

Pirkimas - 7947859

TECHNOLOGINIO PAŽEIDŽIAMUMO ĮVERTINIMO IR ATSPARUMO KIBERNETINĖMS ATAKOMS DIDINIMO PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

Pirkimo objektas - Technologinio pažeidžiamumo įvertinimo ir atsparumo kibernetinėms atakoms didinimo paslaugos.

Paslaugų suteikimo terminas – 30 dienų nuo sutarties įsigaliojimo dienos.

Nr.	Paslaugų aprašymas
1.	<p>Išorinio kompiuterinio tinklo perimetro patikrinimas. Išorinio kompiuterinio tinklo perimetro patikrinimas (patikrinimas atliekamas turint minimalias žinias apie tikrinamos organizacijos IT (Informacinių technologijų) infrastruktūrą imituojant potencialaus įsilaužėlio iš interneto veiksmus):</p> <ul style="list-style-type: none"> 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.). Perimetro tinklo mazgų, pasiekiamų iš interneto nustatymas. Perimetro tinklo mazguose veikiančių OS (Operacinių Sistemų) nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas (įjungus/išjungus WAF (Cloudflare) paslaugą). Perimetro tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas, bei konfigūracijos analizė (papildomos informacijos apie sistemą surinkimas per klaidų, sisteminius pranešimus, servisų programinę realizaciją). Nustačius pažeidžiamumus atliekamas įsilaužimo testas. Jei aptinkama iš interneto pasiekiamų tarnybų, reikalaujančių vartotojo autentifikacijos, tuomet atliekamas išorinės paslaugos slaptažodžių auditas. Tikrinama ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti. rekomenduojamos priemonės saugiam perimetrui susikurti.
	<p>Vidinių / išorinių informacinių sistemų ir interneto svetainių, veikiančių WEB aplikacijų pagrindu, REST API servisų patikrinimas.</p> <p>Informacinė sistemos / interneto svetainės: https://priemimas-kursuok.mokausi.lt/ , https://admin-priemimas-kursuok.mokausi.lt/ Turi būti patikrintos visos WEB aplikacijų paslaugos, atlikti įsilaužimų testai, DDOS apkrovos testai</p> <ul style="list-style-type: none"> Turi būti atliktas WEB aplikacijų taikomųjų programų ir paslaugų saugumo patikrinimas neturint naudotojo prisijungimo ir turint prisijungimus. Informacijos apie sistemas surinkimas (informacija apie sistemą, periferines/pagalbines sistemas) ir testavimo ribų nustatymas. Tinklo mazguose veikiančių tarnybų nustatymas ir atitinkamų, šiai dienai žinomų, pažeidžiamumų patikrinimas, bei konfigūracijos analizė Serviso konfigūracijos patikrinimas (darbinės direktorijos pakeitimas, serviso teisių eskalavimas, informacijos atskleidimas per klaidų pranešimus). Pažeidžiamumų paieška (vartotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos) automatizuotais WEB/REST API pažeidžiamumo skeneriais.

