|  |
| --- |
| Technická specifikace k veřejné zakázce |
| **„****Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“** |
| **Dále též jen „Veřejná zakázka“** |
| **Zadavatel:** |
| **Kancelář veřejného ochránce práv**  Údolní 658/39  602 00, Brno |

OBSAH

[1. Technologie a zkratky 3](#_Toc173601920)

[2. Informace k veřejné zakázce 4](#_Toc173601921)

[2.1. Důvody vyhlášení veřejné zakázky 4](#_Toc173601922)

[2.2. Cíle projektu 4](#_Toc173601923)

[2.3. Předmět projektu 4](#_Toc173601924)

[3. Předmět veřejné zakázky 5](#_Toc173601925)

[3.1. Současný stav 5](#_Toc173601926)

[3.2. Požadované dodávky a základní služby 7](#_Toc173601927)

[3.3. Funkční a nefunkční požadavky 9](#_Toc173601928)

[3.4. Další požadované služby 10](#_Toc173601929)

[4. Technologická a aplikační architektura řešení 13](#_Toc173601930)

[4.1. Prvky technologické a aplikační architektury: 14](#_Toc173601931)

[4.2. Popis technologické a aplikační architektury 15](#_Toc173601932)

[5. Vazba na druhou část veřejné zakázky 16](#_Toc173601933)

[6. Harmonogram 16](#_Toc173601934)

# Technologie a zkratky

|  |  |
| --- | --- |
| AD | Active Directory |
| ADS | Anomaly Detection Systém |
| DMZ | Demilitarizovaná zóna |
| EDR | Endpoint Detection & Response |
| EPS | Events Per Second |
| FW | Firewall |
| HA | High Availability |
| HD | Help Desk |
| IDM | Identity Management |
| IPS | Intrusion Prevention System |
| IS | Informační systém |
| NBD | Next Bussines Day |
| NBAD | Network behavior anomaly detection |
| NDR | Network Detection & Response |
| KVOP | Kancelář veřejného ochránce práv |
| MFA | Multifaktorová autentizace |
| OTP | One Time Password |
| PAM | Privileged Access Management |
| RDP | Remote Desktop Protocol |
| SAN | Storage Area Network |
| SIEM | Security Information and Event Management |
| SLA | Service Level Agreement |
| SOC | Security Operation Centrum |
| TIF | Technologická infrastruktura |
| VLAN | Virtuální LAN |
| ZKB | Zákon č. 181/2014 Sb = Zákon o kybernetické bezpečnosti |

# Informace k veřejné zakázce

## Důvody vyhlášení veřejné zakázky

Veřejná zakázka s názvem „Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv“ (dále jen „Veřejná zakázka“ nebo „Zadávací řízení“) je veřejnou zakázkou na dodávky. Je realizovaná v rámci stejnojmenného projektu, který bude spolufinancován z Integrovaného regionálního operačního programu.

Zadavatel bude projektem realizovat technické opatření dle § 5 odst. 3) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB), z těchto oblastí:

* nástroj pro ochranu integrity komunikačních sítí,
* nástroj pro ověřování identity uživatelů
* nástroj pro ochranu před škodlivým kódem
* nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
* nástroj pro detekci kybernetických bezpečnostních událostí
* nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

## Cíle projektu

Hlavním cílem projektu je pořídit a implementovat bezpečnostní nástroje, pomocí nichž bude možno efektivně spravovat a řídit kybernetickou bezpečnost a vyhovět zákonným požadavkům. Výsledkem projektu bude posílení zabezpečení informačních a komunikačních systémů zadavatele, zesílení schopnosti a připravenosti žadatele předcházet kybernetickým útokům a dalším potenciálním hrozbám a případně je řešit. Všechny zamýšlené aktivity projektu mají přímou vazbu na zvýšení úrovně kybernetické bezpečnosti dle mezinárodních standardů.

