**Příloha č. 3 Funkční specifikace**

**MULA Funkční specifikace 2025**

Obsah

[1 První fáze projektu – dodávka HW 3](#_Toc200007480)

[1.1 Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení 3](#_Toc200007481)

[1.1.1 Hardware 3](#_Toc200007482)

[1.1.2 Implementační práce 7](#_Toc200007483)

[1.2 Produkt pro pravidelné testování zranitelnosti prvků infrastruktury 8](#_Toc200007484)

[1.3 Řešení centrálního ukládání a analýzy logů a reportů 9](#_Toc200007485)

[1.4 Aktivní přístupové prvky, řízení přístupu do vnitřní sítě, 802.1X, detekce síťového provozu, monitoring provozu 13](#_Toc200007486)

[1.4.1 Hardware, software 13](#_Toc200007487)

[1.5 Zvýšení úrovně bezpečnosti přístupu k informacím 23](#_Toc200007488)

[2 Druhá fáze projektu – implementace 24](#_Toc200007489)

[2.1 Implementační práce zahrnují: 24](#_Toc200007490)

[2.2 Business continuity 25](#_Toc200007491)

[2.2.1 Zapracování nálezů z GAP analýzy 25](#_Toc200007492)

[2.2.2 Pravidla pro tvorbu hesel 25](#_Toc200007493)

[2.3 Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti 26](#_Toc200007494)

[2.3.1 Jmenná konvence serverů 26](#_Toc200007495)

[2.3.2 Implementace do stávajícího datového centra 26](#_Toc200007496)

[2.3.3 Příprava hardware 27](#_Toc200007497)

[2.3.4 Instalace virtuálních serverů 27](#_Toc200007498)

[2.3.5 Migrace serverů 29](#_Toc200007499)

[2.4 Produkt pro testování a vyhodnocování zranitelností prvků infrastruktury 31](#_Toc200007500)

[2.5 Řešení centrálního ukládání a analýzy logů 32](#_Toc200007501)

[2.6 Aktivní přístupové prvky, monitoring síťového provozu, provozní monitoring 33](#_Toc200007502)

[2.6.1 Firewall 33](#_Toc200007503)

[2.6.2 2x Core switch 35](#_Toc200007504)

[2.6.3 Implementace 802.1X – NAC server 36](#_Toc200007505)

[2.6.4 Konfigurace virtuální appliance 36](#_Toc200007506)

[2.6.5 Konfigurace přepínačů 37](#_Toc200007507)

[2.6.6 8x Wifi AP 38](#_Toc200007508)

[2.6.7 Implementace nástroje pro detekci síťového provozu 39](#_Toc200007509)

[2.6.8 Implementace nástroje pro provozní monitoring 39](#_Toc200007510)

[2.7 Zvýšení úrovně bezpečnosti přístupu k informacím 40](#_Toc200007511)

[2.7.1 Migrační práce 41](#_Toc200007512)

[2.7.2 Konfigurace zálohování systému pro spolupráci 42](#_Toc200007513)

[2.8 Implementační bezpečností testy 43](#_Toc200007514)

[2.8.1 Ošetření nálezů z penetračních testů 44](#_Toc200007515)

[2.9 Ošetření nálezů z penetračních testů 44](#_Toc200007516)

[3 Třetí fáze projektu - zkušební provoz 45](#_Toc200007517)

[4 Čtvrtá fáze projektu – ostrý provoz 45](#_Toc200007518)

[5 Dokumentace 45](#_Toc200007519)

[5.1 Implementační dokumentace 45](#_Toc200007520)

[5.1.1 Popis fyzické infrastruktury 45](#_Toc200007521)

[5.1.2 Instalace serverů, virtuálního prostředí, systémů a aplikací 45](#_Toc200007522)

[5.1.3 Monitorování a dohled 45](#_Toc200007523)

[5.1.4 Zapracování konkrétní vstupů od Zadavatele 46](#_Toc200007524)

[5.1.5 Časový harmonogram projektu 46](#_Toc200007525)

[5.1.6 Zálohovací strategie 46](#_Toc200007526)

[5.1.7 Zapracovaní legislativních požadavků a doporučení z GAP analýzy 47](#_Toc200007527)

[5.1.8 Ošetření nálezů z penetračních testů 47](#_Toc200007528)

[5.2 Dokumentace skutečného provedení 47](#_Toc200007529)

[6 Obecné podmínky 49](#_Toc200007530)

[7 Harmonogram projektu 51](#_Toc200007531)

[7.1 Časový přehled plnění projektu 51](#_Toc200007532)

[8 Akceptační testy 52](#_Toc200007533)

[8.1 Akceptační protokol aktivních prvků 52](#_Toc200007534)

[8.2 Akceptační protokol firewall 53](#_Toc200007535)

[8.3 Akceptační protokol implementace ověřování 802.1X 56](#_Toc200007536)

[8.4 Akceptační protokol virtualizace datového centra 57](#_Toc200007537)

[8.5 Akceptační protokol diskových polí a SAN infrastruktury 58](#_Toc200007538)

[8.6 Akceptační protokol virtualizace produkčního a VDI datového centra 59](#_Toc200007539)

[8.7 Akceptační test zálohování 60](#_Toc200007540)

[8.8 Akceptační testy doménových serverů 61](#_Toc200007541)

[8.9 Akceptační testy aplikačních serverů 63](#_Toc200007542)

[8.10 Akceptační testy monitoringu síťového provozu 64](#_Toc200007543)

[8.11 Akceptační protokol systému pro spolupráci 65](#_Toc200007544)

[8.12 Akceptační protokol testování zranitelností 65](#_Toc200007545)

[8.13 Akceptační test centrálního systému logování 67](#_Toc200007546)

[8.14 Akceptační test provozního monitoringu 68](#_Toc200007547)

[8.15 Akceptační test dokumentace 69](#_Toc200007548)

**Účel dokumentu**

Účelem tohoto dokumentu je poskytnout detailní přehled o všech hardwarových a softwarových technologiích, které jsou součástí projektu s názvem "Kybernetická bezpečnost –Městského úřadu Lanškroun“. 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 dvou 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.

První fáze projektu – dodávka HW

První fáze projektu počítá s implementací následujících opatření:

* Implementační dokumentace
* Hardware pro datacentrum a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení
* Pravidelné testování zranitelností prvků infrastruktury
* Hardware pro řešení centrálního ukládání a analýzy logů
* Hardware pro aktivní přístupové prvky, řízení přístupu do vnitřní sítě, detekce síťového provozu, monitoring provozu
* Zvýšení úrovně bezpečnosti přístupu k informacím

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

Dodávka počítá s testováním hardware, zahoření a základní konfigurací nových serverů, diskových polí, zálohovací sever, zálohovací úložiště a systém 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.**

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 2.9 Ghz, cache alespoň 22 MB
* rychlost paměti alespoň 5600 MT/s
* RAM modul o kapacitě alespoň 32 GB
* celkem osazeno 384 GB RAM
* interní řadič pro 2x M.2 SSD karty sloužící pro instalaci hypervisoru o kapacitě 480 GB v RAID1
* min. 2x 10/25 Gbps SFP28+ porty pro LAN
* min. 4x 10/25 Gbps SFP28+ porty pro iSCSI
* min. 2x 1 Gbps RJ-45 porty pro LAN
* čelní kryt serveru včetně LCD displeje
* redundantní napájecí zdroje o výkonu alespoň 1100 W
* 4x Twinax kabely SFP28 to SFP28, 25 Gbps, alespoň 3 metry dlouhé
* Licence:
  + - 1x Windows Server 2025 Datacenter odpovídající požadovanému procesoru
    - 55x Windows User CAL licence
    - 1x Microsoft SQL Server 2022 core – 2 Core License Pack + software assurance 3roky
* 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 56 000 bodů v testu passmark, alespoň 28 jader, frekvence alespoň 2.0 Ghz, L3 cache alespoň 52 MB
* rychlost paměti alespoň 5600 MT/s
* RAM modul o kapacitě alespoň 64 GB
* celkem osazeno 512 GB RAM
* interní řadič pro 2x M.2 SSD karty sloužící pro instalaci hypervisoru o kapacitě 480 GB v RAID1
* min. 2x 10/25 Gbps SFP28+ porty pro LAN
* min. 4x 10/25 Gbps SFP28+ porty pro iSCSI
* min. 2x 1 Gbps RJ-45 porty pro LAN
* čelní kryt serveru včetně LCD displeje
* redundantní napájecí zdroje o výkonu alespoň 1100 W
* 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

**1x Server pro doménový řadič**

* 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, 12 výpočetních jader z licenčních důvodů, frekvence alespoň 2.0 Ghz, L3 cache alespoň 30 MB
* rychlost paměti alespoň 5600 MT/s
* RAM modul o kapacitě alespoň 16 GB
* celkem osazeno 32 GB RAM
* hardwarový diskový řadič s podporou RAID 0, 1, 10
* alespoň 2x 480 GB SSD Read Intensive
* min. 2x 1 Gbps RJ-45 porty pro LAN
* čelní kryt serveru včetně LCD displeje
* redundantní napájecí zdroje o výkonu alespoň 700 W
* 4x Twinax kabely SFP28 to SFP28, 25 Gbps, alespoň 3 metry dlouhé
* Licence:
  + - 1x Windows Server 2025 Standard odpovídající požadovanému procesoru
* 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. 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 16 GB cache
* podpora RAID 1,5,6,10 a distribuovaný erasure coding odpovídající RAID6.
* back-end SAS 3.0 12 Gb/s, vyžadovány jsou minimálně dva SAS 3.0f, 12 Gb/s porty na každý řadič
* konektivita řadiče alespoň 4x 25 Gbps SFP28
* interní backplane pro 24x 2,5“ disky s rozhraním 12 Gb SAS
* diskové pole osazeno alespoň 14x 3,84 TB SSD disky typu SAS, read intensive
* možnost připojení rozšiřovací jednotky o dalších 48 disků
* podpora minimálně 1024 snapshotů na diskovém poli
* 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
* 8x Twinax kabely SFP28 to SFP28, 25 Gbps, alespoň 3 metry dlouhé
* podpora technologií VMware vSphere 8, Windows Server 2022, 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
* kabeláž a příslušenství nutné k propojení se servery uvedenými výše
* 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
* 4x min. 12 TB HDD kompatibilních s NAS s možností vyčítání SMART
* Záruka min. 5 let na NAS i HDD

**1x Zaškolení administrátorů**

Školení zaměřené na serverové technologie zařízení v kapitole 1.1.1 poskytuje komplexní přehled o x správě, konfiguraci a optimalizaci těchto technologií. Školení seznámí administrátory s klíčovými vlastnostmi serverů včetně jejich architektury, podpory virtualizace, údržby a řešení případných problémů. Školení se bude zabývat i konfigurací a základní obsluhou diskového, konfigurace SAN a iSCSI prostředí a pokročilé funkce, jako jsou snapshoty. Školení je ve formě praktického workshopu s dodanou technologií přímo v místě zadavatele v rozsahu 2 MD.

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.

Servery produkční a pro virtuální desktopy (VDI servery) a doménový řadič

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 Practise výrobce serveru pro danou technologii připojení.

Diskové pole pro virtualizační infrastrukturu

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 40-40-20 % kapacity SSD 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.

Produkt pro 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.

**2x Zaškolení administrátorů**

Školení pro administrátory zaměřené na hardwarový produkt pro testování zranitelností, na konfiguraci hardware a jeho připojení do sítě spolu s konfigurací síťových protokolů pro zprovoznění tohoto produktu rozsahu 1 MD. Školení pro administrátory zaměřené software pro testování zranitelností a pro detekci bezpečnostních událostí. Školení naučí kontrolu provozovaných služeb a identifikaci verze softwaru obsahující známé zranitelnosti či konfigurační chyby na všech zařízeních připojených k síti, včetně serverů, koncových stanic, tiskáren a síťových prvků. Školení zahrnuje práci s interaktivním dashboardem pro vizualizaci reálných dat o zranitelnostech, generování zpráv shrnujících nalezené problémy s doporučenými řešeními a nastavení opakovaných testů během běžného provozu infrastruktury v rozsahu 2 MD. Důraz je kladen na pasivní detekci bez aktivního zneužívání zranitelností. Jedna položka školení obsahuje celkem 3MD.

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 EventLog.
* Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených), šifrovaná komunikace, agent obsahující buffer pro případ ztráty komunikace a nahrání dat chybějících při ztrátě komunikace a to i zpětně.
* 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.

