**Příloha č. 2 Zadávací dokumentace: Technická specifikace a požadavky zadavatele**

# **Monitoring síťového provozu v počítačové síti NPK**

Nemocnice Pardubického kraje, a.s. (dále jen „**NPK**“ nebo „**Zadavatel**“) je nemocnice krajského typu s pracovišti rozmístěnými na území celého kraje. Hlavní lokality, kde jsou pracoviště nemocnice rozmístěny, jsou:

* Pardubická nemocnice, Kyjevská 44, 53203 Pardubice,
* Chrudimská nemocnice, Václavská 570, 537 27 Chrudim,
* Svitavská nemocnice, Kollárova 7, 568 25 Svitavy,
* Litomyšlská nemocnice, J. E. Purkyně 652, 570 14 Litomyšl,
* Orlickoústecká nemocnice, Čs. armády 1076, 562 18 Ústí nad Orlicí.

V NPK je realizován elektronický informační systému IS NPK, v rámci kterého je provozováno velké množství informačních a komunikačních systémů. Technologické prostředí je tvořeno rozlehlou síťovou infrastrukturou s decentralizovanými datovými centry ve všech lokalitách NPK.

NPK je provozovatelem základních služeb státu v oblasti zdravotnictví. To ukládá nemocnici povinnost zajistit **úroveň** **kybernetické bezpečnosti** dle požadavků ***zákona 181/2014 Sb.*** *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*, resp. dle požadavků ***vyhlášky č. 82/2018 Sb.,*** *vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*, a to zejména dle paragrafů vyhlášky:

* **§14** - Zvládání kybernetických bezpečnostních událostí a incidentů
* **§23** - Detekce kybernetických bezpečnostních událostí
  + specificky **§23, 1a** – Povinná osoba …. používá nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi
* **§27 -** Zajišťování úrovně dostupnosti informací
  + specificky **§27c** – dostupnost důležitých technických aktiv

Součástí systému zvládání kybernetických bezpečnostních událostí a incidentů je nepřetržitý automatizovaný monitoring síťového provozu a přenášených dat ve vnitřní počítačové síti Zadavatele a monitoring provozu webových i databázových aplikací.

Zadavatel, jako provozovatel základních služeb státu v oblasti zdravotnictví, je povinen nasadit a využívat nástroje pro detekci kybernetických bezpečnostních událostí s cílem zajistit nepřetržitý detailní bezpečnostní monitoring sítě a stavu aplikací, provozovaných Zadavatelem.

Z výše uvedených důvodů Zadavatel poptává **nástroj pro automatizovaný monitoring síťového a aplikačního provozu**, který zajistí jednotnou detailní nepřetržitou kontrolu a monitorování dění na počítačové sítí Zadavatele.

## **Specifikace rozsahu díla - dodávky nástroje pro automatizovaný monitoring síťového a aplikačního provozu**

V rámci dodávky řešení **automatizovaného monitoringu síťového a aplikačního provozu** je požadováno, aby se realizace díla skládala z minimálně následujících fází:

* **Vstupní analýza** – vytvoření „*Implementačního plánu projektu*“ realizace díla,
* **Instalace** – instalace řešení do prostředí Zadavatele,
* **Implementace** – – provedení nastavení všech požadovaných modulů, konfigurace včetně všech provozních nastavení dle požadavků Zadavatele.
* **Testování** – testování funkčnosti dodávaného řešení před akceptací díla,
* **Dokumentace** – vypracování dokumentace k nasazenému řešení,
* **Zaškolení** **správců** – odborné zaškolení správců, administrátorů dodávaného řešení,
* **Akceptace –** provedení akceptačních procedur a předání do ostrého provozu.
* **Záruka výrobce** – záruka pokrývá všechny dodávané hardwarové a softwarové prostředky po dobu 1 roku v rozsahu definovaném tabulkou „*Požadavky na* ***záruční podporu výrobce“***

Dále též popis požadovaných služeb uvedený v příloze **Příloha č. 3 - Smlouva o dílo.**

### **Vstupní analýza**

Zhotovitel provede v rámci realizace díla vstupní analýzu a zpracuje „*Implementačního plánu projektu*“ dle kterého bude dílo následně realizováno. Součástí Implementačního plánu projektu bude technický popis řešení, vč. finální podoby implementace (nastavení) dodávaného řešení, testovací scénáře, popis akceptačních procedur a akceptační protokoly, harmonogram realizace projektu, potřebné instalační postupy a požadavky na zajištění součinnosti.

