# Vysvětlení, změna či doplnění zadávací dokumentace č. 3

**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 zakázky tyto informace k zadávací dokumentaci.

**DOTAZ č. 1**

V ZD zadavatel požaduje v rámci dodávky log management systému kolektor pro sběr flow, ačkoliv tento systém byl soutěžen v rámci předchozí veřejné zakázky, a to dne 23. 10. 2020 v rámci výběrového řízení s názvem: "Dodávka systému pro monitoring síťových aktivit". Tento požadavek na integrovaný kolektor pro sběr flow dat vede po důsledném průzkumu trhu pouze k jednomu výrobci a nabízenému řešení, a to ke společnosti DATASYS s.r.o., která vyvinula systém Elisa Security Manager. S ohledem na výše uvedené skutečnosti je zřejmé, že tento požadavek je diskriminační, a navíc nemá technické opodstatnění právě z důvodů již předchozí soutěžené zakázky.
Předpokládáme, že tyto parametry se ocitly v zadávací dokumentaci omylem a zadavatel nemá v plánu pořizovat stejnou technologii za veřejné finance dvakrát. Vzhledem k technologickému neopodstatnění požadavku vedoucího zároveň k nehospodárnosti s veřejnými finančními prostředky žádáme o jeho odstranění ze ZD.

**ODPOVĚĎ č. 1**

V Minimálních technických požadavcích je na straně 2 v části **Požadované funkcionality, vlastnosti bezpečnostního dohledu** doslovně uvedeno: *„Musí umožnovat základní analýzu datového toku podporovaných síťových zařízení (netflow)"*. Není zde předepsáno, jakým způsobem ji má dodavatel zajistit a už vůbec se nejedná o duplicitní požadavek na zmíněné výběrové řízení naopak NBA technologie bude integrována do požadovaného řešení jako jeden ze zdrojů. Rovněž není požadována funkcionalita kolektoru pro netflow. Dodavatelé mohou ve své nabídce navrhnout, že tento požadavek naplní využitím systému pro "Dodávku systému pro monitoring síťových aktivit".

Dále na straně 3 v části **Obecné požadavky na systém pro centralizovanou správu logů a událostí je v bodu 3 uvedeno toto:** Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně), TCP 20515 (RELP, šifrovaně) a NETFLOW (minimálně verze v9 a IPFIX). Přijaté logy systém standardizuje do jednotného formátu a normalizuje základní atributy, ale zároveň systém uchovává i originální verzi zpráv.

**Netflow je standardní síťový protokol a jako takový je podporovaný většinou řešení pro příklad uvádíme dvě řešení, které tento protokol podporují. Nejde tedy v žádném případě o diskriminační požadavek. Nenabízí jej jen společnost DATASYS s.r.o.**

AllientVault OSSIM- https://cybersecurity.att.com/documentation/usm-appliance/network-data/netflow-configuration.htm?Highlight=netflow%20collection

IBM QRadar - https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_adm_netflow.html

**Opodstatnění této funkcionality je podpora pro dříve soutěžený systém pro** monitoring síťových aktivit, možnosti propojení s tímto systémem a možného doplňkového sběru dat při výpadku této technologie. Nejde o požadavek na znovupořízení této technologie, ale o její vylepšení a využití v rámci vyhodnocování bezpečnostních událostí a zvýšení dostupnosti.

**Z výše uvedených důvodů požadavek na odstranění ze ZD zamítáme.**

V Krnově dne 16. 11. 2020

MUDr. Ladislav Václavec, MBA
ředitel