**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 3 MB
* Min. 4 GB RAM s možností rozšíření až na 32 GB
* Min. 2x 1 GbE RJ-45
* Podpora hardwarového šifrování
* Podpora jumbo frame
* 2x min. 16 TB HDD, 7200 ot/min kompatibilních s NAS s možností vyčítání SMART a podporou aktualizace firmware
* Záruka min. 5 let a NAS a 5 let na 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 minimálně 12 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby po dobu dalších 2 let.

Systém musí zajistit integritu archivu. Dodávané řešení musí být standardní Log/Event Management, který musí umožnit budoucí rozšíření o další systémy (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.

**2x Zaškolení administrátorů**

Zaškolení administrátorů pro oblast HW zahrnuje školení pro administrátory systému Log/Event Management má za cíl pochopit HW konfiguraci a vysvětlit běžné procesy údržby serverového hardware pro systém i pro archivaci logů. Školení provede konfigurací těchto technologií pro naučení běžné správy technologií. Školení pro administrátory pro oblast SW systému Log/Event Management má za cíl naučit efektivní správu centralizovaného systému pro archivaci a analýzu logů. Školení se zaměřuje na konfiguraci a správu systému, který zajišťuje sjednocené ukládání logů s důrazem na jejich dostupnost, důvěrnost a integritu. Školení provede systémem, jeho konfigurací a projde nastavování multikriteriálního vyhledávání pro analýzy a audity a generování přehledných reportů. Školení zahrnuje praktické ukázky pokročilé analýzy bezpečnostních a provozních událostí, integrace s firewall SSO agenty, RADIUS logy a adresářovými službami pro mapování vazby IP-uživatel-čas, a nastavení notifikací pro aktivní detekci rizik. Administrátoři se seznámí s ovládáním systému přes jednotnou grafickou konzoli dostupnou přes HTTPS, správou databáze pro sjednocené vyhledávání a zajištěním imutability logů. Jedna položka školení obsahuje školení v rozsahu 2MD.

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

Hardware, software

**1x Firewall**

Na perimetru sítě bude doplněn druhý identický FW ke stávajícímu FW FG-101F, a nově budou tyto FW tvořit HA pár v režimu Active-Passive.

Stávající FW FG-101F je provozovaný s UTP předplatným a Forticare Premium Supportem.

Nově dodaný FW musí být identický a UTP předplatné a Forticare Premium support jsou požadovány v délce 60 měsíců.

**2x Core switch**

Core LAN sítě bude bude realizováno jako stack dvou kusů 48-portových metalických MultiGig přepínačů osazených uplinkovými moduly s podporou 10/25Gbit SFP+ rozhraní, která budou využita pro připojení zbytku LAN infrastruktury. MultiGig porty Core přepínačů budou zároveň využity pro připojení serverové infrastruktury úřadu. Core musí pro tyto účely splňovat následující specifikaci:

|  |  |
| --- | --- |
| **Požadovaná funkcionalita** | **Způsob splnění požadované funkcionality** |
| Výrobce zařízení | Uvedení výrobce |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém -bo anglickém jazyce | Uvedení požadovaného odkazu |
| Typ přepínače | L2/L3 přepínač |
| Formát přepínače | Stohovatelný |
| Počet dedikovaných stohovacích portů | 2 |
| Minimální počet zařízení ve stohu | 8 |
| Minimální kapacita sběrnice stohu | 1 000 Gb/s |
| Stateful Switch Over v rámci stohu | ANO |
| Min. přepínací kapacita | 2 Tbps |
| Min. paketový výkon přepínače | 1488 Mpps |
| Formát zařízení 1RU | ANO |
| Min. velikost sdíleného systémového bufferu | 32 MB |
| Redundantní ventilátory vyměnitelné za chodu zařízení | ANO |
| Non-stop Forwarding | ANO |
| Sdílení výkonu napájecích zdrojů napříč celým stohem | ANO |
|  |  |
| Možnost instalovat interní redundantní napájecí zdroj | ANO |
| Interní redundantní napájecí zdroj vyžadován | ANO |
| Možnost redundance zdrojů v režimu N+1 | ANO |
| Stohovací zdrojový kabel vyžadován (1.5m) | ANO |
| Stohovací datový kabel vyžadován (1m) | ANO |
| Počet portů 10/100Mb/1/2,5/5/10Gbps | 48 |
| Možnost přepínač rožšířit o modul s volitelným fyzickým rozhraním vyžadován | ANO |
| Rozšiřující modul s 8x 1/10/25Gbps SFP+ porty | ANO |
|  |  |
| 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) | ANO |
| IEEE 802.3ad přes více přepínačů ve stohu -bo více šasis | ANO |
| Minimálně 8 li-k jako součást Link Aggregation Group trunku | ANO |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 128 |
| IEEE 802.1Q | ANO |
| Minimální počet aktivních VLAN | 1000 |
| IEEE 802.1x | ANO |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | ANO |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | ANO |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | ANO |
| RADIUS CoA | ANO |
| Podpora instance spanning-tree protokolu per VLAN | ANO |
| IEEE 802.1w - Rapid Spanning Tree Protocol | ANO |
| Protokol MVRP -bo VTP pro definici a správu VLAN sítí | ANO |
| Podpora jumbo rámců (min. 9198 bytes) | ANO |
| Detekce protilehlého zařízení (např. CDP -bo LLDP) | ANO |
| Směrování protokolů IPv4 a IPv6 v hardware | ANO |
| OSPFv2 | ANO |
| OSPFv3 | ANO |
| EIGRP (dle RFC draft-savage-eigrp-05 nebo RFC 7868) | ANO, povýšením firmware |
| ISIS | ANO, povýšením firmware |
| BGPv4 | ANO, povýšením firmware |
| VXLAN s BGP EVPN | ANO, povýšením firmware |
| Policy based routing uvnitř VRF | ANO, povýšením firmware |
| Graceful Insertion and Removal | ANO, povýšením firmware |
| IP Multicast ( PIM SSM, PIM SM) | ANO, povýšením firmware |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | ANO, povýšením firmware |
| MPLS VPN | ANO, povýšením firmware |
| MPLS VPN přes GRE tunely | ANO, povýšením firmware |
| MPLS VPN - 6VPE | ANO, povýšením firmware |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | ANO |
| Reverse path check (uRPF) pro IPv4 i IPv6 | ANO |
| IGMPv2, IGMPv3 | ANO |
| IGMP snooping | ANO |
| MLD snooping | ANO |
| DHCP relay | ANO |
| Minimální počet HW QoS front | 8 |
| QoS classification – ACL, DSCP, CoS based | ANO |
| QoS marking - DSCP, CoS | ANO |
| QoS - Strict Priority Queue | ANO |
| Automatické nastavení QoS parametrů (AutoQoS -bo ekvivalentní) | ANO |
| QoS Policing | ANO |
| QoS-Per Flow policing | ANO |
| QoS-Hierarchical QoS | ANO, min. 2 úrovně |
| First Hop Redundancy Protokol pro IPv6 (HSRP -bo VRRP) | ANO |
| IPv6 services (Tel-t, SSH, Syslog, DHCP) | ANO |
| IPv6 QoS | ANO |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | ANO |
| IPv6 Port ACL, VLAN ACL | ANO |
| Možnost definovat povolené MAC adresy na portu | ANO |
| PACL, VACL | ANO |
| IEEE 802.1ae (AES-GCM-128) na uplink portech | ANO |
| IEEE 802.1ae (AES-GCM-256) na uplink portech | ANO, povýšením firmware |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení -autorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | ANO |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | ANO |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | ANO |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | ANO |
| Podpora SUDI (IEEE 802.1AR) autentizace | ANO |
| IEEE 802.3az | ANO |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | ANO |
| Multicast DNS (mDNS) gateway | ANO |
| Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) | ANO, povýšením firmware |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | ANO |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | ANO |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | ANO |
| Full Flexible Netflow | ANO |
| SSHv2 | ANO |
| CLI rozhraní | ANO |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu |  |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | ANO |
| Python scripting | ANO |
| Linux shell | ANO |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | ANO |
| Application hosting | ANO, povýšením firmware |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | ANO |
| Streaming telemetrie prostřednictvím NETCONF/XML | ANO |
| SNMPv2/v3 | ANO |
| Podpora -twork boot (iPXE) pres IPv4 i IPv6 | ANO |
| Inventarizovatelnost komponent integrovanou RFID identifikací | ANO |
| TACACS+ -bo RADIUS klient pro AAA (autentizace, autorizace, accounting) | ANO |
| AVC (NBAR2) | ANO, povýšením firmware |
| Vzdálený port mirroring (ERSPAN) | ANO, povýšením firmware |
| NTPv3 server | ANO |

**8x bezdrátový přístupový bod**

V rámci projektu je nutné zajistit rozšíření stávajícího wifi řešení o další Access Pointy, pro pokrytí požadovaných prostor úřadu. Stávající wifi řešení je realizováno Access pointy od společnosti Cisco Systems – konkrétně se jedná o AP Cisco 9115AXI-E. Řízení wireless prostředí je realizováno integrovaným wireless kontrolerem (Embeded wireless kontroler) na vybraných AP. Nové AP musí být schopny se do stávající WIFI infrastruktury plně integrovat. Minimální HW požadavky na AP níže:

|  |  |
| --- | --- |
| **Požadovaná funkcionalita/vlastnost** | **Způsob splnění požadované funkcionality/vlastnosti** |
| Výrobce zařízení | Uvedení výrobce |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |
| Access Point určený pro instalaci na strop/podhled | ANO |
| Typ antén | Integrované pro všechny pásma |
| Access Point vybavený radiem pro 2,4 a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax) | ANO |
| Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax | ANO |
| Minimální počet inzerovaných SSID (BSSID) per radio | 8 |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | ANO |
| Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma | ANO |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | ANO |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | ANO |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | ANO |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | ANO |
| Access Point obsahuje Bluetooth low-energy (BLE) 5.0 rádio a USB 2.0 port | ANO |
| 1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz | ANO |
| Možnost 802.3af/at PoE napájení AP z přepínače nebo injectoru, v případě použití 802.3af AP běží minimálně v režimu 2x2 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu | ANO |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | ANO |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | ANO |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem | ANO |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | ANO |
| Plná podpora AP na stávajícím kontroleru (EWC) | ANO |

**1 x Ověřování 801.x, NAC server**

V rámci portové konfigurace je nasazeno bezpečností řešení řízení přístupu do sítě, kdy přístup je povolen pouze v rámci domény a známým zařízením.

Je prováděn monitoring a analýza datových toků formou portového zrcadlení provozu na CORE přepínači do sondy, která je schopna vyhodnocovat provoz na základě principů bezpečnostní analýzy (behaviorální analýza a jiné).

Sonda zná běžné chování sítě a je schopna reagovat v případě anomálního chování. Je dále schopna prostřednictvím komunikace s firewallem a jinými bezpečnostními technologiemi zablokovat původce anomálie a odstavit ho ze sítě.

Je implementován centrální sběr bezpečnostních logů a jeho komunikace s dalšími bezpečnostními technologiemi.

Perpetuální licence je pro minimálně 250 koncových zařízení. Nabízené řešení bude

mimo jiné sloužit pro zpřehlednění sítě, správu hostovských zařízení (BYOD).

Produkt bude umožňovat napojení na produkt monitoringu síťového provozu, se kterým bude spolupracovat v případě incidentů a automaticky na tyto incidenty reagovat, dle nastaveného flow.

Produkt bude instalován v serverovně zákazníka.

Hlavní vlastnosti produktu:

* Virtuální appliance pro virtualizační prostředí zákazníka
* centralizovaná správa uživatelských práv a přístupových politik,
* autentizace uživatelů a zařízení s funkcí fingerprintingu,
* možnost definovat role a oprávnění pro uživatele a zařízení,
* monitorování síťového provozu a detekce podezřelých aktivit,
* sledování koncových zařízení, zdali se shodují s nastavenými pravidly,
* blokování neautorizovaných zařízení a aplikací,
* RADIUS server využívající MAC, user credentials, certifikát a fingerprinting,
* možnost vytvářet automatizované workflow na základě daných aktivit,
* možnost napojení na antivirový software,
* automatické přeřazení do jiné VLAN,
* automatické odpojení infikovaných koncových bodů,
* možnost nasazení agenta, který se instaluje na zařízení, která jsou mimo spravované aktivní prvky,
* notifikace a generování a exportování reportů o bezpečnostních incidentech,
* otevřené rozhraní API pro integraci s dalšími systémy,
* možnost rozšiřovat funkcionalitu pomocí doplňků,
* auditování aktivit uživatelů a změn v síti,
* automatická vizualizace síťových komponent,
* záruka výrobce po dobu 5 let, kdy jsou dodávány aktualizace, je předplacená technická podpora výrobce produktu.

