SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne
Naše zn. 83586/2022-SŽ-GŘ-O8
Listů/příloh 2/1

Vyřizuje Veronika Nováková
Mobil
E-mail NovakovaM@spravazeleznic.cz

Datum 7. prosince 2022

Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem „*Network Detection and Response*"

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „*Zadavatel*") Vás touto cestou informuje o tom, že připravuje zadávací řízení na veřejnou zakázku „*Network Detection and Response*". Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen „*PTK*"), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení a způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Zadavatel jako subjekt povinný v souladu s ustanoveními §3 písm. c), d), ve znění §2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále také „ZoKB"), je na základě platného Plánu zvládání rizik v oblasti kybernetické bezpečnosti zavázána provádět bezpečnostní opatření (viz §5 ZoKB) pro zajištění kybernetické bezpečnosti informačních a komunikačních systémů spravovaných Zadavatelem. Detekce kybernetických bezpečnostních událostí v síti Zadavatele je jedním ze způsobů, jak naplnit tyto povinnosti.

Jako technické opatření k naplnění výše uvedeného se Zadavatel připravuje k realizaci implementace systému pro zajištění detekce projevů kybernetických hrozeb a podpory návazných procesů, tedy systému Network Detection and Response (NDR). Tento nástroj zajistí sběr informací o síťovém provozu, jeho zpracování, detekci nebezpečných projevů, které jsou ve sledovaném síťovém provozu ukryty a přispěje ke schopnosti takové události vyšetřit a rychle na ně reagovat.

Network Detection and Response bude implementován v prostředí Zadavatele, které tvoří velmi rozsáhlá a komplikovaná ICT infrastruktura rozmístěná v lokalitách rozprostřených po celém území České republiky.

PTK je podle Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. 2. 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES a podle § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „*Zákon*") možností zadavatele předtím, než vyhlásí veřejnou zakázku, přičemž zadavatel má možnost v rámci PTK komunikovat s dodavateli (případně dalšími relevantními osobami) s cílem připravit zadání veřejné zakázky a informovat hospodářské subjekty (resp. dodavatele) o svých plánech a požadavcích při zadávání veřejných zakázek – zadavatel přitom může v rámci PTK i zjišťovat možnosti dodavatelů a případně i jejich návrhy řešení.

Správa železniční dopravní cesty, 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.szdc.cz

Generální ředitelství
Dlážděná 1003/7
110 00 Praha 1

Forma předběžné tržní konzultace: písemná (s možností pokračování ústní formou)

V rámci PTK žádáme o zodpovězení dotazů zadavatele uvedených v příloze č. 1 této pozvánky. Odpovědi, které obdrží Zadavatel budou pečlivě analyzovány a vyhodnoceny. S ohledem na účel PTK Zadavatel přihlédne i k opožděným odpovědím, bude-li to možné a vhodné pro účel PTK. Zadavatel však žádá účastníky, aby stanovené termíny dodrželi. Dojde-li Zadavatel k závěru, že některá témata zůstávají nadále nejasná, sporná či vyvstane potřeba objasnění dalších doplňujících dotazů, přistoupí Zadavatel ke konání dalšího kola PTK, které může být uskutečněno opět písemnou formou, případně si Zadavatel vyhrazuje možnost požádat zástupce dodavatelů o realizaci prezenčního jednání. Tento postup bude Zadavatelem opakován, dokud nebudou obdrženy veškeré informace potřebné ke správnému nastavení parametrů veřejné zakázky s názvem „Network Detection and Response". Zadavatel o dalším průběhu PTK osloví vždy minimálně ty dodavatele, kteří projevili zájem o PTK v předcházejícím kole.

V případě Vašeho zájmu o účast na této PTK, zašlete své odpovědi na otázky uvedené v příloze č. 1 této pozvánky na emailovou adresu: hemzova@spravazeleznic.cz

Svoji odpověď prosím doručte nejpozději do 16. 12. 2022.

