VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Atlikus tyrimą dėl asmens duomenų saugumo pažeidimo, priimtas sprendimas dėl IT bendrovės negebėjimo užtikrinti nuolatinio duomenų tvarkymo sistemų ir paslaugų konfidencialumo, vientisumo, prieinamumo ir atsparumo

2022 m.

SUTRUMPINTAS APIBENDRINIMAS

Sprendimo kontekstas

Sprendimo data: 2022-05-02
Nacionalinis atvejis
Valdytojas IT bendrovė
Teisinės nuorodos: *gebėjimas užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą (BDAR 32 str. 1 dalies b punktas)*
Sprendimas: *administracinė bauda 35 tūkst. Eur*

Sprendimo santrumpa

Bylos priežastis

Gautas pranešimas apie asmens duomenų saugumo pažeidimą (toliau – ADSP), kurio metu buvo pažeistas daugiau kaip 130 000 duomenų subjektų (vartotojų) asmens duomenų konfidencialumas. Šio ADSP pagrindu Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija) savo iniciatyva atliko IT bendrovės tikrinimą.

Pagrindinės išvados

Tikrinimo metu nustatyta, kad ADSP įvyko pasinaudojus IT bendrovės darbuotojo paskyros prisijungimo duomenimis prie elektroninės parduotuvės valdymo panelės ir prisijungus prie elektroninės parduotuvės, kuri buvo pasiekiama iš išorinio tinklo, įkelta kenkėjiška rinkmena (.gif), kurios pagalba serveris užkrėstas virusu ir tokiu būdu nutekinti IT bendrovės klientų duomenys.

Be kita ko nustatyta, kad ADSP tiesiogiai lėmė neįgyvendintos organizacinės ir techninės saugumo priemonės prieigų kontrolės ir autentifikavimo, darbo stočių ir tinklo saugos srityse, t. y. IT bendrovė, neužtikrindama tinkamos prieigos kontrolės ir vartotojų autentifikacijos, neužtikrindama tinkamos darbo stočių apsaugos, nefiksuodama ir nekaupdama techninių žurnalų įrašų, leidžiančių identifikuoti ir stebėti, sekti naudotojų veiksmus, sudarė sąlygas tretiesiems asmenims be autorizacijos pasiekti IT bendrovės klientų duomenis, nesilaikė ISO/IEC 27002:2017 standarto 9.2.3, 9.3.1, 12.4.1, 12.5.1 punktų nuostatų bei pažeidė BDAR 32 straipsnio 1 dalies b punkto reikalavimus.

Sprendimas

Už nustatytus BDAR 32 straipsnio 1 dalies b punkto nuostatų pažeidimus bendrovei skirta 35 tūkst. eurų dydžio administracinė bauda.

PLATESNIS APIBENDRINIMAS

Inspekcijos tyrimo priežastys

Inspekcija gavo pranešimą, kuriame nurodyta, kad IT bendrovėje 2021-03-22 įvyko asmens duomenų saugumo pažeidimas, kaip jis apibrėžiamas BDAR 4 straipsnio 12 punkte, kurio metu buvo pažeistas didelio skaičiaus duomenų subjektų (IT bendrovės klientų) asmens duomenų, įskaitant ir asmens kodus, konfidencialumas. Toks ADSP vertintinas kaip galintis kelti didelį pavojų fizinių asmenų (duomenų subjektų) teisėms ir laisvėms, todėl Inspekcija 2021-08-04 įsakymu inicijavo tyrimą, susijusį su galimu BDAR nuostatų pažeidimu.

Tikrinimui aktualios BDAR nuostatos

BDAR 5 straipsnio 1 dalies f punkte nustatyta, kad asmens duomenys turi būti tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas). Pagal BDAR 5 straipsnio 2 dalį, duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi BDAR 5 straipsnio 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).

Pagal BDAR 24 straipsnio 1 dalį, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.

Vadovaujantis BDAR 32 straipsnio 1 dalimi, atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas. Pagal BDAR 32 straipsnio 2 dalį, nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

Pagal BDAR 28 straipsnio 1 dalį, kai duomenys turi būti tvarkomi duomenų valdytojo vardu, duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.

Tyrimo metu nustatytos aplinkybės

ADSP įvyko pasinaudojus IT bendrovės darbuotojo paskyros prisijungimo duomenimis prie elektroninės parduotuvės valdymo panelės ir prisijungus prie elektroninės parduotuvės, kuri buvo pasiekiama iš išorinio tinklo, įkelta kenkėjiška rinkmena (.gif), kurios pagalba užkrėstas virusu serveris ir tokiu būdu nutekinti IT bendrovės klientų duomenys.

Įvykus ADSP, IT bendrovė ėmėsi priemonių pašalinti IT bendrovės tyrimo metu nustatytus organizacinius ir techninius saugumo trūkumus, t. y. buvo pakeisti IT bendrovės darbuotojų prisijungimų slaptažodžiai, iš elektroninės parduotuvės pašalintos kenkėjiškos rinkmenos, taip pat IT bendrovė pradėjo naudoti privatų virtualų tinklą (angl. *Virtual Private Network*) bei diegti ir atnaujinti antivirusines programas, sudarė galimybę vartotojams prisijungimui prie Elektroninės parduotuvės naudoti dviejų lygių

autentifikaciją. Taip IT bendrovė pašalino dalį asmens duomenų saugumo pažeidimo tyrimo metu nustatytų pažeidimų / trūkumų, kurie tiesiogiai buvo susiję su įvykusio asmens duomenų saugumo pažeidimo priežastimi.