**1x Monitoring síťového provozu a detekce anomálií**

***Server pro detekci síťového provozu***

* + určeno pro software pro detekci síťového provozu
  + TPM 2.0
  + 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 2.0 Ghz, cache alespoň 30 MB
  + rychlost paměti alespoň 5600 MT/s
  + RAM modul o kapacitě alespoň 32 GB
  + celkem osazeno 64 GB RAM
  + interní řadič pro NVME disky s podporou RAID 0, 1, 5, 6, 10, 50, 60
  + 2x 3.84 TB SSD NVME Read Intensive
  + min. 4x 1/10 Gbps Base-T porty pro SPAN
  + min. 2x 1 Gbps 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 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 zajištuje 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 (MS 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.

**1x Provozní monitoring**

* Zprovoznění lokálního softwarového dohledového systému:
* Instalace operačního systému serveru v aktuální verzi,
* Aktualizace všech součástí systému na nejnovější verze,
* Instalace a konfigurace všech požadovaných komponent pro provoz systému dle doporučení výrobce,
* Nastavení dle dokumentace výrobce a požadavků NIS2
* Nastavení bezpečných přihlašovacích údajů pro server, databázi a systém jako takový,
* Konfigurace dohledového nástroje, odstranění chyb podle logu instalace,
* Nastavení denní automatické aktualizace,
* Konfigurace retence dat na minimálně 30 dní,
* Konfigurace automatické detekce nových zařízení,
* Konfigurace SNMP v3 a SNMP v2 pro zařízení kde není možno použít v3,
* Zabezpečení komunikace SNMP, zákaz defaultních hodnot,

**2x Zaškolení administrátorů**

Školení pro administrátory pro oblast HW je navrženo pro základní konfigurační úkony dodaného hardware, zapojení aktivních prvků i firewall, správa operačního systému pro NAC.

Školení pro administrátory pro oblast SW je navrženo pro správu a zabezpečení pokročilé síťové infrastruktury zahrnující firewall v režimu v HA, dále zaškolení pro aktivní prvky a také pro Wi-Fi 6 přístupové body . Školení bude zaměřené na konfiguraci a používání NAC server pro řízení přístupu a systém pro monitoring síťového provozu s detekcí anomálií. Položka školení obsahuje 2MD.

Zvýšení úrovně bezpečnosti přístupu k informacím

**1x Zálohovací NAS pro cloudové služby**

* Rack NAS s 12 HDD SATA 3,5“ pozicemi s redukcí pro 2,5“ disky
* Disky vyměnitelné za provozu
* Možnost připojení expanzní jednotky a rozšíření o 36 disků
* CPU o výkonu alespoň 7000 bodů dle passmark, alespoň 4 jader, cache alespoň 4 MB
* Min. 8 GB RAM s možností rozšíření až na 32 GB
* Podpora RAID 0,1,5,6 hybrid RAID, JBOD
* Min. 1x 10 GbE 10G Base-T
* Min. 2x 1 GbE RJ-45
* Podpora hardwarového šifrování
* Podpora jumbo frame
* Ližiny pro montáž do 19“ racku
* Software musí umožnit zálohování cloudových služeb
  + - Zálohování poštovních schránek, e-mailů, kontaktů, kalendářů a úkolů.
    - : Zálohování webů, seznamů, knihoven dokumentů a dalšího obsahu.
    - Zálohování souborů a složek jednotlivých uživatelů uložených v cloudu.
    - Zálohování týmů, kanálů (včetně privátních a sdílených), konverzací a souborů.
    - Zálohování uživatelů, skupin, registrací aplikací a dalších objektů konfigurovaných v cloudu.
    - Možnost nastavení četnosti záloh (např. hodinově, denně, týdně).
    - Podpora nezměnitelných záloh pro ochranu před ransomware a neoprávněnými změnami.

**Obnova dat**

* + - Granulární obnova: Možnost obnovy jednotlivých položek (např. konkrétní e-mail, soubor, tým) nebo hromadná obnova více uživatelů či objektů.
    - Rychlá obnova: Obnova dat ve třech krocích pro minimalizaci prostojů, s podporou samoobslužného portálu pro uživatele.
    - Flexibilita obnovy: Podpora obnovy do původního umístění, jiné lokality nebo exportu do různých formátů (např. PST pro e-maily).

**Úložiště a škálovatelnost**

* + - Flexibilní úložiště: Podpora různých typů úložišť, včetně:
    - Lokálních úložišť (DAS, SAN, SMB 3.0).
    - Cloudových objektových úložišť (Amazon S3, Azure Blob, IBM Cloud, S3-kompatibilní úložiště).
    - Imutabilní kopie: Možnost ukládání nezměnitelných záložních kopií v Azure Blob/Archive, Amazon S3/Glacier nebo jiných S3-kompatibilních úložištích.

**Bezpečnostní funkce**

* + - Šifrování: Použití 256bitového šifrování pro zajištění bezpečnosti dat během přenosu i uložení.
    - Vícefaktorová autentizace (MFA): Zvýšená bezpečnost přístupu k zálohám.
    - Role-Based Access Control (RBAC): Definice rolí a oprávnění pro různé uživatele (administrátoři, technici, koncoví uživatelé).
    - Ochrana před ransomware: Imutabilní zálohy a oddělení záloh od původního tenanta pro zvýšení odolnosti.

**Správa a monitorování**

* + - Webové rozhraní: pro správu záloh, obnovu dat a monitorování stavu prostředí.
    - eDiscovery: Rychlé vyhledávání a lokalizace dat v zálohách pro právní a regulační účely.
    - Automatické aktualizace: Pravidelné aktualizace softwaru a databáze zranitelností pro zajištění aktuálnosti.

**1x Zaškolení administrátorů**

Školení pro administrátory je zaměřeno na správu a zabezpečení cloudových služeb pro e-mailovou komunikaci, ukládání a sdílení souborů a týmovou spolupráci, spolu s robustním zálohovacím řešením pro ochranu dat. Školení má za cíl naučit administrátory konfigurovat a spravovat e-mailové schránky, kalendáře a kontakty, nastavovat sdílení dokumentů a webových stránek pro interní i externí spolupráci, a zajišťovat bezpečné ukládání souborů s možností rychlé obnovy. Školení zahrnuje praktické ukázky nastavení zálohovacího systému pro automatické uchovávání dat těchto služeb, včetně konfigurace imutabilních záloh, granulární obnovy a integrace s lokálními a cloudovými úložišti. Důraz je kladen na bezpečnostní politiky, správu přístupových práv, monitorování provozu a soulad s regulatorními požadavky, s pětiletou zárukou podpory a aktualizací. Školení bude v rozsahu 4 MD.

Druhá fáze projektu – implementace

Implementační práce zahrnují:

* Dokumentaci provedených prací
* Zaškolení administrátorů na práci s novým zařízením
* Implementace datového centra na uvažovaných technologiích musí splňovat legislativní požadavky Zákona o kybernetické bezpečnosti (ZKB), doporučení NÚKIB a normu ISO 27001. Klíčové je řízení přístupů (MFA, RBAC), monitorování a logování událostí (SIEM, IDS/IPS) a správa zranitelností (pravidelné aktualizace, hardening). Důraz je kladen na ochranu před kybernetickými hrozbami, včetně segmentace sítě, zabezpečení virtualizace a bezpečnostní dohled.

Veškeré nově instalované operační systémy a aplikace budou zahrnuty do zálohovacích plánů v rámci stávajícího zálohovacího řešení. Veškeré zálohy budou řádně zkonfigurovány, zadokumentovány a ověřena jejich funkčnost obnovení. Zálohy budou konfigurovány v rámci stávající politiky zálohování zadavatele

Business continuity

Z pohledu business continuity a compliance je nutné zajistit zálohování a disaster recovery plán (Immutable Backup, Veeam, geografická redundance) a pravidelně testovat reakce na incidenty. ISO 27001 vyžaduje řízení rizik, šifrování dat a bezpečnostní audity, zatímco NÚKIB doporučuje oddělení bezpečnostních zón, simulaci útoků a pravidelná školení administrátorů. Splnění těchto opatření minimalizuje rizika kybernetických incidentů a zajistí soulad s regulacemi, čímž se datové centrum stává bezpečnějším a odolnějším vůči útokům.

* Implementační dokumentace
* Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti a zálohy napájení, migrační práce datacentrových systémů, migrační práce aplikačních serverů
* Aktivní přístupové prvky, monitoring síťového provozu, provozní monitoring
* Pravidelné testování zranitelnosti prvků infrastruktury
* Řešení centrálního ukládání a analýzy logů

Zapracování nálezů z GAP analýzy

Implementační práce budou vycházet z doporučení uvedených v GAP analýze, která identifikovala nedostatky v síťové infrastruktuře, datovém centru, aplikacích a interní doméně. Tyto práce budou zahrnovat úpravy konfigurací a nastavení na základě navržených opatření, aby byla zajištěna vyšší bezpečnost a soulad s legislativními požadavky. Proces bude zahrnovat analýzu jednotlivých doporučení, jejich prioritizaci podle závažnosti a následnou realizaci ve všech dotčených oblastech IT prostředí. Cílem ošetřit všechny identifikované slabiny, posílit bezpečnost infrastruktury a splnit legislativní požadavky.

Pravidla pro tvorbu hesel

Veškerá hesla vytvořená pro správu fyzického hardware, virtualizace a doménových komponent musí splňovat určitou komplexitu. **V žádném případě nesmí být ponechána defaultní hesla od výrobce**. Kde je to možné, je vyžadováno použití multifaktorové autentikace.

Komplexitu hesel lze rozdělit do dvou kategorií podle toho, kde se hesla budou používat:

* **kritická hesla (root, admin)**
  + délka minimálně 20 znaků
  + použití malých a velkých písmen
  + minimálně 4 číslice
  + minimálně 4 speciální znaky
* **běžná hesla (servisní účet, monitoring účet…)**
  + délka minimálně 16 znaků
  + použití malých a velkých písmen
  + minimálně 4 číslice
  + minimálně 4 speciální znaky

Kritická hesla slouží pro klíčové prvky infrastruktury, kterými jsou přístupy na servery, disková pole, hesla k obnovení záloh apod.

Běžná hesla se používají například ke správě monitorovacího systému a pro jiné aplikace, které nejsou součástí kořenové infrastruktury.

Doplnění HW datacentra a virtualizace pro zajištění vysoké dostupnosti

Komponenty datového centra projdou testováním hardware, zahoření a základní konfigurací nových serverů, diskových polí, zálohovací sever, zálohovací úložiště a systém pro zálohu napájení. Součástí jsou též dodané licence a pomocný materiál nutný pro zapojení do stávajícího datového centra.

Jmenná konvence serverů

Veškeré virtuální servery budou mít prefix *SRV – a* dále jméno serveru, odpovídající roli serveru, kterou zastává (např. *SRV-DC*=Domain Controller, *SRV-SQL*=SQL Server, *SRV-BCK* = zálohovací server apod.). V případě, že serverů se stejnou rolí bude více bude potom doplněno pořadové číslo (Např.DomainControllery – *SRV-DC01*, *SRV-DC02*)

Implementace do stávajícího datového centra

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.

Implementace zahrnuje instalaci a konfiguraci serverů do stávajícího výpočetního clusteru. Součástí této implementace je compliance kontrola, jestli nové zařízení splňuje konfigurační požadavky organizace, je plně integrované do infrastruktury, má nastaveny bezpečnostní politiky, přístupové údaje a zařazení do doménové struktury. Součástí je ověření plné funkcionality clusteru jako je migraci virtuálních serverů, vysoká dostupnost, přístup na stávající diskové pole. Implementace se týká produkčních serverů i datového centra pro virtuální desktopy.

