařízení do rozvaděčů. Je provedeno řádné fyzické označení všech zařízení dle jmenné konvence.	ANO / NE	
Kontrola infrastrukturního propojení (uplinky)	Vizuální kontrola. Propojení (uplinky) jednotlivých zařízení je provedeno dle ZD. Je provedeno řádné fyzické označení všech propojů (uplinků).	ANO / NE	
Napájení	Zdroje serveru jsou připojené redundantně, každý na jinou napájecí větev a jsou řádně označeny.	ANO / NE	
Kontrola aktuálnosti Firmware/OS	Firmware v rámci jednotlivých zařízení je sjednocený na poslední STABLE/doporučovanou verzi.	ANO / NE	
Kontrola IP adresace	Adresace jednotlivých VLAN sítí a terminace jejich SVI rozhraní je provedena dle ZD. Kontrola specifických VLAN – L2 transportní VLAN, VLAN terminované na Firewallu dle ZD.	ANO / NE	
Kontrola přístupových pravidel VLAN	Je provedena kontrola přístupových pravidel pro jednotlivé VLAN sítě.	ANO / NE	
Síťová konektivita	Servery jsou redundantně připojené do aktivních prvků dle dokumentace. Po odpojení jedné větve nedochází ke ztrátě komunikace?	ANO / NE	
Přístupy	Pro přístup se používají hesla dle dokumentace, přístup je pouze skrze šifrované připojení z administračních VLAN.	ANO / NE	
Synchronizace času	Kontrola konfigurace NTP a test synchronizace data a času na všech aktivních prvcích.	ANO / NE	
Funkčnost err-disable	Při vyvolání poruchového stavu (záměrnou chybnou konfigurací) dojde k deaktivaci libovolného portu do err-disable stavu. Po xx minutách dojde k automatické aktivaci portu.	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	
HW konfigurace	Odpovídá HW konfigurace zadávací dokumentaci.	ANO / NE	

7.2 Akceptační protokol implementace ověřování 802.1X

Název testu	Postup ověření	Výsledek	Výhrady
Doplnění licencí	Licence byly navýšeny o 100 jednotek.	ANO / NE	

7.3 Akceptační protokol virtualizace datového centra

Název testu	Postup ověření	Výsledek	Výhrady
Kontrola fyzického umístění	Vizuální kontrola. Umístění zařízení do rozvaděčů. Je provedeno fyzické označení všech zařízení dle jmenné konvence.	ANO / NE	
Kontrola infrastrukturního propojení (uplinky)	Vizuální kontrola. Propojení (uplinky) jednotlivých zařízení je provedeno dle ZD. Je provedeno řádné fyzické označení všech propojů (uplinků).	ANO / NE	
Napájení	Zdroje serveru jsou připojené redundantně, každý na jinou napájecí větev a jsou řádně označeny.	ANO / NE	
Kontrola aktuálnosti Firmware serverů	Všechny Firmware, BIOS a ovladače jsou na poslední stabilní vydané verzi.	ANO / NE	
Přístupy	Pro přístup se používají hesla dle dokumentace, přístup je pouze skrze šifrované připojení z administračních VLAN.	ANO / NE	
Notifikace	Nastavení notifikací v případě problému serveru, test emailové notifikace.	ANO / NE	
Kontrola alertů	Ověření, že server na sobě nemá žádné aktivní alerty	ANO / NE	
Síťová konektivita	Servery jsou redundantně připojené do aktivních prvků dle dokumentace. Po odpojení jedné větve nedochází ke ztrátě komunikace.	ANO / NE	
Synchronizace času	Kontrola konfigurace NTP a test synchronizace data a času na všech prvcích (pole, SAN infrastruktura).	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	
HW konfigurace	Odpovídá HW konfigurace zadávací dokumentaci.	ANO / NE	