### **Instalace**

Zhotovitel realizuje dodávané řešení v prostředí Zadavatele ve shodě s Implementačním plánem projektu,

* veškeré náklady související s dopravou a instalací jdou na vrub Zhotovitele,
* technici Zhotovitele splňují veškeré podmínky dané výrobcem dodávaného nástroje pro jeho instalaci,

### **Implementace**

Zhotovitel provede potřebnou konfiguraci a nastavení systému Uchazeč provede potřebnou konfiguraci a nastavení všech modulů – tj. pro behaviorální analýzu vč. odladění základních fals positive, nastavení základních dashboardů v součinnosti se Zadavatelem, nastavení analýzy výkonnosti aplikací a nastavení modulu pro automatickou analýzu zachyceného provozu a interpretaci dat z paketů.

### **Testování**

Zhotovitel zajistí řádné otestování dodávaného řešení dle navržených testovacích scénářů v Implementačním plánu projektu. Zejména budou provedeny následující testy:

* funkční testy,
* bezpečnostní testy,
* DR testy (testy obnovitelnosti po havárii).

### **Dokumentace**

Součástí dodávky musí být dokumentace v následujícím rozsahu:

* Implementační plán projektu, vč. popisu architektury řešení a finální konfigurace,
* produktová dokumentace výrobce ke všem dodávaným prostředkům,
* instalační dokumentace (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj dodávaného řešení) a dokumentace k integrovaným systémům,
* administrátorské a uživatelské příručky (manuály),
* popis havarijních plánů pro obnovu služeb dodávaného systému po havárii.

Dokumentace uvedená je požadována v českém jazyce. Produktová dokumentace výrobce, včetně dokumentace výrobce popisující strukturu a význam logů, je akceptovatelná v anglickém nebo českém jazyce.

Pravidelná aktualizace dokumentace bude prováděna v rámci služeb servisní podpory, a to pravidelně při jakékoliv změně v architektuře či funkcionalitě dodaného řešení, např. aktualizacích firmware, rozvoji řešení apod., pokud nebude dohodnuto jinak.

### **Školení a zaškolení**

* Zajištění školení i zaškolení ICT specialistů proběhne v prostorách Zadavatele. Konkrétní termíny a místo bude určené po vzájemné dohodě. Školení i zaškolení proběhne v českém jazyce.
* Základní školení pro předem definovaný počet lidí se zaměří na základní seznámení s produktem, jeho instalací, konfigurací a uvedením do provozu. Cílem je porozumění dané technologii pracovníky Zadavatele, srovnání pojmů pro další komunikaci.
* Zaškolení pro správce tohoto řešení poskytne určeným pracovníkům komplexní informace v takovém rozsahu, aby tito pracovníci dokázali samostatně a dlouhodobě administrovat a provozovat dodané řešení. Součástí zaškolení bude i obnova řešení po havárii.

### **Akceptace**

Zhotovitel a Zadavatel provedou společně akceptační testy a procedury. Akceptace díla je stvrzena podpisem akceptačních protokolů oběma stranami. Podpisem akceptačních protokolů:

* přebírá Zadavatel dílo do užití (do ostrého provozu),
* ukončuje platnost Smlouvy o dílo,
* vzniká Zhotoviteli nárok na úhradu ceny díla,
* spouští platnost Smlouvy o poskytování servisních služeb.

### **Licenční zajištění**

Součástí dodávky musí být veškeré licenční zajištění v rámci díla nezbytné pro legální provozování dodaného řešení.

## **Specifikace servisních služeb – servisní podpora dodavatele na dílo dodávka nástroje pro automatizovaný monitoring síťového a aplikačního provozu**

V rámci dodávky řešení **automatizovaného monitoringu síťového a aplikačního provozu** je požadováno, aby bylo dílo po předání do ostrého provozu zajištěno servisními službami dodavatele, které bude dodavatel poskytovat na základě samostatné servisní smlouvy. Základní vymezení požadovaných služeb:

* **Garance softwarové podpory**
* **Servisní garance dle definovaných SLA**
* **Garance příjmu hlášení chybových stavů a požadavků**
* **Garance vybraných služeb:**
* **Preventivní prohlídky a profylaxe.**
* **Konzultační služby a návštěvy**
* **Záruka výrobce** – záruka výrobce pokrývá všechny dodávané hardwarové a softwarové prostředky v rozsahu definovaném tabulkou „*Požadavky na* ***záruční podporu výrobce“*** a je/bude součástí servisní smlouvy **od druhého roku po předání díla do ostrého provozu.**

Detailní popis požadovaných služeb je uveden v příloze **Příloha č. 4 - Smlouva o poskytování servisních služeb (zejména Příloha č. 2 Sjednané služby a ujednání o kvalitě služeb (SLA) ):**

## **Technická a funkční specifikace dodávky nástroje pro automatizovaný monitoring síťového a aplikačního provozu**

## **Technická specifikace dodávky nástroje pro automatizovaný monitoring síťového a aplikačního provozu**

Požadavky na vybavení dodávaného řešení **technickými prostředky** pro zajištění monitoringu síťového provozu ve všech pěti lokalitách, kde působí Zadavatel.

Pozn: Lokalita Pardubice je považována za centrální lokalitu, tzv. CENTRÁLU, ostatní lokality jsou označovány jako POBOČKY.

| *Požadavky na*  ***technické vybavení CENTRÁLY (lokalita Pardubice)*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| 2ks monitorovacího zařízení 4x10Gb Ethernet monitorovací port – vyžadováno zařízení s hardwarovou akcelerací |  |  |
| 17 ks monitorovacího zařízení pro monitorovací systém provozu sítě centrála Pardubice s virtuálním 1x10Gb Ethernet monitorovacím portem, předpokládá se provoz na VMware |  |  |
| 1 ks monitorovacího zařízení 1x1GbE monitorovací port-měď |  |  |
| 8 ks SFP+ modulů pro připojení 4x10Gb Ethernet monitorovacích zařízení |  |  |
| 1ks úložiště s kapacitou 48TB, které bude sloužit pro vyhodnocování a analýzu z monitorovacích zařízení |  |  |
| 1ks úložiště virtuální licence na 3TB, které bude sloužit jako backup pro vyhodnocování a analýzu z monitorovacích zařízení |  |  |
| monitoring výkonu aplikací: 30 000 tpm, 1/10GbE, centrální konzole, možnost monitorovat 8 aplikací (kritické i významné) |  |  |
| monitoring anomálií – minimálně pro až 5000 toků/s |  |  |
| záznam a diagnostiku paketů síťového provozu min. 8 sond, 1/10GbE, centrální konzole |  |  |

| *Požadavky na*  ***technické vybavení POBOČEK celkem***  ***(lokality Chrudim, Litomyšl, Svitavy a Ústí nad Orlicí)*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| 4ks monitorovacího zařízení s 2x10Gb s Ethernet monitorovacím portem SFP+ |  |  |
| 8 ks SFP+ modelů pro připojení monitorovacích zařízení |  |  |

Požadavky na záruční podporu výrovce technických prostředků dodávaného řešení. Záruční podpora výrobce musí zahrnovat tyto služby:

| *Požadavky na* ***záruční podporu výrobce*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| záruka řešení chybových stavů Next Business Day – v případě hardwarového problému řešeno v místě Zadavatele certifikovaným technikem |  |  |
| pravidelné aktualizace a upgrady veškerého softwarového vybavení dodávaného řešení |  |  |
| podpora v českém jazyce – zahrnuje přístup k webovému zákaznickému centru výrobce, podporu na telefonu a e-mailu, vzdálenou podporu přes SSH a konzultace síťového / bezpečnostního technika v režimu 8x5. |  |  |
| školení poskytovaná výrobcem |  |  |
| ​možnost prodloužit záruku na hardwarové vybavení minimálně na 5 let |  |  |
| garance zvýhodněné obnovy hardware po uplynutí 5 let placené záruky – pořízení nových hardwarových prostředků se slevou min. 50% z koncové ceny |  |  |
| přístup do aktuální reputační databáze pro přesnější detekci infikovaných stanic nebo odhalení komunikace s botnet command & control centry a aktualizaci vzorů chování detekčních metod pro odhalování nejnovější hrozby (zero-day zranitelnosti) aj. |  |  |