Nr.	Paslaugų aprašymas
	<ul style="list-style-type: none"> • pažeidžiamumą remiantis „OWASP testing guide“ metodikos punktais patikrinimas. • Rekomenduojamos priemonės pažeidžiamumams aptikti ir šalinti.
3.	<p>Vidinio tinklo ir darbo vietų saugumo patikrinimas:</p> <ul style="list-style-type: none"> • Microsoft Entra debesų kompiuterijos, OneDrive vartotojų ir įmonės konfigūravimo testavimas • tikrinama, ar naudotojai negali eskaluoti savo teisių sistemoje, atlikti veiksmus ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu; • kiti testai pagal paslaugos teikėjo naudojamą metodologiją. • Remiantis surinkta informacija, patikrinimo metu nustatyta realia padėti, geriausiąją praktiką ir standartais, įvertinamas vidinio duomenų perdavimo tinklo saugumas. • Pateikiamos darbuotojų dirbančių nuotoliu su tarnybinėmis stotimis konfigūracijų rekomendacijos saugiam darbui užtikrinti • Tikrinamas tarnybinių stočių operacinės sistemos ir jose veikiančios sisteminės programinės įrangos atnaujinimo lygis ir ar jos nėra pažeidžiamos remiantis šiai dienai žinomomis saugumo spragomis. • Tikrinamas tarnybinių stočių ir jose veikiančios sisteminės programinės įrangos konfigūracijos saugumas. • Tikrinama ar vartotojai negali eskaluoti savo teisių sistemoje, atlikti veiksmus ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu.
4.	<p>Atliktų darbų etapų ataskaitų parengimas (įforminama priėmimo – perdavimo aktu):</p> <ul style="list-style-type: none"> • Tikrintų objektų aprašymas. • Patikrinimo tikslai ir eiga. • Aprašomos aptiktos spragos, pateikiami įrodymai (pridėti ekrano vaizdai su įrodymais) ir pašalinimo rekomendacijos. • Pateikiamas įsilaužimo scenarijus – detalai aprašyta veiksmų seka kaip išnaudoti vieną ar kitą saugumo trūkumą (pateikiamas tik esant technologiniam pažeidžiamumui). • Po visų tinklapio audito etapų turi būti parengta ir pateikta ataskaita. Ataskaita pateikiama lietuvių kalba DOCX ir PDF formatuose. Ataskaitos pradžioje turi būti pateikta apibendrinanti lentelė su visais reikalavimuose išvardintais punktais (tikrintomis tarnybomis, technologijomis), prie kiekvieno iš jų turėtų būti aprašyta būklė: pažeidžiamumų nerasta, netaikytina ar aptikti pažeidžiamumai. Toliau turi būti pateikta informacija iš informacijos surinkimo etapo ir aptiktų pažeidžiamumų aprašymas. Informacijos surinkimo etapo metu surinkta informacija turi būti susisteminta pagal aptiktus duomenis ir jų šaltinius, turi būti pateiktos rekomendacijos dėl perteklinės informacijos šalinimo. Pažeidžiamumo aptikimo atveju, jis turi būti aprašomas ataskaitoje, pateikiamas realus jo išnaudojimo pavyzdys (jei įmanoma, su kodu reikalingu jam įvykdyti), pateikiamas galimas sprendimo būdas. Turi būti įvertinta kiekvieno aptikto pažeidžiamumo ar pavojaus riziką, atsižvelgiant į tai, kokie duomenys gali būti sugadinti ar suklustoti, kokią įtaką tai gali turėti tinklapio veikimui. Pažeidžiamumas turi būti vertinamas trimis lygiais: „žemas“, „vidutinis“ ir „aukštas“: <ol style="list-style-type: none"> 1. Žemo (low) lygio rizika reiškia, kad pažeidžiamumas yra nedidelis. Tokiu lygiu įvertinami dažniausiai papildomos informacijos suteikiantys pažeidžiamumai; 2. Vidutinio lygio rizika reiškia (warning), kad šiai dienai dar nėra sukurtų automatinių ir viešai prieinamų pažeidimų išnaudojančių programinių priemonių, bet jis yra žinomas ir gali būti panaudotas atitinkamas žinias turinčių asmenų. Taip pat šiam lygiui priskiriami pažeidžiamumai, kurių pavojingumas gali priklausyti ir nuo kitų faktorių (pvz., organizacijoje dirbančių asmenų) arba kurių išnaudojimui nepakanka vien tik specifinių techninių žinių ir tinkamos įrangos; 3. Aukšto lygio rizika reiškia (high), kad pažeidžiamumais galima nesunkiai pasinaudoti ir jais galima padaryti žalą arba išgauti svarbią informaciją. Taip pat šiam lygiui priskiriami

Nr.	Paslaugų aprašymas
	<p>pažeidžiamumai, kuriems jau būna sukurtos automatinės įsiskverbimo priemonės ir kuriomis norint pasinaudoti nebūtinos specifinės žinios. Tokie pažeidžiamumai, kuriais gali pasinaudoti asmenys, net ir neturintys specifinių žinių, yra vieni pavojingiausių.</p> <ul style="list-style-type: none"> • Taip pat turi būti įvertinta kiekvieno aptikto pažeidžiamumo ar pavojaus išnaudojimo galimybė, atsižvelgiant į tai, koku būdu jis galėtų būti išnaudojamas: <ol style="list-style-type: none"> 1. nuotoliniu būdu; 2. iš vietinio tinklo; 3. tik turint fizinę prieigą. • Detali rekomendacija – pateikiamas detalus planas nustatytų rizikų mažinimui, pažeidžiamumų taisymui bei silpnųjų vietų stiprinimui. • Rekomendacijos prevencijai – gerųjų praktikų, sistemų kūrimo gairių, kurios padėtų išvengti dažniausiai daromų saugumo klaidų, pateikimas ar pristatymas. • Atlikto technologinio pažeidžiamumo vertinimo rezultatų pristatymas gyvai.
5.	Pakartotinis aptiktų klaidų patikrinimas po jų ištaisymo (aptiktoms klaidoms ištaisyti Perkančiajai organizacijai skiriama 20 d.d.)

2. Bendrieji reikalavimai paslaugų teikimui

2.1. Paslaugos turi būti teikiamos vadovaujantis Lietuvos standartu LST ISO/IEC 27001:2017 (arba lygiavėrčiu, pareiga įrodyti lygiavertiškumą tenka paslaugų teikėjui). Ne vėliau kaip per 5 d.d. nuo Sutarties įsigaliojimo dienos, Paslaugų teikėjas privalo pateikti atitiktį reikalavimui patvirtinantį dokumentą. Nepatvirtinus atitikties nustatytu terminu, tai laikoma esminiu Sutarties pažeidimu, dėl Sutarties būtų nutraukiama, Paslaugų teikėjas įtraukiamas į nepatikimų tiekėjų sąrašą bei pritaikomos kitos Sutartyje numatytos priemonės.