7.4 Akceptační protokol diskových polí a SAN infrastruktury

Název testu	Postup ověření	Výsledek	Výhrady
Kontrola fyzického umístění	Vizuální kontrola. Umístění zařízení do rozvaděčů. Je provedeno fyzické označení všech zařízení dle jmenné konvence.	ANO / NE	
Kontrola infrastrukturního propojení (uplinky)	Vizuální kontrola. Propojení (uplinky) jednotlivých zařízení je provedeno dle ZD. Je provedeno řádné fyzické označení všech propojů (uplinků).	ANO / NE	
Napájení	Zdroje pole a SAN prvků jsou připojeny redundantně, každý na jinou napájecí větev a jsou řádně označeny.	ANO / NE	
Kontrola aktuálnosti Firmware/OS	Firmware (disků, controllerů, zdrojů, OS) v rámci jednotlivých zařízení je sjednocený na poslední STABLE/doporučovanou verzi.	ANO / NE	
Konfigurace RAID	Kontrola nastavení RAID svazků dle dokumentace.	ANO / NE	
Přístupy	Pro přístup se používají hesla dle dokumentace, přístup je pouze skrze šifrované připojení z administračních VLAN.	ANO / NE	
Síťová konektivita - pole	Pole je redundantně připojené do aktivních prvků dle dokumentace. Po odpojení jedné větve nedochází ke ztrátě komunikace.	ANO / NE	
Synchronizace času	Kontrola konfigurace NTP a test synchronizace data a času na všech prvcích (pole, SAN infrastruktura).	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	
HW konfigurace	Odpovídá HW konfigurace zadávací dokumentaci.	ANO / NE	

7.5 Akceptační protokol virtualizace produkčního a VDI datového centra

Název testu	Postup ověření	Výsledek	Výhrady
Kontrola nastavení Hypervisor	Instalovaná poslední stabilní verze, nastavení dle Best Practices.	ANO / NE	
Bezpečnostní role	Existence všech bezpečnostních rolí na Hypervisor.	ANO / NE	
Zařazení do uživatelských rolí	Správné zařazení uživatelů do bezpečnostních rolí na Hypervisor, dle dokumentace.	ANO / NE	
Hypervisor zabezpečení	Na Hypervisor se přihlásíme účty se sníženým oprávněním a testujeme, zdali se uživatel nedostane mimo vymezená práva.	ANO / NE	
Kontrola nastavení management virtualizace	Instalovaná poslední stabilní verze, nastavené High Availability, přidání identity source, vytvořené template pro instalaci serverů, nastavení Update Manager na automatické stahování updatů a notifikace.	ANO / NE	
Bezpečnostní role	Existence všech bezpečnostních rolí.	ANO / NE	
Zařazení do uživatelských rolí	Správné zařazení uživatelů do bezpečnostních rolí dle dokumentace.	ANO / NE	
Konfigurace virtuálních switchů	Testovací virtuální stroj postupně připojíme do všech VLAN sítí a otestujeme komunikaci vzhledem ke gateway.	ANO / NE	
Virtuální switche	Fyzické odpojení jednoho LAN kabelu a otestování komunikace pro všechny VLAN.	ANO / NE	
Konfigurace iSCSI svazků	Kontrola nastavení a viditelnost svazků dle dokumentace na diskovém poli.	ANO / NE	
Cluster High Availability	Po odpojení všech LAN kabelů od jednoho hostitele dojde k nastartování VM na zbylých hostitelích.	ANO / NE	
SAN multipath	Fyzické odpojení jednoho SAN twinaxu ze serveru. Nesmí dojít k žádnému výpadku konektivity na pole.	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	

7.6 Akceptační protokol doménových serverů

Název testu	Postup ověření	Výsledek	Výhrady
Výpadek DC	Vypnutím SRV-DC1 nedošlo k problémům s překladem adresy na jméno a jména na adresu.	ANO / NE	
Replikace	Všechny řadiče jsou schopny provádět replikace s ostatními řadiči.	ANO / NE	
Sdílené adresáře SYSVOL	Všechny řadiče mají vytvořen adresář SYSVOL.	ANO / NE	
Funkčnost AD	Všechny výstupy z „dcdiag /test:CheckSecurityError" neobsahují chyby, které zabraňují správnému fungování doménových řadičů a AD.	ANO / NE	
Test DNS	Všechny výstupy z „dcdiag /test:dns" neobsahují chyby, které zabraňují správnému fungování doménových řadičů a AD.	ANO / NE	
Test AD	Všechny výstupy z „dcdiag/v" neobsahují chyby, které zabraňují správnému fungování doménových řadičů a AD.	ANO / NE	
Test AD	Všechny výstupy z „dcdiag/q" neobsahují chyby, které zabraňují správnému fungování doménových řadičů a AD.	ANO / NE	
Test AD	Všechny výstupy z „repadmin /replsum" neobsahují chyby, které zabraňují správnému fungování doménových řadičů a AD.	ANO / NE	
DFS replikace	Event Viewer v sekci DFS Replication neobsahuje závažné chyby zabraňující správnému fungování AD.	ANO / NE	
DHCP Role	Na obou DC je nainstalována role DHCP, oba servery jsou autorizovány, nastaveny serverové OPTIONS.	ANO / NE	
Scope and Options	Pro rozsahy, které mají mít adresy přidělovány dynamicky jsou vytvořeny odpovídající Scopes a ScopeOptions.	ANO / NE	
DHCP Failover	Pro všechny Scopes je nakonfigurována funkcionalita DHCP failover. Vypnutím SRV-DC1 nedošlo k problémům s přidělováním a obnovováním adres koncovým zařízením.	ANO / NE	