Dílčí cíle projektu:

* zvýšit kybernetickou bezpečnost KVOP,
* zajistit bezpečné doručení IT služeb uživatelům KVOP
* zvýšit úroveň zajištění kontinuity chodu úřadu

## Předmět projektu

Předmětem realizace projektu je zajištění komplexní bezpečnosti všech služeb ICT, které využívají uživatelé KVOP. V rámci projektu KVOP provede **modifikaci architektury bezpečnostních řešení**. Tam, kde to jde, chce KVOP opustit koncept řešení ve formě HW appliance (včetně dedikovaných fyzických serverů). Bezpečnostní aplikace chce převést na infrastrukturu virtuálních serverů, což umožní lepší řízení kapacit bezpečnostních služeb. Dalšími aktivitami jsou **náhrady systémů**, které jsou na konci své životnosti a **rozšíření bezpečnostního řešení o nové systémy.** Všechny změny umožní naplnit cíle projektu komplexním bezpečnostním monitoringem ICT prostředků, kontrolou činností registrovaných uživatelů, sledováním datového provozu informační infrastruktury, registrováním útoků na prostředky ICT a průběžným odhalováním případných interních a externích útočníků, atd

# Předmět veřejné zakázky

## Současný stav

### Konceptuální popis

Informační bezpečnost je v současnosti zajišťována takto zajišťována takto:

* Veškeré IS a podpůrné systémy jsou aktuálně provozovány v rámci jediné virtualizace postavené na platformě VMware.
* Business Continuity Management: Zálohování probíhá prostřednictvím produktu Veeam. Primární zálohy jsou umístěny odděleně od produkčního prostředí. Zálohují se celé disky. Přes týden inkrementální zálohování, o víkendu celková záloha. V oddělené lokalitě je umístěna pásková mechanika a další server pro zálohování (aktuálně v procesu zavádění).
* Uživatelské identity jsou spravovány prostřednictvím IDM nástroje Easy IDM a on-premise MS Active Directory. Uživatelé nemají privilegovaná oprávnění v rámci koncových stanic. Jsou používána komplexní hesla (12 znaků, historie 10 předchozích, 1x ročně změna).
* Pro ochranu perimetru je využíván Firewall Kernun zapojený v HA. Firewall je na konci své morální životnosti a zadavatel nepočítá s nákupem maintenance pro tento stávající FW
* Internetové připojení je dublované s automatickým přepojováním protokolem BGP.
* Připojení do vnitřní sítě je řízeno prostřednictvím MS Active Directory. Počítače, které nejsou zavedené, se do sítě nedostanou
* V síti KVOP je provedena segmentace sítě. Jsou oddělené servery a uživatelské stanice, DMZ pro poštu a Exchange OWA a CITRIX Netscaler. Dále VLAN pro management switchů. VLAN pro virtuální diskové pole. WIFI je fyzicky oddělenou sítí
* Provozní monitoring infrastruktury je realizován prostřednictvím produktu Centreon. Ten zajišťuje Performance a Capacity Management
* Logy jsou uchovávány a spravovány prostřednictvím Log Management nástroje od společnosti Balabit (nyní One Identity). Nástroj je provozován ve formě HW Appliance. Zadavatel požaduje migraci na řešení se SW Appliance.
* Monitoring NetFlow a vyhodnocení anomálií v síti je realizována prostřednictvím nástroje od společnosti Flowmon. Je pořízena jedna sonda 4x1 GbE CU s vestavěným kolektorem a instalovaným Anomaly Detection Systémem.
* Pro ochranu koncových stanic a serverů je využíváno antivirového řešení od společnosti Symantec. Cca 15 % stanic je chráněno Microsoft Defenderem. Řešení zajišťuje zejména antivirovou ochranu, nepokrývá však situace, kdy je škodlivý kód do společnosti zavlečen prostřednictvím dosud málo rozšířeného malware (ransomware, APT, zeroday, atd.), jehož chování není na bázi vzorků a signatur dosud není stávajícím antivirovým produktem zmapováno
* V rámci KVOP není využíváno dvou faktorové ověřování (2FA). Dodavatelé a zaměstnanci přistupují prostřednictvím VPN a prostřednictvím RDP serverů na základě zadání jména a hesla
* KVOP využívá monitoring privilegovaných účtů PAM od společnosti Balabit (nyní One Identity). V současnosti jsou nahrávána všechna RDP spojení na servery. Z technických důvodů není dosud monitorován Citrix. Zadavatel požaduje migraci na řešení se SW Appliance.
* Pro management zranitelností je využíváno produktu Nessus od společnosti Tenable.
* KVOP využívá pro řízení bezpečnostních událostí SIEM od společnosti ArcSight. Pro SIEM je dedikován fyzický HW. Zadavatel požaduje migraci na řešení se SW Appliance.
* KVOP v současné době nemá dostatečné kapacity nezbytné k provoznímu zajištění plánovaných bezpečnostních služeb, plánuje využívat služby třetí strany.