Dodavatel by ve své odpovědi měl uvést minimálně:

- název dodavatele a sídlo dodavatele;
- IČO dodavatele;
- jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail);
- odpovědi na přiložené otázky.

Pro bližší informace ohledně PTK se lze obrátit na tuto emailovou adresu: cnitptk@spravazeleznic.cz

Zadavatel sděluje, že připravovaná veřejná zakázka je plánována k zadání jako nadlimitní sektorová veřejná zakázka.

Předpokládaný počátek plnění předmětu veřejné zakázky je 2. polovina 2023. Předpokládaná délka trvání veřejné zakázky je 12 měsíců, přičemž tato délka může být na základě realizované PTK upravena.

PTK nesmí vést k porušení základních zásad Zákona. Průběh i výsledek PTK proto bude zaznamenán ve zprávě vytvořené Zadavatelem. Informace z PTK užité v zadávacích podmínkách veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na PTK podílely. Zadavatel současně uvede v zadávacích podmínkách i všechny podstatné informace, které byly obsahem PTK a ovlivnily nastavení zadávacích podmínek.

Děkuji za spolupráci.

S pozdravem

Ing. David Miklas
08.12.2022 09:56
Podepsáno elektronicky

Ing. David Miklas
ředitel Správy železničních informačních technologií

Přílohy:
Příloha 1 – Otázky pro písemnou část PTK

Předběžná tržní konzultace – Network Detection and Response – Příloha 1

Dotazy k technickému řešení

Uveďte, zda vámi nabízené řešení podporuje požadované funkcionalita a pokud „ANO", tak specifikujte, jakým způsobem.

Požadovaná funkcionalita řešení NDR	ANO/NE	Způsob naplnění
Umožňuje řešení záznam popisných metadat o síťové komunikaci pro její pozdější analýzu? Záznamem je myšleno uložení popisných informací přímo v nabízením řešení, kde bude probíhat také jejich následná analýza. Pokud „ANO", tak uveďte detail, který je o komunikaci zaznamenán v případě, že se jedná o: - nešifrované SMTP spojení (e-mail nesoucí .DOCX jako přílohu) - šifrované SMTP spojení - nešifrovaný přístup k webové stránce (http), ze které byl stahován soubor - šifrovaný přístup k webové stránce (https) Popište způsob uložení metadat (např. logy, databáze)		
Probíhá analýza síťového provozu pro veškerý IT síťový provoz, a to bez ohledu na použité komunikační protokoly, probíhající spojení a síťové porty?		
Pracuje funkcionalita analýzy a záznamu síťového provozu nad zrcadleným provozem sítě?		
Zahrnuje řešení připravená pravidla pro analýzu provozu umožňující definovat podmínky odkazující se na přenášený obsah a parametry aplikační vrstvy? (Například odhalit přenášené soubory, kde koncovky soborů nesouhlasí s obsahem, nebo čísla typických portů nesouhlasících s typem rozpoznaného komunikačního protokolu.) (*V sekci **Způsob naplnění** uveďte i typ a počet takových pravidel.)*		
Umožňuje řešení přizpůsobení pravidel pro analýzu provozu nebo tvorbu vlastních pravidel pro analýzu?		
Umožňuje řešení definovat pravidla hledající souběh událostí nebo posloupnost událostí v síťovém provozu a generovat upozornění (alerty) a to kontinuální analýzou okamžitého dění i analýzou již uložených historických záznamů o provozu zpětně?		
Jsou historické informace o provozu s určenou dobou retence pro následnou analýzu chráněna před narušením jejich integrity?		
Umožňuje řešení provádět analýzu šifrovaného spojení a detekci narušení i při nevyužívání SSL dešifrování (např. díky kontrole konzistence použitých certifikátů, kvality šifrovacích algoritmů, nebo JA3 tagů)?		
Je detekce malware prováděna pomocí vyhledávání signatur?		
Je detekce malware prováděna pomocí heuristické analýzy?		
Je detekce malware prováděna pomocí vyhledávání typického chování (behaviorální analýza)?		

