Viešajai įstaigai „Plačiajuostis internetas“ 2020-09-01 Nr. PSL200804DJR2-01

TECHNINĖ SPECIFIKACIJA

I. BENDROJI DALIS

I.1. Įvadas

VšĮ „Plačiajuostis internetas“ (toliau – Perkančioji organizacija arba Užsakovas), siekdama užtikrinti tinkamą informacijos apsaugą plačiajuosčio ryšio tinklo Lietuvoje valdymo IT infrastruktūroje, vykdo kibernetinio saugumo įrangos bei jos įdiegimo pirkimą. Šio pirkimo tikslas – modifikuoti esamą plačiajuosčio ryšio tinklo Lietuvoje valdymo IT infrastruktūrą bei įdiegti papildomas informacijos apsaugos priemones, kad būtų užtikrinta tinkama informacijos apsauga IT infrastruktūroje ir būtų užtikrinta IT infrastruktūros atitiktis pagal 2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ priedo "Techninių kibernetinio saugumo reikalavimų, taikomų subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, sąrašą".

Apsaugos sprendimai diegiami su tikslu apsaugoti Perkančiosios organizacijos IT infrastruktūrą ir joje saugomus duomenis nuo kibernetinių grėsmių, tokių kaip: interneto paslaugų sutrikdymas, internetinio incidento poveikis kritinei infrastruktūrai, perimetro pažeidimas, socialinės inžinerijos grėsmės, kenkimo programinei įrangai (toliau – PĮ) grėsmės, techninės ar programinės įrangos patikimumo grėsmės, interneto svetainių grėsmės, elektroninių ryšių tinklų žvalgybos grėsmės, konfigūravimo klaidos, logikos ir produktų architektūros klaidos, tinklo atakos, tiesioginis informacijos nutekėjimas, žmogiškosios rizikos, netiesioginis informacijos nutekėjimas, klientams teikiamų paslaugų sutrikdymas. Sprendimai turi būti diegiami taip, kad siūlomos priemonės nuo grėsmių maksimaliai apsaugotų tinklą ir jose dirbančias informacines sistemas bei įrenginius.

I.2. Esama situacija

Esama modifikuojama IT infrastruktūra apima:

- Hyper-Converged tipo serverių infrastruktūrą, išdėstytą per du duomenų centrus;
- Serverių infrastruktūroje įdiegtą virtualizavimo platformą;
- Virtualizavimo platformoje įdiegtą veiklos ir infrastruktūros valdymo programinę įrangą;
- Duomenų perdavimo tinklo įrangą;
- Informacijos apsaugos įrangą;
- Administratorių ir darbuotojų kompiuterines darbo stotis.

IT infrastruktūroje veikia tokios sistemos ir tarnybos:

- Centralizuota naudotojų ir prieigos valdymo sistema (Microsoft Active Directory pagrindu);
- Microsoft Exchange elektroninio pašto serveris;
- Duomenų bazių valdymo sistemos, aptarnaujančios veiklos ir infrastruktūros valdymo sistemas (Microsoft SQL, Oracle);
- Veiklos valdymo informacinės sistemos (CRM, buhalterinės apskaitos ir personalo valdymo, interneto tinklapis ir kitos);
- Infrastruktūros stebėjimo ir valdymo sistemos (patalpų stebėjimo, tinklo valdymo, įrangos inventoriaus valdymo ir kitos);
- Pagalbinės tarnybos – CA, DHCP, RADIUS, Log Server, Antivirus ir kitos.

Informacinės sistemos yra skirstomos į dvi pagrindines kategorijas:

- Biuro veiklos palaikymo sistemos, skirtos biuro darbuotojams;
- Tinklo palaikymo, saugos ir valdymo sistemos, skirtos aptarnaujamam tinklui ir jo įrenginiams valdyti.