### Detailní popis vybraných systémů:

Endpoint Protection systém:

Řešení je nasazeno v rozsahu:

* Symantec Endpoint Security
* Microsoft Defender for Endpoint P1

Firewall Kernun:

Řešení je nasazeno v rozsahu:

* Kernun UTM 200 cluster (HW appliance)
* All-in-one HW+OS+SW
* 8x1 Gbps Ethertnet, 1 x remote console, podpora agregace a redundance interface
* Propustnost IP inspekce 1Gbps per port, proxy inspekce 600 Mbps per port, šifrování 400 Mbps per port
* Podpora NAT/PAT, VLAN, IPv6, SNMP
* QoS – řízení šířky pásma podle uživatele portu i typu souboru
* ukončení TLS / SSL komunikace na FW
* Antivirová kontrola provozu pro HTTP, HTTPs, SMTP, POP3, IMAP4, FTP
* IPS (Intrusion Prevention System) ochrana stanic a uživatelů
* Integrovaná VPN brána (Podpora IPsec a OpenVPN)
* Podpora ICAP rozhraní
* Podpora Autentizace Kerberos
* Podpora Integrace s Microsoft Active Directory včetně řízení dle skupin uživatelů a podpory SSO tj. transparentní autentizace bez nutnosti ověřování mezi klientem a firewallem
* Podpora Syslog, možnost exportu logu
* Řízení a filtrování webového přístupu dle kategorizace obsahu webových stránek (realizovaný formou web proxy)
* Podpora diagnostiky spojení s možností úplného záznamu IP komunikace
* DNS proxy, podpora DNSSEC

NetFIow systém Flowmon:

* Invea Flowmon Probe 4000
* Flowmon ADS Standard – modul detekce anomálií a analýzy chování sítě (NBAD) nad síťovou infrastrukturou
* čtyřportová sonda s vestavěným kolektorem a instalovaným modulem ADS. HW appliance
* detailní monitoring síťového provozu v reálném čase
* monitoring a analýza skutečného provozu mezi uživatelem a aplikační infrastrukturou.
* detekce cílených útoků nebo identifikace neznámého malware na síťové úrovni – reakce na tyto hrozby
* identifikace hrozeb, pro které neexistuje signatura, i prostřednictvím
* identifikace hrozeb prostřednictvím heuristické analýzy antivirových systémů.

Log Management Syslog-NG:

* syslog-ng Store Box
* HW appliance
* technologie je sice nadále výrobcem podporována, ale již není tak aktivně vyvíjena
* Licence na 250 zdrojů, výkon 75k+ EPS
* Disková kapacita řešení zajišťuje uložení všech logů v RAW podobě po dobu 12 měsíců
* logování přes syslog protokol

SIEM ArcSight:

* ArcSight ESM Express 1000 EPS (Je tedy využívána licence o velikosti 1000 EPS)
* Web GUI rozhraní pro práci s Expresem
* Provoz na dedikovaném HW – HW appliance
* Součástí řešení jsou i dva HW servery určené pro sběr logů
* řešení je navrhnuto pro minimalizaci výpadků sběru a uchovávaní logů (ZERO DROP) pomocí nasazení v „HA“ zapojení.
* Součástí řešení je VA nástroj pro odhalování zranitelností, provázaný s korelační vrstvou řešení
* Součástí je plně integrovaný nástroj pro řízení celého životního cyklu incidentu
* ESM Express je na úrovni konektorů napojen na Log Management přes syslog protokol
* Logující zařízení - Windows, CISCO IOS, MSSQL, VMWARE, sonda FlowMon a proprietární aplikace

