Technická specifikace dílčí části B) Konsolidace LAN a bezpečnostní infrastruktura TC ORP

Vymezení předmětu dodávky – technické specifikace

Informace a údaje uvedené v oddílu - **Vymezení předmětu dodávky – technické specifikace**, v tomto dokumentu vymezují závazné požadavky technických specifikací zadavatele na plnění veřejné zakázky. Tyto požadavky je uchazeč povinen respektovat v plném rozsahu při zpracování své nabídky.

Uchazečem nabízené řešení musí splňovat (pokud není výslovně uvedeno jinak) níže uvedené požadavky a parametry, které jsou definovány jako minimální a musí být **splněny nebo překročeny**.

Splnění zde uvedených požadavků je nezbytnou podmínkou hodnocení uchazeče v zadávacím řízení.

Nabízené řešení musí respektovat existující datovou a aplikační infrastrukturu v prostředí LAN/WAN, která zajišťuje provoz aplikací zadavatele – více viz Příloha č. 4 - Popis stávajícího stavu.

Předmětem plnění je dodání níže uvedeného HW, SW a to v těchto oblastech:

Dvouúrovňová (dvoufaktorová) autentizace
Dodání vhodného technického řešením pro ověřování identity uživatelů za použití USB a OTP tokenů zaručujícím vysokou úroveň bezpečnosti.

Základní požadavky

- Zadavatelem je kladen velký důraz na kompatibilitu dodaného řešení s dnes provozovaným HW (PC, grafické terminály – zero client) a operačním systémem (desktopy/serverů), včetně využívaného VDI prostředí - viz Příloha č. 4 - Popis stávajícího stavu.

- 1x SW autentizační server – s možností integrace na stávající ověřovací službu.
- 120x USB token –pro uložení digitálních certifikátů:
  - ochrana obsahu tokenu pomocí PINu,
  - podpora - MS-CAPI and PKCS#11,
  - možnost použití bez nutnosti instalace driveru nebo middleware vrstvy,
  - podpora Auto-Enrollment pro držitelé tokenů (automatická obnova doménových certifikátu),
  - úložný prostor 64KB,
  - plná kompatibilita s USB 1.1/2.0.
  - Možnost využití tokenů při přihlašování do klientského operačního systému zadavatele s vazbou na stávající ověřovací službu AD/LDAP - dvouúrovňová autentizace.
  - Možnost využití tokenů při přihlašování ke službě CzechPoint.

- 10x OTP token (One Time Password):
  - neomezená platnost licence tokenu,
  - plná podpora software klienta (SSL VPN a IPSec VPN) pro potřeby realizace šifrovaného spoje a autentizaci administrátorů vůči stávajícímu centrálnímu Firewallu - viz Příloha č. 4 - Popis stávajícího stavu.

Sběr logů, analýza dat - SIEM

Dodání a implementace SW pro aktivní dohled nad technickým stavem HW a SW s důrazem na bezpečnost celé provozované IT infrastruktury.

Základní požadavky

- sběr událostí z HW prvků sítě (switche, servery, routry, apod.),
- sběr událostí z SW aplikací – aplikační logy (Evenlog, DNS, DHCP, syslog apod.),
- aktivní monitorování provozu na perimetru lokální sítě (firewall),
- možnost přijmu a zpracování informací o datových tocích v síti (formáty NetFlow, IPFIX, Jflow, Sflow). Sondy mohou být od různých výrobců a musí být integrovatelné bez nutnosti dodatečných úprav na straně SIEM řešení.

- 1x Log Management + SIEM:
  - jednotná zpráva celého prostředí v grafickém režimu,
  - ověřování uživatelů vůči MS Active Directory nebo obecnému LDAP systému - systém ale musí rovněž umožňovat přihlašování pomocí lokálních účtů (v případě nedostupnosti externích autentizačních mechanismů),
  - možností efektivního vyhodnocování bezpečnostních/technických rizik v reálném čase či následné detailní analýzy v čase,
  - možnost trvalého příjmu událostí z logů: minimálně 100 událostí za sekundu,
  - možnost provozu nabízeného řešení i v prostředí virtualizace,
  - licenčně neomezenou velikost úložiště historických dat,
  - pro sběr logů agentním způsobem jsou využíváni softwaroví agenti obsažení v ceně řešení (nejsou zvláště zpoplatněni),
  - možnost agentového i bezagentového způsobu sběru dat z logů,
  - SW agent je schopen provádět dočasné lokální ukládání v případě výpadku komunikace se zbytkem systému,
  - funkce konsolidace, klasifikace, filtrace a vyhodnocení na základě pravidel,
  - korelace síťových událostí pro efektivnější analýzu dat,
  - možnost vytvářet vlastní předdefinované dotazy do databáze logů,
  - možnost vytvářet vlastní reporty,
  - pravidelná tvorba reportů minimálně ve formátech PDF a CSV,
  - zasílání email notifikací o zjištěných nestandardních bezpečnostních událostech,
  - aktualizace obsahu (pravidel, sond, apod.) pomocí internetu,
  - schopnost samostatného "učení" normálního stavu - podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií,
  - automatické vytváření souhrnných informací o bezpečnostních hrozbách na základě korelace dílčích událostí,
  - systém musí být schopen využít detekované anomálie a informace ze sítě pro korelaci s logy do jednotných incidentů, pro zpřesnění kontextu a snížení false-positives.