I.3. Bendrieji reikalavimai perkamai įrangai

1. Pateikiama įranga bus įdiegta pagal techninėje specifikacijoje nurodytus reikalavimus (jeigu reikalavimai įdiegimui nepateikti – tos dalies įrangą būtina tik pateikti). Nurodytų įdiegimo darbų kaina bus įskaityta į pasiūlymo kainą.
2. Tiekėjas su pasiūlymu pirkimui pateikia detalų siūlomos techninės ir programinės įrangos sąrašą pagal kiekvieną pirkimo dalį. Sąraše nurodyti visos siūlomos techninės ir programinės įrangos sudėtinių dalių:
   2.1. pavadinimus,
   2.2. kiekius,
   2.3. gamintojus,
   2.4. modelius,
   2.5. gamintojo suteiktus kodus,
   2.6. jeigu yra – sudėtinius įrangos komponentus (pavadinimus, kodus, kiekius),
   2.7. jeigu siūloma įranga licencijuojama, būtina pateikti licencijų pavadinimus bei kodus ir trumpą funkcionalumo aprašymą, kurį kiekviena licencija suteikia;
   2.8. nuorodą į gamintojo tinklapį, kuriame yra pateikiamos siūlomos įrangos aprašymas.
3. Visa pateikiama įranga, licencijos, techninio palaikymo kontraktai bus Perkančiosios organizacijos vardu užregistruoti gamintojų palaikymo sistemose, jeigu tokios yra.
4. Visi techninėje specifikacijoje aprašomi komponentai bus suderinami tarpusavyje su kitais toje dalyje aprašytais komponentais bei po diegimo sudaryti integruotą pilnai paruoštą naudojimui sprendimą.
5. Visa siūloma įranga ir jos komponentai bus nauji, negalima siūlyti naudotos arba naudotos ir atnaujintos (angl. *remarketing/refurbished*) įrangos.
6. Visos siūlomos įrangos elektros maitinimo šaltinių elektros maitinimo įtampa turi atitikti Lietuvos Respublikoje naudojamai kintamai įtampai. Kartu su įranga bus pateikti visi jai prijungti prie Užsakovo įrengto elektros maitinimo tinklo reikalingi elektros maitinimo kabeliai.
7. Visi darbai ar medžiagos, kurie gali būti pagrįstai laikomi būtinais darbų užbaigimui ir tinkamam eksploatavimui, bus privalomai atlikti ir (ar) įrengiami nepriklausomai nuo to, ar jie yra apibūdinti šioje techninėje specifikacijoje, ar ne (kabeliai, jungtys, montavimo medžiagos ir pan.).
8. Visos prekės ir paslaugos tenkina atitinkamus Lietuvos Respublikoje ir Europos Sąjungoje galiojančius teisės aktus.
9. Įrangos diegimą, konfigūravimą atliekantys specialistai moka lietuvių kalbą arba bus be papildomo mokesčio užtikrintos kokybiškos vertimo paslaugos.
10. Tiekėjas visiškai atsako už Lietuvos Respublikos darbuotojų saugos ir sveikatos įstatymo bei Lietuvos Respublikos įstatymų, reglamentuojančių darbų saugą, reikalavimų vykdymą.
11. Tiekėjas privalės sumontuoti diegiamą fizinę įrangą remiantis aprašytais fiziniais parametrais ir gamintojų reikalavimais. Visi sumontuoti komponentai bus markiruoti unikaliais žymenimis, suderintais su Užsakovu. Žymuo bus gerai matomas. Kabeliai markiruojami abiejuose galuose. Markiravimo duomenys pateikiami Microsoft Excel formatu (ne žemesne nei 2000 versija) prieš įrangos priėmimo-perdavimo akto pasirašymą. Montavimo darbai bus atliekami vadovaujantis darbų saugos technikos taisyklėmis, EĮĮT normomis, priešgaisrinės saugos reikalavimais ir kitais šiuos darbus reglamentuojančiais teisės aktais.
12. Visus integracinius darbus, kuriuose bus galimas IT infrastruktūros paslaugų veikimo nutrūkimas ar naujų paslaugų sukūrimas, Tiekėjas suderins su Užsakovu prieš protingą laiką iš anksto.
13. Visi IT infrastruktūros įrangos konfigūravimo darbai bus suderinami ir atliekami pagal Užsakovui pateiktą dokumentaciją (būsimos konfigūracijos fizinės ir loginės schemos ir kt.),
14. Jei šioje techninėje specifikacijoje numatytai įrangai yra keliamas reikalavimas atitikti standartus, Tiekėjas turi teisę pasiūlyti įrangą, atitinkančią standartus, kurie yra lygiaverčiai techninėje specifikacijoje nurodytiems standartams.
15. Jei Tiekėjui bus poreikis įdiegti siūlomą valdymo programinę įrangą diegiamos įrangos valdymui, Perkančioji organizacija suteiks reikiamą kiekį virtualių serverių VMware aplinkoje. Siūlomam sprendimui reikalingų operacinių sistemų ir kitos programinės įrangos licencijas turės pateikti Tiekėjas.
16. Reikalavimai įrangos garantijai:
   16.1. Siūlomai įrangai bus suteikta ne mažiau kaip 60 mėnesių gamintojo ar gamintojo autorizuoto serviso centro garantija, įskaitant visą techninę ir programinę įrangą.
   16.2. Garantinės priežiūros laikotarpiu gamintojas ar gamintojo autorizuotas serviso centras garantuos nemokamą aparatinės įrangos reikalingų dalių tiekimą ir nemokamus remonto darbus.
   16.3. Garantinės priežiūros laikotarpiu gamintojas ar gamintojo autorizuotas serviso centas suteiks programinės įrangos atnaujinimus, naujas versijas, klaidų šalinimus bei pagalbą sprendžiant siūlomų sprendimų programinės įrangos sutrikimus.
   16.4. Garantinės priežiūros laikotarpiu techninė pagalba ir konsultacijos bus teikiamos lietuvių arba anglų kalbomis.
   16.5. Kompiuterių baterijoms taikoma ne trumpesnė nei 12 mėn. garantija.