PAM systém Balabit (nyní One Identity):

* BalaBit PSM Shell Control Box
* Nyní OneIdentity Safeguard for Privileged Sessions
* forma HW appliance
* Licence je pořízena pro 25 hostovaných systémů
* Nahrávají se všechny RDP spojení na servery
* Řešení zaznamenává aktivitu uživatele na cílovém systému, umožňuje přehrávat všechny
* uživatelské aktivity
* Možnost exportovat kompletní stav appliance pro další analýzu svého stavu.

Systém testování zranitelností (Vulnerability Management) NESSUS

Nessus Professional, zachycující:

* vstupní informace testu
* testovací žurnál
* identifikaci testovacích nástrojů a jejich konfiguraci při testu
* úplný výpis výsledků
* postup a závěr hodnocení
* manažerské shrnutí testu.

## Požadované dodávky a základní služby

### Podrobný návrh cílového konceptu řešení

Zadavatel požaduje, aby Dodavatel v rámci Fáze č.1 zpracoval podrobný cílový koncept vč. implementačního plánu a harmonogramu, který bude podrobně definovat implementaci HW a SW ve Fázi č. 2.

### Požadované služby a dodávky FW systému pro ochranu perimetru

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace HW nebo SW[[1]](#footnote-1) (zadavatel připouští řešení formou HW i SW appliance) včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace;
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky NDR systému (Network Detection & Response)

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace HW (a SW provozovaného na HW appliance) včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace;
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky EDR systému (Endpoint Detection & Response)

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace SW včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace; SW bude implementován na virtuální server realizovaný v rámci druhé části zakázky a na stávající pracovní stanice a notebooky
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky Log Management systému

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace SW včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace; SW bude implementován na virtuální server realizovaný v rámci druhé části zakázky. Do systému budou integrovány všechny komponenty dle výše uvedené architektury v tom smyslu, že Log Management bude zpracovávat jejich bezpečnostní stav.
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky PAM systému (Privileged Access Management)

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace SW včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace; SW bude implementován na virtuální server realizovaný v rámci druhé části zakázky
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky SIEM systému (Security Information and Event Management)

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace SW včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace; SW bude implementován na virtuální server realizovaný v rámci druhé části zakázky. Do systému budou integrovány všechny komponenty dle výše uvedené architektury v tom smyslu, že SIEM bude monitorovat jejich bezpečnostní stav
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky Svolávacího systému = nástroje pro automatizaci komunikace (svolávání a distribuce informací) při řešení incidenčních workflow

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace SW včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace; SW bude implementován na virtuální server realizovaný v rámci druhé části zakázky.
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

### Požadované služby a dodávky integrace

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky jednorázově poskytl Zadavateli následující dodávky a služby v souladu s níže uvedenými požadavky a předal jejich výstupy:

* Fáze 2: Dodávka a implementace SW zajišťující integrace včetně licencí a nasazení konfigurace dle cílového konceptu do produkčního prostředí, otestování řešení a dodávka kompletní dokumentace.
* Fáze 3: Pilotní provoz SW technologie po dobu 1 měsíce
* Fáze 4: Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2 projektu

SW zajišťují integrace bude dodán v rozsahu definovaném architekturou specifikovanou v následné kapitole tohoto dokumentu. SW bude zajišťovat všechny vazby uvedené v architektuře. Řešení integrace bude provedeno tak, aby plně vyhovovalo požadavkům zákona o kybernetické bezpečnosti platného v době implementace požadovaného řešení

### Požadované služby a dodávky TIF = technologické infrastruktury pro provoz bezpečnostních systémů a nástrojů

Požadované služby a dodávky jsou součástí druhé části veřejné zakázky

### Požadované služby SOC (Security Operation Centrum)

Zadavatel požaduje, aby Dodavatel v rámci veřejné zakázky průběžně poskytoval v rámci fáze 4 (Údržba a podpora po dobu 60 měsíců od ukončení Fáze 2) Zadavateli následující služby v souladu s níže uvedenými požadavky:

* zodpovědnost za identifikaci a nahlášení bezpečnostních incidentů Zadavateli
* analytické práce v případě výskytů incidentů, alertů
* kompatibilita a integrace SIEM dodavatele se SIEM KVOP
* technický monitoring v režimu 24x7, operátor v režimu on line 5x8 a v režimu pohotovosti 7x24

## Funkční a nefunkční požadavky

Funkční a nefunkční požadavky jednotlivých výše uvedených částí veřejné zakázky jsou obsahem Přílohy 1.1.1 – funkční a nefunkční požadavky řešení část 1 této technické specifikace.

## Další požadované služby

### Projektové řízení

Dodavatel ve všech fázích 1 až 3 zajistí projektové řízení (plánování, organizaci, sledování a řízení aktivit) dle metodik PRINCE2 / IPMA / PMI.

Platí pro všechny systémya služby uvedené v kapitole 3 s výjimkou služby SOC.

### Dodávka potřebných licencí k produktu

Nejpozději na konci Fáze 2 dodá Dodavatel veškeré potřebné SW licence (včetně SW licencí k HW appliance či k SW licencím dodaným spolu se zařízeními) a zajistí jejich maintenance na dobu 60 měsíců.

Platí pro všechny systémy a služby uvedené v kapitolách 3.2.2 až 3.2.9.

### Školení

Dodavatel návrhu cílového konceptu připraví plán školení pro proškolení obsluhujícího personálu. Cílem proškolení obsluhujícího personálu je předání informací k obsluze implementovaného řešení v takové míře, aby mohl být proveden pilotní provoz

Platí pro všechny systémy a služby uvedené v kapitolách 3.2.2 až 3.2.8.

### Uvedení systému do pilotního provozu

Dodavatel uvede systém do pilotního provozu. Účelem pilotního provozu je ověření funkčních vlastností implementovaného systému. Uvedení systému do pilotního provozu zahrnuje následující aktivity:

* Přenesení relevantních konfigurací ze starých komponent na nové HW a SW komponenty HW.
* Ověření nasazených komponent HW a SW v ostrém provozu
* Vyhodnocení pilotního provozu a realizace případných nápravných opatření.

Platí pro všechny systémy a služby uvedené v kapitolách 3.2.2 až 3.2.9.

### Uvedení systému do produkčního provozu

Dodavatel uvede systém do produkčního provozu akceptací řešení po ukončení pilotního provozu. Uvedení systému do produkčního provozu zahrnuje následující aktivity:

* Aktualizace dokumentace
* Finální akceptace.

Platí pro všechny systémy a služby uvedené v kapitolách 3.2.2 až 3.2.9.

### Údržba systému

Do úkonů údržby se zahrnují:

**Profylaxe** – Dodavatel provádí pravidelnou kontrolu a vyhodnocení stavu systému. Dodavatel na základě vyhodnocení stavu systému upozorňuje Zadavatele na nepravidelnosti v provozu systému a provádí změny konfigurací a další úkony potřebné k zajištění spolehlivého běhu systému. Dodavatel dále na základě vyhodnocení stavu systému doporučuje opatření k zajištění zdrojů pro udržení výkonu systému.

Minimální četnost: 1x za 12 měsíců nebo dle aktuální potřeby;

**Dodávka a aplikace záplat a** aktualizací – Dodavatel průběžně sleduje bezpečnostní upozornění, bezpečnostní a funkční záplaty a aktualizace systému včetně doporučení k jejich nasazení vydané výrobcem. Dodavatel vydané záplaty a aktualizace otestuje a doporučí Zadavateli termín a způsob jejich nasazení. Zadavatel rozhodne o doporučení. Dodavatel následně provádí úkony podle rozhodnutí Zadavatele.

Četnost: průběžně;

Platí pro všechny systému a služby uvedené v kapitolách 3.2.2 až 3.2.8.