Je detekce malware prováděna detekcí na sandboxu virtuálním provedení?		
Je součástí dodávky pravidelná služba aktualizace signatur (definice chování malware) a aktualizace pravidel sandboxu? (*V sekci **Způsob naplnění** uveďte obvyklý interval jejich aktualizací.)*		
Je řešení schopné detekovat také malware skrytý hluboko v přenášeném obsahu? (Například v komprimovaných souborech, v embeded obsahu dokumentů kancelářských aplikací).		
Podporuje řešení pro účel huntingu obsahovou analýzu?		
Je možné definovat vlastní pravidla pro analýzu a detekci obsahu?		
Je možné pracovat s metadaty popisujícími obsahové části síťového provozu?		
Poskytuje řešení webové uživatelské rozhraní pro analýzu zaznamenaného provozu bezpečnostními specialisty, které bude součástí jednotného uživatelského rozhraní?		
Poskytuje uživatelské rozhraní vysokou granularitu řízení přístupových oprávnění k jednotlivým modulům systému a zpracovávaným/zaznamenaným metadatům? Umožňuje řešení řídit oprávnění pro pracovníky pracoviště SOC v úrovních: - L1 operátor, který musí pracovat jen s přiděleným alertem a jemu relevantními metadaty - L2 analytik pracující napříč aletry a jim přidruženými metadaty - L3 security exprt, který může provádět hunting, tedy vyhledávání nespecifických metadat		
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 40Gbps?		
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 25Gbps?		
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 10Gbps?		
Podporuje řešení monitorování provozu na rozhraních Ethernet s rychlostí 1Gbps?		
Umožňují komponenty systému, které uchovávají data pro analýzu, provoz v on-premise prostředí? *(Pro Zadavatele není přípustné přenášet data o síťovém provozu do cloudových platforem výrobce.)*		
Jaké jsou podporované způsoby nasazení nabízeného řešení? (např. fyzické appliance výrobce, open-servery, virtualizace, …)		
Podporuje řešení logování a napojení do systému log managementu? (*V sekci **Způsob naplnění** specifikujte i používané protokoly a možnost úpravy logovaných informací.)*		
Podporuje řešení napojení do systému SIEM? (*V sekci **Způsob naplnění** specifikujte typ předávaných informací i používané protokoly.)*		

Rozšiřitelnost řešení a integrace

Zadavatel uvažuje o dalším rozšiřování platformy pro detekci a reakci na kybernetické hrozby, proto uveďte, zda je nabízené řešení komplementární s nástrojem Endpoint Detection and Response (EDR) a to s takovým nástrojem stejného výrobce jako NDR, nebo produktem třetí strany.

Zadavatel požaduje, aby případné spojení nástrojů NDR a EDR bylo na úrovni:

- Integrace GUI nástrojů, se kterými pracuje analytický tým SOC
- Vzájemném obohacování informací o událostech mezi NDR a EDR
- Podpora automatizačních procesů při reakci na události

Popište, zda a jakým způsobem, je integrace NDR a EDR podporována ve vámi nabízením řešení.

Licenční model a podmínky

Popište licenční model a licenční podmínky platné pro všechny součásti řešení. Jaký je licenční model produktu NDR, tedy dle jakých vstupních údajů se odvíjí licencování a výkonnostní plánování řešení.

- objem síťového provozu
- množství síťových zařízení, která se účastni sledovaného provozu
- objem dat, generovaných nástrojem pro analýzu
- počet administrátorů systému
- případně uveďte jiné licenční parametry

Potřebné informace pro návrh a nacenění nabídek k budoucí veřejné zakázce

Uveďte, jaké jsou potřebné informace, které by Zadavatel měl uvést v rámci zadávací dokumentace tak, aby budoucí uchazeči mohli sestavit svou nabídku včetně nabídkové ceny za poptávané plnění. V případě, že pro tento účel využíváte formuláře pro sběr potřebných dat, prosíme o jejich přiložení k odpovědi.