16.6. Įranga ir licencijos bus pas gamintoją registruotos perkančiosios organizacijos vardu.
16.7. Terminai:
16.7.1. Techninei įrangai (angl. Hardware) palaikymas 8 x 5 režimu (8 val. per parą, 5 dienos per savaitę);
16.7.2. Programinei įrangai (angl. Software) palaikymas 8 x 5 režimu (8 val. per parą, 5 dienos per savaitę);
16.7.3. Kreipinių valdymas, pagalbą ir konsultacijas (produkto naudojimo, konfigūravimo ir problemų sprendimo klausimais) kreipiantis telefonu, el. paštu ar internetiniame portale, prieiga prie techninių resursų (angl. Knowledge Base) palaikymas 8 x 5 režimu (8 val. per parą, 5 dienos per savaitę);
16.7.4. Gedimo atveju įranga bus suremontuota arba pateikta nauja įranga ne vėliau, kaip per 10 darbo dienų nuo pranešimo apie gedimą pateikimo.
16.8. Garantinis laikotarpis pradedamas skaičiuoti nuo atitinkamo priėmimo-perdavimo akto pasirašymo dienos.
16.9. Garantinis aptarnavimas atliekamas įrangos buvimo vietoje.
16.10. Garantinio laikotarpio metu Tiekėjas be papildomo mokesčio pašalins tinkamai eksploatuotos įrangos gedimus.
16.11. Garantiniu laikotarpiu galios teisė Užsakovui nemokamai gauti techninės įrangos vidinės programinės įrangos (firmware) atnaujinimus ir naujas versijas.
17. Įdiegęs atitinkamos pirkimo dalies įrangą Tiekėjas privalės pateikti išpildomąją dokumentaciją, kurioje turės būti:
17.1. Įdiegtos fizinės įrangos (jei yra) sujungimo schema;
17.2. Įdiegtos įrangos loginė sujungimo schema;
17.3. Įdiegto sprendimo aprašymas;
17.4. Kita pagal pirkimo dalies įrangos pobūdį reikalinga informacija, būtina įdiegtam sprendimui eksploatuoti.
18. Visa dokumentacija bus pateikta popieriniu ir elektroniniu formatu:
18.1. Visi dokumentacijos brėžiniai ir schemos bus atlikti ir pateikti Microsoft Visio programinėje aplinkoje;
18.2. Visos dokumentacijoje pateikiamos lentelės bus pateiktos Microsoft Word ar Microsoft Excel programinėje aplinkoje;
18.3. Pateikiamose schemose naudojami primityvai bus iš anksto suderinti su Perkančiąja organizacija.
19. Dalis informacijos apie Perkančiosios organizacijos turimą IT infrastruktūrą nebus viešai atskleista dėl galimų kibernetinių grėsmių. Dėl to detalesnė informacija apie IT infrastruktūrą galės būti pateikta dalyviui CVP IS priemonėmis pateikus prašymą pateikti nurodytą informaciją, bei pateikus pasirašytą pasižadėjimą gautos informacijos neplatinti ir nenaudoti kitais tikslais, išskyrus pasiūlymo parengimą šiam pirkimui.

Reikalavimai II pirkimo daliai „Web aplikacijų saugos sprendimas“

Tiekėjas užtikrins sprendimo diegimą, sukonfigūravimą ir Web aplikacijų saugos sprendimo funkcionavimą Perkančiosios organizacijos Web tinklapiams bei atlikti veikiančio aplikacijų saugos sprendimo patikrinimą pagal žemiau aprašytus reikalavimus.

2 lentelė. Reikalavimai perkamam sprendimui.

