VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS PATARIMAI.

2024-03-15

1. PAVIEŠINTI VARTOTOJŲ PRISIJUNGIMO DUOMENYS, KAIP ELGTIS?

1.1. Pastaruoju metu Valstybinė duomenų apsaugos inspekcija (toliau – VDAI) gauna organizacijų pranešimus, kad „juodajame internete“ buvo paviešinti jų vartotojų asmens duomenys (prisijungimo prie informacinių sistemų vardai, slaptažodžiai).

2. KOKIŲ PRIEMONIŲ DĖL TOKIOS SITUACIJOS REIKĖTŲ IMTIS DUOMENŲ VALDYTOJAMS?

2.1. Gavusi informaciją apie galimai nutekintus prisijungimo vardus, slaptažodžius, organizacija (Duomenų valdytojas) turėtų atlikti pirminį tyrimą ir nustatyti, ar įvyko duomenų valdytojo tvarkomų asmens duomenų konfidencialumo, vientisumo ar prieinamumo pažeidimas, t. y. ar buvo pažeisti organizacijos informacinėse sistemose tvarkomi asmens duomenys *(ar buvo pažeistos saugumo priemonės, ar neįgalioti asmenys gavo prieigą prie asmens duomenų ir pan.)*. Kitaip tariant, ar yra duomenų, leidžiančių daryti prielaidą, kad įvyko asmens duomenų saugumo pažeidimas *(toliau – ADSP)*.

3. JEI JŪSŲ TVARKOMI ASMENS DUOMENYS NEBUVO PASIEKTI NEĮGALIOTŲ ASMENŲ:

3.1. Įvertinkite Duomenų subjektams kylančias rizikas ir imkitės veiksmų joms valdyti bei užkirsti kelią galimoms neigiamoms pasekmėms *(blokuokite vartotojų paskyras, kurių prisijungimo duomenys sutapo su nutekintais duomenimis, sugeneruokite naujus laikinus slaptažodžius ir išsiųskite paveiktiems duomenų subjektams, aktyvuokite dviejų faktorių autentifikaciją ir pan.)*. Praneškite darbuotojams ir vartotojams, kokių veiksmų jie patys galėtų imtis šioje situacijoje.

Nesant asmens duomenų saugumo pažeidimo (ADSP) požymių, Duomenų valdytojui nekyla pareiga teikti pranešimo VDAI pagal BDAR 33 straipsnį.

4. JEI JŪSŲ TVARKOMI ASMENS DUOMENYS BUVO PASIEKTI NEĮGALIOTŲ ASMENŲ:

4.1. Atlikite išsamų tyrimą**,** kad galėtumėte nustatyti asmens duomenų pažeidimo mastą ir įvertinti galimas pasekmes Duomenų subjektams.

4.2. Imkitės neatidėliotinų priemonių ir praneškite Duomenų subjektams apie asmens duomenų pažeidimo mastą ir tuo atveju, jei kyla ar gali kilti didelis pavojus fizinių asmenų (Duomenų subjektų) teisėms ir laisvėms *(pvz. nustatyti neteisėti prisijungimai prie vartotojų paskyrų arba nėra galimybės vienareikšmiai nustatyti, kad tokių prisijungimų nebuvo, nustatyti neteisėti veiksmai paskyrose ir pan.)*, privaloma imtis neatidėliotinų priemonių asmens duomenų pažeidimo (ADSP) pasekmėms sumažinti ir apie tai informuoti Duomenų subjektus pagal BDAR 34 straipsnį.

4.3. Apie nustatytą asmens duomenų pažeidimą, asmens duomenų pažeidimo mastą ir galimas pasekmes Duomenų subjektams, praneškite Valstybinei duomenų apsaugos inspekcijai (VDAI) per 72 valandas nuo tada, kai sužinoma apie asmens duomenų pažeidimą (ADSP).

5. VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA (VDAI) ATKREIPIA DĖMESĮ, KAD DUOMENŲ VALDYTOJAI TURĖTŲ SKIRTI PAKANKAMĄ DĖMESĮ SLAPTAŽODŽIŲ SUDARYMUI IR VALDYMUI:

5.1. Užtikrinkite, kad vartotojų slaptažodžiai būtų saugūs, sudėtingi ir sudaryti bent iš 12 simbolių *(raidžių, skaičių, bent vienos didžiosios raidės ir specialaus simbolio)* bei periodiškai keičiami.

5.2. Įdiekite papildomas saugumo priemones, pavyzdžiui, papildomą autentifikaciją ar saugumo įspėjimus. Daugiau patarimų apie slaptažodžius:
https://www.nksc.lt/doc/biuleteniai/2023-03-29%20Apie%20slaptazodzius.pdf
https://www.nksc.lt/doc/biuleteniai/NKSC_Slaptazodziu_saugumo_biuletenis.pdf

6. KOKIŲ ATSARGUMO PRIEMONIŲ REIKĖTŲ IMTIS DUOMENŲ SUBJEKTAMS?

6.1. Dėl bendro atsargumo Valstybinė duomenų apsaugos inspekcija (VDAI) pataria panašiais atvejais Duomenų subjektams (žmonėms) imtis šių atsargumo priemonių:

a) pasikeiskite slaptažodį į naują ir unikalų;
b) jei naudojote tą patį slaptažodį ir kitose sistemose, taip pat keiskite ir juos;

c) užtikrinkite, kad Jūsų slaptažodžiai būtų saugūs ir sudėtingi. Jie turėtų būti sudaryti bent iš 12 simbolių: raidžių, skaičių, bent vienos didžiosios raidės ir specialaus simbolio;
d) nesaugokite savo slaptažodžių naršyklėse. Naršyklės gali turėti spragų ir pažeidžiamumų, kurie gali būti išnaudojami kenkėjiškoms programoms gauti slaptažodžius iš naršyklės saugyklos;
e) atidžiai stebėkite susijusius pranešimus ir sekite naujienas arba pranešimus iš paslaugų teikėjo, VDAI ar Nacionalinio kibernetinio saugumo centro;
f) susilaikykite nuo dalijimosi asmenine informacija ir būkite atsargūs dalydamiesi asmenine informacija internete arba su trečiosiomis šalimis, ypač jei gavote įtartinų pranešimų;
g) nedelsdami praneškite apie įtartinus veiksmus paslaugų teikėjui jei pastebite kokius nors įtartinus veiksmus savo paskyroje arba susijusiose sistemose;
h) įdiekite ir reguliariai atnaujinkite antivirusinę programinę įrangą savo įrenginiuose, kad būtumėte apsaugoti nuo kenkėjiškų programų.

Pagarbiai

EB Law & Consulting
EB Teisė ir konsultacijos

Josifas Lovkys
Teisininkas -konsultantas
UAB „EB teisė ir konsultacijos“
Ukmergės g. 369A, 8 a., LT-12142, Vilnius
Mob. +370 698 11214
El. paštas: dap@eblaw.lt