Příprava hardware

**Servery produkční**

* Instalace a konfigurace hypervisorů, aby je bylo možné implementovat do stávající infrastruktury, nastavit dle best practise vendora hardware, připojit do stávající infrastruktury. Otestovat veškeré funkcionality jakou jsem síťové rozhraní v High availability režimu, redundace interních disků, napojení na infrastrukturu objednatele a kompatibilitu s ostatními systémy.
* Propojení serverů s diskovým polem, otestování spojení na všech síťových rozhraních, testování datové propustnosti, zdali odpovídá plánovanému sizing diskového pole dle best practise výrobce, testování latence a vysoké dostupnosti (trhací kabelové testy), otestování vypínání a zapínání serverové infrastruktury.
* Připojení nového datového centra paralelně do stávající infrastruktury objednatele a otestování komunikace na všech VLAN.

Instalace virtuálních serverů

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 template serverů pro verze Windows Server 2022 a 2025

* Vytvoření nového virtuálního serveru
* Procesor 2 vCPU
* RAM 4 GB
* Systémový disk 60 GB
* Network Adapter 1Gbps
* Minimálně NET Framework 4.8
* Instalace operačního systému z ISO obrazu v nejvyšší podporované verzi
* Nastavení výchozího hesla pro administrátora
* Nastavení správné časové zóny
* Nastavení statické IP adresy
* Instalace nejnovějších ovladačů
* Instalace dostupných aktualizací
* Nastavení firewallu dle Best Practices
* Nastavení politiky silných hesel
* Provedení potřebných nastavení operačního systému, zejména instalace agenta bezpečnostního software v aktuální verzi
* Vypnutí legacy protokolů SMB 1, TLS1 a další zastaralé protokoly
* Aktivace Bitlocker šifrování
* Finalizování pro použití jako template

Instalace dvou virtuálních serverů pro doménový řadič

* Instalace serveru doménového řadiče z vytvořeného template
* Nastavení pevné IP adresy
* Přidání do domény organizace
* Nastavení názvu serveru dle jmenné konvence
* Přidání role AD a DNS a připojení do domény
* Ověření z logu o přidání serveru jako plnohodnotného AD
* Ověření vytvoření Global Catalogu na novém AD
* Kontrola a nastavení Reverse Lookup Zones
* Kontrola a nastavení DNS Aging and Scavenging
* Instalace agenta bezpečnostního software
* Konfigurace bezpečnostních politik v doméně a konfigurace dle doporučení ZKB
* Konfigurace agenta a pravidel pro zasílání logů z AD a DNS do centrálního log management systému
* Konfigurace do zálohovacího systému zadavatele

Instalace a nastavení DHCP

* Přidání role DHCP na doménovém řadiči
* Inicializace DHCP
* Vytvořeni Scopů dle VLAN
* Nastavení Scopu (Adress Pool, Gate, DNS, Lease Time, atd.)
* Přidání rezervací
* Přidání role DHCP na druhém doménovém řadiči
* Aktivace DHCP Failover služby na prvním DHCP
* Nastavení DHCP Failover (Hot Standby, State Switch interval 5minut, Maximum Client Lead Time 1 h)
* Scheduled Tasks pro pravidelnou replikaci nastavení na druhý DHCP
* Konfigurace agenta a pravidel pro zasílání logů z DHCP do centrálního log management systému

Instalace a konfigurace SQL serveru

* Instalace serveru z připraveného template
* Vložení SQL Serveru do domény
* Aktualizace OS a SQL serveru jeho CU a service pack
* Instalace management studia pro obsluhu
* Příprava doménových účtů pro běh SQL
* Konfigurace lokálního firewallu – firewall aktivní, povoleny jen potřebné porty pro fungování SQL
* Instalace agenta bezpečnostního software
* Příprava a formátování disků pro provoz SQL, umístění dat, logů, temp a záloh
* SQL server NESMÍ být instalován na systémový disk
* Instalace a konfigurace SQL serveru s důrazem na bezpečnost a výkon
* Vytvoření účtu **sa** se silným heslem, ověření funkčnosti a uložení do trezoru. Účet sa nesmí být nadále používám pro běžnou správu.
* Přiřazení oprávnění **sysadmin** konkrétnímu uživateli – nutno použít doménový účet
* Konfigurace auditu a přistup k němu
* Revize a nastavení parametrů na základě parametrů starého SQL serveru – vše s důrazem na bezpečnost, stabilitu a bestices
* Migrace databází a běžných uživatelů
* Revize uživatelů v privilegovaných rolích
* Konfigurace agenta a pravidel pro zasílání logů z SQL serveru do centrálního log management systému
* Nastavení přístupu k MS SQL dle best practices a požadavků aplikací
* Konfigurace maintenance operací
* Konfigurace do zálohovacího systému zadavatele

Instalace aplikace pro zálohování M365

* Instalace aktuální verze zálohovací aplikace dle best practise výrobce,
* Propojení s tenantem a využitím API, vytvoření a nastavení práv pro aplikaci v rámci Entra ID. Práva musí pokrývat pouze potřeby zálohování,
* Nastavení cíle záloh konzistentně s existujícími zálohovacími systémy,
* Konfigurace zálohovacích úloh pro zálohování uživatelských a společných dat z prostředí cloudové služby,
* Vytvoření samostatných zálohovacích úloh minimálně pro tato data:
  + Uživatelské mailové schránky,
  + Uživatelské datové úložiště (Onedrive, Sharepoint),
  + Společná úložiště (Sharepoint, skupiny, sdílené schránky),
  + Teams
* Konfigurace úloh pro běh minimálně jednou denně,
* Konfigurace notifikačních kanálů – minimálně mail při neúspěšném běhu nebo při stavu „varování“,
* Konfigurace retence na 10 let a podle jednotlivých položek – tak, že jednotlivá položka bude odstraněna ze záloh pokud její datum vytvoření nebo modifikace přesahuje retenční periodu

Instalace serverů pro provoz aplikací

* Servery budou generovány z vytvořené template popsané výše
* Analýza aktuálního stavu aplikace na stávajícím serveru
* Analýza potřebného diskového prostoru pro aplikaci a data
* V případě externích aplikací konzultace s externím dodavatelem aplikace
* Ověření existence funkční zálohy aplikace
* Instalace a nastavení nového serveru dle potřeb aplikace a požadavků výrobce
* Ověření fungování serveru dle potřeb aplikace
* Konfigurace do zálohovacího systému zadavatele

Migrace serverů

Migrace Active direktory dvou doménových řadičů

* Ověření fungování replikace mezi doménovými řadiči
* Ověření vytvoření všech potřebných záznamů v DNS
* Přesun FSMO rolí na nový doménový řadič
* Kontrola Domain a Forest level, zda jsou na požadované úrovni
* Backup a migrace DHCP na nový server
* Vytvoření a nastavení DHCP Failover, pokud je požadováno
* Nahraní a instalace poslední verze ADMX template
* Kontrola nastavení Forwareders v DNS
* Kontrola politiky Default Domain Polici a Default Domain Controllers Policy
* Nastavení funkcionality Scavenging a Aging na Forward a Reverse Lookup Zones
* Kontrola fungování DFS replikace SYSVOL
* Vypnutí starého doménového řadiče pro ověření správného fungování nového doménového řadiče
* Opětovné zapnutí starého doménového řadiče
* Odebrání role AD na starém doménovém řadiči
* Ověření, že starý doménový řadič již nefunguje jako řadič
* Vymazání nepotřebných DNS záznamu na starý doménový řadič
* Odebrání starého doménového řadiče z domény a vypnutí starých serverů

Post migrační práce

* Revize a případné povýšení Domain level a Forest level
* Revize Default domain policy vzhledem k aktuálním požadavkům na bezpečnost
* Audit stávajících objektů v AD (uživatelů, skupin, počítačů…)
* Revize DNS záznamů
* Sjednocení jmenné konvence objektů

Migrace aplikačních serverů

Migrace se týká 25 virtuálních serverů a bude provedena formou čisté instalace, na zcela nové servery, které jsou instalovány z template popsané výše, případně na image dodané výrobcem software. Na nově instalované servery budou postupně přeneseny aplikace a služby z původních systémů. Celý proces bude pečlivě naplánován tak, aby se minimalizovaly prostoje spojené s plánovanou implementací. Níže v tabulce jsou vypsané aplikace, jejich časová náročnost, a zda se budou podílet na migracích i externí dodavatelé. Dodavatel v rámci cenové nabídky musí nacenit své činnosti na migraci aplikací, které jsou níže popsané.

|  |  |  |
| --- | --- | --- |
| **Název aplikace/role** | **Dodavatel zakázky VŘ hodin (odhad)** | **Dodavetel** |
| GFI mail essential | 20 hod | Dodavatel |
| GFI archiver | 20 hod | Dodavatel |
| Veeam Backup, Veeam ONE produkce | 4 hod | Dodavatel |
| Veeam Backup, Veeam ONE desktopová virtualizace | 4 hod | Dodavatel |
| VMware Horizon | 10 hod | Dodavatel |
| VMware UAG | 6 hod | Dodavatel |
| Dell Open Manage | 4 hod | Dodavatel |
| File server | 10 hod | Dodavatel |
| Microsoft SQL server | 20 hod | Dodavatel |
| LibreNMS dohledový nástroj | 4 hod | Dodavatel |
| Network Policy Server | 4 hod | Dodavatel |

Migrace aplikačních serverů se smlouvou se součinností dodavatelů

Zadavatel má uzavřenou smlouvu s dodavateli aplikací uvedených níže v tabulce. Zadavatel požaduje součinnost v rozsahu 2 hodin pro každou aplikaci spočívající v přípravě serveru dle požadavku dodavatele aplikace, instalace požadovaných rolí, služeb a nastavení korektního zálohování daného serveru.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Program** | **Dodavatel** | **Celkem hodin (odhad)** | **Cena** | **Dodavatel zakázky VŘ** |
| Alvao | Alvao s.r.o. | 5 | 13 600 |  |
| Derik | Ing. Jan Štindl | 8 | 8000 |  |
| Ginis | GORDIC spol. s.r.o. | 40 | 118 800 |  |
| Evi,Espi | INISOFT s.r.o | 2 | 2 500 |  |
| Webcall | Kadlec-elektronika, s.r.o. | 10 | 20 000 |  |
| Vema | Seyfor, a.s. | 10 | 20 000 |  |
| Vita | VITA software, s.r.o. | 5 | 7 200 |  |
| Ev. Myslivosti | Karel Janeček Ing. YAMACO Software | 2 | 3 600 |  |
| Misys | GEPRO spol. s.r.o. | 10 | 6000 Kč |  |

Produkt pro testování a vyhodnocování zranitelností prvků infrastruktury

Produkt bude konfigurován s automatickými výstupy v podobě technického reportu popisující nalezené problémy a jejich množná řešení, v poslední fázi navíc i manažerské shrnutí nalezených problémů a jejich dopadů po dobu 5 let.

Produkt bude schopen automaticky skenovat všechna zařízení komunikující v síti zadavatele. Skenování zahrnuje:

* **Aktivní síťové prvky**: směrovače, přepínače, firewally a další zařízení zajišťující síťovou konektivitu.
* **Servery**: fyzické i virtuální servery, včetně webových, aplikačních a databázových serverů.
* **Klientské stanice**: pracovní stanice, notebooky a další koncová zařízení připojená k síti.
* **Aplikace**: webové aplikace, interní softwary a další aplikace běžící v infrastruktuře.
* **Databázové servery**: systémy jako MySQL, PostgreSQL, Oracle nebo MS SQL, které uchovávají kritická data.
* **Další síťová zařízení**: IoT zařízení, tiskárny, IP telefony a další periferie připojené k síti.

Skenování bude prováděno pravidelně dle nastaveného harmonogramu s možností okamžitého spuštění na vyžádání.

Produkt bude integrován do infrastruktury v rámci lokálního nasazení. Konfigurace produktu zahrnuje definici rozsahu skenování (např. IP adresy, subnety, specifické porty) spolu s nastavením citlivosti skenování pro minimalizaci dopadu na provoz sítě.

Výstupem skenování je report, který bude dostupný ve formátu PDF (v češtině), HTML a CSV pro snadný import do jiných aplikací. Report bude ve dvou kategoriích:

* **Technický report zranitelností**
  + Klasifikace podle závažnosti (např. kritická, vysoká, střední, nízká dle CVSS skóre).
  + Technický popis zranitelnosti (např. CVE identifikátor, popis útoku, potenciální dopady).
  + Kontext zranitelnosti (např. konkrétní zařízení, port, služba nebo aplikace).
  + Návrh řešení k opravě zranitelnosti
* **Manažerské shrnutí**
  + Stručné shrnutí nalezených zranitelností s důrazem na jejich dopady na obchodní procesy a bezpečnostní politiku.
  + Grafy a tabulky znázorňující trendy v bezpečnostních hrozbách.
  + Srovnání aktuálního stavu s předchozími skeny pro sledování pokroku v odstraňování zranitelností.
  + Přehledný dokument ve formátu PDF nebo PowerPoint vhodný pro prezentaci vedení.

