AB „CIVINITY“

UAB „Adwisery“ Nr.2021-11-23/01
Konstitucijos pr. 7, 09308 Vilnius

APIE SĖKMINGAI ĮVYKDYTĄ SUTARTĮ (PROJEKTĄ)

2021-11-23

AB “Civinity” veikianti pagal bendrovės įstatus, patvirtina, kad UAB „Adwisery“, įmonės kodas 302524912, pagal 2021 m. gegužės 26 d. sudarytą paslaugų teikimo sutartį Nr. ISVP/2021/05/07, nuo 2021 m. gegužės 26 d. iki 2021 m. lapkričio 9 d. sėkmingai įgyvendino sutartį (projektą):

Projekto pavadinimas	**Įgyvendintos projekto veiklos (suteiktos paslaugos)**	**Vertė, Eur be PVM**	**Vertė, Eur su PVM**
„Informacijos saugumo rizikos analizės paslaugos“	AB Civinity saugumo rizikos analizės paslaugų projekto objektas buvo IS, įskaitant ir Organizacijos interneto svetainių, IP adresų skenavimą, siekiant nustatyti IS infrastruktūros ir programinės įrangos pažeidžiamumą. Projekto įgyvendinimo metu buvo atliktas: **1. Technologinių pažeidžiamumų auditas, kurio metu buvo atlitas:** 1.1. *Išorinio kompiuterinio tinklo technologinio pažeidžiamumo patikrinimas:* • Nustatytiems pažeidžiamumams buvo atliekamas įsilaužimo testas; • Buvo atliktas slaptažodžių auditas; • Internetinio tinklapio (-ių), nustatytų testavimų metu, automatizuotas patikrinimas; • Serviso konfigūracijos patikrinimas. 1.2. *Vidinio tinklo infrastruktūros saugumo patikrinimas:* • Serverių saugumo patikrinimas (naudojant anoniminį/nesankcionuotą prisijungimą ir/arba turint eilinio naudotojo prisijungimo duomenis); • Serverių operacinės sistemos ir jose veikiančios sisteminės programinės įrangos atnaujinimo lygio patikrinimas; • Serverių ir jose veikiančios sisteminės programinės įrangos konfigūracijos saugumo patikrinimas; • IS Naudotojų kompiuterių darbo vietų saugumo patikrinimas (naudojant anoniminį/nesankcionuotą prisijungimą ir/arba turint eilinio naudotojo prisijungimo duomenis); • Naudotojų kompiuterių darbo vietų operacinių sistemų ir jose veikiančių programų atnaujinimo lygio patikrinimas; • Naudotojų kompiuterių darbo vietų ir jose veikiančių programų konfigūracijos saugumo patikrinimas; • Slaptažodžių auditas; • Duomenų bazių valdymo sistemų patikrinimas; • DBVS atnaujinimo lygio ir konfigūracijos saugumo tikrinimas (laisva prieiga, per didelės naudotojų, ar programų teisės, galimybė vykdyti sistemines komandas iš DBVS); • Tinklo įrangos auditas. *Atlikus pažeidžiamumų auditą buvo parengta ir suderinta Pažeidžiamumų audito ataskaita su rekomendacijomis kaip pašalinti nustatytus*	12 430,00	15 040,30

	pažeidžiamumus ir saugumo spragas. Joje atsispindėjo statistika, tendencijos, bendra saugumo būklė, pavojingiausi pažeidžiamumai, saugumo trūkumai ir prioretizuotos saugumo gerinimo kryptys. **2. IS informacijos saugumo valdymo atitikties šiems standartams, reglamentuojantiems informacijos saugos valdymą, vertinimas:** • Standartui LST ISO/IEC 27001:2017 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.“ (tapatus ISO/IEC 27001:2017); • Standartui LST EN ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ (tapatus EN ISO/IEC 27002:2013). *Atlikus atitikties Lietuvos standartų LST ISO/IEC 27001:2017 ir LST EN ISO/IEC 27002:2017 reikalavimams vertinimas parengta ir su Užsakovu suderinta Atitikties vertinimo ataskaita ir nustatytų neatitikčių šalinimo planas.* **3. Informacijos saugumo rizikos įvertinimas, kurio metu buvo atlikta**: • Parengtas Organizacijos informacinių išteklių sąrašas, atliktas poveikio vertinimas; • Nustatytas ir su Organizacija suderintas toleruotinų sistemos duomenų praradimo dydžių (angl. *Recovery Point Objective*) sąrašas; • Nustatytas ir su Organizacija suderintas minimalūs informacinių išteklių atstatymo laiko dydžių (angl. *Recovery Time Objective*) sąrašas; • Nustatytos ir išanalizuotos rizikos; • Nustatytos ir aprašytos grėsmės ir pažeidžiamumai; • Nustatyti ir su informacinių išteklių savininkais suderinti rizikos lygiai ir rizikos priimtinumo lygiai; • Parengtas informacijos saugumo rizikų valdymo planas bei kalendorinis jo įgyvendinimo grafikas. Informacijos saugumo rizikos vertinimas atliktas vadovaujantis tarptautinių standartų ISO/IEC 27005:2018, ISO 31000:2018 ir BSI rizikų klasifikatoriumi. Vertinimas apėmė organizacijos valdomą ir tvarkomą IS ir šiuos informacinius išteklius, susijusius su vertinama IS: • Vykdomas veiklos funkcijas, susijusias su vertinamų IS priežiūra ir palaikymu; • Visų tipų informaciją (žodinę, elektroninę, popierinę); • IS techninę infrastruktūrą (serverius, kompiuterių tinklus, duomenų saugyklas ir pan.); • Organizacijos patalpas bei įrengimus (elektros energijos tiekimą, kondicionavimą, fizinę saugą, ryšius, apsaugą nuo ugnies ir vandens poveikio ir pan.); Atlikus saugumo rizikos vertinimą parengta bei su AB Civinity suderinta rizikos vertinimo ataskaita ir informacijos saugumo rizikų valdymo planas bei kalendorinis jo įgyvendinimo grafikas.		

AB „Civinity“ saugumo rizikos analizė, technologinių pažeidžiamumų auditas ir atitikties LST ISO 27001:20017 ir LST EN ISO/IEC 27002:2017 reikalavimams vertinimas atlikti profesionaliai ir laiku. AB „Civinity“ yra patenkinta projekte dalyvavusių ekspertų kompetencija, gebėjimu įsigilinti į įmonės poreikius ir sutartinių įsipareigojimų įgyvendinimo terminais.

AB „Civinity“
IT Vadovas (CTO) Merūnas Jokubauskas