Pirkimo specialiųjų sąlygų 2 priedas

**PAŽEIDŽIAMUMŲ SKENAVIMO PROGRAMINĖS ĮRANGOS (C TIPO) NUOMOS TECHNINĖ SPECIFIKACIJA**

1. Pirkimo objektas yra pažeidžiamumų skenavimo programinės įrangos (C tipo) nuoma (toliau – PĮ ar prekė).
2. PĮ yra skirta Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – perkančioji organizacija) atliekamų atsparumo kibernetinėms grėsmėms patikrinimų metu tinkle veikiančių įrenginių ir paslaugų pažeidžiamumų identifikavimui.
3. Tiekėjas kartu su pasiūlymu turi pateikti siūlomų Prekių gamintojo dokumentus, patvirtinančius atitiktį nustatytiems techniniams reikalavimams, nurodytiems šioje techninėje specifikacijoje. Tiekėjas gali kartu su pasiūlymu pateikti nuorodas į interneto svetainę (-es) ar joje (jose) esantį (-čius) gamintojo dokumento (-tų) ekranvaizdį (-žius) (angl. printscreen), pilnai įrodantį (-čius) atitikimą atitinkamam techninės specifikacijos reikalavimui. Tiekėjo kartu su pasiūlymu teikiami gamintojo parengti dokumentai (bukletai ir pan.) turi būti originalo kalba, o reikalaujamų parametrų (jeigu jie pateikti kita nei anglų kalba) – ir lietuvių kalba.
4. Pažeidžiamumų skenavimo programinės įrangos (C tipo) galiojimo terminas 36 mėn. nuo priėmimo-perdavimo akto pasirašymo dienos.
5. Pirkimo objektui apibūdinti nurodyti konkretūs techniniai parametrai, technologijos, procesai, gamintojai ar prekės ženklai, standartai, tipai yra tik informacinio pobūdžio. Tiekėjas gali siūlyti ir lygiaverčius produktus, tačiau siūlomų lygiaverčių produktų parametrai negali būti prastesni nei reikalaujami. Siūlomų „lygiaverčių” prekių lygiavertiškumą turi įrodyti tiekėjas. Jeigu tiekėjas siūlo įsigyti lygiavertę programinę įrangą, jis įsipareigoja už siūlomą įsigijimo kainą suteikti siūlomos lygiavertės programinės įrangos diegimo, apmokymo naudotis lygiaverte programine įranga paslaugas.
6. Tiekėjas turi užtikrinti, kad gamintojas nėra paskelbęs žinios apie siūlomos PĮ tobulinimo pabaigą (angl. End of life arba Discontinued). Kartu su pasiūlymu turi būti pateiktas tiekėjo patvirtinimas ar kitas reikalavimą patvirtinantis dokumentas.