## **Funkční specifikace dodávky řešení pro automatizovaný monitoring síťového a aplikačního provozu**

Dodávané řešení musí splňovat minimálně tyto požadavky:

| ***Obecné požadavky na dodávané řešení*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| Monitorovací systém musí být nezávislý na použité síťové infrastruktuře a svou funkcí neovlivňoval sledovanou síť |  |  |
| Monitorovací systém musí umožňovat dlouhodobé detailní monitorování dění na počítačové síti. Získané informace o dění na síti a chování uživatelů musí systém umožnit v reálném čase sledovat a vyhodnocovat |  |  |
| Monitorovací systém musí umožňovat sledování a kontrolu stavu webových a databázových aplikaci |  |  |
| Monitorovací systém musí umožňovat automatickou analýzu zachyceného (nahraného) provozu a interpretaci dat z paketů |  |  |
| Ze strany monitorované sítě nesmí být prostředky monitorovacího systému detekovatelné |  |  |
| Monitorovací systém musí zahrnovat funkce pro automatické detekce útoků, hrozeb, síťových anomálií |  |  |
| Monitorovací systém musí umožnit měření výkonu webových a databázových aplikací a databází samotných |  |  |
| Monitorovací systém musí disponovat předdefinovanou sadou pravidel pro odhalování obecných anomálií v síti |  |  |
| Součástí monitorovacího systému musí být přehledný dashboard s okamžitou indikací problémů a top statistik |  |  |
| Vyhodnocování incidentů musí probíhat na základě implementace standardu Bidirectional flows (RFC 5103) |  |  |
| Do monitorovacího systému musí být integrovány informace ze služeb DNS, WHOIS a geolokační služby |  |  |
| Monitorovací systém musí umožnit provádět interaktivní vizualizace událostí |  |  |
| Monitorovací systém musí umožnit exporty statistik o provozu na síti, a to ve vhodné formě pro prokazování incidentů |  |  |
| Monitorovací systém musí umožňovat reportování detekovaných událostí emailem |  |  |
| Monitorovací systém musí umožňovat generování výstupů událostí protokolem Syslog ve formátu CEF |  |  |
| Snadná instalace do síťové infrastruktury Zadavatele v řádech dnů |  |  |
| Možnost rozšiřitelnosti funkcionality pomocí dalších modulů. |  |  |
| Návody a uživatelské rozhraní v českém jazyce |  |  |
| Možnost instalovat řešení nebo jeho jednotlivé části na virtuální servery. |  |  |
| Monitorovací systém musí podporovat integraci se systémem pro centrální zpracovávání logů (LogManagement), centrální síťové služby (DDI) a řízení privilegovaných účtů (CyberArk), provozovaný Zadavatelem |  |  |
| Monitorovací systém musí podporovat integraci se systémem pro řízení privilegovanách účtů centrální zpracovávání logů (LogManagement) provozovaný Zadavatelem |  |  |

| *Požadavky na technické parametry – část* ***SONDY*** *(generátory flow)* | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| 100% přesný nezávislý autonomní zdroj NetFlow a IPFIX statistik s podporou IPv4, IPv6, VLAN, MPLS, GRE, ERSPAN, VxLAN, ESP |  |  |
| detekce aplikací dle standardu NBAR2, monitorování a analýza MAC adres, HTTP provozu (včetně položek URL, hostname), VoIP statistik (jiter, zpoždění, ztráta paketů), DNS provozu, DHCP, HTTP, SMTP, Samba a MSSQL |  |  |
| snadná instalace do stávající síťové infrastruktury |  |  |
| rack mount zařízení |  |  |
| pasivní zapojení bez vlivu na monitorovanou síť (prostřednictvím SPAN portu aktivních zařízení) |  |  |
| zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS |  |  |
| správa uživatelů a přístupových práv na zařízení |  |  |
| časová synchronizace zařízení proti centrálnímu zdroji času na síti |  |  |
| jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky |  |  |
| možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232) |  |  |
| použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména |  |  |
| podpora autentizace vůči LDAP (Active Directory) |  |  |
| podpora pro nastavení časů u aktivní a neaktivní expirace toků |  |  |
| podpora vzorkování na úrovni paketů |  |  |
| podpora vzorkování na úrovni toků |  |  |
| podpora filtrování dat na základě IP prefixů a VLAN |  |  |
| podpora vyplňování AS na základě vestavěného či dodaného seznamu |  |  |

