Príloha č. 1

OPIS PREDMETU ZÁKAZKY

Stručný opis zákazky

V rámci prevencie pred známymi hrozbami je zámerom verejného obstarávateľa implementovať v rámci svojej IKT infraštruktúry neinvazívny nástroj na podrobné zisťovanie a monitorovanie zraniteľností na jej významných komponentoch vrátane serverov, sieťových prvkov a vybraných koncových bodoch infraštruktúry. Predmetom zákazky je dodanie a implementácia nástroja na detekciu a centralizovaný manažment zraniteľností (VMS), vrátane dodávky príslušných licencií systému VMS a služieb. Nástroj VMS zabezpečí zvýšenie úrovne kybernetickej bezpečnosti jednotlivých IT aktív organizácie, ako aj celej infraštruktúry organizácie. Verejný obstarávateľ požaduje vybudovanie riešenia, ktoré bude podporovať jednu centrálnu správu v kombinácií s viacerými skenovacími servermi.

Podrobný opis zákazky

V súčasnosti je v prostredí verejného obstarávateľa zabezpečená správa zraniteľností procesmi vyhodnocovania bezpečnostných varovaní výrobcov prevádzkovaných softvérových riešení manuálne a nezahŕňa podporný nástroj na detekciu a manažment zraniteľností. Implementáciou VMS chce verejný obstarávateľ zvýšiť úroveň bezpečnosti zabezpečením rýchlejšej, efektívnejšej a spoľahlivejšej identifikácie existujúcich zraniteľností a ich následný manažment.

Od dodávateľa VMS riešenia sa očakáva návrh optimálneho variantu implementácie jednotlivých komponentov VMS riešenia do prostredia organizácie so zreteľom na riadnu prevádzku, potenciálne dopady, funkčnosť a dostupnosť riešenia.

V rámci riešenia musí byť zabezpečená integrácia VMS riešenia s externými systémami:

- interný mailový server IBM Lotus Notes alebo schopnosť odosielať emaily zo samotného servera zraniteľností,
- MS ActiveDirectory.

Požadovaná je možnosť offline a aj online zálohy a následnej obnovy VMS riešenia zo zálohy. Záloha musí byť kompletná, teda je potrebné zálohovať nie len preddefinované skeny a politiky, ale aj samotné nastavenie systému a používateľmi vytvorené skeny a politiky.

VMS riešenie musí umožňovať pravidelné automatické aj ad-hoc skenovanie siete a zariadení (minimálne serverov a koncových bodov, databáz, sieťových prvkov, aplikačných a webových serverov, Active Directory) a poskytovať nástroje na analýzu zraniteľností. V rámci organizácie musí byť zabezpečené skenovanie najmä IT aktív na nasledovných platformách:

- MS Windows 2012, 2019,
- Linux Centos 7, Rocky Linux, Oracle Linux,
- SPARC Solaris 11.4.

Súčasťou dodávky VMS riešenia musí byť aj dodanie licencií, ktoré umožnia plnohodnotnú prevádzku riešenia na 5 rokov pre:

- skenovanie 600 cieľových systémov (IP adries),

  - 300 serverov,
  - 150 sieťových zariadení,
  - 150 vybraných iných IT aktív,
- skenovacie servery napojené na centrálny manažment pre zníženie nárokov na sieťové prepojenia (počet skenovacích serverov nesmie byť licenčne obmedzený),
- uchovávanie histórie skenov minimálne na 1 rok.

Infraštruktúra organizácie je alokovaná v dvoch dátových centrách a v ďalších vybraných 10 lokalitách v SR, t. j. sídlo GPSR v lokalite Štúrova Bratislava, Register trestov GPSR v lokalite Kvetná, Bratislava a sídla krajských prokuratúr v jednotlivých krajských mestách SR.

Predpokladá sa implementácia potrebných modulov a súčastí do prostredia implementácie na virtualizačnej platforme VMWare prevádzkovanej verejným obstarávateľom.

