VŠEOBECNÁ ZDRAVOTNÁ POISŤOVŇA

Vysvetlenie súťažných podkladov č. 1

Verejný obstarávateľ: Všeobecná zdravotná poisťovňa, a.s.
Predmet zákazky: Testovanie zraniteľnosti interných systémov
Číslo zákazky: 978

Otázka č. 1 – Infraštruktúra potrebná na prevádzku riešenia

Znenie otázky uchádzača

Zo súťažných podkladov vyplýva, že predmetom obstarávania je aj hardvérová alebo infraštruktúrna platforma centrálnej konzoly. Nie je však jednoznačne uvedené, na akej infraštruktúre majú byť prevádzkované ostatné komponenty riešenia, najmä distribuované alebo prídavné skenery.

Žiadame verejného obstarávateľa o vysvetlenie, či budú ostatné komponenty riešenia, najmä distribuované alebo prídavné skenery, nasadené na existujúcej infraštruktúre verejného obstarávateľa, alebo či má potrebnú serverovú, virtualizačnú, úložiskovú, operačnú a databázovú infraštruktúru dodať úspešný uchádzač (nie je obsahom aktuálnej súťaže).

Odpoveď verejného obstarávateľa

Distribuované a prídavné skenery budú prevádzkované na existujúcej infraštruktúre verejného obstarávateľa.

Verejný obstarávateľ zabezpečí potrebnú serverovú, virtualizačnú, výpočtovú, pamäťovú, úložiskovú, sieťovú a systémovú infraštruktúru vrátane príslušných operačných a databázových komponentov potrebných na prevádzku distribuovaných a prídavných skenerov.

Súčasťou dodávky poskytovateľa budú potrebné softvérové komponenty a licencie VM riešenia, ich inštalácia, konfigurácia a integrácia s centrálnou konzolou.

Rozsah dodávky centrálnej konzoly zostáva v súlade so súťažnými podkladmi.

Otázka č. 2 – Počet sieťových segmentov a lokalít

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 3, verejný obstarávateľ požaduje podporu pokrytia požadovaných segmentov siete. Počet segmentov a lokalít však nie je v predmetnom ustanovení špecifikovaný.

Žiadame verejného obstarávateľa o uvedenie:

- predpokladaného počtu sieťových segmentov určených na skenovanie,
- predpokladaného počtu fyzických alebo geografických lokalít,
- počtu dátových centier,
- predpokladaného počtu oddelených skenovacích zón,
- informácie, či sú jednotlivé segmenty a lokality vzájomne sieťovo dostupné,
- informácie, či sa v prostredí nachádzajú izolované alebo offline segmenty bez priameho spojenia s centrálnou konzolou.

Uvedené informácie sú potrebné na stanovenie počtu distribuovaných skenerov a správne dimenzovanie architektúry riešenia.

Odpoveď verejného obstarávateľa

Na účely dimenzovania riešenia sa vychádza z približne 600 sieťových segmentov, 100 geografických lokalít, 2 dátových centier a 5 oddelených skenovacích oblastí.

V prostredí verejného obstarávateľa sa nachádzajú aj izolované alebo offline sieťové segmenty bez priameho sieťového spojenia s centrálnou konzolou. Nemožno preto predpokladať vzájomnú sieťovú dostupnosť všetkých segmentov a lokalít.

Riešenie musí podporovať distribuované skenovanie vrátane prevádzky v izolovaných prostrediach, pri rešpektovaní bezpečnostných obmedzení verejného obstarávateľa.

Konkrétne umiestnenie skenovacích komponentov, nastavenie sieťovej komunikácie a spôsob bezpečného prenosu výsledkov z izolovaných prostredí budú určené v rámci implementačnej analýzy.

Otázka č. 3 – Autentifikované skenovanie Microsoft Windows

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 5, sa požaduje vykonávanie credentialed skenov pre systémy Microsoft Windows. Žiadame uviesť operačné systémy a ich verzie (serverové a klientske), predpokladaný počet Windows serverov a pracovných staníc, doménové členstvo a spôsob poskytnutia účtov a oprávnení.

Odpoveď verejného obstarávateľa

Na účely dimenzovania riešenia sa vychádza z orientačného počtu 300 serverov Microsoft Windows a 1 800 pracovných staníc a notebookov.

