



Vysvětlení, změna či doplnění zadávací dokumentace č. 1

Zadavatel: Sdružené zdravotnické zařízení Krnov, příspěvková organizace
Se sídlem: I.P. Pavlova 552/9, Pod Bezručovým vrchem, 794 01 Krnov
IČO: 00844641
Zastoupena: MUDr. Ladislavem Václavcem, MBA, ředitelem

Veřejná zakázka:

„Dodávka log management systému“

Číslo spisu: **SZZ/Otr/2020/25/log management systém**

Číslo zakázky: **P20V00000313**

(dále také „VZ“)

Na základě požadavku účastníka ZŘ poskytuje zadavatel k výše uvedené Veřejné zakázce tyto informace k zadávací dokumentaci.

DOTAZ č. 1

Požadavky na implementaci:

a. Instalace agentů, pokud jsou pro daný systém potřeba.

Zadavatel požaduje instalaci agentů, pokud jsou potřeba, to je nestandardní požadavek, protože pro instalaci agentů je zapotřebí administrátorský přístup na produkční servery zadavatele. Standardní způsob dodání je podpora při instalaci agentů, nikoliv přístup třetí strany na produkční servery.

Žádáme zadavatele o upřesnění tohoto požadavku a především potvrzení, zda opravdu umožní zhotoviteli plný přístup k produkčním serverům zadavatele.

ODPOVĚď č. 1

Zadavatel upřesňuje, že požadavkem na instalaci agentů je myšleno odladění a zdokumentování všech instalačních postupů agenta, které jsou nutné pro integraci zdrojů logů Zadavatele, a poskytování technické podpory pracovníkům Zadavatele při provádění instalace agentů do produkčního prostředí.

DOTAZ č. 2

Požadavky na implementaci:

b. Analýza a nastavení systému pro logování sledovaných aplikací.

Žádáme o specifikaci aplikací, ze kterých se budou sbírat logy, tato informace v ZD chybí, je zde pouze uveden seznam severů a hardware, nikoliv další aplikace jako je v nemocničním prostředí NIS a další (strava, PAX, atd.). V případě, pokud zadavatel nechce napojit další aplikaci či informační systém, žádáme o potvrzení tohoto požadavku

ODPOVĚď č. 2

Zadavatel požaduje provedení kompletní integrace logů pro technologie uvedené v tabulce na straně 2 v příloze č. 4 Minimální technické požadavky, tj. analýzy potřebného nastavení těchto

technologií a provedení konfigurace nastavení dodávaného systému účastníkem ZŘ tak, aby byly prokazatelně sbírány a log management systémem rozpoznávány kategorie bezpečnostních událostí, které v §22 bod (2) definuje vyhláška č.82/2018 Sb.

DOTAZ č. 3

Požadavky na implementaci:

c. Vytvoření parserů pro aplikace uvedené v rámci zadávací dokumentace.

Chybí specifikace aplikací, prosíme o doplnění jejich názvu a počtu.

ODPOVĚď č. 3

Zadavatel požaduje vytvoření parserů pro provedení kompletní integrace logů pro technologie uvedené v tabulce na straně 2 v příloze č. 4 Minimální technické požadavky tak, aby byly log management systémem rozpoznávány kategorie bezpečnostních událostí, které v §22 bod (2) definuje vyhláška č.82/2018 Sb.

DOTAZ č. 4

Požadované funkcionality, vlastnosti bezpečnostního dohledu:

Konkrétně požadavek: Musí umožňovat základní analýzu datového toku podporovaných síťových zařízení (netflow). V rámci zadávací dokumentace Zadavatel nepoptává řešení na analýzu netflow, ale logmanagement systém. Žádáme o potvrzení, že nabízený systém musí pouze podporovat napojení na řešení, které analyzuje síťový provoz, a to pouze na úrovni logů.

ODPOVĚď č. 4

Zadavatel požaduje, aby log management systém mohl být použit přímo jako NetFlow kolektor a podporoval minimálně tyto verze protokolu: v5, v7, v9 a IPFIX. Systém musí dále umožňovat provádět základní analýzu datových toků, tj. poskytovat i základní statistické přehledy dle položek obsažených v NetFlow paketech.

DOTAZ č. 5

Retence dat, zálohování, obnova a podpora pro budoucí instalaci v režimu vysoké dostupnosti a. Zde požadujete podporu vysoké dostupnosti, máme tím chápat, že si přejete dodat systém rovnou ve vysoké dostupnosti, nebo pouze, aby vysokou dostupnost podporoval pro budoucí rozšíření?

ODPOVĚď č. 5

Zadavatel požaduje pouze podporu pro budoucí instalaci v režimu vysoké dostupnosti. Řešení v režimu vysoké dostupnosti není předmětem této veřejné zakázky.

DOTAZ č. 6

Bod 1 v Obecné požadavky na systém pro centralizovanou správu logů a událostí. Systém pracuje jako virtuální appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací vyjma podpory sběru na pobočkách, agenta pro sběr Windows logů a logů z databází.

Předpokládáme, že když v další části Zadávací dokumentace je uvedeno, že Zadavatel (konkrétně bod 61) vyžaduje: Jedna hardwarová appliance o velikosti max. 2U – zadavatel chce dodat HW aplianci, a ne virtuální řešení. Prosím o potvrzení tohoto požadavku.

ODPOVĚď č. 6

Zadavatel požaduje dodávku hardwarového appliance a správné znění bodu 1 v obecných

požadavcích je proto "Systém pracuje jako hardwarový appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti."

V Krnově dne 12. 11. 2020

Bc. Robert Orel
V době nepřítomnosti ředitele SZZ K
pověřen jeho zastupováním



MUDr. Ladislav Václavec, MBA
ředitel