Tikrinimo metu nustatyta, kad ADSP tiesiogiai lėmė IT bendrovės neįgyvendintos organizacinės ir techninės saugumo priemonės prieigų kontrolės ir autentifikavimo, darbo stočių ir tinklo saugos srityse, t. y. IT bendrovė, neužtikrindama tinkamos prieigos kontrolės ir vartotojų autentifikacijos, neužtikrindama tinkamos darbo stočių apsaugos, nefiksuodama ir nekaupdama techninių žurnalų įrašų, leidžiančių identifikuoti ir stebėti, sekti naudotojų veiksmus, sudarė sąlygas tretiesiems asmenims be autorizacijos pasiekti IT bendrovės klientų duomenis, nesilaikė ISO/IEC 27002:2017 standarto 9.2.3, 9.3.1, 12.4.1, 12.5.1 punktų nuostatų bei pažeidė BDAR 32 straipsnio 1 dalies b punkto reikalavimus.

Be to, tyrimo metu nustatyti ir kiti, mažesnės reikšmės pažeidimai, kurie negalėjo būti pripažinti kaip turintys tiesioginę įtaką duomenų praradimui.

Dėl IT bendrovės gebėjimo (negebėjimo) užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą

Duomenų valdytojas yra atsakingas už tai, kad būtų užtikrintas nuolatinis duomenų tvarkymo sistemų ir paslaugų konfidencialumas, vientisumas, prieinamumas ir atsparumas (BDAR 32 straipsnio 1 dalis), nepriklausomai nuo to, kokios yra IT bendrovės naudojamų priemonių galimybės, atliktų veiksmų dažnumas ir pobūdis ar asmens duomenų tvarkymo trukmė.

Tikrinimo metu nuspręsta pradėti administracinės baudos skyrimo procedūrą dėl BDAR 32 straipsnio 1 dalies b, c ir d punktų bei BDAR 34 straipsnio 2 dalies nuostatų pažeidimų, tačiau pagrindinis motyvas, lėmęs nagrinėjamą ADSP, yra tikrinimo metu nustatytas IT bendrovės negebėjimas užtikrinti nuolatinio duomenų tvarkymo sistemų ir paslaugų saugumo dėl nustatytų pažeidimų prieigų kontrolės ir autentifikavimo, tarnybinių stočių apsaugos, techninių žurnalų įrašų ir stebėsenos srityse (pagal BDAR 32 str. 1 dalies b punktą). Šie pažeidimai taip pat sietini su BDAR 24 straipsnio 1 dalies, kuri nustato, kad atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.

Nors IT bendrovė po Inspekcijos siūlymo skirti baudą neigė priežastinį ryšį tarp Inspekcijos nustatytų pažeidimų, neužtikrinus tinkamų techninių ir organizacinių saugumo priemonių, tačiau žodinio bylos nagrinėjimo metu pripažino, kad po incidento įdėtos pastangos ir įdiegtos naujos (papildomos) saugumo priemonės būtų apsaugoję IT bendrovės vartotojų duomenis nuo pažeidėjo piktavališkų veiksmų, kad IT bendrovė tik po incidento suprato, kaip svarbu yra nuolat peržiūrėti ir atnaujinti turimas technines ir organizacines priemones, kurios užtikrintų tinkamą duomenų saugumo lygį.

Inspekcijos vertinimu, tvarkomų asmens duomenų saugumą nuo nustatytų pažeidimų prieigų kontrolės ir autentifikavimo, tarnybinių stočių apsaugos, tinklo ir komunikacijos saugos, techninių žurnalų įrašų ir stebėsenos srityse būtų apsaugojusios tinkamai panaudotos bent viena iš toliau nurodytų įprastinių saugumo priemonių: prieiga prie tarnybinės stoties tik IT bendrovės darbuotojams naudojant kelių dalių autentifikavimą (MFA); prisijungimas prie tarnybinės stoties naudotojų administravimo iš vidinio kompiuterių tinklo ir / arba naudojant VPN; tinkamas kompiuterių tinklo įsilaužimo aptikimas ir prevencija, naudojant tam skirtą techninę ir programinę įrangą; tinkama tarnybinės stoties operacinės sistemos apsaugą.

Nors bendrovė buvo pasisamdžiusi duomenų tvarkytoją, pagal BDAR 5 straipsnio 2 dalyje nurodytą atskaitomybės principą būtent duomenų valdytojui tenka pagrindinė atsakomybė už tinkamą BDAR nustatytų reikalavimų laikymąsi. Pažymėtina, kad IT bendrovė ne tik turėjo pasirinkti tinkamą duomenų tvarkytoją, tačiau turėjo pareigą duomenų tvarkytojui nustatyti reikalavimus dėl saugumo priemonių užtikrinimo, kuriuos duomenų tvarkytojas privalėjo įgyvendinti, bei pateikti duomenų tvarkytojui tikslesnę, konkretesnę informaciją apie tai, kaip bus laikomasi reikalavimų.