A picture containing text, clipart

Description automatically generated LŠTA apžvalga

2022-03-29

Kibernetinis saugumas

Lietuvos šilumos tiekėjų asociacijoje ( toliau – Asociacija) š. m. kovo 28 d. vyko nuotolinis mokymas tema „Kibernetinio saugumo reikalavimai ir jų įgyvendinimas praktikoje“. Lektorius iš Mykolo Romerio universiteto, prof. dr. Darius Štitilis, pristatė kibernetinio saugumo gaires ir jų svarbą. Mokymuose apžvelgė svarbiausius teisės aktus, susijusius su kibernetiniu saugumu. Akcentuotos šilumos tiekėjų įmonės, kurios turi daugiau kaip 10 000 tūkst. vartotojų, kadangi joms taikomi papildomi saugumo reikalavimai, užtikrinant vartotojų duomenų apsaugą. Asociacijos teisininko nuomone, svarbu išskirti šiuos žemiau pateiktus aspektus kibernetinės saugos srityje. Kiekviena CŠT įmonė turi užtikrinti šiuos minimalius kibernetinio saugumo reikalavimus:

1. CŠT įmonės turi užtikrinti turimų vartotojų duomenų (asmens kodas, gyv. vieta, tel. Nr.) ir pan. saugą dėl. Jei duomenys saugomi vidiniuose įmonės serveriuose, duomenys apsaugomi prisijungimais ir slaptažodžiais, kad būtų galima identifikuoti darbuotojus, kurie turi šią prieigą.

2. Atleisti darbuotojai, kurie turėjo prieigą prie vartotojų duomenų, turi būti nedelsiant atjungti nuo galimo prisijungimo prie duomenų serverio.

3. Darbuotojai, atsakingi už duomenų apsaugą, ypač tie asmenys, kurie turi teisę naudotis vartotojų duomenimis, prisijungimo prie serverių slaptažodžių negali laikyti matomoje vietoje (priklijuoti lapukai prie monitoriaus ekrano ar pan.).

4. Asmenys, kurie turi teisę jungtis prie įmonės duomenų bazių nuotoliniu būdu, jų kompiuterinės darbo vietos turi būti šifruotos, t. y turi turėti galimybę tokią darbo vietą blokuoti per atstumą. (pvz., pavogtas kompiuteris, turintis teisę prisijungus matyti vartotojų duomenis).

Greitu laiku turėtų įsigalioti „Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 2, 17, 25, 27, 35, 37, 39, 45, 47, 51, 90 ir 92 straipsnių pakeitimo įstatymas, kuriame bus nustatyta, kad jei įmonė vykdo viešuosius pirkimus, turės atsižvelgti į jos patikimumą. Vadinasi sudarant sutartį su atitinkamomis įmonėmis, organizacijomis, daugiau dėmesio reikės skirti tiekėjo pajėgumui (gebėjimui) užtikrinti paslaugos įgyvendinimą. Perkančioji organizacija galės prašyti įrodyti (pažymomis, sertifikatais), kad paslaugos davėjas pajėgus įvykdyti paslaugą. Taip pat svarbu kokiai saugumo kategorijai CŠT įmonė priskirta, pvz. ypatingos svarbos ar kritinės infrastruktūros. Kritinei infrastruktūrai priskirtos įmonės ir apie joms keliamus reikalavimus – informuojamos asmeniškai. Ypatingos svarbos informacinė infrastruktūra – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams. Detalesni reikalavimai įmonėms dėl kibernetinio saugumo reikalavimų nustatomi pagal jų aptarnaujamų gyventojų skaičių ir kitus parametrus, galima rasti Nacionalinės kibernetinio saugumo strategijoje, patvirtintoje Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818.