2025 - - sutarties Nr. _____
1 priedas

TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS

1. Pirkimo objektą sudaro akcinės bendrovės Klaipėdos valstybinio jūsų uosto direkcijos (toliau – KVJUD) informacijos ir kibernetinio saugumo atitikties reikalavimams ir rizikos vertinimo, informacinių sistemų techninių pažeidžiamumų vertinimo ir atsparumo įsilaužimui testavimo paslaugos (toliau – Paslaugos), kurios apima:

1.1. KVJUD informacinių sistemų (toliau – KVJUD IS) informacinės saugos kontrolės priemonių atitikties vertinimas ir atitikties gerinimo rekomendacijų parengimas šiems reikalavimams:

1.1.1. Lietuvos Respublikos kibernetinio saugumo įstatymo reikalavimams;

1.1.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtinto kibernetinio saugumo reikalavimų aprašo reikalavimams;

1.1.3. Lietuvos standarte LST ISO/IEC 27001 A priede numatytiems reikalavimams;

1.2. KVJUD IS rizikos vertinimas, poveikio veiklai analizė ir rizikos mažinimo priemonių parinkimas;

1.3. kompiuterinio tinklo išorinio perimetro, KVJUD IS techninių pažeidžiamumų vertinimą ir atsparumo įsilaužimui testavimą, pažeidžiamumų pašalinimo rekomendacijų teikimą.

2. SIEKIAMI REZULTATAI

2. Paslaugų teikimo rezultatuose turi būti parengta ir pateikta:

2.1. informacijos ir kibernetinio saugumo atitikties ir rizikos vertinimo ataskaitos. Jose turi būti informacijos ir kibernetinio saugumo gerinimo rekomendacijos, kuriomis būtų pasiūlytos techninės ir organizacinės priemonės, leidžiančios iki priimtino lygio sumažinti informacijos ir kibernetinio saugumo rizikas ir pašalinti vertinimo metu nustatytas neatitiktis reikalavimams;

2.2. kompiuterinio tinklo išorinio perimetro, KVJUD IS techninių pažeidžiamumų vertinimo ataskaita ir techninių pažeidžiamumų pašalinimo rekomendacijos;

2.3. atsparumo įsilaužimui testavimo ataskaita.

3. TRUMPAS ESAMOS SITUACIJOS APRAŠYMAS

3. KVJUD dirba apie 230 darbuotojų. Kompiuterizuotų darbo vietų yra apie 150, tarnybinių stočių – 29. Tinklą sudaro: vidinis įmonės tinklas ir uosto magistralinis tinklas su 12 komunikacinių mazgų Klaipėdos valstybiniame jūrų uoste. Įmonėje veikia 11 verslo informacinių sistemų, uosto televizinės apžvalgos sistema, laivų eismo radiolokacinės kontrolės sistema, 3 pagalbinės informacinės sistemos, 7 kompiuterių tinklo administravimo ir saugos informacinės sistemos. Tarp jų yra viena ypatingos svarbos informacinė infrastruktūra ir viena valstybės informacinė sistema.

4. BENDRIEJI REIKALAVIMAI INFORMACIJOS IR KIBERNETINIO SAUGUMO ATITIKTIES REIKALAVIMAMS IR RIZIKŲ VERTINIMO PASLAUGOMS BEI PASLAUGŲ TEIKIMO VALDYMUI

3. Informacijos ir kibernetinio saugumo atitikties reikalavimams ir rizikų vertinimas turi būti atliktas vadovaujantis Lietuvos Respublikos elektroninės informacijos saugą bei kibernetinį saugumą reglamentuojančiais teisės aktais.

4. Teikiamos Paslaugos neturi daryti įtakos KVJUD veiklai ir teikiamoms paslaugoms bei netrikdyti atliekamų funkcijų.

5. informacijos ir kibernetinio saugumo atitikties reikalavimų vertinimui naudoti Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941.

6. Rizikos vertinimas turi būti atliktas vadovaujantis ARSIS metodu, kurio aprašymas pateiktas Nacionalinio kibernetinio saugumo centro (NKSC) prie Krašto apsaugos ministerijos interneto svetainėje adresu https://www.nksc.lt/akreditacija.html.

7. Saugos patikrinimo būdus, metodus ir priemones Teikėjas suderina su KVJUD prieš pradėdamas informacinės sistemos saugumo patikrinimą.