Nr.	Parametras	Reikalaujama reikšmė	Siūloma reikšmė
1.	Sprendimo teikimo laikotarpis	Sprendimas turi pradėti veikti ne vėliau kaip per 1 mėnesį nuo sutarties įsigaliojimo. Sprendimo veikimas turi būti užtikrintas 60 mėnesių nuo jo veikimo pradžios.	Sprendimas pradės veikti ne vėliau kaip per 1 mėnesį nuo sutarties įsigaliojimo. Sprendimo veikimas bus užtikrintas 60 mėnesių nuo jo veikimo pradžios.
2.	Sprendimo teikimas	Sprendimo apimtyje Tiekėjas turi užtikrinti visas reikiamas technines ir programines priemones sprendimo vykdymui bei palaikymui visu teikimo laikotarpiu.	Sprendimo apimtyje Tiekėjas užtikrins visas reikiamas technines ir programines priemones sprendimo vykdymui bei palaikymui visu teikimo laikotarpiu.
3.	Domenų skaičius	Sprendimas turi veikti su ne mažiau kaip dviem skirtingais Perkančiosios organizacijos domenais.	Sprendimas veiks su ne mažiau kaip dviem skirtingais Perkančiosios organizacijos domenais.
4.	Sprendimo diegimas	Visas internetinių vartotojų duomenų srautas į Perkančiosios organizacijos internetinę aplikaciją turi būti nukreiptas per apsaugos nuo įsilaužimų sprendimą. Nukreipimas turi būti realizuojamas atliekant internetinio vardo (angl. *domain*) DNS įrašų nukreipimą į Tiekėjo nurodytą IP adresą. Sprendimo teikimui užtikrinti neturi būti reikalingi papildomi Perkančiosios organizacijos internetinės aplikacijos programinio kodo pakeitimai ar naudojami kiti techniniai ar programiniai sprendimai Perkančiosios organizacijos IT infrastruktūroje.	Visas internetinių vartotojų duomenų srautas į Perkančiosios organizacijos internetinę aplikaciją bus nukreiptas per apsaugos nuo įsilaužimų sprendimą. Nukreipimas bus realizuojamas atliekant internetinio vardo (angl. *domain*) DNS įrašų nukreipimą į Tiekėjo nurodytą IP adresą. Sprendimo teikimui užtikrinti nebus reikalingi papildomi Perkančiosios organizacijos internetinės aplikacijos programinio kodo pakeitimai ar naudojami kiti techniniai ar programiniai sprendimai Perkančiosios organizacijos IT infrastruktūroje.

5.	Sprendimo funkcionalumas	Sprendimas turi apimti: – Visuotinio žiniatinklio tinklavietės įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. – Visuotinio žiniatinklio tinklavietės saugumo priemonės turi gebėti automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti ir panašiai). – Turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų visuotinio žiniatinklio tinklavietės įeinantį ir išeinantį duomenų srautą. – Įvykus įtartinai veiklai, tai turi būti užfiksuojama audito įrašuose ir automatizuotai kuriamas pranešimas visuotinio žiniatinklio tinklavietės administratoriui. – Visuotinio žiniatinklio tinklavietės saugumo priemonės turi užtikrinti: o koreguojamas taisykles; o SSL sertifikato pasirinkimą; o apsaugą nuo „sausainėlių“ (angl. *Cookies*) vagysčių; o apsaugą nuo konfidencialių vartotojų duomenų perėmimo; o informacinių sistemų valdymo perėmimo apsaugą; o apsaugą nuo turinio sistemos valdymo perėmimo; o apsaugą nuo atminties buferio perpildymo; o apsaugą nuo L7 HTTP/URL turinio perrašymo; o apsaugą nuo turinio iškraipymo.	Sprendimas apims: – Visuotinio žiniatinklio tinklavietės įsilaužimo atakų pėdsakai (angl. *attack signature*) bus atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. – Visuotinio žiniatinklio tinklavietės saugumo priemonės gebės automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti ir panašiai). – Bus įdiegtos ir veiks automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų visuotinio žiniatinklio tinklavietės įeinantį ir išeinantį duomenų srautą. – Įvykus įtartinai veiklai, bus užfiksuojama audito įrašuose ir automatizuotai kuriamas pranešimas visuotinio žiniatinklio tinklavietės administratoriui. – Visuotinio žiniatinklio tinklavietės saugumo priemonės užtikrins: o koreguojamas taisykles; o SSL sertifikato pasirinkimą; o apsaugą nuo „sausainėlių“ (angl. *Cookies*) vagysčių; o apsaugą nuo konfidencialių vartotojų duomenų perėmimo; o informacinių sistemų valdymo perėmimo apsaugą; o apsaugą nuo turinio sistemos valdymo perėmimo; o apsaugą nuo atminties buferio perpildymo; o apsaugą nuo L7 HTTP/URL turinio perrašymo; o apsaugą nuo turinio iškraipymo.