Řešení centrálního ukládání a analýzy 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.

* Základní popis instalace, nasazení a konfigurace Log management systému
* Definování skupin v AD pro uživatele a administrátory, aby mohli přistupovat do Log managementu (nebude to na konkrétní osoby ale skupiny s daným oprávněním)
* Konfigurace AD pro připojení do Log managementu (konfigurace audit logů, konfigurace beat agenta, napojení, ověření funkčnosti
* Konfigurace Beat agentů, GPO pro centrální deployment Log management agenta na Windows Servery
* Ověření deployment agentů na nové i stávající servery
* Příprava prefixlistů pro kategorizaci zařízení (NAS, servery, switche, UPS, firewall, AP) dle implementační dokumentace
* Popis konfigurace HW zařízení pro napojení na syslog včetně počtu, kterých se to týká jak nových, tak stávajících zařízení
* Konfigurace archivace logů na šifrovaná archivační úložiště s digitálním otiskem proti zneužití a manipulaci s daty

**Konfigurace Log management systému**

* Vytvoření šesti dashboardů zobrazující následující informace spolu s tvorbou automatických reportů
  + Týdenní report na nepovedené pokusy o přihlášení k doménovému řadiči spolu s reportem zamčených účtů
  + Týdenní report konfiguračních změn na aktivních prvcích
  + Týdenní report provozu na firewall
  + Týdenní report spojení na VPN úspěšné i neúspěšné
  + Týdenní report o událostech na HW (KVM serverů, MGMT NAS, UPS...)
  + Týdenní report práce se soubory na souborovém úložišti
  + Týdenní report přístupů ke cloudovým službám zahrnující neoprávněné pokusy o přihlášení
  + Týdenní report sdílených odkazů mimo organizaci
  + Týdenní report o provozu SQL serveru, připojení aplikací
* Vytvoření automatických alertů a okamžité emailové notifikace pro následující usecase
  + Vytvoření nového AD účtu s vysokým oprávněním
  + Přidání účtu do skupiny (Domain Admin, Schema Admin, Enterprise Admin, atd.)
  + Více jak 10 pokusů o přihlášení v jedné minutě
  + Uzamknutí účtu ve skupině Domain Admin
  + Restart a vypnutí serveru
  + Neúspěšný přístup k Remote Desktop
  + Detekce selhání hardwaru (disky, paměti, procesory)
  + Network Policy Server neúpěšný přístup
  + Vytvoření Scheduled Task na serverů
  + Vložení, úprava registru
  + Vypnutí, modifikace Firewallu
  + Změna systémového času
  + Podezřelé aktivity na přenosových protokolech (HTTP, HTTPS, FTP, SMTP, atd.)

Aktivní přístupové prvky, monitoring síťového provozu, provozní monitoring

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.

Firewall

1. Analýza aktuální konfigurace stávajícího firewallu

* Analýza jmenné konvence
* Analýza stávajících konektivit
* Analýza segmentace sítě
* Analýza IP adresace rozhraní
* Analýza konfigurace port-channelů
* Analýza routingu
* Analýza admin přístupů a jejich oprávnění (rolí)
* Analýza prostupových pravidel
* Analýza konfigurace adres objektů
* Analýza konfigurace služeb
* Analýza překladů NAT/PAT
* Analýza synchronizace času
* Analýza StS VPN
* Analýza VPN pro administrativní přístup
* Analýza VPN pro uživatelský přístup
* Analýza VPN pro externí subjekty
* Analýza módů HA
* Analýza použití webových filtrů
* Analýza použití DNS filtrů
* Analýza virtualizace firewallu
* Analýza ověřování uživatelů
* Analýza logování na lokální disk/vzdálený server
* Analýza retence uchování dat
* Analýza rozsahu logování (co se loguje)
* Analýza použití IPS/IDS
* Analýza emailových upozornění
* Analýza zálohování
* Analýza konfigurace reportů

1. Úprava konfigurace firewallu
   * Upgrade firmware na poslední výrobcem doporučenou verzi
   * Konfigurace HA v režimu Active – Passive (doplnění nového FW do HA)
   * Systémová konfigurace – název firewallu,
   * Konfigurace SNMP v3 pro dohledové NMS nástroje
   * Odesílání Netflow dat na centrální kolektor
   * Konfigurace síťových rozhraní (Fyzických / SVI)
   * Definice bezpečnostních zón / inter a intra zone komunikace
   * Konfigurace SSO pro identity based pravidla
   * Konfigurace uživatelských skupin
   * Definice přístupových pravidel
   * Aktivace UTM funkcionalit nad přístupovými pravidly ( IDS/ IPS, Antivirus, sandbox)
   * Řízení webového provozu (URL / Content filtering)
   * Konfigurace Remote access VPN přístupů
   * Přesun inter-vlan routingu z CORE přepínače na firewall
   * Registrace FW do Forticloudu
   * Zálohování konfigurace (automation script)
   * Konfigurace reportů
2. Fyzická instalace nového FW do datového rozvaděče

* Nainstalování nového firewallu do rozvaděče
* Zapojení primárního zdroje do zálohovaného elektrického obvodu
* Zapojení sekundárního zdroje do nezálohovaného elektrického obvodu
* Fyzické propojení firewallů do HA

1. Fyzické propojení s ISP

* Fyzické propojení se zařízením poskytovatele internetových služeb
* Fyzické propojení se zařízením poskytovatele CMS
* Kontrola ustavení spojení

1. Fyzické propojení se zbytkem LAN infrastruktury

* Fyzické propojení firewallů s páteřními přepínači v rámci HA
* Kontrola ustavení spojení

1. Otestování správnosti konfigurace / akceptační testy

* Kontrola konfigurace nového firewallu
* Kontrola vysoké dostupnosti / redundance

2x Core switch

1. Analýza aktuální konfigurace stávajících páteřních přepínačů

* Analýza konfigurace hostname
* Analýza konfigurace administrátorských profilů
* Analýza adresace IP rozhraní
* Analýza konfigurace VLAN
* Analýza GVRP/VTP
* Analýza konfigurace NTP
* Analýza konfigurace ověřování uživatelů
* Analýza konfigurace port-channelů
* Analýza konfigurovaného módu portů jako přístupový pro jednu VLAN/více VLAN
* Analýza popisů portů
* Analýza konfigurace logování
* Analýza konfigurace SNMP
* Analýza zálohování
* Analýza směrování
* Analýza STP
* Analýza vysoké dostupnosti

2. Konfigurace nového přepínače

* Upgrade firmware na poslední výrobcem doporučenou verzi
* Konfigurace systémového nastavení – NTP, časová zóna, název zařízení, doména, lokální logování konfiguračních činností, konfigurace SNMP, logování na centrální logovací server, odesílání Netflow dat na centrální kolektor
* Konfigurace administrátorských účtů
* Konfigurace rozhraní pro management přístup
* Konfigurace management protokolů (jen šifrované varianty HTTPS / SSH, délka klíčů min. 2048 bitů)
* Konfigurace vysoké dostupnosti (HA / Stack)
* Páteřní konektivity budou řešeny redundantně
* Konfigurace VLAN
* Konfigurace SVI
* Konfigurace STP
* Konfigurace fyzických rozhraní (včetně port-channelů)
* Konfigurace směrování
* Konfigurace zálohování konfigurací (po uložení konfigurace / na periodické bázi)

3. Fyzická instalace do datového rozvaděče

* Nainstalování přepínače do rozvaděče
* Zapojení primárního zdroje do zálohovaného elektrického obvodu
* Zapojení sekundárního zdroje do elektrického obvodu

4. Fyzické propojení se zbytkem LAN infrastruktury

* Fyzické propojení přepínače s firewallem
* Fyzické propojení přepínače s přístupovými přepínači
* Fyzické propojení s kontrolérem bezdrátové infrastruktury
* Fyzické propojení se síťovým úložištěm
* Fyzické propojení se zdrojem nepřerušovaného napájení
* Fyzické propojení se servery
* Kontrola ustanovení spojení

5. Otestování správnosti konfigurace / akceptační testy

* Otestování redundance zdrojů
* Otestování redundance linek
* Otestování redundance přepínačů
* Otestování správnosti konfigurace směrování
* Otestování konfigurace systémového nastavení – (NTP, časová zóna, název zařízení, doména, lokální logování konfiguračních činností, konfigurace SNMP, logování na centrální logovací server, odesílání Netflow dat na centrální kolektor)

Implementace 802.1X – NAC server

Konfigurace virtuální appliance

**Nasazení VA**

* Stažení a nasazení virtuální appliance (VA) na podporovanou virtualizační platformu (např. VMware ESXi).
* Inicializace appliance a ověření správného spuštění.

**Adresace management interface VA**

* Nastavení IP adresy management rozhraní (statická IP, maska, brána).
* Konfigurace DNS a základní síťové konektivity.

**Systémová konfigurace VA**

* Nastavení NTP serveru pro synchronizaci času.
* Vytvoření administrátorských účtů pro správu.
* Konfigurace automatických záloh dat a obnovovacích mechanismů.
* Nastavení emailových upozornění (SMTP server, adresáti).
* Instalace certifikátu pro zabezpečenou komunikaci.
* Aktivace a konfigurace SNMP.

**Konfigurace SNMP v3 pro vyčítání informací z LAN infrastruktury**

* Nastavení SNMP v3 (uživatelské účty, hesla, typ autentizace a šifrování).
* Otestování konektivity a správné funkce SNMP s přepínači a dalšími síťovými prvky.

**Konfigurace network device discovery**

* Nastavení pravidel pro objevování síťových zařízení (rozsah IP adres, SNMP).
* Otestování detekce zařízení.

**Konfigurace skupin síťových zařízení**

* Vytvoření skupin na základě typů zařízení (např. přepínače, routery, tiskárny).

**Navázání na zdroj identit (AD/ LDAP atd.)**

* Integrace se systémem Active Directory nebo LDAP pro autentizaci.
* Mapování uživatelských skupin a rolí.

**Konfigurace certifikátů a napojení na CA (CRL)**

* Import certifikátů z certifikační autority (CA).
* Nastavení ověřování revokačních seznamů (CRL).

**Konfigurace (definice) skupin pro koncová zařízení**

* Určení kategorií zařízení (např. uživatelské stanice, IP telefony, tiskárny).

**Rozdělení koncových zařízení do skupin**

* Automatizované nebo ruční přiřazení zařízení do skupin dle pravidel (např. MAC adresy, typ protokolu).

**Konfigurace politik pro ověřování jednotlivých skupin zařízení do LAN**

* Definice pravidel, která určují přístup jednotlivých typů zařízení.
* Otestování správné aplikace politik.

**Konfigurace politik pro ověřování jednotlivých skupin uživatelů do LAN**

* Nastavení přístupových pravidel na základě uživatelských skupin.
* Otestování přístupu uživatelů.

**Konfigurace politik pro ověřování administrátorů k administraci LAN zařízení**

* Nastavení přístupových pravidel na základě uživatelských skupin.
* Otestování přístupu uživatelů.

Konfigurace přepínačů

**Kontrola konfigurace SNMP**

* Zajištění správné konfigurace SNMP pro komunikaci s MACMON.

**Konfigurace AAA pro ověření přístupu do LAN**

* Nastavení autentizačního serveru (RADIUS/TACACS+).
* Otestování AAA komunikace.

**Portová konfigurace 802.1X**

* Aktivace 802.1X na portech přepínačů.
* Nastavení fallback módu (např. MAC bypass pro starší zařízení).
* Testování funkčnosti na jednotlivých portech.
* Konfigurace AD

**Konfigurace doménových politik – nastavení supplicantů na koncových stanicích**

* Automatická distribuce supplicant konfigurace pomocí Group Policy Object (GPO).
* Nastavení politik pro 802.1X (např. PEAP, EAP-TLS).
* Testování ověření přístupu

**Otestování přístupu uživatelských stanic**

* Kontrola autentizace uživatelů přes 802.1X.
* Otestování fallback módu (MAC bypass nebo guest VLAN).