1. lentelė

|  |  |  |
| --- | --- | --- |
| ***Eil. Nr*** | ***Reikalaujama charakteristika***  ***(ne blogiau kaip)*** | **Tiekėjo siūlomų Prekių techninės charakteristikos** *(pildo tiekėjas)*  *(šioje skiltyje tiekėjas įrašo konkrečius prekių modelių pavadinimus ir gamintojus, konkrečias charakteristikas pagal šios lentelės 2 stulpelio reikalavimus, nepalieka „turi būti“, „ne mažiau“, „ne daugiau“, „ne prasčiau“, „ne ilgiau“ ir pan., nepalieka sąvokos „arba lygiavertis“ ir pan., rašyti „atitinka“ ar „taip“ neleidžiama.*  *Taip pat dėl prekių parametrų nurodo prie pasiūlymo pridedamo**dokumento pavadinimą / bylos pavadinimą arba pateikia nuorodą į konkretų internetinį puslapį ir konkrečią reikalaujamo parametro atitikimo vietą ir tos vietos ekranvaizdį)* |
| ***Gamintojas ir Programinės įrangos licencijos pavadinimas*** | | ***[įrašyti programinės įrangos gamintoją ir programinės įrangos licencijos pavadinimą, kartu pateikiama nuoroda į gamintojo internetinį puslapį ar pridedamas ekranvaizdis]*** |
| 1. | PĮ turi turėti ne mažiau kaip 50000 CVE - Common Vulnerabilities and Exposures (CVE) aprašų. |  |
| 2. | PĮ funkcionalumas: | |
| 2.1. | Turi leisti tikrinti tinklo įrenginius, operacines sistemas, paslaugas ir aplikacijas. |  |
| 2.2. | Turi turėti sukonfigūruotų šablonų, kurių pagalba atliekamas greitas tinklu pasiekiamų įrenginių patikrinimas, siekiant identifikuoti kibernetinio saugumo pažeidžiamumus. |  |
| 2.3. | Turi leisti atlikti pažeidžiamumų skenavimą nelimituotam taikinių skaičiui. Taikinius galima ištrinti ir keisti kitais. |  |
| 2.4. | Atlikus taikinių skenavimą, turi būti galimybė pasirinkti kibernetinio saugumo pažeidžiamumų ataskaitas iš sąrašo, sąrašas sudarytas iš nemažiau kaip keturių pasirinkimų:  2.4.1. Aptiktų kibernetinio saugumo pažeidžiamumų sutrumpinta ataskaita.  2.4.2. Aptiktų kibernetinio saugumo pažeidžiamumų detalioji ataskaita.  2.4.3. Aptiktų taikiniuose veikiančių operacinių sistemų ataskaita.  2.4.4. Aptiktų taikiniuose naudojamų nebepalaikomų programinių įrankių ataskaita. |  |
| 2.5. | Turi leisti elektroniniu paštu siųsti ataskaitas įvykdžius patikrinimą |  |
| 2.6. | Turi būti galimybė PĮ valdymo skyde: |  |
| 2.7. | Sukonfigūravus naudoti PROXY, atliekant taikinių skenavimus. |  |
| 2.8. | Stebėti programinio įrankio būklę (angl. health). |  |
| 2.9. | Turi galėti dirbti neprisijungus prie interneto; |  |
| 2.10. | Turi būti galimybė atlikti sistemų pažeidžiamumų analizę; |  |
| 2.11. | Turi būti galimybė atlikti sistemos patikrą nediegiant agento į tikrinamą sistemą; |  |
| 2.12. | Turi nustatyti kokių pataisymų trūksta tikrinamoje sistemoje ir kokie yra tikrinamos sistemos nustatymai; |  |
| 2.13. | Turi nustatyti aktyvius IP adresus; |  |
| 2.14. | Turi nustatyti aktyvius (atvirus) prievadus; |  |
| 2.15. | Turi būti palaikomi nuskaitymo protokolai - icmp, udp, tcp; |  |
| 2.16. | Turi būti galimybė automatiškai surasti tinkle esančias sistemas ir įrenginius, bei bandyti nustatyti juose naudojamas operacines sistemas, programinę įrangą; |  |
| 2.17. | Turi būti galimybė atlikti automatinį pažeidžiamumų nustatymo skenavimą nurodytu laiku; |  |
| 2.18. | Turi būti galimybė atlikti skenavimus reguliariai nustatytu periodiškumu; |  |
| 2.19. | Turi būti skenavimo rezultatų eksportas XML arba CSV formatais; |  |
| 2.20. | Turi būti pažeidžiamumų duomenų bazių atnaujinimai; |  |
| 2.21. | Turi būti galimybė prioretizuoti aptiktus pažeidžiamumus; |  |
| 2.22. | Turi būti galimybė reitinguoti aptiktus įrenginius pagal kritiškumą; |  |
| 2.23. | Turi atlikti patikrinimus su įgaliojimais (kredentialais); |  |
| 2.24. | Turi būti galimybė integruoti su privilegijuotų paskyrų valdymo sprendimais (PAM), atnaujinimų valdymo (Patch Management) trečiųjų šalių sprendimais; |  |
| 2.25. | Turi būti gebėjimas atlikti vidinių ir išorinių adresų nuskaitymą; |  |
| 2.26. | Turi skenuoti Linux, MacOS, Windows tipo operacines sistemas ir tinklo įrenginius (Cisco, HPE, F5, Palo Alto); |  |
| 2.27. | Turi būti diegiama įstaigos patalpose (on premises); |  |
| 2.28. | Turi būti galimybė naudotis API sistemos veikimo automatizavimui. |  |
| 3. | Programinė įranga turi būti pateikta užtikrinant 36 mėnesių gamintojo palaikymą, suteikiant teisę gauti programinės įrangos naujas versijas, atnaujinimus, pataisymus. Šiuo laikotarpiu perkančioji organizacija turi teisę registruoti pastebėtas programinės įrangos klaidas, gedimus ir apie tai pranešti el. paštu. | *Deklaruoja tiekėjas* |
| 4. | Prekės neturi kelti grėsmės nacionaliniam saugumui vadovaujantis LR Viešųjų pirkimų įstatymo 37 straipsnio 9 dalimi. | *Pateikiamas užpildytas pirkimo sąlygų 9 priedas „Nacionalinio saugumo reikalavimų atitikties deklaracija“.* |