*Poznámka: součásti předmětu technické specifikace dílčí části B),. Článek „*Sběr logů, analýza dat*" není dodávka HW a je předpoklad využití vlastních zdrojů z Technologického centra ORP.*

Diskové subsystémy
Rozšíření stávajícího diskového pole o níže uvedený výčet disků z důvodu alokace dostatečné diskové kapacity pro nově zaváděné systémy a dnes využívaný AIS včetně dostatečné kapacity pro zálohování provozované infrastruktury.

Oblast - produkční diskové pole

- 6x HDD 3,5“ - SAS NearLine, 2TB - 7.2K otáček/s
- 12x HDD 3,5“ - SAS 600GB - 15K otáček/s

Součástí dodávky musí být veškeré potřebné příslušenství, které je třeba pro bezproblémový chod dodaných HDD – v případě potřeby – rozšíření licenční podpory diskového pole, HDD rámečky aj.

Oblast - zálohování

- 6x HDD 3,5“ - SATA III, 4TB - 7.2K otáček/s

Zadavatelem je kladen velký důraz na kompatibilitu dodaných HDD s dnes provozovaným HW. Přesná typová specifikace polí viz Příloha č. 4 - Popis stávajícího stavu.

Aktivní prvky LAN

- 1x Ethernet switch Layer 2:
  - 48 portů 10/100/1000 Base-T, auto-sensing,
  - 2x10Gb/SFP uplink,
  - celková propustnost 170 Gbps,
  - link aggregation, 802.1x, sflow,
  - podpora stohování (stack),
  - PoE podpora standardu IEEE 802.3af. Při maximálním odběru (15,4 W/port) možnost napájení minimálně 24 portů. Možnost připojení externího podpůrného PoE zdroje.
  - podpora IPv4 a IPv6,
  - management (Command-line interface, GUI prostřednictvím web-browseru, SNMP protokol).

Příslušenství:

- 2x Twinax 10Gb SFP – délka 3m,
- 1x PoE podpůrný externí zdroj 600W.

Implementace

- Instalace a konfigurace všech komponent hardware v prostorách zadavatele při součinnosti pracovníků ORP.
- Součástí dodávky musí být veškerá potřebná kabeláž pro oživení a provoz dodaných zařízení.
- Integrace do stávajícího prostředí.
- Testování celkové funkčnosti dodaného řešení.
- Základní uživatelské seznámení a proškolení s dodanou technologií (předpoklad cca 12 hodin).
- Vypracování dokumentace realizovaného řešení.

Záruky a servis

Součástí veškeré dodávané technologie bude záruka na HW a technická podpora (servis - maintenance) na pořízený SW. Záruka (HW) a podpora (SW) zařízení bude realizována dodavatelem případně prostřednictvím odpovídajícího servisního kanálu výrobce.

HW

Záruka na pořízený HW je požadována v rozsahu:

- 3 roky na USB tokeny a OTP tokeny,
- 5 let na HDD disky „Oblast – zálohování“, aktivní prvky LAN (switch),
- HDD disky „Oblast - produkční disková pole“ – zadavatel požaduje nově dodané HDD zahrnout pod již běžící SLA (příslušného diskového pole) – zajistí uchazeč. Nastavený režim SLA (24x7x368), řešení závad s čtyřhodinovou odezvou od nahlášení problému, servis je poskytován výrobcem v místě instalace zařízení. Přesná typová specifikace polí viz Příloha č. 4 - Popis stávajícího stavu.

SW

Technická podpora (servis - maintenance) na pořízený SW je požadována na dobu 5 let.

Podpora bude realizována ve formě tzv. podpory aktualizací SW s možnosti využití linky zákaznické podpory.

Projekt Virtualizace IT a zvýšení bezpečnosti TC v ORP Dvůr Králové nad Labem vč. elektronizace procesů (reg. č. CZ.1.06/2.1.00/22.09367) je financován z prostředků Evropské unie, Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu a z rozpočtu města Dvůr Králové nad Labem.