| *Požadavky na technické parametry – část* ***KOLEKTORY*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| zabezpečený kolektor NetFlow statistik s databází pro plné uložení síťových statistik |  |  |
| možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru |  |  |
| snadná instalace do stávající síťové infrastruktury – racková montáž |  |  |
| dva administrativní porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat |  |  |
| zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,víceuživatelský přístup včetně možnosti definovat, k jakým datům má jednotlivý uživatel přístup |  |  |
| podpora autentizace vůči LDAP (Active Directory) |  |  |
| HOT SWAP disky, HW RAID včetně SMART detekce |  |  |
| integrace dohledového systému pro kontrolu dostupnosti (SNMP) |  |  |
| časová synchronizace zařízení proti centrálnímu zdroji času na síti |  |  |
| jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky, možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232) |  |  |
| použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména |  |  |
| nutnost ukládání síťových statistik bez jakékoliv redukce |  |  |
| možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru |  |  |
| víceuživatelský přístup – vč. možnosti definovat, k jakým datům má jednotlivý uživatel přístup |  |  |
| integrace dohledového systému pro kontrolu dostupnosti (SNMP) |  |  |
| časová synchronizace zařízení proti centrálnímu zdroji času na síti |  |  |
| jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky |  |  |
| analýza HTTP provozu - včetně položek typu URL, hostname |  |  |
| analýza VoIP statistik (jitter, latence, ztrátovost), podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace, DNS provozu, DHCP, HTTP, SMTP, Samba a MSSQL vč. obsahu daného dotazu |  |  |
| drill-down – možnost dohledat každý jednotlivý zaznamenaný tok |  |  |
| detekce aktivních zařízení na sítí - pro podporu konceptu BYOD |  |  |
| podpora geolokace na základě IP adresy |  |  |
| otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh |  |  |

Součástí zařízení (kolektoru) musí být nástroj či funkcionalita pro automatickou detekci anomálií na základě behaviorální analýzy, aby bylo sledováno a vyhodnocováno nestandardní chování a anomálie na úrovni datové sítě a to zejména:

| *Požadavky na* ***BEZPEČNOSTNÍ (BEHAVIORÁLNÍ) ANALÝZU*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| detekce útoků na síťové služby s cílem získat neoprávněný přístup k zařízení nebo službě |  |  |
| detekce komunikace s potenciálně nežádoucími IP adresami, mezi které patří stanice šířící malware, botnet comman & control centra, známí útočníci nebo systémy šířící nevyžádanou poštu |  |  |
| detekce anomálií DNS provozu indikující infikované stanice, nežádoucí software nebo chybné konfigurace |  |  |
| detekce anomálií DHCP provozu indikující stanice pokoušející se o odposlech síťové komunikace nebo chybné konfigurace |  |  |
| detekce skenování portů a další projevy infikovaných stanic nebo nežádoucího software |  |  |
| detekce potenciálně nežádoucí síťové aplikace jako jsou P2P sítě nebo on-line komunikátory |  |  |
| detekce anonymizační služby jako např. TOR (The Onion Router) s cílem obcházet bezpečnostní opatření a přistupovat na zablokované webové stránky, obcházení PROXY serveru |  |  |
| detekce výpadků síťových služeb a špatné konfigurace síťových služeb |  |  |
| detekce pohybu dat z interní sítě do internetu, tj. potenciální únik dat a využívání služeb pro výměnu dat na internetu (webová úložiště apod.) |  |  |
| detekce útoků na internetovou telefonii, ústředny a přístroje připojené do IP sítě |  |  |
| detekce nestandardní poštovní komunikace a šíření nevyžádané pošty |  |  |
| detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti |  |  |