Požadovaná vlastnosť / Hodnota parametra
Riešenie musí vykonávať automatizované testovanie zraniteľnosti zariadení.
Riešenie musí podporovať skenovanie aj bez agentov na aktívach.
Riešenie musí poskytovať centralizovaný server na zhromažďovanie a správu bezpečnostných informácií, ktoré sa nachádzajú v lokálnej sieti organizácie
Centrálny manažment server, ako aj jednotlivé skenovacie servery pod správou centrálneho manažmentu musia byť inštalované vo virtuálnom prostredí organizácie a následne logicky pripojené do sietí, kde budú vykonávať pravidelné skenovanie
Skenovanie a detekcia musí byť možná agentovým i bez agentovým spôsobom, formou neinvazívnej a tiež kontinuálnej kontroly stavu - cyklický proces systematickej identifikácie nápravy zraniteľností.
Riešenie musí obsahovať rozsiahlu databáza zraniteľnosti od viacerých výrobcov.
VMS riešenie musí zabezpečiť pravidelnú aktualizáciu skenovacích serverov a databázu zraniteľností. Skenovacie servery musia umožňovať offline a aj online aktualizáciu. Aktualizácie je nutné nastavovať podľa aktuálnych preferencií.
Riešenie musí umožňovať aktualizáciu zraniteľností manuálne, alebo ak bude centralizovaný manažment pripojený do siete internet, tak automaticky bez nutnosti manuálneho zásahu. V prípade pripojenia centralizovaného manažmentu na internet sa požaduje okamžitá aktualizácia pri publikovaní novej zraniteľnosti.
Je potrebné, aby VMS riešenie umožňovalo prideľovanie rôznych úrovní privilégií pre každého používateľa / administrátora systému samostatne.
Riešenie musí umožňovať integráciu centralizovaného manažmentu zraniteľností s existujúcim MS Active Directory systémom a zároveň poskytnúť možnosť prihlásenia sa do systému aj kombináciou mena a hesla len na báze overenia voči serveru. Potrebné je aj „tagovanie“ skenovaných zariadení, a teda aby bolo možné, aby administrátor videl len skenované zariadenia pridelené na jeho meno.
Riešenie musí umožňovať testovanie dynamicky prideľovaných IP adries prostredníctvom služby DHCP a monitorovanie ich histórie a podávanie správ pomocou "DNS name" alebo "Host name."
Konzola pre centrálnu správu ako aj skener musia podporovať inštaláciu na Windows alebo Linux operačné systémy.
Musí podporovať hybridné formy nasadenia ako fyzické, virtualizované a cloud prostredie.
Riešenie musí podporovať izolované on-premise nasadenie s manuálnou aktualizáciou databáz zraniteľností.

Riešenie musí umožniť automatickú aktualizáciu tagov v databáze aktív podľa týchto pravidiel dynamického označovania.
Riešenie musí umožňovať automatické aktualizácie všetkých SW komponentov celej architektúry riešenia s najnovšími dostupnými verziami jednotlivých SW komponentov počas celého obdobia predplatného.
Riešenie musí umožniť automatickú centralizáciu všetkých nájdených aktívnych systémov a ich atribútov: verzií operačného systému, verzií aplikácií, otvorených portov TCP a UDP a sieťových protokolov do jednej databázy aktív s možnosťou definovať statické a dynamické hierarchické tagy a podľa týchto tagov vykonávať filtrovanie aktív, testovanie a vykazovanie výsledkov.
Riešenie musí podporovať automatické zisťovanie aktív, pričom sa zohľadnia minimálne tieto parametre adresy IP, adresy MAC a názvu hostiteľa, aby sa zabránilo duplicite.
Musí podporovať centrálnu správu v geograficky rozptýlenom nasadení skenerov.
Musí podporovať prístup založený na rolách s preddefinovanými aj vlastnými rolami.
Musí podporovať automatizáciu pracovných postupov, ako je plánovanie skenovania, upozornenia na udalosti a zraniteľnosti skenovania a generovanie a distribúcia správ.
Plánované skenovanie musí podporovať opakované skenovanie v určitých časových oknách a intervaloch.
Musí podporovať neinvazívne aj invazívne kontroly. Používatelia môžu určiť rušivosť akéhokoľvek skenovania úpravou výkonu skenovania a vykonávaných kontrol. Administratívne poverenia možno použiť na hĺbkové autentifikované skenovanie, ktoré kontroluje aktíva na širší rozsah zraniteľností alebo porušení bezpečnostných politík.
Musí označovať nebezpečné kontroly a umožniť používateľom vypnúť ich na základe jednotlivých skenov.
Musí podporovať overené skenovanie. Zoznam podporovaných typov poverení.
Distribuované skenery musí spravovať centrálna konzola.
Pri skenovaní cez IPv4 musí zistiť systémy s podporou IPv6 a naopak.
Musí poskytovať pokrytie zraniteľností z NVD, CERT, SANS, Bugtraq a Secunia.
Musí automaticky korelovať a konsolidovať jednotlivé zraniteľnosti plánu prostredníctvom nápravného opatrenia.
Musí podporovať vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti.
Musí podporovať automatické zisťovanie a inventarizáciu majetku (pomocou IP adresy, MAC adresy).
Musí poskytovať dodatočné pokrytie a upozornenie na zraniteľnosti v aplikáciách, ktoré poskytujú prístup k back-end systémom.
Musí poskytovať skenovanie webových aplikácií.
Musí podporovať vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti.
Hodnotenie rizík musí zahŕňať hodnotenie CVSS, možnosť zneužitia aktív a náchylnosť k súborom škodlivého softvéru.
V rámci prepočtu CVSS musí riešenie brať do úvahy aj treťostranné zdroje dát (Threat Intelligence – napr. AttackerKB, Metasploit, ExploitDB, Project Lorelei, CISA KEV) a na základe toho stanoviť skóre rizikovosti. Táto funkcionalita musí byť v základnej cene riešenia.
Riešenie musí podporovať hodnotenie kritickosti aktív definované používateľom, ktoré sa musí zohľadniť v hodnotení rizík.
Riešenie musí poskytovať viacero modelov hodnotenia rizík.
Musí podporovať vlastné modely hodnotenia rizík definované používateľom.
Musí podporovať identifikáciu a správu výnimiek zo zraniteľnosti.

