SPRÁVA ŽELEZNIC

Naše zn. 48759/2023-SŽ-GŘ-O8

Vyřizuje Dagmar Strnadová

Věc: Vysvětlení zadávací dokumentace č. 1

Sektorová nadlimitní veřejná zakázka dle § 56 zákona č. 134/2016 sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „Zákon") na služby s názvem:

„**Implementace systému Extended Detection and Response (XDR)**"

Správa železnic, státní organizace (dále jen „Zadavatel") obdržela dne 19. 7. 2023 v 11:51 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 bodě č. 2.3.4.1, dokumentu Příloha č. 1 (Technická specifikace), stejně tak v Příloze č. 19 (XDR dotazník) zadavatel požaduje pro NDR systém:
   - *detekce v sandboxu pomocí virtuálního spuštění (detonace) - detekce anomálií.*
   - *Detonace/virtuální spuštění podezřelého obsahu, který mohl být zachycen v jakémkoli místě dohledované sítě, **v místním sandboxu** s podrobným výstupem výsledku detonace v jednotné konzoli bezpečnostního analytika.*

   Vzhledem k tomu, že

   - je dnes většina dat přenášena šifrovanými protokoly (dle dat Google z roku 2021 94%, dnes určitě více) nebo datovými tunely útočníka, kdy se NDR řešení bez koncové aplikace nemá možnost ke kritickým datům vůbec dostat a sandbox využít, je přínos požadovaného parametru praktický nulový,
   - se jedná o požadavek, který nepatří do oblasti NDR řešení (např. dle Gartner nebo Forrester) a de facto vylučující pro naprostou většinu jiných NDR výrobců
   - se jedná o kompetenci bezpečnostních technologií typu firewall, GW a endpoint ochrany,
   - v případě kvalitní next-gen endpoint ochrany s přechodem na AI a implementaci různých Deep Learnig AI enginů do endpoint ochrany (u TOP výrobců) je prováděna „Detonace" přímo na klientovi bez nutnosti využívání externích sandboxů,
   - rovněž z ekonomického pohledu je NDR se sandbox technologií v jednom řešení násobně dražší než ostatní konkurence,

   na základě tohoto navrhujeme zadavateli přehodnotit požadavek na sandbox technologii v oblasti NDR (Network Detection and Response) jako volitelný a zaměřit se na skutečné funkcionality NDR, jako jsou analýza chování zařízení ve vnitřní síti založená na algoritmické detekci a detekci známých projevů útoků, hrozeb a anomálií.

   Dotaz 1: Může zadavatel potvrdit, že souhlasí s plněním daného požadavku v technologii NDR jako nepovinným nebo volitelným?

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

Odpověď č. 1:
Požadavek vychází z potřeby ochrany síťového provozu, který může být jak interního, tak externího charakteru, a proto je vyžadována tato funkcionalita pro veškerý provoz, který bude sondami NDR rozmístěnými v infrastruktuře zadavatele zpracováván. Navíc je předpokládáno, že provoz, který budou zpracovávat NDR sondy, nebude v interakci pouze se zařízeními, na kterých bude instalován Endpoint agent. Proto není možné spoléhat na přenesení této funkcionality na koncové zařízení.
Z ekonomického hlediska se jedná o požadavek vedoucí právě k úspoře finančního prostředků, neboť je vyžadováno, chránit jediným nástrojem pro detonaci podezřelého obsahu všechny určené rizikové komunikace organizace.
Samozřejmě byl při přípravě technické specifikace zadávací dokumentace zohledňován i případný poměr šifrovaného a nešifrovaného provozu, ale uvedené údaje od Google ze zaslaného dotazu v žádném případě neodpovídají charakteristice interního provozu zadavatele, kde je výrazně větší podíl nezabezpečeného provozu, než uvádí Google ve svých statistikách o internetovém provozu.

Požadavek zadavatele zůstává povinný.