**Otestování přístupu zařízení dle typu**

* Otestování autentizace IP telefonů, tiskáren a dalších zařízení.
* Validace konfigurace politik pro speciální zařízení.
* Konfigurace nástroje do zálohovacího systému zadavatele

8x Wifi AP

1. Fyzická instalace AP na definované pozice

* Označení AP jeho příslušným ID dle dané jmenné konvence
* Fyzická instalace držáku
* Fyzická instalace AP
* Fyzické zapojení AP do LAN infrastruktury

1. Napojení AP na LAN infrastrukturu a jejich napájení (úprava portových konfigurací)

* Konfigurace PoE na fyzickém rozhraní
* Konfigurace VLAN
* Konfigurace portového profilu na daném rozhraní

1. Napojení AP na centrální kontroléry

* Adaptace AP centrálními kontroléry

1. Nasazení konfigurace z centrálních kontrolérů

* Zařazení AP do správné AP skupiny

1. Otestování funkčnosti z klientských zařízení

* Připojení zařízení k vybranému SSID
* Kontrola přiřazení správné IP adresy

1. Ověření post-implementační ho pokrytí wifi signálem
   * Dodavatel provede post-implementační Site-Survey, kde doloží

* Report o kvalitativních parametrech wifi sítě v jednotlivých prostorách zadavatele
* Bude provedeno pasivní i aktivní Site Survey doložené závěrečným reportem

Implementace nástroje pro detekci síťového provozu

* Příprava serveru pro implementaci nástroje pro monitoring síťového provozu
* Zmapování podsítí infrastruktury a příprava implementace subnetů
* Identifikace klíčových prvků v síti
* Příprava síťových prvků pro monitoring provozu
* Zajištění toku testovacích subnetů a kontrola správnosti konfigurace
* Integrace nástroje s active directory
* Eliminace false positive alertů a eventů
* Kalibrace nástroje na základě posbíraných dat z provozu
* Definice alarmů a notifikací na základě požadavků NIS2
* Testování nástroje simulovaných port scannem v rámci sítě
* Konfigurace dashboardů pro rychlou kontrolu
* Nastavení pravidelného reportu nálezů a technická sumarizace
* Nastavení pravidelného reportu manažerského
* Zaškolení techniků pro obsluhu nástroje

Implementace nástroje pro provozní monitoring

* Rozdělení do kategorií podle typu a umístění zařízení, zprovoznění systému webhook, minimálně mailem, ale pokud možno více kanály (SMS, webhook,…),
* Zmapování topologie sítě, definice klíčových prvků, kategorizace zařízení a definice požadavků na monitoring podle následujících bodů,
* Nastavení monitoringu nejdůležitějších údajů, zejména pak:
  + Dostupnost zařízení,
  + Využití systémových zdrojů (CPU, Paměť, disk…),
  + Síťový provoz – propustnost, objem, chybovost podle možností zařízení,
  + Teplota zařízení, je-li tato informace poskytována,
  + Stav disků – hlášené chyby SMART.
* Podle typu zařízení pak dále monitoring zejména těchto metrik:
  + Síťové prvky (switch, router, AP atp.):
    - Využití šířky pásma (příchozí a odchozí provoz na jednotlivých portech),
    - Chybovost (počet ztracených/zahozených paketů na portech),
    - Události přihlášení uživatelů, zejména administrátorů,
    - Stav a výkon firewallu u prvků kde je součástí,
    - Počet připojených klientů pro bezdrátové prvky,
    - Síla signálu (kvalita připojení klientů) u bezdrátových prvků,
    - Konfigurační změny
    - Kontrola stavu konektivity zadavatele
  + Tiskárny
    - Počty vytištěných stránek,
    - Stav tiskového média (toner nebo inkoust),
    - Chybové stavy tiskových úloh,
    - Notifikace údržby – informace o potřebě údržby nebo výměny dílu
  + Koncové stanice a servery Windows
    - Zaplnění systémového disku
  + UPS
    - Úroveň nabití,
    - Zbývající doba běhu,
    - Matriky napájení – vstupní a výstupní napětí, frekvence,
    - Aktuální zátěž (procento kapacity),
    - Dodávaný výkon ve Wattech,
    - Události a alarmy,
    - Stav baterie
* Nastavení pravidel notifikací:
  + Definice a popis pravidel notifikací pro jednotlivé typy zařízení,
  + Nastavení prahových hodnot s přihlédnutím k
  + Co největší eliminace false positive alertů,
  + Definice skupin pro příjem notifikací z jednotlivých zařízení, rozdělené dle typu zařízení a jeho umístění,
  + Definice frekvence zasílání notifikací,
  + Vytvoření standardní šablony notifikací (formát a obsah) pro usnadnění orientace v hlášeních
* Nastavení přístupových práv pro administrátory,
* Definice neadministrátorských rolí v systému a nastavení oprávnění podle typu role a oblasti sledování (umístění, typ zařízení),
* Integrace s dalšími dohledovými systémy zákazníka, pokud existují,
* Vytvoření group policy nebo jiné automatické řešení pro Windows zařízení, které bude bez manuálního zásahu administrátora nastavovat Windows zařízení – zapne podporu SNMP a nakonfiguruje ji pro automatické rozpoznání dohledovým systémem,
* Vytvoření manuálu pro přidávání nových zařízení do monitoringu a vyřazování trvale odpojených
* Do provozního monitoringu bude implementováno aktivní emailové alertování.

Zvýšení úrovně bezpečnosti přístupu k informacím

Migrační práce zahrnují přechod ze stávajícího systém Microsoft Exchange 2013 onpremise do cloudových sužeb v rámci zvýšení úrovně bezpečnosti přístupu k informacím.

**Analýza a audit aktuální infrastruktury:**

* Zmapování současného systému Microsoft Exchange 2013:
  + Počet poštovních schránek, jejich velikost a typy (uživatelské, sdílené, systémové).
  + Nastavení domén, aliasů, skupin, MX záznamů.
  + Použití kalendářů, úkolů a dalších funkcí poštovního systému
* Identifikace integrací s třetími stranami:
  + Aplikace třetích stran využívající e-mailové služby.
  + Procesy a skripty, které interagují s Microsoft Exchange.

**Analýza požadavků na nový systém pro spolupráci:**

* Počet licencí a jejich typ.
* Specifické požadavky zadavatele na bezpečnost a compliance (např. zdravotnické normy GDPR, HIPAA).
* Integrace se systému provozovanými zadavatelem

**Technické požadavky na migraci:**

* Přenos dat mezi servery Microsoft Exchange a nového Systému pro spolupráci.
* Dostupnost a šířka pásma internetové konektivity
* Nutnost migrace mimo pracovní dobu

Migrační práce

**Návrh migrace a konfigurace prostředí**

* Návrh struktury uživatelů, schránek a oprávnění v rámci systému pro spolupráci
* Návrh struktury pro sdílené schránky
* Návrh konektorů pro interní aplikace a systémy zadavatele
* Příprava uživatelských skupin a účtů pro správu prostředí
* Návrh migračního plánu pro provedení migrace mezi systémy

**Příprava systému pro spolupráci:**

* Registrace a vytvoření tenanta systému pro spolupráci.
* Vytvoření výchozího správce tenanta systému pro spolupráci a nastavení hesla.
* Přidání domény tenanta systému pro spolupráci.
* Základní ověření domény tenanta systému pro spolupráci.
* Nastavení DNS záznamu dle doporučení systému pro spolupráci.
* Synchronizace uživatelů z onpremise Active Directory do systému pro spolupráci

1. **Microsoft Exchange 2013**

* Záloha schránek uživatelů a osobních dat
* Zjištění celkového počtu migrovaných schránek a jejich velikost.
* Export schránek uživatelů do CSV pro nastavení migračních dávek.
* Povolení portů pro nastavení migračních úloh.
* Vytvoření testovací migrační dávky.
* Vytvoření migračního bodu testovací migrační dávky.
* Aktivace testovacího migračního dávky.
* Ověření úspěšného dokončení testovacího migrační dávky.
* Vytvoření produkční migrační dávky z CSV seznamu schránek uživatelů.
* Vytvoření migračního bodu produkční migrační dávky.
* Aktivace produkční migrační dávky.
* Monitorování migrace a oprava nepodařených migrací.
* Ověření úspěšného dokončení produkční migrační dávky.
* Ověření úspěšného přesunu schránek do systému pro spolupráci.
* Ověření fungování schránek po přesunu (odeslaní, příjem).

1. **Hybridní stav Microsoft Exchange – systému pro spolupráci:**

* Aktivace patřičných licencí dle požadavků.
* Ruční přiřazení licenci jednotlivým schránkám dle pravidel.
* Nastavení oprávnění a rolí.
* Vytvoření a nastavení skupin (bezpečnostní, distribuční, dynamické, týmové atd.).
* Vytvoření konektoru pro zařízeni (tiskárny, informační systémy atd.), které nezvládají nové ověřování pro posílání emailu přes systému pro spolupráci.
* Rekonfigurace informačních systému, tiskáren a jiných zařízení využívajících pro zasílaní upozornění email.
* Nastavení pravidel pro velikost schránek, maximální velikost zasílané zprávy atd. a automatické činnosti po jejich dosažení nebo překročení.

1. **Ukončení hybridního stavu Microsoft Exchange – systému pro spolupráci:**

* Změna hodnoty MX záznamu dle doporučení tenantu systému pro spolupráci
* Ověření doručování dle nového MX záznamu.
* Na koncových stanicích v programu Outlook zrušit profil pro připojení ke starému řešení
* Na koncových stanicích v programu Outlook nastavit nový profil pro připojení k uživatelské schránce k systému pro spolupráci
* Nastavení připojení alternativních programu pro přístup k emailové poště.
* Export kontaktů do .csv.
* Import kontaktů v Outlooku pomocí „Import/Export“ z .csv.
* Export kalendáře do .ics.
* Import kalendáře v Outlooku pomocí „Import/Export“ z .ics.
* Pro větší množství migrovaných kontaktů a kalendářů je nutno použít nastroj třetích stran, například MigrationWiz, Codetwo atd.
* Ověření úspěšného odeslaní a přijmu emailů z nově nastavené schránky.
* Zrušení migrační úlohy a migrační dávky
* Instalace a nastavení Microsoft Entra Connect, pokud je požadována synchronizace objektů z AD
* Připojení sdílených schránek dle požadavků

1. **Po migrační práce:**

* Záloha Microsoft Exchange a ukončení všech jeho služeb.
* Nastavení zálohování systému pro spolupráci na NAS nebo jiné vhodné uložiště.
* Kontrola smazání všech DNS záznamů směřujících na Microsoft Exchange (SPF, DKIM, DMARC atd.).
* Vypnutí serveru Microsoft Exchange.
* Školení administrátorů pro správu systému pro spolupráci v rozsahu 2 MD
* Školení uživatelů pro plné využívání služeb systému pro spolupráci v rozsahu 2 MD
* Ověření fungování webového přístupu ke schránce.
* Nastavení MFA, pokud je požadováno.
* Analýza logů v systému pro spolupráci.
* Nasazení automatizace procesů (Power Automate), pokud je požadováno.
* Integrace systému pro spolupráci s nástroji, které organizace používá (např. CRM, ERP).
* Vytvoření a nastavení sdílených kalendářů (dovolená, zasedačka, auta atd.), pokud je požadováno.
* Dokumentace skutečného provedení.

Konfigurace zálohování systému pro spolupráci

**Konfigurace cíle záloh**

* Zapojení NAS do oddělené VLAN, zajištění oddělení od ostatních VLAN,
* Konfigurace NAS podle následujících minimálních požadavků:
  + Vytvoření volume s fault tolerancí minimálně jednoho disku,
  + Konfigurace NAS pro automatický start při obnově napájení,
  + Napojení na UPS a konfigurace řízeného vypínání,
  + Povolení Wake on Lan pro zapínání pomocí UPS,
  + Vytvoření šifrovaného svazku, uložení klíčů do datového trezoru a zajištění automatického připojení po restartu zařízení,
  + Aktualizace na nejnovější verze systému a balíčků,
  + Konfigurace zasílání notifikací administrátorům pro úroveň upozornění Warning,
  + Vytvoření sdílené složky jako cíle záloh,
  + Definice uživatelského účtu s oprávněním pouze na tuto složku
* Konfigurace přístupu pomocí protokolu SMB verze 2 a vyšší, zákaz SMBv1

**Konfigurace zálohovacího procesu**

* Konfigurace dedikovaného virtuálního serveru pro provoz zálohovacího nástroje,
* Konfigurace přístupu do internetu a k datovým úložištím pro zálohy,
* Instalace zálohovacího nástroje,
* Napojení na tenant formou aplikace,
* Konfigurace záloh systému pro spolupráci prostředí v rozsahu zahrnujícím minimálně:
  + mailboxy uživatelů a shared mailboxy,
  + Stránky dokumentových knihoven,
  + Osobní úložiště
* Konfigurace oddělených úloh pro jednotlivé typy obsahu se spouštěním minimálně jedenkrát denně,
* Konfigurace retenčních politik,
* Konfigurace notifikací o průběhu zálohování,
* Vytvoření dokumentace procesu zálohování a kontroly záloh

Implementační bezpečností testy

S ohledem na ZKB a požadavky na bezpečnost budou prováděny pravidelné bezpečnostní testy ve čtyřech fázích v průběhu implementace jednotlivých technologií.