Prostredie zahŕňa najmä operačné systémy Windows Server 2019, Windows Server 2022, Windows Server 2025 a Windows 11.

Autentifikované skenovanie musí umožňovať identifikáciu známych zraniteľností operačných systémov, chýbajúcich bezpečnostných aktualizácií a podporovaných bezpečnostných konfigurácií.

Potrebné účty a oprávnenia zabezpečí verejný obstarávateľ v súčinnosti s poskytovateľom. Autentifikácia a rozsah oprávnení budú nastavené v súlade s bezpečnostnými politikami verejného obstarávateľa a princípom minimálnych oprávnení.

Otázka č. 4 – Autentifikované skenovanie Linux

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 6, sa požadujú credentialed skeny pre Linux. Žiadame uviesť distribúcie a verzie, predpokladaný počet serverov alebo zariadení, verzie alebo rady jadra, požadovaný spôsob autentifikácie a spôsob poskytnutia účtov, kľúčov a oprávnení.

Odpoveď verejného obstarávateľa

Na účely dimenzovania riešenia sa vychádza z orientačného počtu 200 serverových systémov Linux, najmä distribúcií Red Hat Enterprise Linux, Ubuntu, Debian a Rocky Linux.

Autentifikované skenovanie musí umožňovať identifikáciu známych zraniteľností operačných systémov, nainštalovaných softvérových balíkov, chýbajúcich bezpečnostných aktualizácií a podporovaných bezpečnostných konfigurácií.

Autentifikácia bude realizovaná prostredníctvom SSH s využitím hesla alebo SSH kľúča, prípadne s použitím mechanizmu sudo, ak je potrebný na vykonanie príslušných kontrol.

Potrebné účty, kľúče a oprávnenia zabezpečí verejný obstarávateľ bezpečným spôsobom v súčinnosti s poskytovateľom.

Otázka č. 5 – Autentifikované skenovanie sieťových zariadení

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 7, sa požadujú credentialed skeny sieťových zariadení. Žiadame typy, výrobcov, produktové rady a verzie firmvéru, počty smerovačov, prepínačov, firewallov, bezdrôtových zariadení, load balancerov, VPN zariadení a ostatných prvkov, ako aj autentifikačné protokoly, rozhrania a spôsob poskytnutia oprávnení.

Odpoveď verejného obstarávateľa

Na účely dimenzovania riešenia sa vychádza z orientačného počtu 700 sieťových a bezpečnostných zariadení, najmä smerovačov, prepínačov, firewallov, VPN zariadení, bezdrôtových sieťových zariadení a load balancerov.

Skenovanie bude zamerané na identifikáciu známych zraniteľností operačných systémov a firmvéru zariadení, dostupných bezpečnostných aktualizácií a podporovaných bezpečnostných konfigurácií.

Autentifikované kontroly budú využívať SSH, HTTPS/API, SNMPv3 alebo iné bezpečné rozhrania podľa technických možností zariadení a podporovaných funkcií dodávaného riešenia.

Potrebné účty a oprávnenia zabezpečí verejný obstarávateľ v súčinnosti s poskytovateľom.

Otázka č. 6 – Autentifikované skenovanie databáz

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 8, sa požaduje vykonávanie credentialed skenov pre databázy.

Žiadame verejného obstarávateľa o uvedenie typov, výrobcov a verzií databázových systémov, ktoré majú byť predmetom credentialed skenovania, ako aj predpokladaného počtu databázových serverov alebo inštancií.

Zároveň žiadame objasniť, či sa požaduje:

- skenovanie operačného systému databázového servera,
- autentifikované preverenie databázovej platformy,
- kontrola konfigurácie databázy,

- identifikácia zraniteľností databázového softvéru,
- alebo kombinácia uvedených činností.

Verejného obstarávateľa zároveň žiadame uviesť, či poskytne účty a oprávnenia potrebné na vykonanie požadovaných kontrol.

Odpoveď verejného obstarávateľa

Požaduje sa podpora autentifikovaného skenovania databázových platforiem, najmä Microsoft SQL Server.

Požadovaný rozsah zahŕňa identifikáciu známych zraniteľností databázového softvéru, chýbajúcich bezpečnostných aktualizácií a podporovaných bezpečnostných konfigurácií.