8. Teikėjas bus atsakingas už paslaugų teikimo komunikaciją, rizikų valdymą, dokumentų šablonų suderinimą ir ataskaitų ir rekomendacijų perdavimą.

9. Paslaugos bus teikiamos pagal su KVJUD suderintą kalendorinį darbų grafiką (paslaugų vykdymo planą), kuris turi būti paruoštas per 10 darbo dienų nuo sutarties įsigaliojimo.

10. Paslaugų teikimo eigos kontrolė bus atliekama remiantis kalendoriniu darbų grafiku, reguliariai pateikiant atliktų darbų tarpinius rezultatus.

11. Teikėjo parengti ataskaitų dokumentai turi būti pateikiami lietuvių kalba (išskyrus automatinių skenavimo įrankių sugeneruotus rezultatus, kurie pateikiami originalo kalba).

12. Paslaugos turi būti suteiktos per 3 mėn. nuo sutarties įsigaliojimo dienos.

5. REIKALAVIMAI, KELIAMI INFORMACIJOS IR KIBERNETINIO SAUGUMO ATITIKTIES VERTINIMO PASLAUGAI

13. Informacinių technologijų saugos valdymo atitikties vertinimas turi būti atliktas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika.

14. Informacinių technologijų saugos valdymo atitiktis turi būti atlikta šiems Lietuvos teisės aktų reikalavimams:

14.1. Lietuvos Respublikos kibernetinio saugumo įstatymui;

14.2. Kibernetinio saugumo reikalavimų aprašui, patvirtintam Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

14.3. Lietuvos standartams LST ISO/IEC 27001:2022, LST ISO/IEC 27002:2022.

6. REIKALAVIMAI, KELIAMI RIZIKOS VERTINIMO PASLAUGAI

15. Rizikos vertinimas turi būti atliktas vadovaujantis 4 punkto papunkčiuose nurodytais teisės aktais pagal 4.3 punkte nurodytą metodologiją ir naudojant ARSIS metodus.

16. Apimtis: KVJUD tvarkomos ir valdomos informacinės sistemos.

17. Rizikos vertinimo metu turi būti atlikta:

17.1. vertinamos sistemos kritiškumo nustatymas;

17.2. grėsmių ir jų tikimybės nustatymas;

17.3. esamų pažeidžiamumų ir kontrolės priemonių, mažinančių grėsmių rizikas, nustatymas;

17.4. rizikos lygio nustatymas;

17.5. priimtinos rizikos nustatymas;

17.6. nepriimtinos rizikos valdymo būdo parinkimas;

17.7. likutinės rizikos apskaičiavimas;

17.8. rizikos vertinimo ataskaitos parengimas.

18. Teikėjas parengia ir suderina su KVJUD įgaliotais atstovais trūkumų šalinimo plano projektą, kuriame identifikuojamos priemonės, kurias įgyvendinus rizika būtų sumažinta iki priimtino lygio bei šio plano priemonių rekomenduojami įgyvendinimo prioritetai.

7. REIKALAVIMAI KOMPIUTERINIO TINKLO IŠORINIO PERIMETRO, KVJUD IS TECHNINIŲ PAŽEIDŽIAMUMŲ VERTINIMUI

19. Kompiuterinio tinklo išorinio perimetro (ne mažiau kaip 20 IP adresų) patikrinimas atliekamas turint minimalias žinias apie tikrinamos KVJUD IS infrastruktūrą, imituojant potencialaus įsilaužėlio iš interneto veiksmus:

19.1. informacijos apie tiriamą objektą surinkimas iš viešai prieinamų šaltinių: interneto paieškos portalų, forumų, DNS (Domain Name Service) tarnybų ir oficialių interneto valdymo institucijų (RIPE, Domreg ir pan.);

19.2. tinklo mazgų, pasiekiamų iš interneto nustatymas;

19.3. tinklo mazguose veikiančių operacinių sistemų nustatymas ir pažeidžiamumo patikrinimas;

19.4. tinklo mazguose veikiančių tarnybų nustatymas ir pažeidžiamumo patikrinimas;

19.5. internetinio tinklapio www.portofklaipeda.lt automatizuotas pažeidžiamumų patikrinimas (Input Validation, XSS, SQL Injection ir pan.);

19.6. šifravimo technologijų ir saugių protokolų (HTTPS ir pan.) realizacijos interneto aplikacijoje (-ose) analizė siekiant identifikuoti pažeidžiamumus duomenų vientisumui ir konfidencialumui bei sistemų pasiekiamumui.