* Instalace a konfigurace nástroje pro detekci zranitelností (otevřené porty, chybějící aktualizace, známé zranitelnosti síťových prvků, operačních systémů nebo aplikací),
* Zpřístupnění všech subnetů pro testovací nástroj

**Postup testování**

* Definice cílů skenování v každé fázi testování – servery, routery, switche, pracovní stanice atd. podle aktuálního postupu implementace,
* Shromáždění informací o připojených zařízeních,
* Instalace a konfigurace testovacího nástroje na dedikované stanici, instalace nejnovějších verzí testovacích pluginů, definic zranitelností atd.,
* Naplánování skenování na vhodnou denní dobu dle typu skenovaných zařízení (v době jejich provozu),
* Způsoby detekce budou zahrnovat skenování portů, kontrolu dostupných služeb a identifikaci verzí obsahující známé zranitelnosti,
* Bude generována zpráva, která shrne nalezené problémy včetně možností jejich řešení,
* V průběhu testování se nástroj nebude pokoušet o aktivní použití nalezených zranitelností, ale pouze na jejich detekci,
* Testovaná zařízení budou všechna zařízení připojená k síti, ať jde o síťový prvek, server, koncovou stanici, tiskárnu nebo jiné zařízení, včetně zařízení, která nebyla definována v plánu testování,
* Testování bude prováděno opakovaně

**Oblasti testování budou zahrnovat:**

* Operační systémy – zranitelnosti v běžných OS jako Windows, Linux a MacOS,
* Aplikace – zranitelnosti v přístupných aplikacích a službách (webservery, databázové systémy, mail servery..)
* Síťová zařízení – zranitelnosti v routerech, switchích a dalších prvcích sítě včetně firewallu,
* Konfigurační nedostatky – nesprávné nebo ne zcela bezpečné konfigurace dostupných služeb a zařízení,
* Detekce nezměněných defaultních přihlašovacích údajů,
* Detekce neplatných nebo expirovaných certifikátů a slabých verzí šifrování.

**Testování bude prováděno průběžně, tedy v těchto fázích:**

* 1. po implementaci hardwarových zařízení
* 2. po migraci aplikací a doménových služeb
* 3. po migraci aplikací a služeb během zkušebního i ostrého provozu
* 4. po skončení implementace všech prvků hardwarových i softwarových,

Výstupem bude vždy technický report popisující nalezené problémy a jejich množná řešení, v poslední fázi navíc i manažerské shrnutí nalezených problémů a jejich dopadů

Ošetření nálezů z penetračních testů

V rámci penetračních testů bylo nalezeno několik problémů týkajících se konfigurace stávajících systémů a technologií provozovaných v datovém centru. V rámci implementace dojde k nápravě těchto nálezů a vyřešení bezpečnostních problémů vycházejících z penetračních testů.

Obecně se jedná o tyto nálezy:

* Active Directory konfigurace a vynucení komplexity používaných hesel
* Technologie datového centra nesmí používat defaultní hesla od výrobce
* Technologie používají porty, skrze které lze zařízení ovládat, je nutné aplikovat ACL
* Odstranění používání zastaralých protokolů např. SMB v1, TLS v1, FTP anonymous apod.
* Nasazení MFA na služby, které jsou používané v internetu
* Zabezpečení SNMP protokolu v rámci datového centra

Ošetření nálezů z penetračních testů

V rámci penetračních testů bylo nalezeno několik problémů týkajících se konfigurace stávajících aktivních prvků a technologií provozovaných v datovém centru. V rámci implementace dojde k nápravě těchto nálezů a vyřešení bezpečnostních problémů vycházejících z penetračních testů.

Obecně se jedná o tyto nálezy:

* Technologie používají porty, skrze které lze zařízení ovládat, je nutné aplikovat ACL
* Odstranění používání zastaralých protokolů např. TLS v1, FTP anonymous apod.
* Zabezpečení SNMP protokolu v rámci datového centra
* Omezení prostupu mezi subnety v rámci interní sítě

Třetí fáze projektu - zkušební provoz

V rámci zkušebního provozu bude probíhat testování a validace veškerých dodaných technologií, migrací aplikací, aktivních prvků.

Čtvrtá fáze projektu – ostrý provoz

Spuštění ostrého provozu infrastruktury po akceptaci dílčích částí.

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.

Implementační dokumentace

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.

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.

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.

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

Zapracování konkrétní 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.

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.

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.

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.

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 opsány oblasti, který se nálezy týkají. Součástí této kapitoly dokumentace bude seznam ošetřených nálezů, které vycházejí z penetračních testů. Neošetřené nálezy budou zdůvodněny.

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.

1. **Akceptační testy**
   * Záznam výsledků všech akceptačních testů, včetně případných odchylek a jejich řešení.
   * Potvrzení splnění všech akceptačních kritérií a schválení zadavatelem.
2. **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.
3. **Změnové řízení**
   * Přehled všech změn oproti původnímu plánu a jejich důvody.
   * Záznam schválení změn zadavatelem.
4. **Závěrečné shrnutí a doporučení**
   * Návrhy na budoucí zlepšení a doporučení pro další rozvoj.
   * Přehled potenciálních rizik nebo problémů, které mohou nastat v budoucnu.

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: Datové centrum, Logmanagement, Monitoring síťového provozu, Aktivní prvky.

**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 – viz. Tabulka.
* Školení administrátorů
* 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
    - Zranitelnosti
    - Ostatní
  + Práce spojené s mitigací nálezů z testů zranitelnosti během implementace
  + Doplnění firewallové soustavy do režimu vysoké dostupnosti - zapojení, instalace a migrace nového UTM Firewallu v DC
* Instalace a zprovoznění 802.1x s NAC server v celé organizaci
* Zapojení, instalace, konfigurace CORE 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 treshholdů, konfigurace politik a automatického vyhodnocování potencionálních incidentů.
* Implementace nástroje pro bezpečný přístup k informacím
  + Zprovoznění, konfigurace, propojení se stávajícím prostředím
  + Konfigurace zabezpečení včetně MFA
  + Zprovoznění, konfigurace a migrace dalších cloudových aplikací (teamová spolupráce, plánování projektů, automatizace/elektronizace firemních procesů, interní aplikace intranetu atd.)
* Zajištění koordinace všech zúčastněných stran a dodavatelů technologií
* Implementační dokumentace
* Dokumentace skutečného provedení

Harmonogram projektu

Časový přehled plnění projektu

Dnem začátku plnění je den podpisu smlouvy, čas T0.

Termínem se rozumí nejzazší termín pro splnění dané fáze.

|  |  |  |
| --- | --- | --- |
| Fáze | Činnosti | Termín |
| Fáze projektu 1 | | |
| Dodávka HW a SW | Kompletní dodávka hardware a software, zahoření a základní konfigurací nových serverů, diskových polí, zálohovací sever, zálohovací úložiště a ostatních technologií. Součástí jsou též licence a pomocný materiál nutný pro zapojení do stávajícího datového centra | T0 + 90 dní |
| Vytvoření implementační dokumentace | Vytvoření implementační dokumentace dle ZD | T0 + 90 dní |
| Převzetí 1. Fáze | Převzetí 1. Fáze | T0 + 90 |
|  |  |  |
| Fáze projektu 2 | | |
| Implementace | Migrace serverů, dat, aplikací, služeb Active directory, DNS a DHCP služeb na nové servery, revize a zabezpečení domény. Implementace aktivních prvků řízení přístupu do sítě, monitoring provozní a detekce síťových anomálií implementace centrálního systému pro logování a implementace zvýšení bezpečnosti přístupu k informacím. | T0 + 240 dní |
| Převzetí 2. Fáze | Převzetí 2. Fáze |  |
| Fáze projektu 3 | | |
| Zkušební provoz | Testovací provoz všech součástí infrastruktury. | 15. 3. 2026 – 15.4.2026 |
| Dokumentace a školení | Předání dokumentace skutečného provedení a zaškolení administrátorů. | Do 15.4.2026 |
| Akceptace infrastruktury a jejích dílčí součástí | odstranění nedostatků z penetračních testů, akceptace jednotlivých částí projektu. | 15.4. 2026 |
| Převzetí 3. Fáze | Převzetí 3. Fáze |  |
|  |  |  |
| Fáze projektu 4 | | |
| Ostrý provoz | Spuštění ostrého provozu infrastruktury po akceptaci dílčích částí | Od 15.4.2026 |

Akceptační testy

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

.

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 |  |
| Kontrola napájení zařízení | Vizuální kontrola. Napájení zařízení je dle požadavků ZD. Přívodní napájecí kabely jsou řádně fyzicky označeny štítkem identifikujícím napájené zařízení. | ANO / NE |  |
| Kontrola verze OS (firmware) | Kontrola z CLI. Firmware v rámci jednotlivých zařízení je sjednocený na poslední STABLE / doporučovanou verzi. | ANO / NE |  |
| Kontrola IP adresace | Kontrola z CLI. Adresace jednotlivých VLAN sítí a terminace jejich SVI rozhraní je provedena dle ZD.  Kontrola specifických VLAN – L2 transportní VLAN, VLAN terminované na FW dle ZD. | ANO / NE |  |
| Kontrola přístupových pravidel pro jednotlivé VLAN sítě (ACL) | Kontrola z CLI. Je provedena kontrola přístupových pravidel (ACL záznamů pro jednotlivé VLAN) dle ZD. | ANO / NE |  |
| Redundance CORE přepínačů | Vizuální kontrola toho, že CORE přepínače jsou připojeny na separátních napájecích okruzích. Odpojením jednoho ze zdrojů od elektrického napájení nedojde k výpadku zařízení připojených k ATS. | ANO / NE |  |
| Přihlášení přes SSH – oprávněné. | Test bude proveden kontrolou úspěšného přihlášení uživatele s definovaným administrátorským profilem z povolené IP adresy pomocí protokolu SSH. Uživatel se úspěšně přihlásí a přepne do konfiguračního módu. | ANO / NE |  |
| Přihlášení přes SSH – nepovolená IP adresa | Test bude proveden kontrolou neúspěšného přihlášení uživatele s definovaným administrátorským profilem z nepovolené IP adresy pomocí protokolu SSH. Uživatel se nepřihlásí na firewall. | ANO / NE |  |
| Synchronizace času | Kontrola správného s NTP serverem synchronizovaného 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 |  |