Dotaz č. 2:

2. V bodě č. 2.3.4.1 dokumentu Příloha č. 1 (Požadavky na Network Detection and Response), stejně tak v Příloze č. 19 (XDR dotazník) je požadována funkcionalita:
   - *DROP při in-line zapojení, nebo TCP Reset pro out-of-band připojení.*

   Vzhledem k tomu, že

   - tato funkcionalita, může být efektivně splněna požadovanou komponentou EDR nebo XDR, nebo případně prostřednictvím integrací s jinými architektonickými bezpečnostními prvky jako např. firewall nebo Network Access Control,
   - v bodě č. 2.1, dokumentu Příloha č. 1 (Technická specifikace) zadavatel umožňuje využití jak NDR, tak EDR komponenty: *„Požadovaná bezpečnostní platforma musí umožnit identifikaci nebezpečných projevů v síťovém provozu, jehož analýzu bude řešení provádět na základě pasivního odposlechu a bez jeho jakéhokoli ovlivnění a na koncových zařízeních prostřednictvím softwarového agenta.“*

Dotaz 2: Povoluje zadavatel splnění uvedeného požadavku prostřednictvím EDR komponenty, nebo v případě, že nikoliv, prostřednictvím integrace s některým z jiných architektonických bezpečnostních prvků zadavatele jako např. firewall nebo Network Access Control?

Odpověď č. 2:
Zadavatel nepovoluje splnění uvedeného požadavku prostřednictvím EDR komponenty. Stejně jako u předchozího dotazu je třeba chápat prostředí zadavatele tak, že nebude možné zajistit ochranu všech koncových zařízení agentem EDR, který by mohl provádět reakční/blokační procesy. Z tohoto důvodu, je požadováno, aby v případě potřeby, umožňovalo NDR řešení takovou funkcionalitu a pomohlo tak včas reagovat na případné šíření nákazy.
Integrace s nástroji NAC, firewally a podobnými prvky není možná ve všech lokalitách zadavatele, neboť takové prvky nemusejí být všude dostupné.

Požadavek zadavatele tak zůstává beze změny.

Dotaz č. 3:

3. V bodě č. 2.3.4.1 dokumentu Příloha č. 1 (Požadavky na Network Detection and Response), stejně tak v Příloze č. 19 (XDR dotazník) je požadována funkcionalita:
   - *Schopnost umístit škodlivý email do karantény.*

   Vzhledem k tomu, že

   - tato uvedená funkcionalita může být efektivně splněna požadovanou komponentou EDR, která zabrání spuštění škodlivého souboru přijatého emailem nebo eliminuje techniky útočníků jako je emailový phising,
   - v bodě č. 2.1, dokumentu Příloha č. 1 (Technická specifikace) zadavatel umožňuje využití jak NDR, tak EDR komponenty: *„Požadovaná bezpečnostní platforma musí umožnit identifikaci nebezpečných projevů v síťovém provozu, jehož analýzu bude řešení provádět na základě pasivního odposlechu a bez jeho jakéhokoli ovlivnění a na koncových zařízeních prostřednictvím softwarového agenta."*

   Dotaz 3: Povoluje zadavatel splnění uvedeného požadavku prostřednictvím EDR komponenty?

Odpověď č. 3:
Stejně jako u předchozího dotazu je třeba chápat prostředí zadavatele tak, že nebude možné zajistit ochranu všech koncových zařízení agentem EDR, který by mohl provádět detekci škodlivého kódu v elektronické poště s reakcí umístění takové nákazy do karantény.
Cílem je, aby bylo možné využít řešení NDR k ochraně vnitřních síťových komunikací a pro komunikace nad protokolem elektronické pošty šlo použít akci „umístit do karantény" namísto pouhé detekce, nebo opakovaných pokusů o zastavení provozu na úrovni TCP-RST, neboť mailové servery mají ze své podstaty ambice pokoušet se doručovat zprávy elektronické pošty opakovaně.

Požadavek zadavatele zůstává povinný a není možné přenést tuto funkci pouze na komponenty EDR.

Dotaz č. 4:

4. V dokumentu přílohy č.5 - Harmonogram je fáze F3 „Školení" navázána na fázi F2.a. Fáze F3 běží paralelně s fází F2.b „Napojení na platformu Log management / SIEM" a konec je pro obě fáze identický.

   Dotaz 4: Znamená to, že toto napojení, resp. funkcionality vyplývající z požadovaných výstupů F3, nemusí být součástí školení?

Odpověď č. 4:
Ano, výstupy Fáze F3 nebudou součástí školení. Školení bude realizováno po dokončení fáze F2.a (Optimalizace bezpečnostní / detekční politiky řešení).

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 14. 8. 2023 do 10:00 hodin.

Ing. David Miklas
20.07.2023 09:59
Podepsáno elektronicky

.....

Ing. David Miklas
ředitel Správy železniční telematiky