Monitorovací systém musí umožňovat **sledování a kontrolu stavu webových a databázových aplikací**, a to zejména:

| *Požadavky na* ***APLIKAČNÍ KONTROLU*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| vizualizace stavu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek s možnou analýzou stavu jednotlivých částí aplikace a v aplikaci probíhajících transakcí |  |  |
| uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů, možnost přizpůsobení a vkládání vybraných widgetů uživatelem í souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů) |  |  |
| reportování pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací včetně doby odezvy aplikace, zpoždění sítě a zpoždění samotné aplikace |  |  |
| monitorování aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice |  |  |
| monitorování aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu |  |  |
| umožnění nasazení monitoringu výkonu samostatně na jedné sondě, nebo na více sondách s centrální správou a webovým uživatelským rozhraním na kolektoru |  |  |
| umožnění monitoringu komunikace mezi klienty aplikace a aplikačním serverem na bázi protokolu HTTP a HTTPS, v případě použití protokolu HTTPS musí systém podporovat automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují |  |  |
| monitorovat komunikaci mezi aplikačními servery a databázovými servery Oracle, MS SQL, Postgres SQL, MySQL, MariaDB |  |  |
| umožňovat definovat pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy, systém musí kontinuálně vyhodnocovat všechny transakce a stanovovat celkový status výkonu aplikace na základě vložených parametrů odpovídajících plnění SLA k dané aplikaci |  |  |
| flexibilně umožňovat definici aplikace pro monitoring, a to minimálně v rozsahu IP adresy, portu, hostu, URL vč. regulárních výrazů |  |  |
| korelaci zpoždění na úrovni uživatelské transakce na aplikačním serveru a transakce mezi aplikačním a databázovým serverem. Pro každou uživatelskou transakci musí pak být možné zobrazit SQL transakce, které byly v rámci uživatelské transakce vykonány |  |  |
| definování skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů) |  |  |
| přepočítávání historických statistik pro nově vytvořené skupiny |  |  |
| vytváření reportů dostupných prostřednictvím webového GUI, ve formátu PDF. Reporty musí být možné automaticky odesílat e-mailem |  |  |
| dostupnost detailů pro každou transakci minimálně v rozsahu URL, parametrů, user agentů, objemu přenesených dat, návratových hodnot, cookies... |  |  |
| nutnost dostupnosti detailů pro každou transakci minimálně v rozsahu SQL dotazu v plném rozsahu, velikost dotazu a odpovědi, typ SQL dotazu, čas vzniku dotazu i odpovědi a doba odezvy |  |  |
| filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu mít možnost získávat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná atd. |  |  |
| export informací o transakcích ve formátu CSV |  |  |

Monitorovací systém musí umožňovat **automatickou analýzu zachyceného (nahraného) provozu a interpretaci dat z paketů**. Tento systém musí umožňovat zejména:

| *Požadavky na*  ***ANALÝZU ZACHYCENÉHO SÍŤOVÉHO PROVOZU A INTERPRETACI DAT Z PAKETŮ*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| řešit problémy, pro které informace z flow data nejsou dostačující |  |  |
| zachytávat a diagnostikovat síťový provoz a výsledky poskytovat ve formě událostí s detailním popisem zjištěných problémů |  |  |
| poskytnout expertní znalost a pro chybová hlášení událostí navrhnout řešení |  |  |
| podporovat distribuovanou architekturu |  |  |
| zadávat požadavky na záznam provozu centrálně z kolektoru a ovládat tak všechny sondy s nainstalovaným modulem |  |  |
| uložení prvních „N“ paketů pro každý flow a tak umožnit zachytit i komunikace započaté před vytvořením požadavku na záchyt |  |  |

## **Servisní smlouva**

Základní vymezení požadovaných servisních služeb dodavatele:

Pozn.: Detailní popis požadovaných služeb je uveden v příloze **Příloha č. 4 - Smlouva o poskytování servisních služeb (zejména Příloha č. 2 Sjednané služby a ujednání o kvalitě služeb (SLA) ):**

| *Požadavky na*  ***SERVISNÍ SLUŽBY DODAVATELE*** | ***Splněno: ANO/NE*** | ***Popis splnění požadavků*** |
| --- | --- | --- |
| **Garance softwarové podpory** |  |  |
| **Servisní garance dle definovaných SLA** |  |  |
| **Garance příjmu hlášení chybových stavů a požadavků** |  |  |
| **Garance vybraných služeb:** |  |  |
| **Preventivní prohlídky a profylaxe.** |  |  |
| **Konzultační služby a návštěvy** |  |  |
| **Záruka výrobce** – záruka výrobce pokrývá všechny dodávané hardwarové a softwarové prostředky v rozsahu definovaném tabulkou „*Požadavky na* ***záruční podporu výrobce“*** a je/bude součástí servisní smlouvy **od druhého roku po předání díla do ostrého provozu.** |  |  |