20. Kompiuterinio tinklo perimetro iš interneto patikrinimo rezultate, ataskaitoje Teikėjas turi pateikti:

20.1. tikrintų objektų aprašymą;

20.2. patikrinimo tikslus ir eigą;

20.3. detalų techninį aptiktų pažeidžiamumų aprašymą;

20.4. identifikuotas trumpalaikes (taktines) pažeidžiamumų švelninimo priemones;

20.5. išvadas su identifikuotomis ilgalaikėmis (esminėmis) pažeidžiamumų šalinimo rekomendacijomis.

21. Elektroninėje laikmenoje turi būti pateikti visų kompiuterinio tinklo išorinio perimetro kibernetinio saugumo patikrinimų (skenavimų) originalūs rezultatai.

22. Kompiuterinio tinklo išorinio perimetro) saugos testavimo metu KVJUD neturi būti sukeltos papildomos rizikos (paslaugų pasiekiamumo praradimas, konfidencialios informacijos praradimas, kt. jautrios informacijos praradimas ir pan.).

8. REIKALAVIMAI ATSPARUMO ĮSILAUŽIMUI TESTAVIMUI

23. Vieno internetinių paslaugų testinio serverio techninių pažeidžiamumų vertinimo ir atsparumo įsilaužimui testavimo apimtis ir (ar) veiksmai:

23.1. atlikti vienam testiniam serveriui pagal KVJUD pateiktus internetinius adresus imituojančius potencialaus įsilaužėlio iš viešojo kompiuterių tinklo veiksmus, turint minimalias žinias apie KVJUD informacinių sistemų infrastruktūrą;

23.2. parengiamas pažeidžiamumų nustatymo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti išorinių kibernetinių atakų tipai, galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (ar) techniniai įrankiai ir priemonės, naudojamos pažeidžiamumus nustatyti, nurodomos už pažeidžiamumų nustatymo plano vykdymą atsakingų asmenų teisės ir pareigos. Pažeidžiamumų nustatymo planas turi būti iš anksto suderintas su KVJUD atsakingais darbuotojais, nurodytais sutartyje;

23.3. nustačius pažeidžiamumus, pateikiama ataskaita, kurioje turi būti aprašytos aptiktos spragos, pateikiami įrodymai (automatizuotų testavimo įrankių rezultatai) ir spragų pašalinimo rekomendacijos;

23.4. testiniam serveriui turi būti atliktas realus įsilaužimo patikrinimas pasinaudojant bent vienu iš nustatytų pažeidžiamumų (jei tokie buvo atrasti).

24. Ataskaitoje pateikiama:

24.1. scenarijus – detaliai aprašyta veiksmų seka, kaip buvo išnaudotas pasirinktas saugos trūkumas, pateikiami įrodymai (automatizuotų testavimo įrankių rezultatai ir sėkmingų įsiskverbimų momentinės ekranų kopijos);

24.2. testuotojo duomenys, kvalifikacija ir rolės;

24.3. testavimo data ir laikas;

24.4. vykdytų testų tipas;

24.5. vykdytų testų ribos;

24.6. nurodyti visi susitarimuose ar reikalavimuose neapibrėžti rezultatai ir anomalijos, gautos testavimo metu.

9. KITI REIKALAVIMAI

25. Teikdamas paslaugas Teikėjas turi laikytis Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 5 d. nutarimu Nr. 818 patvirtintų organizacinių ir techninių kibernetinio saugumo reikalavimų.

26. Teikėjo informacijos saugos valdymo sistema turi atitikti ISO/IEC 27001 tarptautinio standarto arba kitų lygiaverčių informacijos saugos valdymo sistemų reikalavimus.

27. Perkant Paslaugą taikomas LR aplinkos ministro 2011 m. birželio 28 d. įsakymo Nr. D1-508 4.4.3 p., t. y. pirkimas laikomas žaliu, nes perkama tik nematerialaus pobūdžio (intelektinė) ar kitokia paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos.

28. Teikėjas ar jį kontroliuojantis asmuo negali būti registruoti (jeigu gamintojas ar jį kontroliuojantis asmuo yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytose valstybėse ar teritorijose.

29. Paslaugų teikimas negali būti vykdomas iš Viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje numatytame sąraše nurodytų valstybių ar teritorijų.