MOKAUSI LIETUVOJE

Pirkimas – 7947859

Atsakome į pateiktą pirkimo dalyvio klausimą

Klausimas*	Atsakymas
Pasitikslinimas, pagal ISO 27001 direktyvą, atliekant kibernetinį saugumo auditą, nėra daromi proaktyvūs veiksmai norint įsilaužti į sistemas. O yra daromi veiksmai, tikrinant spragas organizaciniame, administraciniame, žmogiškajame ir technologiniame lygmenyje tikrinant teoriškai o ne praktiškai. Tad klausimas yra, ar jūs tikitės, kad būtų imituotos DDOS atakos? Jų skaičius fiksuojamas ir pamatuojama žala ir pažeidžiumumas? Ar norite įmonėje atlikti auditą pagal ISO 27001?	Taip, vykdant sutartį turės būti imituotos DDOS atakos. Auditas šiuo pirkimu n4ra perkamas.
<...prašome paaiškinti, ar kvalifikacijos reikalavime nurodytos „Technologinio pažeidžiamumo įvertinimo ir atsparumo kibernetinėms atakoms didinimo paslaugos" apima kibernetinio saugumo vadovo (CISO) paslaugas, kurių metu buvo atliekami informacinių sistemų saugumo vertinimai, rizikų analizė bei saugumo priemonių rekomendavimas.>	Neapima.
Susipažinę su pirkimo Nr. 7947859 „Technologinio pažeidžiamumo įvertinimo ir atsparumo kibernetinėms atakoms didinimo paslaugų pirkimas" technine specifikacija, atkreipiame dėmesį į reikalavimą, pagal kurį tikrinant WEB aplikacijų paslaugas turi būti atlikti „įsilaužimų testai, DDOS apkrovos testai" . Prašome šį reikalavimą patikslinti arba pakeisti, nes dabartinė formuluotė „DDOS apkrovos testai" yra teisiškai, etiškai ir techniškai rizikinga. <...> Taip pat prašome aiškiai patvirtinti, kad pirkimo sąlygose nereikalaujama ir nebus reikalaujama naudoti DDoS atakų, DDoS įrankių, botnetų ar kitos neteisėtos / neetiškos infrastruktūros, o paslaugos turės būti teikiamos tik teisėtais, etiškais ir iš anksto su Perkančiąja organizacija suderintais metodais.	Vykdant sutartį turės būti patikrintos WEB aplikacijos atsparumas, atlikti įsilaužimų testai ir teisėti, kontroliuojami našumo, apkrovos, paslaugos prieinamumo po sutrikimų testai. Šie testai turės būti atliekami tik iš anksto raštu suderinus testavimo apimtį, laiką, ribas, metodus, srauto šaltinius, maksimalias apkrovas su atsakingais asmenimis. Testavimas, turi būti atliekamas tik naudojant teisėtą testavimo infrastruktūrą.
<...> prašome paaiškinti ir, esant poreikiui, patikslinti Techninės specifikacijos 2.1 punkto nuostatas dėl LST ISO/IEC 27001:2017 standarto. 1. Ar reikalavimas vertintinas kaip sutarties vykdymo sąlyga, ar kaip tiekėjo kvalifikacijos reikalavimas? Pirkimo sąlygų 5 punkte ISO/IEC 27001 nenurodytas, todėl prašome patvirtinti, kad atitiktį patvirtinančio dokumento kartu su pasiūlymu pateikti nereikia.	1. Reikalavimas vertinamas kaip sutarties vykdymo sąlygą; 2. 3. Pasiūlymų teikimo pirkimo dalyvis jau turėtų būti įsidiegęs atitinkamą standartą, kad galėtų tinkamai vykdyti sutartį. Jei pirkimo dalyvis atitiktį grįs kitu standartu, pareiga įrodyti lygiavertiškumą tenka pirkimo dalyviui.

2. Prašome paaiškinti, koks dokumentas laikomas tinkamu atitiktį patvirtinančiu dokumentu - ar reikalaujama akredituotos sertifikavimo įstaigos išduoto galiojančio sertifikato, ir kokius standartus bei dokumentus PO pripažintų lygiaverčiais. 3. Atkreipiame dėmesį, kad LST ISO/IEC 27001:2017 sertifikavimo procesas (informacijos saugumo valdymo sistemos įdiegimas ir nepriklausomas auditas) realiai trunka kelis mėnesius, todėl jo neįmanoma įgyvendinti per 2.1 punkte nustatytas 5 darbo dienas nuo Sutarties įsigaliojimo. Toks terminas faktiškai reiškia reikalavimą turėti galiojantį sertifikatą jau pasiūlymo pateikimo metu, t. y. kvalifikacinį reikalavimą, perkeltą į sutarties vykdymo etapą aplenkiant pirkimo sąlygų 5 punktą. <...> Atsižvelgdami į tai, prašome PO pagrįsti, kodėl būtent visos organizacijos ISO/IEC 27001 sertifikavimas būtini ir proporcingi šio konkretaus pirkimo objektui?.	Toks reikalavimas kildinamas atsižvelgiant į Kibernetinio saugumo įstatyme įtvirtintas nuostatas bei įpareigoja PO reikalauti, jog atitinkamas paslaugas teiktų asmenys procesus valdantys laikantis standarto nustatytų reikalavimų, t.y., užtikrins teisingą jautrios informacijos valdymą.

*kalba netaisyta.