LIETUVOS RESPUBLIKOS
KRAŠTO APSAUGOS MINISTERIJA

Telia

Atnaujintas kibernetinio saugumo įstatymas

Ką turi žinoti kiekvienas organizacijos vadovas?

Kodėl kibernetinis saugumas tapo svarbiu ES ir Lietuvos prioritetu?

Europoje kibernetinių atakų skaičius ir sudėtingumas 2023–2024 m. laikotarpiu toliau auga: daugiausiai atakų buvo susiję su paslaugų nepasiekiamumu (DDoS atakomis) ir duomenis šifruojančios programinės įrangos (angl. ransomware) grėsmėmis. Toliau auga duomenų vagystės, socialinės inžinerijos principais grįstos atakos (angl. phishing) ir tiekimo grandinės pažeidimai. Piktavaliai dažniau taikosi į smulkius ir vidutinius verslus bei viešąjį sektorių, o dėl aštrėjančios geopolitinės situacijos, taikiniais tampa ir kritinė infrastruktūra.

TIS 2 direktyva ir Kibernetinio saugumo įstatymas

ES priimtos Tinklų ir informacinių sistemų direktyvos (TIS2) nuostatos yra perkeltos į atnaujintą Kibernetinio saugumo įstatymą, kuris įsigalios nuo 2024 m. spalio 18 d. TIS 2 direktyvos tikslas – padidinti ES svarbiuose sektoriuose veikiančių organizacijų tinklų ir informacinių sistemų kibernetinį atsparumą, o įvykus kibernetiniam incidentui – efektyviau suvaldyti sukeliamą žalą.

Kuo tai svarbu Jūsų organizacijai?

Jei jūsų organizacija veikia viename iš Kibernetinio saugumo įstatyme / TIS 2 direktyvoje nurodytų sektorių, pvz., energetikos, transporto, sveikatos, maisto gamybos ir kt., Jums bus privaloma užtikrinti kibernetinio saugumo reikalavimus, t. y. pasitvirtinti kibernetinio saugumo politikos dokumentus, periodiškai analizuoti ir valdyti savo kibernetinio saugumo rizikas, priskirti už kibernetinį saugumą atsakingus asmenis, valdyti kibernetinio saugumo incidentus ir apie juos teikti ataskaitas, užtikrinti savo tiekimo grandinės saugumą, diegti technines kibernetinio saugumo priemones ir kt.

Atsakomybės ir baudos

Organizacijos vadovas privalo užtikrinti, kad jo organizacija laikytųsi šių reikalavimų. Už reikalavimų nevykdymą ar kitus pažeidimus Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos gali skirti įvairias poveikio priemones, kaip vadovo nušalinimas nuo pareigų, laikinas veiklos sustabdymas, galiausiai – baudas iki 10 mln. eurų arba iki 2 proc. bendros pasaulinės metinės apyvartos.

Veiksmai, kurių reikia imtis pirmiausiai

1

Įsivertinti, ar jūsų organizacija patenka į Kibernetinio saugumo įstatymo reguliavimo sritį

Dėmesį turi atkreipti tie vadovai, kurių organizacija veikia sektoriuose, kurie Kibernetinio saugumo įstatyme yra išskirti kaip itin svarbūs ES socialinei ir ekonominei gerovei (įstatymo 1 ir 2 priedai).
Pagal bendrą taisyklę, svarbus organizacijos dydžio kriterijus, todėl dėmesį atkreipti pirmiausiai turėtų visos vidutinės ir didelės įmonės, veikiančios arba teikiančios paslaugas minėtuose sektoriuose. Mažos ir labai mažos įmonės į Kibernetinio saugumo reguliavimo sritį bus įtraukiamos tik išimtiniais atvejais, pavyzdžiui, kai tokios įmonės yra vieninteliai paslaugų teikėjai arba kai paslaugų teikimo sutrikimas gali turėti reikšmingų pasekmių visuomenės saugumui arba visuomenės sveikatai ir pan.

2

Pradėti ruoštis atitikti kibernetinio saugumo reikalavimus jau dabar

Bendra taisyklė, kad Kibernetinio saugumo įstatymo ir jo įgyvendinamųjų teisės aktų nuostatos pradedamos taikyti nuo 2024 spalio 18 d. Tačiau organizaciniai ir techniniai kibernetinio saugumo reikalavimai identifikuotiems kibernetinio saugumo subjektams bus pradėti taikyti per ne trumpesnį kaip 12 mėnesių terminą, skaičiuojamą nuo jų įtraukimo į Kibernetinio saugumo subjektų registrą momento.
Siūlome nedelsti ir jau dabar pradėti ruoštis atitikti Kibernetinio saugumo įstatyme nustatytus kibernetinio saugumo reikalavimus. Ankstyvas pasiruošimas ne tik leidžia sutaupyti, bet ir gauti kokybiškesnes paslaugas bei paruošti ir / ar pasamdyti geresnius specialistus.

3

Suburti komandą informacijos saugos valdymo sistemos diegimui savo organizacijoje

Kibernetinio saugumo reikalavimų įgyvendinimas – tai komandinis darbas tiek planuojant ir pradedant reikalavimų diegimo darbus, tiek vėliau, užtikrinant reikalavimų atitiktį operacinėje veikloje. Rekomenduojame, kad tokią komandą organizacijoje sudarytų už įvairius saugumo aspektus atsakingi darbuotojai, pvz., informacijos saugumo pareigūnas (angl., Chief Information Security Officer (CISO)), fizinės saugos, reagavimo į kibernetinius incidentus specialistas (arba turima Saugumo operacijų centro (angl., Security Operations Center (SOC)) komanda), teisininkas ir /ar atitikties pareigūnas, už kibernetinio saugumo mokymus ir kibernetinio saugumo kultūrą atsakingas koordinatorius ir kt. Kibernetinio saugumo vadovas yra ta pareigybė organizacijoje, kurią organizacijos vadovas privalės paskirti pagal atnaujinto Kibernetinio saugumo įstatymo reikalavimus.

4

Pradėti diegti kibernetinio saugumo kultūrą savo organizacijoje

Kibernetinės higienos praktika organizacijoje ir reguliarūs kibernetinio saugumo mokymai yra vienas iš Kibernetinio saugumo įstatymo reikalavimų, už kurių laikymąsi bus atsakingas organizacijos vadovas. Viena iš organizacijoje paskirto kibernetinio saugumo vadovo atsakomybių bus organizuoti ir vykdyti kibernetinio saugumo mokymus: visi organizacijos darbuotojai privalės dalyvauti kibernetinės higienos mokymuose, išklausyti kitas svarbias kibernetinio saugumo aktualijas. Be to, ir pats organizacijos vadovas (valdymo organų nariai) privalės ne rečiau kaip kartą per 2 metus išklausyti kibernetinio saugumo mokymus.

5

Stebėti ir užtikrinti tiekimo grandinės saugumą

Kibernetinio saugumo įstatymas didelį dėmesį skiria tiekimo grandinėms. Tiekimo grandinėse atsiveriančios spragos šiuo metu kelia dideles grėsmes, todėl kibernetinio saugumo subjektai turės kelti saugumo reikalavimus ir tiekimo grandinės tiekėjams ar rangovams. Todėl, norėdama teikti paslaugas, tokia, iš pirmo žvilgsnio į įstatymo reguliavimo apimtį nepatenkanti įmonė, turės atitikti Kibernetinio saugumo įstatymo reikalavimus.