Súčasťou požadovanej funkcionality je skenovanie operačného systému databázového servera a autentifikované preverenie databázovej platformy prostredníctvom podporovaných rozhraní.

Potrebné účty a oprávnenia poskytne verejný obstarávateľ v rámci implementácie v súlade s bezpečnostnými politikami a princípom minimálnych oprávnení.

Otázka č. 7 – Ďalšie relevantné typy aktív

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 9, sa požadujú credentialed skeny pre ďalšie relevantné typy aktív podľa prostredia verejného obstarávateľa.

Uvedené vymedzenie neumožňuje uchádzačom jednoznačne určiť rozsah požadovaného plnenia.

Žiadame verejného obstarávateľa o presnú špecifikáciu ďalších relevantných typov aktív, ktoré majú byť predmetom credentialed skenovania.

Pri každom type aktíva žiadame podľa dostupnosti uviesť:

- kategóriu aktíva,
- výrobcu,
- produktový rad alebo konkrétny produkt,
- používanú verziu,
- predpokladaný počet aktív,
- požadovaný spôsob autentifikácie,
- požadovaný rozsah skenovania.

Odpoveď verejného obstarávateľa

Na účely dimenzovania riešenia sa vychádza z orientačného rozsahu infraštruktúry zahŕňajúceho približne 1 800 pracovných staníc a notebookov, 300 serverov Microsoft Windows, 200 serverov Linux a 700 sieťových a bezpečnostných zariadení.

Požadovaná minimálna licenčná kapacita VM riešenia zostáva 2 500 zariadení v súlade so súťažnými podkladmi.

Uvedené orientačné počty predstavujú informáciu o rozsahu prostredia a nemenia požadovanú minimálnu licenčnú kapacitu. Riešenie musí umožňovať plánovanie skenovania podľa skupín aktív, harmonogramov a prevádzkových potrieb verejného obstarávateľa pri dodržaní licenčných podmienok ponúkaného riešenia.

Riešenie musí podporovať evidenciu aktív, identifikáciu zraniteľností, vyhodnocovanie ich závažnosti, sledovanie stavu nápravných opatrení a reporting.

Podpora ďalších technologických platforiem, najmä hypervízorov, virtualizačných prostredí, dátových úložísk, zálohovacích systémov a aplikačných platforiem, predstavuje možnosť budúceho rozšírenia riešenia. Tieto kategórie nepredstavujú požiadavku na samostatné kapacitné navýšenie základného rozsahu dodávky.

Otázka č. 8 – Segmentácia dát

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 16, sa požaduje segmentácia dát. Zo súťažných podkladov nie je jednoznačné, aký konkrétny spôsob segmentácie verejný obstarávateľ požaduje.

Žiadame verejného obstarávateľa o spresnenie požiadavky na segmentáciu dát, najmä o uvedenie, podľa akých kritérií majú byť dáta oddelené.

Žiadame objasniť, či sa má segmentácia realizovať napríklad podľa:

- organizačných útvarov,
- lokalít,
- sieťových segmentov,
- dátových centier,
- vlastníkov aktív,
- typov aktív,
- kritickosti aktív,
- používateľských rolí,
- skenovacích zón,
- alebo iných kritérií.

Zároveň žiadame uviesť, či sa požaduje iba logické oddelenie a obmedzenie prístupu prostredníctvom rolí a oprávnení, alebo aj samostatné dátové repozitáre, samostatné skenovacie zóny, samostatné reportovanie alebo iný spôsob technického oddelenia údajov.

Odpoveď verejného obstarávateľa

Požaduje sa logická segmentácia údajov v rámci centrálnej platformy, najmä podľa organizačného zaradenia, lokalít, sieťových segmentov, vlastníkov aktív, typov a kritickosti aktív, skenovacích oblastí a používateľských rolí.

Riešenie musí podporovať riadenie prístupových oprávnení prostredníctvom rolí (RBAC), vytváranie skupín aktív, filtrovanie výsledkov a samostatné reportovanie podľa definovaných skupín aktív.

Fyzicky oddelené dátové repozitáre ani samostatné centrálne konzoly na účely segmentácie údajov sa nepožadujú.

Otázka č. 9 – Export dát do SIEM

Znenie otázky uchádzača – dostupná časť

V časti 5. Technické požiadavky, bod 18, sa požaduje export dát do SIEM.