### Standardní servisní podpora systému

Pro účely poskytování servisní podpory definuje Zadavatel:

* SLA: jedná se o domluvenou úroveň kvality služeb, kterou Dodavatel garantuje Zadavateli.
* Závada: znamená nesoulad skutečné funkčnosti systému s funkčností, jež je popsána technickou dokumentací.
* Hlášení závady: jedná se o Ticket popisující výskyt závady. Obsahuje popis závady, čas hlášení, kontaktní osobu, kategorii závady. Ticket posílá Zadavatel Dodavateli emailem nebo jej zadává do helpdeskového systému
* Doba odezvy: jedná se o dobu od okamžiku zadání uživatelského požadavku (příp. hlášení závady) do okamžiku, kdy je Zadavateli sděleno, že Ticket s jeho požadavkem (resp. hlášením) je přijat a bylo zahájeno jeho zpracování.
* Doba nápravy: jedná se o dobu počínající okamžikem nahlášení závady (příp. zadání požadavku), do okamžiku, kdy je, a to buď dočasným, nebo kompletním řešením, závada odstraněna (resp. požadavek vyřešen) vyřešen.

Životní cyklus hlášení závady a uživatelského požadavku je definován skrze následující stavy:

* Zadáno – Ticket byl korektně nahlášen, začíná měření doby odezvy a doby nápravy;
* Čekající – Řešení Ticketu čeká na aktivitu Zadavatele nebo třetí strany, doba nápravy je pozastavena;
* Vyřešen – Ticket je Dodavatelem vyřešen.

Poskytování podpory zahrnuje:

* Hot-line prostřednictvím HelpDesku, telefonu či e-mailu pro vyjmenované pracovníky Zadavatele (tj. odpovědi na otázky k užívání a fungování systému);
* Řešení závad

Podrobná specifikace služeb (SLA):

|  |  |
| --- | --- |
| Pracovní doba služby Hot-line | 5x8, Po-Pá 8:00 – 16:00 |
| Pracovní doba služby zadávání Ticketů (email, web = HelpDesk) | 7x24 |
| Pracovní doba služby Řešení závad | Dle detailu priorit v následující tabulce |
| Doba odezvy | Dle detailu priorit v následující tabulce |
| Řešení (Fix time) | Dle detailu priorit v následující tabulce |

Kategorie priorit řešení jednotlivých ticketů = řešení závady:

1. Kritická závada systému, jedná se o stav předmětu veřejné zakázky, kdy je znemožněna práce s předmětem veřejné zakázky, nelze použít alternativní zásah.
2. Méně závažná závada systému, jedná se o stav předmětu veřejné zakázky, který lze dočasně překlenou jiným postupem koncového uživatele. Součástí této závady je také nesoulad předmětu veřejné zakázky s platnou legislativou.
3. Marginální závada neohrožující funkčnost. Závada pouze snižuje komfort práce uživatele.

SLA parametry služby řešení závady:

| Systém | **Pracovní doba** | **Kategorie** | **Doba odezvy** | **Doba nápravy** |
| --- | --- | --- | --- | --- |
| FW | 8x5 | A | 4h | NBD |
| B | 8h | 2 NBD |
| C | NBD | 10 NBD |
| NDR | 8x5 | A | 8h | 2 NBD |
| B | NBD | 4 NBD |
| C | 2 NBD | 15 NBD |
| EDR | 8x5 | A | 4h | NBD |
| B | 8h | 2 NBD |
| C | NBD | 10 NBD |
| LOG MNG | 8x5 | A | 4h | NBD |
| B | 8h | 2 NBD |
| C | NBD | 10 NBD |
| PAM | 8x5 | A | 8h | 2 NBD |
| B | NBD | 4 NBD |
| C | 2 NBD | 15 NBD |
| SIEM | 8x5 | A | 4h | NBD |
| B | 8h | 2 NBD |
| C | NBD | 10 NBD |
| SAIW | 8x5 | A | NBD | 5 NBD |
| B | 2 NBD | 15 NBD |
| C | 5 NBD | 30 NBD |

# Technologická a aplikační architektura řešení

Strukturální pohled na požadovanou technologickou a aplikační architekturu:

Obsah obrázku text, snímek obrazovky, diagram, Plán

Popis byl vytvořen automaticky

Poznámka: Tento pohled na technologickou a aplikační architekturu je za účelem přehlednosti dodán v rámci zadávací dokumentace i ve formátu PNG. V tomto formátu lze identifikovat veškerý potřebný detail architektury.