Otestování funkcionality DHCP	Adresy všech SCOPES jsou přidělovány, funkcionalita DHCP failover je otestována.	ANO / NE	
Internet DNS	Na obou DNS funguje resolvování internetových doménových jmen.	ANO / NE	
Aging	Funkcionalita Aging je nakonfigurována a funkční.	ANO / NE	
Scavenging	Funkcionalita Scavenging je nakonfigurována a funkční.	ANO / NE	
Autorizovaný přístupu na Internet	Vypnutím SRV-DC1 nedošlo k problémům s výpadkem ověřování uživatelů AD vůči centrálnímu Firewallu - autorizace přístupu na Internet.	ANO / NE	
Členství v doméně	Všechny potřebné servery se nacházejí v doméně zadavatele.	ANO / NE	
Jmenné konvence	Všechny nové servery mají název dle jmenné konvence a IP adresaci dle požadavku Zadavatele.	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	

7.7 Akceptační protokol aplikačních serverů

Název testu	Postup ověření	Výsledek	Výhrady
Kontrola instalace rolí	Kontrola nainstalovaných rolí na daném serveru, zdali odpovídají dokumentaci a GAP analýze Zadavatele.	ANO / NE	
Členství v doméně	Je server členem domény nebo je v DMZ dle dokumentace a GAP analýzy Zadavatele.	ANO / NE	
Kontrola oprávnění	Kontrola konfigurace oprávnění pro správné role uživatelů, služeb a servisních účtů dle dokumentace.	ANO / NE	
Kontrola provozovaných aplikací	Kontrola funkčnosti aplikace na serveru z hlediska dostupnosti všech služeb.	ANO / NE	
Kontrola databázového serveru	Databáze jsou umístěny na dedikovaném a datovém disku a defaultní umístění pro nové DB je nastaveno na tento disk. Jsou nastaveny maintenance tasky pro údržbu databází.	ANO / NE	
Kontrola napojení na monitoring	Je napojen server na monitoring.	ANO / NE	
Kontrola zálohování	Je správně konfigurována úloha pro zálohování.	ANO / NE	
Air-Gap zálohy	Jsou nakonfigurovány Air-Gap zálohy	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	

7.8 Akceptační protokol monitoringu síťového provozu

Název testu	Postup ověření	Výsledek	Výhrady
Instalace a konfigurace	Server je korektně zapojen dle ZD, správně konfigurovány SPAN porty, zrcadlený provoz je směrován do zařízení, porty jsou konfigurovány dle Best Practices výrobce.	ANO / NE	
Integrace s infrastrukturou	Systém je integrován s Active Directory a dalšími prvky infrastruktury.	ANO / NE	
Topologie	Systém zobrazí síťovou topologii včetně všech podsítí.	ANO / NE	
Kontrola detekce	Systém detekuje všechny požadované anomálie a problémy dle mittre attack tabulky a další definované v ZD.	ANO / NE	
Test detekce	Systém detekuje uměle vyvolaný port scan na uživatelské podsíti.	ANO / NE	
Výkonost	Systém zpracovává požadovaný datový tok bez ztráty paketů.	ANO / NE	
Reportování	Systém reportuje a alertuje požadované stavy, reportuje aktuální problémy na email nebo do centrálního systému logování.	ANO / NE	
Auditování	Systém audituje důležité aktivity v systému.	ANO / NE	
Aktualizace	Systém pravidelně aktualizuje databázi zranitelností, signatur a detekcí z on-line zdrojů.	ANO / NE	
Požadavky zahrnuté v příloze č. 2.1	Splněny požadavky zahrnuté v dokumentu popisujícím migraci aplikací a interní konfigurace infrastruktury, dle popisu v příloze č. 2.1 ZD - Technický popis k veřejné zakázce - neveřejná část.	ANO / NE	

