SPRÁVA ŽELEZNIC

Naše zn. 73558/2023-SŽ-GŘ-O8

Věc: Vysvětlení zadávací dokumentace č. 2

Sektorová nadlimitní veřejná zakázka na dodávky s názvem:

„**Log management a SIEM**"

Správa železnic, státní organizace (dále jen „Zadavatel") obdržela dne 24. 10. 2023 v 12:22 hodin žádost o vysvětlení zadávací dokumentace. Zadavatel formou Vysvětlení zadávací dokumentace odpovídá na tuto žádost doručenou k veřejné zakázce následovně:

Dotaz č. 1:

1.

V zadávací dokumentaci je v kapitole "2.4.9 SIEM" bod 4. následující informace:" *Integrace s Log managementem: SIEM musí být plně integrované s nabízeným Log management řešením. Tím se zajišťuje, že logy z různých zdrojů jsou k dispozici pro analýzu a monitorování bezpečnostních událostí a zároveň poskytuje holistický pohled na bezpečnostní situaci organizace (SŽ). Toto však neznamená, že všechny logy uložené v prostředí Log management budou zpracovávány komponentou SIEM. SŽ požaduje, aby bylo možné licenčně rozlišit data ukládaná jen v Log management a data, která budou určena ke zpracování v komponentě SIEM*".

Dále pak kapitole "2.4 Parametry poptávaného řešení" je uvedeno, že hodnota: "Celkem událostí za vteřinu" je 40000 EPS.

Z výše uvedeno lze dovodit, že zadavatel požaduje 40000 EPS a jinou, v zadávací dokumentaci neuvedenou hodnotu EPS, která má být odbavována komponentou SIEM. To je nakonec i logický způsob, jak se architektury podobné velikosti řeší.

Předmětem této otázky je tedy kolik EPS (z celkových 40000 EPS) zadavatel požaduje odbavovat komponentou SIEM?.

Tato informace je důležitá z minimálně dvou důvodů:

(1) optimální celková cena, protože EPS pro SIEM je obecně dražší než EPS pro Log Management (i když se jedná o jeden ucelený produkt).

(2) správný návrh velikosti potřebné infrastruktury, protože SIEM je obecně náročnější na výkon než Log Management.

Oba dva výše uvedené důvody mají přímou vazbu na hodnotící kritéria a proto považujeme za nutné informaci o EPS zpracovávaných komponentou SIEM doplnit.

Odpověď:

Zadavatel počítá v projektu s napojením takových zdrojů logů, které jsou využitelné technologií SIEM a zároveň dostatečné pro naplnění souladu s legislativními požadavky na uchování logů z prostředí v Log managementu. Z tohoto důvodu nebyly specifikovány různé hodnoty požadovaných EPS pro log management a pro část SIEM, neboť v obou případech se jedná o

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

stejnou hodnotu 40000 EPS. Tazatel tedy chybně dovozuje, že Zadavatel vedle uvedené hodnoty 40000 EPS pro Log Management určí ještě jinou hodnotu, která má být odbavována technologií SIEM.
Požadavek na možnost rozlišit logy určené jen pro Log management je důležitý pro pokrytí možných stavů budoucích (neřízený nárůst počtu logů vlivem provozního stavu prostředí, nebo při kybernetickém ohrožení), nebo změn prováděných v prostředí Zadavatele, kdy mohou vznikat požadavky na logování provozních a bezpečnostních událostí bez nutnosti vyhodnocování jejich bezpečnostního kontextu komponentou SIEM.

Závěr

Zadavatel setrval na zadávacích podmínkách. Jeho vysvětlení zcela odpovídá původnímu znění zadávací dokumentace. Neprovedl tak žádnou změnu zadávací dokumentace. Lhůta pro podání nabídek se tak nemění a je stanovena na den 7. 11. 2023 do 8:30 hodin.

Ing. Dalibor Fajkus
27.10.2023 12:36
Podepsáno elektronicky

.....
Ing. Dalibor Fajkus
náměstek ředitele organizační jednotky pro rozvoj