**Tato architektura zachycuje všechny vazby požadované v kapitole 3.2.9**

## Prvky technologické a aplikační architektury:

| **Typ prvku** | **Název prvku** | **Popis prvku** |
| --- | --- | --- |
| ApplicationComponent | EDR | Aplikace End Point Protection = antivir, antimalware, antispam, antiransonware … ochrana stanic a serverů. |
| ApplicationComponent | FW | Aplikace firewall - aplikace ochrany perimetru, segmentace sítě, apod. |
| ApplicationComponent | Log Management | Aplikace Log Management = systém pro správu bezpečnostních logů |
| ApplicationComponent | NDR | Aplikace Netflow = monitorování síťového provozu na základě IP toků. |
| ApplicationComponent | NESSUS | Stávající systém pro management zranitelností |
| ApplicationComponent | PAM | Aplikace PAM = systém pro ochranu privilegovaných účtů |
| ApplicationComponent | Provozní monitoring CENTREON | Stávající systém provozního monitoringu |
| ApplicationComponent | Svolávací systém | Svolávací systém = Systém pro automatizaci incidenčních workflow |
| ApplicationComponent | SIEM | SIEM včetně rozšíření pro SOAR |
| ApplicationComponent | SIEM dodavatele | SIEM dodavatele integrovaný se SIEMem KVOP |
| BusinessService | Služby SOC | Služby Security Operations Center = služby bezpečnostního operačního centra |
| Device | Diskové pole | Stávající diskové pole |
| Device | Diskové pole (nové) | Nové diskové pole |
| Device | FW - HW Appliance | Alterantiva FW k SW Applianci FW |
| Device | Multifunkce / tiskárny | Multifunkce / tiskárny |
| Device | NDR kolektor - HW Appliance | Netflow kolektor nový - HW Appliance |
| Device | NDR sonda- HW Appliance | Net Flow sonda nová - HW Appliance |
| Device | Nové fyzické servery pro KYBEZ | Nový fyzický servery - zdroje virtualizace. Není předmětem této části zakázky, je předmětem druhé části zakázky. |
| Device | PC | Pracovní stanice a notebooky |
| Device | Pásková mechanika | Druhá záloha v oddělené místnosti |
| Device | Stávající fyzické servery pro IT a KYBEZ | Stávající fyzický servery - zdroje virtualizace. Na nich virtuály pro:   * Nessus - stávající vulnerability management * Centreon - stávající provozní monitoring |
| Device | UPS | UPSky |
| Device | WIFI AP | WIFI přístupové body |
| Node | LAN Switch | síťové přepínače |
| Node | Nové virtuální servery pro KYBEZ | Nové virtuální servery pro bezpečnostní aplikace |
| Node | SAN switch | SAN přepínače |
| Node | Virtulání servery Linux, Windows pro IT | Virtulání servery Linux, Windows pro IT |
| SystemSoftware | Citrix NetScaler | Cachování webových aplikací |
| SystemSoftware | DHCP | DHCP server |
| SystemSoftware | DNS | DNS server |
| SystemSoftware | Exchange | MS Exchange |
| SystemSoftware | Linux | o.s. Linux |
| SystemSoftware | RDBMS - MS SQL, MY SQL, POSTGRE SQL? | Používané relační databáze |
| SystemSoftware | VMWare ESXi a vCenter | SW pro virtualizaci serverů |
| SystemSoftware | Webové a aplikační servery (IIS, Apache, Nginx) | Používané webové a aplikační servery |
| SystemSoftware | Windows | o.s. Windows |
| SystemSoftware | Zálohování Veeeam Backup and Replication | Zálohovací SW |
| Grouping | ZDROJE PRO CENTREON | Zdroje pro Centreon |
| Grouping | ZDROJE PRO CENTREON, LOG MANAGEMENT A SIEM | Zdroje pro Centreon Log Management a SIEM |

## Popis technologické a aplikační architektury

Klíčovým prvkem bezpečnostní architektury je stávající systém provozního monitoringu CENTREON, který monitoruje provozní stav prvků technologické infrastruktury[[2]](#footnote-2).