Riešenie musí podporovať integráciu so SIEM riešením.
Riešenie musí podporovať integráciu s PAM riešením. T.j. zamedziť v rámci autentifikovaných skenov assetov, aby došlo k zneužitiu hesiel (typ útoku - pass-the-hash attack)
Musí podporovať integráciu s platformami na penetračné testovanie.
Musí podporovať integráciu s produktmi na analýzu topológie siete a rizík.
Musí podporovať integráciu s virtuálnymi prostrediami
Musí podporovať možnosť stanovenia cieľov nápravných opatrení podľa kritérií ako sú: - stanovený termín ukončenia realizácie nápravných opatrení - odstránenie zraniteľností podľa závažností - odstránenie konkrétnych zraniteľností -odstránenie aktív s nepodporovaným operačným systémov
Zoznam podporovaných formátov správ musí zahŕňať min. formáty HTML, PDF, CSV a XML

Súčasťou predmetu zákazky je dodávka implementačných a konfiguračných prác minimálne v rozsahu:

- Vypracovanie detailného návrhu riešenia do 10 pracovných dní od nadobudnutia účinnosti zmluvy – naplnenie funkčných požiadaviek, návrh architektúry riešenia so začlenením do prevádzkovej infraštruktúry, vypracovanie dokumentu detailného návrhu riešenia, vypracovanie testovacích scenárov, vypracovanie harmonogramu dodávky.
- Implementácia riešenia na základe predloženého plánu riešenia a jeho schválenia verejným obstarávateľom – nasadenie centrálnych komponentov, konfigurácia integračných rozhraní, konfigurácia politík potrebných pre riadny chod VMS riešenia.
- Overenie funkčnosti riešenia – realizácia testov na základe pozitívnych a negatívnych testovacích scenárov.
- Školenie pre rolu – administrátor a správca systému.
- Dokumentácia riešenia minimálne v rozsahu – architektúra riešenia, inštalačná a konfiguračná príručka, administrátorská príručka.
- Spustenie riešenia do prevádzky – inicializácia všetkých požadovaných prístupov.

Post implementačná podpora:

- Post implementačná podpora v trvaní 1 mesiac – zvýšený monitoring a ladenie výkonu VMS riešenia.

Onsite technická podpora

- Onsite technická podpora prevádzky riešenia po dobu 60 mesiacov od termínu aktivácie licencií systému VMS, certifikovaným špecialistom, ktorá zahŕňa vykonávanie pravidelnej profylaktiky VMS riešenia minimálne 1 x za kvartál a riešenie problémov pri prevádzke riešenia