Akceptační protokol firewall

|  |  |  |  |
| --- | --- | --- | --- |
| Kontrola označení UTM zařízení | Kontrola fyzická +  CLI / WEB. Je provedeno řádné fyzické označení všech zařízení dle jmenné konvence.  Zařízení mají odpovídající management adresu dle ZD. | ANO / NE |  |
| Kontrola infrastrukturního propojení (uplinky) | Kontrola fyzická + CLI / WEB. Propojení (uplinky) jednotlivých zařízení je provedeno dle ZD. Je provedeno řádné označení všech propojů (uplinků) v rámci popisů (description) rozhraní dle ZD. | ANO / NE |  |
| Kontrola verze OS (firmware) | Kontrola z CLI / WEB. Firmware v rámci jednotlivých zařízení je sjednocený na poslední STABLE / doporučovanou verzi. | ANO / NE |  |
| Kontrola zalicencování UTM funkcionalit | Kontrola zalicencování UTM funkcionalit a délky jejich subscriptions. | ANO / NE |  |
| Kontrola nastavení UTM FW a FW / NAT pravidel | Kontrola nastavení UTM FW a pravidel mezi jednotlivými rozhraními / zónami FW. | ANO / NE |  |
| Přihlášení přes SSH – oprávněné. | Test bude proveden kontrolou úspěšného přihlášení uživatele s definovaným administrátorským profilem z povolené IP adresy pomocí protokolu SSH. Uživatel se úspěšně přihlásí a přepne do konfiguračního módu. | ANO / NE |  |
| Přihlášení přes SSH – nepovolená IP adresa | Test bude proveden kontrolou neúspěšného přihlášení uživatele s definovaným administrátorským profilem z nepovolené IP adresy pomocí protokolu SSH. Uživatel se nepřihlásí na firewall. | ANO / NE |  |
| Přihlášení přes SSH – bez profilu | Test bude proveden kontrolou neúspěšného přihlášení uživatele bez definovaného profilu z povolené IP adresy pomocí protokolu SSH. Uživatel se nepřihlásí na firewall. | ANO / NE |  |
| Přihlášení přes HTTPS – oprávněné | Test bude proveden kontrolou úspěšného přihlášení uživatele s definovaným administrátorským profilem z povolené IP adresy pomocí grafického rozhraní přes HTTPS. Uživatel se úspěšně přihlásí. | ANO / NE |  |
| Přihlášení přes HTTPS – nepovolená IP adresa | Test bude proveden kontrolou neúspěšného přihlášení uživatele s definovaným administrátorským profilem z nepovolené IP adresy pomocí grafického rozhraní přes HTTPS. Uživatel se nepřihlásí na firewall. | ANO / NE |  |
| Přihlášení přes HTTPS – bez profilu | Test bude proveden kontrolou neúspěšného přihlášení uživatele bez definovaného profilu z povolené IP adresy pomocí grafického rozhraní přes HTTPS. Uživatel se nepřihlásí na firewall. | ANO / NE |  |
| Přihlášení přes konzolový port – oprávněné | Test bude proveden kontrolou úspěšného přihlášení uživatele s definovaným administrátorským profilem Uživatel se úspěšně přihlásí. | ANO / NE |  |
| Přihlášení přes konzolový port – neoprávněné | Test bude proveden kontrolou neúspěšného přihlášení uživatele bez definovaného profilu. Uživatel se nepřihlásí na firewall. | ANO / NE |  |
| Otevřené porty na firewallu – outside interface | Test bude proveden pomocí nástroje Nmap. Spustí se test pro skenování otevřených TCP a UDP portů na veřejné adrese firewallu. Test ověří, že jsou na veřejné adrese otevřeny pouze požadované porty | ANO / NE |  |
| Navázání VPN – oprávněné | Test bude proveden kontrolou úspěšného navázání VPN pomocí SSL klienta s definovaným uživatelským účtem v AD. VPN se úspěšně sestaví a uživatel bude mít přístup na definované zdroje. | ANO / NE |  |
| Navázání VPN – neoprávněné | Test bude proveden kontrolou neúspěšného navázání VPN pomocí SSL klienta s nedefinovaným uživatelským účtem v AD. Přihlášení se nezdaří. | ANO / NE |  |
| Redundance UTM firewallů | Bude odpojen primární UTM FW, po jeho odpojení bude jeho role převzata sekundárním UTM FW.  Po opětovném připojení primárního UTM FW, dojde opět k převzetí primární role. | ANO / NE |  |

Akceptační protokol implementace ověřování 802.1X

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Instalace | Kontrola instalace nástroje pro ověřování 802.1X | ANO / NE |  |
| Komunikace | Ověření komunikace nástroje s aktivními prvky a RADIUS pro ověřování zařízení a uživatelů | ANO / NE |  |
| RADIUS failover | Ověření RADIUS failover komunikace | ANO / NE |  |
| Přihlášení do sítě EAP-TLS – oprávněné + přihlášení uživatele | Tento test bude proveden kontrolou úspěšného přihlášení stanice (korporátní PC v nové doméně) s nastaveným suplikantem pro ověřování certifikátem a validním certifikátem.  Kontrola stavu autentizace na portu přepínače | ANO / NE |  |
| Přihlášení do sítě MAB - oprávněné | Tento test bude proveden kontrolou úspěšného přihlášení tiskárny s definovaným profilem na NPS serveru.  Kontrola stavu autentizace na portu přepínače | ANO / NE |  |
| Přihlášení do sítě EAP-TLS – neoprávněné | Tento test bude proveden kontrolou neúspěšného přihlášení stanice se správně nastaveným suplikantem pro ověřování pomocí certifikátu, ale s neplatným certifikátem (revokovaným na CA). | ANO / NE |  |
| Přihlášení do sítě MAB - neoprávněné | Tento test bude proveden kontrolou neúspěšného přihlášení tiskárny s nedefinovaným profilem na NPS serveru. | ANO / NE |  |
| MAC Baypass | Ověření MAC-base bypass autentizace |  |  |
| Log management | Ověření napojení na centrální log management | ANO / NE |  |

Akceptační protokol virtualizace datového centra

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Správné fyzické umístění | Vizuální kontrola. Umístění zařízení do rozvaděčů. Je provedeno fyzické označení všech zařízení dle jmenné konvence. | 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 | 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 |  |
| Napájení | Zdroje serveru jsou připojené redundantně, každý na jinou napájecí větev? | ANO / NE |  |
| Síťová konektivita | Servery jsou redundantně připojené do aktivních prvků dle dokumentace. Po odpojení jedné větve nedochází ke ztrátě komunikace? | ANO / NE |  |
| HW Konfigurace | Odpovídá HW konfigurace zadávací dokumentaci? | ANO / NE |  |

Akceptační protokol diskových polí a SAN infrastruktury

|  |  |  |  |
| --- | --- | --- | --- |
| Název testu | Postup ověření | Výsledek | Výhrady |
| Kontrola aktuálnosti firmware | Aktuální firmware disků, controllerů, zdrojů | ANO / NE |  |
| Přístupy | Pro přístup se používají hesla dle dokumentace, přístup je pouze skrze šifrované připojení | ANO / NE |  |
| Konfigurace RAID | Kontrola nastavení RAID svazků dle dokumentace | ANO / NE |  |
| Napájení | Zdroje pole jsou připojené redundantně, každý na jinou napájecí větev | ANO / NE |  |
| Síťová konektivita | Pole je redundantně připojené do aktivních prvků dle dokumentace. Po odpojení jedné větve nedochází ke ztrátě komunikace | ANO / NE |  |
| HW Konfigurace | Odpovídá HW konfigurace zadávací dokumentaci? | ANO / NE |  |

Akceptační protokol virtualizace produkčního a VDI datového centra

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Kontrola nastavení Hypervisor | Instalovaná poslední stabilní verze, nastavení dle best practise | 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 postupně 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 virtuálku 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 |  |

Akceptační test zálohování

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Zálohovací SW | Instalovaná poslední stabilní verze, včetně všech patchů? | ANO / NE |  |
| Kontrola nastavení záloh | Je provedeno nastavení záloh pro všechny zdroje, funkční backup proxy, připojení úložiště, nastavení časových plánů? | ANO / NE |  |
| Backup recovery | Obnovení dat z hlavního zálohovacího úložiště, test funkčnosti síťových služeb | ANO / NE |  |
| Monitoring | Monitoring sleduje virtualizační prostředí, HW, zálohovací software. Monitoring odesílá emaily administrátorovi v případě problémů | ANO / NE |  |

Akceptační testy 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 adesář 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 fungová 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? |  |  |
| DHCP Failover | Pro všechny Scopes je nakonfigurována funkcionalita DHCP faiover dle dokumentace. |  |  |
| Otestování funcionality DHCP | Adresy všech SCOPES jsou přidělovány, funcionalita DHCP faiover je otestována? |  |  |
| Internet DNS | Na obou DNS funguje resolvování internetových doménových jmen | ANO / NE |  |
| Aging | Funkcionalita Aging je nakonfigurována a funkční? |  |  |
| Scavenging | Funkcionalita Scavenging je nakonfigurována a funkční? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Členství v doméně | Všechny nové servery Windows se nacházejí v doméně zadavetele, kromě serverů uvedených v tabulce „Servery mimo doménu“ v zadávací dokumentaci. | ANO / NE |  |
| Členství v doméně | Všechny nové stanice Windows se nacházejí v doméně zadavatele. | ANO / NE |  |
| Jmenné konvence | Všechny nové servery maji název dle instrukcí uvedených v tabulce „Jmenná konvence“ a „IP adresní plán nový“ v zadávací dokumentaci. | ANO / NE |  |
| Jmenné konvence | Všechny nové servery maji přidělenu adresu dle tabulky„IP adresní plán nový“ v zadávací dokumentaci. | ANO / NE |  |
| Users | Active direcory obsahuje uživatelské účty uvedené v tabulce „Uživateské účty“ v zadávací dokumentaci. | ANO / NE |  |
| Groups | Active direcory obsahuje skupiny přístupu uvedené v tabulce „Groups – uživatelé“ v zadávací dokumentaci. | ANO / NE |  |
| DHSCP Failover | Vypnutím SRV-DC1 nedošlo k problémům s přidělováním a obnovováním adres koncovým zařízením. | ANO / NE |  |

Akceptační testy aplikačních serverů

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Kontrola instalace rolí | Kontrola nainstalovaných rolí na daném serveru, zdali odpovídají dokumentaci | ANO / NE |  |
| Členství v doméně | Je server členem domény? | 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 |  |

Akceptační testy 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 practise 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 akuální problémy na email | ANO / NE |  |
| Auditování | Systém audituje důležité aktivity v systému | ANO / NE |  |
| Aktualizace | Systém pravidelně aktualizuje databázi zranitelností, signatur a detekcí z online zdrojů | ANO / NE |  |

Akceptační protokol systému pro spolupráci

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Ověření funkcionalit | Ověření funkcionalit navrhovaného řešení, jestli splňují kritéria v ZD | ANO / NE |  |
| Zabezpečení | Kontrola zabezpečení dodaného řešení dle ZKB a zadávací dokumentace | ANO / NE |  |
| Ověření licencí | Ověření, že dodaná licence splňuje kritéria specifikovaná v ZD | ANO / NE |  |
| Ověření nasazení | Ověření, zdali je řešení nasazeno ve formátu, rozsahu a kvalitě, kterou požaduje ZD | ANO / NE |  |
| Kompatibilita | Ověření kompatibility s používanými zařízeními na straně zadavatele | ANO / NE |  |
| Napojení | Ověření všech systémů napojených na nové řešení z hlediska funkcionality a otestování komunikace | ANO / NE |  |
| Test uživatelé | Ověření funkcionality na uživatelské stanici s připojením do nového řešení | ANO / NE |  |
| Migrace dat | Ověření že došlo k přenosu všech dat, konfigurací, které byly součástí ZD (emaily, osobní data, konfigurace…) | ANO / NE |  |
| Struktura dat | Zachování struktury dat a uživatelských objektů | ANO / NE |  |
| Oprávnění | Ověření správné konfigurace oprávnění pro jednotlivé uživatele | ANO / NE |  |
| Automatizované procesy | Implementace automatizovaných procesů, funkčnost v rámci definované v ZD | ANO / NE |  |
| Dodání zálohovacího HW | Konfigurace dodaného HW pro zálohování systému odpovídá ZD |  |  |
| Konfigurace zálohování | Funkce SW pro zálohování software pro spolupráci a jeho konfigurace, ověření záloh odpovídá ZD |  |  |
| Dokumentace | Ověření dokumentace a jejího obsahu vzhledem k požadavkům v zadávací dokumentaci | ANO / NE |  |
|  |  |  |  |

Akceptační protokol testování zranitelností

|  |  |  |  |
| --- | --- | --- | --- |
| **Název testu** | **Postup ověření** | **Výsledek** | **Výhrady** |
| Nástroj na testování | Implementovaný nástroj na testování zranitelností | ANO / NE |  |
| Funkce nástroj | Funkce odpovídají požadavkům v ZD | 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 |  |

Akceptační test 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 |  |

Akceptační test 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 |  |

Akceptační test 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. |  |  |
| Kontrola úplnosti | Kontrola přítomnosti všech systémů, zařízení, technologií a aplikací v dokumentaci | ANO / NE |  |
| Kontrola visuálních diagramů | Kontrola všech schémat zapojení, propojů a dalších grafických prvků v dokumentaci | ANO / NE |  |
| Kontrola postupů | Kontrola přítomnosti všech postupů pro zajištění kontinuity dle zadávací dokumentace | ANO / NE |  |