7.9 Akceptační protokol testování zranitelností

Název testu	Postup ověření	Výsledek	Výhrady
Nástroj na testování	Implementovaný nástroj na testování zranitelností.	ANO / NE	
Testy	Proběhly všechny fáze implementačního testování dle ZD.	ANO / NE	
Zařízení	Byla otestována veškerá zařízení připojená v síti.	ANO / NE	
Detekce	Byly detekovány druhy OS, typy zařízení a CVE zranitelnosti.	ANO / NE	
Výstupy	Výstupy testu zranitelností byly poskytnuty v souladu se ZD.	ANO / NE	
Řešení	Součástí výstupů jsou i možná řešení daných problémů.	ANO / NE	
Fáze testování	Proběhly všechny testy zranitelností dle fází popsaných v ZD.	ANO / NE	
Funkce nástroje	Funkce odpovídají požadavkům v ZD.	ANO / NE	

7.10 Akceptační protokol centrálního systému logování

Název testu	Postup ověření	Výsledek	Výhrady
Instalace nástroje	Kontrola instalace centrálního nástroje na správu logů dle dokumentace.	ANO / NE	
Konfigurace nástroje	Ověření správné konfigurace nástroje dle požadavků a dokumentace.	ANO / NE	
Kontrola oprávnění	Je korektně nakonfigurováno oprávnění pro správné role uživatelů, služeb a servisních účtů dle dokumentace.	ANO / NE	
Ověření sběru dat	Logovací nástroj správně sbírá logy ze všech relevantních zdrojů.	ANO / NE	
Kontrola čitelnosti logů	Kontrola čitelnosti logů z různých typů zařízení, zdali jsou čitelné a správně parsované: Windows server, aktivní prvek, Firewall, virtualizační cluster, datové úložiště, zálohování…	ANO / NE	
Kontrola archivace	Kontrola nastavení správné archivace dat v pravidelném intervalu dle dokumentace, ověření archivovaných dat.	ANO / NE	
Kontrola dashboardů	Kontrola funkčnosti všech konfigurovaných dashboardů dle zadávací dokumentace, jejich funkčnosti a dat.	ANO / NE	
Funkce nástroje	Funkce odpovídají požadavkům v ZD.	ANO / NE	

7.11 Akceptační protokol provozního monitoringu

Název testu	Postup ověření	Výsledek	Výhrady
Implementace provozního monitoringu	Ověření implementace nástroje pro provozní monitoring.	ANO / NE	
Konfigurace	Ověření konfigurace provozního monitoringu dle dokumentace.	ANO / NE	
Napojení na systémy	Ověření připojení systému aktivních prvků, serverů, virtualizační platformy, napájení.	ANO / NE	
Notifikace	Kontrola konfigurace automatických notifikací, notifikačních pravidel, test emailového upozornění	ANO / NE	
Alerty	Kontrola konfigurace alertování dle zadávací dokumentace	ANO / NE	
Metriky	Kontrola funkčnosti metrik sledovaných parametrů konkrétních zařízení (CPU, využití portů na aktivních prvcích…)	ANO / NE	
Audit log	Kontrola funkčního auditního logu provozního monitoringu	ANO / NE	
Zálohování	Kontrola zálohování konfigurace provozního monitoringu	ANO / NE	

7.12 Akceptační protokol dokumentace

Název testu	Postup ověření	Výsledek	Výhrady
Implementační dokumentace	Kontrola implementační dokumentace dle parametrů v zadávací dokumentaci.	ANO / NE	
Dokumentace skutečného stavu	Kontrola dokumentace skutečného stavu dle parametrů v zadávací dokumentaci.	ANO / NE	
Formát	Kontrola dostupnosti dokumentací ve formátu PDF, DOCX a Visio.	ANO / NE	
Kontrola úplnosti	Kontrola přítomnosti všech systémů, zařízení, technologií a aplikací v dokumentaci	ANO / NE	
Kontrola visuálních diagramů	Kontrola všech schémat zapojení, propojení a dalších grafických prvků v dokumentaci.	ANO / NE	
Kontrola postupů	Kontrola přítomnosti všech postupů pro zajištění kontinuity dle zadávací dokumentace.	ANO / NE	