Některé prvky navíc posílají provozní i bezpečnostní logy do systému Log Managementu, který bude v rámci tohoto projektu modifikován. Připouští se dodávka nového Log Managementu ve formě SW Appliance nebo náhrada stávajícího Log Managementu opět ve formě SW Appliance (viz varianta 1 nebo 2 ve shora uvedené architektuře). Požaduje se integrace na SIEM Arcsight.

Stávající FW bude nahrazen / vyměněn. V případě FW se připouští buď varianta HW Appliance nebo varianta SW Appliance na nových virtuálních serverech. Požaduje se FW nové generace, tedy FW doplněný o vpn, IPS, filtraci webových stránek atd.

Řešení NDR (Network Detection and Response), tedy systému detekce, analýzy a reakce na anomálie v síti bude obsahovat Netflow sondu a Netflow HW kolektor ve formě HW Appliance. Tímto způsobem budou zajištěny služby Netflow (monitoring síťového provozu).

Řešení EDR bude kromě standardních antivirových funkcí detekovat pokročilé typy hrozeb na základě setrvalého monitoringu na koncových zařízeních. Řešení bude dále vyhodnocovat nezvyklé prostřednictvím identifikátorů kompromitace a bude umožňovat reagovat na vzniklé hrozby prostřednictvím automatizované reakce. Jako součást řešení se požaduje i řešení MFA autentizace uživatelů

Požaduje se modernizace PAM spočívající v náhradě stávající HW appliance, která je za hranicí morální udržitelnosti. PAM bude provozována jako transparentní proxy a nebude ovlivňovat pracovní návyky uživatelů a dodavatelů.

Stávající řešení HW Appliance SIEM bude modernizováno, respektive nahrazeno SW appliance SIEM požadovaných vlastností a požadované funkčnosti. Systém bude licenčně rozšířen o SOAR, který bude součástí nabízeného řešení a bude licenčně pokryt = systém orchestrace zabezpečení, automatizace a reakce.

Systém SIEM KVOP bude integrován se systémem SIEM dodavatele za účelem poskytování služeb Security Operations = Security Operations Center = bezpečnostní operační centrum

Bezpečnostní řešení bude doplněno podpůrným nástrojem pro automatizaci incidenčních workflow. Tento nástroj zajistí komunikační podporu při řešení bezpečnostních incidentů.

# Vazba na druhou část veřejné zakázky

Stávající farma serverů, diskových úložišť a dalších HW a systémových SW, jejichž stav je sledován systémem provozního monitoringu CENTREON bude rozšířena o nově pořizované fyzické servery a diskové pole. Ty budou využity pro vytvoření virtuálních serverů, na které budou instalovány nově pořizované či rozšiřované bezpečnostní či podpůrné systémy.

**Veškeré požadované dodávky a služby budou provozované na technologické infrastruktuře (fyzické servery, diskové pole, virtualizační nástroje, operační systémy a databáze) pořízené v rámci druhé části veřejné zakázky.**

# Harmonogram

|  |  |
| --- | --- |
| Fáze | Termín |
| Fáze 1 (F1) | 1 měsíc (1M) |
| Fáze 2 | F1 + 6M |
| Fáze 3 | F2 + 1M |
| Fáze 4 | F3 + 60M |

1. V případě dodávky SW bude tento SW implementován na virtuální server realizovaný v rámci druhé části dodávky [↑](#footnote-ref-1)
2. Jde o komponenty, které jsou na výše uvedeném obrázku označeny jako „ZDROJE PRO CENTREON“ nebo „ZDROJE PRO CENTREON, LOG MANAGEMENT A SIEM“. [↑](#footnote-ref-2)