Žiadame verejného obstarávateľa o uvedenie konkrétneho SIEM riešenia, do ktorého má byť export realizovaný, vrátane:

Odpoveď verejného obstarávateľa

Cieľovým systémom je IBM QRadar prevádzkovaný v infraštruktúre verejného obstarávateľa (on-premises).

Požaduje sa jeden integračný tok umožňujúci automatizovaný export informácií o identifikovaných zraniteľnostiach prostredníctvom kompatibilného syslog alebo API rozhrania.

Prenášané údaje budú zahŕňať minimálne identifikáciu aktíva, identifikátor CVE, ak existuje, závažnosť zraniteľnosti, stav nálezu a čas detekcie.

Export bude realizovaný po ukončení skenovania alebo podľa konfigurovateľného intervalu. Prenos údajov musí byť zabezpečený primeraným spôsobom podľa možností použitých integračných rozhraní.

Otázka č. 10 – Integrácia s ITSM/ticketingovým systémom

Znenie otázky uchádzača

V časti 5. Technické požiadavky, bod 19, sa požaduje integrácia s ITSM alebo ticketingovým systémom.

Žiadame verejného obstarávateľa o uvedenie konkrétneho ITSM alebo ticketingového systému, s ktorým má byť riešenie integrované, vrátane:

- výrobcu a názvu produktu,
- používanej verzie,

- spôsobu nasadenia, teda on-premise, cloud alebo hybrid,
- dostupných integračných rozhraní,
- používaného spôsobu autentifikácie,
- požadovaného rozsahu integračných tokov.

Zároveň žiadame spresniť:

- či má byť integrácia jednosmerná,
- pri akých udalostiach sa má ticket alebo úloha automaticky vytvoriť,
- aké údaje sa majú do ticketu prenášať,
- koľko typov ticketov, formulárov alebo integračných workflowov má úspešný uchádzač implementovať.

Odpoveď verejného obstarávateľa

Cieľovým ITSM/ticketingovým systémom je OTRS.

Požaduje sa jednosmerná integrácia s jedným základným workflowom na automatické vytváranie ticketov pri identifikácii nových zraniteľností s vysokou alebo kritickou závažnosťou.

Prenášané údaje budú zahŕňať identifikáciu aktíva, identifikátor CVE, ak existuje, závažnosť, opis zraniteľnosti a odporúčané nápravné opatrenie.

Integrácia bude realizovaná prostredníctvom podporovaného integračného rozhrania a bude zahŕňať mechanizmus predchádzania vytváraniu duplicitných ticketov pre rovnakú zraniteľnosť na rovnakom aktíve.

Konkrétne technické nastavenie integračného rozhrania a autentifikácie bude určené počas implementácie v súčinnosti s verejným obstarávateľom.

Otázka č. 11 – Offline aktualizácie databázy zraniteľností

Znenie otázky uchádzača

V časti 11. SLA a podpora, bod 7, sa požaduje zabezpečenie aktualizácií databáz zraniteľností. Zo súťažných podkladov nie je jednoznačná požadovaná frekvencia ani spôsob vykonávania aktualizácií v prípade offline režimu.

Žiadame verejného obstarávateľa o uvedenie požadovanej frekvencie aktualizácie databázy zraniteľností v prostredí bez priameho prístupu riešenia k aktualizačnej službe výrobcu.

Zároveň žiadame spresniť:

- či sa požaduje manuálny prenos a import aktualizačných balíkov zo strany poskytovateľa,
- či verejný obstarávateľ umožní vytvorenie riadeného alebo sprostredkovaného aktualizačného spojenia,

- kto bude zodpovedný za stiahnutie, bezpečný prenos a import aktualizačných balíkov,
- či sa aktualizácie budú vykonávať v pracovnom čase alebo aj mimo pracovného času,
- aká je maximálna prípustná doba medzi zverejnením aktualizácie výrobcom a jej nasadením v prostredí verejného obstarávateľa.

Odpoveď verejného obstarávateľa

Aktualizácie databázy zraniteľností musia byť vykonávané najmenej raz týždenne, ak výrobca sprístupnil nové aktualizácie, najneskôr do 7 kalendárnych dní od ich sprístupnenia výrobcom.