2.2. Paslaugų teikėjas atsakingas už administracinius, darbo grupių organizavimo bei informacijos pateikimo ar sąlygų jai gauti užtikrinimo klausimus. Taip pat jis atsakingas už komunikaciją, vykdamas sutartį, sutarties vykdymo rizikų valdymą, dokumentų šablonų suderinimą ir paslaugų perdavimą.

2.3. Visos numatytos paslaugos teikiamos pagal su Perkančiąja organizacija suderintą kalendorinį darbų grafiką, kuris turi būti paruoštas per 5 darbo dienas nuo sutarties įsigaliojimo. Kartu su grafiku privalo būti pasiūlyti ir suderinti: paslaugų teikimo būdai, metodai ir priemonės.

2.4. Paslaugų teikėjo rengiami dokumentai pateikiami lietuvių kalba (esant poreikiui ir anglų kalba).

2.5. Su sutartimi susiję dokumentai turi būti rengiami ir derinami vadovaujantis šiais reikalavimais, tvarka ir terminais:

2.5.1. paslaugų teikėjas privalo suderinti visus pateikiamus suteiktų paslaugų rezultatus su Perkančiąja organizacija;

2.5.2. esant reikalui, daromi papildomi suteiktų paslaugų rezultatų (dokumentų) pakeitimai iki jų priėmimo (ne daugiau nei 2 iteracijomis);

2.5.3. pateiktų dokumentų projektus (dokumentų projektai pateikiami el. paštu, PO patvirtinus jų gavimą) Perkančioji organizacija įvertina per 3 darbo dienas nuo pateikimo dienos ir pateikia pastabas, jeigu tokių būtų.

2.6. Paslaugos baigiamos teikti rezultatų pristatymu Perkančiosios organizacijos atsakingiems specialistams ir vadovybei (jei Perkančioji organizacija pageidauja) ir ataskaitos pateikimu Perkančiajai organizacijai. Viskas įforminama paslaugų perdavimo ir priėmimo aktu.

2.7. Paslaugų teikėjas turi užtikrinti, kad sutarties vykdymas atitiktų asmens duomenų saugos reikalavimus, kaip tai nurodyta 2016 m. balandžio 27 d. Europos parlamento ir Tarybos reglamente (ES) Nr. 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) bei įvertinti ar dėl paslaugų pobūdžio būtina parengti ir pasirašyti susitarimą dėl asmens duomenų tvarkymo tvarkos.

2.8. Teikdamas Paslaugas paslaugų teikėjas turi užtikrinti atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, kaip tai nurodyta Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Aplinkos apsaugos (žalieji) kriterijai

Vykdam Sutartį mažinti popieriaus sunaudojimą, atsisakyti nebūtino dokumentų kopijavimo ir spausdinimo, rengiama techninė dokumentacija, ataskaitos ir (ar) kiti su Sutarties vykdymu susiję dokumentai (įskaitant mokėjimo dokumentus), turi būti teikiami tik elektroniniu formatu, o techninės dokumentacijos galutinės versijos ir (ar) kita dokumentacija, kuri turi būti pasirašoma, pasirašoma elektroniniais parašais. Išimtiniais atvejais su Sutarties vykdymu susiję dokumentai gali būti pateikiami fiziniu dokumentų formatu, jeigu toks formatas privalomas pagal teisės aktus ir (ar) Pirkėjas nurodo tokį būtinumą. Esant būtinybei spausdinti, naudojamas perdirbtas popierius, kuris atitinka aktualios redakcijos Lietuvos Respublikos aplinkos ministro 2011 m. birželio 28 d. įsakymu Nr. D1-508 „Dėl Produktų, kurių viešiesiems pirkimams ir pirkimams taikytini aplinkos apsaugos kriterijai, sąrašo, Aplinkos apsaugos kriterijų ir Aplinkos apsaugos kriterijų, kuriuos perkančiosios organizacijos ir perkantieji subjektai turi taikyti pirkdami prekes, paslaugas ar darbus, taikymo tvarkos aprašo patvirtinimo“ patvirtintus reikalavimus:

Popierius turi būti pagamintas iš:

1) 100 proc. perdirbto popieriaus (naudoto popieriaus ir (ar) gamybos atliekų) plaušų arba

ne mažiau kaip 30 proc. pirminės medienos plaušų, gautų iš miškų, sertifikuotų naudojant Forest Stewardship Council (toliau – FSC, <https://fsc.org/en>) ar Miškų sertifikavimo sistemų pripažinimo programą (angl. Programme for the Endorsement of Forest Certification schemes (toliau – PEFC, <https://www.pefc.org/>) arba lygiavertes miškų sertifikavimo sistemas, kita dalis – iš perdirbto popieriaus plaušų;

2) Nebalintas arba balintas nenaudojant chloro dujų.