Riešenie musí podporovať manuálne získanie, bezpečný prenos a offline import aktualizačných balíkov bez potreby priameho internetového pripojenia skenovacích komponentov.

Poskytovateľ zabezpečí počas 60-mesačného obdobia technickej podpory získanie, bezpečný prenos a aplikovanie dostupných aktualizačných balíkov vrátane offline prostredí, v súčinnosti s verejným obstarávateľom a pri dodržaní jeho bezpečnostných pravidiel.

Bežné aktualizácie sa budú vykonávať v pracovnom čase v rámci dohodnutého režimu technickej podpory. Verejný obstarávateľ zabezpečí potrebnú súčinnosť a schvaľovanie prístupu do izolovaných prostredí.

Aktualizačný mechanizmus musí umožňovať overenie integrity aktualizačných balíkov, kontrolu aktuálnosti databázy a overenie úspešného aplikovania aktualizácií.

Otázka č. 12 – Aktualizácie pluginov, signatúr a detekčných mechanizmov

Znenie otázky uchádzača

V časti 11. SLA a podpora, bod 8, sa požadujú aktualizácie pluginov, signatúr alebo ekvivalentných detekčných mechanizmov. Keďže zabezpečovanie týchto aktualizácií má byť súčasťou podpory poskytovateľa, ich frekvencia má priamy vplyv na rozsah služieb a cenovú ponuku.

Žiadame verejného obstarávateľa o uvedenie minimálnej požadovanej frekvencie aktualizácie pluginov, signatúr alebo ekvivalentných detekčných mechanizmov.

Zároveň žiadame spresniť:

- či sa požiadavka vzťahuje aj na offline prostredie,
- kto bude zodpovedný za prenos a import aktualizačných balíkov,
- aká je maximálna prípustná doba medzi vydaním aktualizácie výrobcom a jej aplikovaním,
- či sa pri kritických alebo aktívne zneužívaných zraniteľnostiach požaduje mimoriadna aktualizácia mimo štandardného aktualizačného intervalu,

- aký postup sa má použiť v prípade, ak výrobca v požadovanom intervale nevydá nový aktualizačný balík.

V prípade manuálneho offline aktualizačného procesu žiadame verejného obstarávateľa, aby uviedol konkrétnu požadovanú frekvenciu, napríklad počet aktualizácií za deň, týždeň alebo mesiac, aby bolo možné zhodnotiť, či zadaný rozsah prác postačuje.

Odpoveď verejného obstarávateľa

Aktualizácie pluginov, signatúr a ekvivalentných detekčných mechanizmov musia byť vykonávané najmenej raz týždenne, ak výrobca sprístupnil nové aktualizácie, najneskôr do 7 kalendárnych dní od ich sprístupnenia.

Táto požiadavka sa vzťahuje aj na offline prostredia.

Pri kritických alebo aktívne zneužívaných zraniteľnostiach, ktoré sú relevantné pre prostredie verejného obstarávateľa, poskytovateľ zabezpečí mimoriadnu aktualizáciu dostupných detekčných mechanizmov najneskôr do 2 pracovných dní od neskoršieho z nasledujúcich okamihov: sprístupnenia príslušnej aktualizácie výrobcom alebo doručenia požiadavky verejného obstarávateľa.

Pri bezprostrednej bezpečnostnej hrozbe môže verejný obstarávateľ požadovať prioritné vykonanie aktualizácie v rámci dohodnutého postupu riešenia bezpečnostného incidentu. Rozsah a lehoty takéhoto zásahu sa riadia zmluvne dohodnutými podmienkami podpory a incidentného režimu.

Poskytovateľ zabezpečí počas 60-mesačného obdobia technickej podpory získanie, bezpečný prenos a aplikovanie dostupných aktualizačných balíkov vrátane offline prostredí, v súčinnosti s verejným obstarávateľom a pri dodržaní jeho bezpečnostných pravidiel.

Riešenie musí podporovať bezpečný manuálny import aktualizačných balíkov, overenie ich integrity a overenie úspešného aplikovania.

Ak výrobca v príslušnom intervale nevydá novú aktualizáciu, nevzniká povinnosť vykonať import neexistujúceho balíka. Poskytovateľ overí aktuálnosť poslednej dostupnej verzie a v prípade potreby informuje verejného obstarávateľa o dostupných alternatívnych detekčných možnostiach.