REKOMENDACIJA
DĖL SAUGIŲ IR STIPRIŲ SLAPTAŽODŽIŲ NAUDOJIMO SVARBOS

2024

Įvadas

Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) parengta rekomendacija skirta duomenų valdytojams, kurie tvarkydami asmens duomenis turi imtis atitinkamų techninių ir organizacinių priemonių, kurios užtikrintų tinkamą asmens duomenų saugumą. Šios rekomendacijos tikslas – **atkreipti duomenų valdytojų dėmesį į saugių ir stiprių slaptažodžių naudojimo svarbą.**

Grėsmės, kylančios dėl silpnų slaptažodžių naudojimo

VDAI dažnai gauna pranešimus apie asmens duomenų saugumo pažeidimus, kuriuose duomenų valdytojai nurodo, kad į jų valdomas duomenų bazes ar sistemas įsilaužė piktavaliai pasinaudoję naudotojų ar privilegijuotas teises turinčių naudotojų prisijungimais, t. y. prisijungimų vardais ir slaptažodžiais.

Pavyzdys: Duomenų valdytojas pranešė, kad piktavalis, atspėjęs privilegijuotas teises turinčio naudotojo prisijungimus (angl. *Brute Force*), prisijungė prie duomenų valdytojo valdomos duomenų bazės, kurioje buvo saugomi asmens duomenys. Piktavaliui prisijungus prie duomenų bazės, duomenys buvo eksfiltruoti, o vėliau ir užšifruoti. Piktavalis paliko grasinantį pranešimą, kad

duomenų valdytojui nesumokėjus išpirkos, duomenys bus paviešinti. Duomenų valdytojui nesumokėjus piktavalio prašomos išpirkos, asmens duomenys buvo paviešinti.

Duomenų valdytojai techninėmis ir organizacinėmis priemonėmis neužtikrinę, kad jų sistemų naudotojai ar privilegijuotas teises turintys naudotojai naudotų stiprius ir saugius slaptažodžius, taip pat reguliariai jie būtų keičiami, gali susidurti su neigiamas pasekmes turinčiomis situacijomis, kai piktavaliai įsilaužia į sistemas pasinaudoję silpnais slaptažodžiais.

Taip pat pasitaiko situacijų, kai duomenų valdytojas, turėdamas interneto svetainę, kurioje lankytojai gali užsiregistruoti ir susikurti savo paskyras, kuriose bus saugomi jų suvesti asmens duomenys, leidžia lankytojams registruojantis susikurti silpnus slaptažodžius, t. y. nepakankamo kompleksiškumo ar ilgio slaptažodžius. Tokiais atvejais duomenų valdytojas, tinkamomis techninėmis priemonėmis neužtikrinęs, kad lankytojai registruodamiesi susikurtų stiprius ir saugius slaptažodžius, susiduria su rizikomis, kad piktavaliai lengvai atspės slaptažodžius (angl. *Brute Force*) ir tokiu būdu neteisėtai prisijungs prie lankytojo paskyros, kurioje yra saugomi asmens duomenys.

Pavyzdys: Duomenų valdytojas pranešė, kad piktavalis, atspėjęs interneto svetainės lankytojų slaptažodžius, prisijungė prie jų paskyrų, susipažino su asmens duomenimis, saugomais lankytojo paskyroje, ir lankytojams nežinant užsakė duomenų valdytojo teikiamas paslaugas. Dėl šio incidento buvo ne tik pažeistas lankytojų asmens duomenų konfidencialumas, tačiau taip pat lankytojai susidūrė su padidintomis sąskaitomis už piktavalių užsakytas paslaugas.

Priežastys, kodėl duomenų valdytojai turi užtikrinti saugių ir stiprių slaptažodžių naudojimą

BDAR[1] kelia griežtus reikalavimus asmens duomenis tvarkantiems duomenų valdytojams, kurie, remiantis BDAR 24 ir 32 straipsniais, visais atvejais prieš tvarkant asmens duomenis turi atlikti rizikos vertinimą, pagal nustatytą riziką duomenų valdytojas turi pasirinkti, kokias technines ir organizacines priemones taikys, siekdamas tinkamai apsaugoti asmens duomenis (žr. tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams (toliau – Gairės).

Papildomai atkreiptinas dėmesys, kad, remiantis Gairių 83 punktu, „Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį.“ ISO standarto[2] 5.17 papunktyje „Autentiškumo patvirtinimo informacija“, taip pat nurodoma, kad: „Autentiškumo patvirtinimo informacijos priskyrimas ir valdymas turėtų būti kontroliuojamas pagal valdymo procesą, įskaitant personalo konsultavimą dėl tinkamo autentiškumo patvirtinimo informacijos tvarkymo.“

[1] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR).

[2] ISO/IEC 27002:2022 standarto „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ (toliau – ISO standartas).

Atsižvelgdami į tai, duomenų valdytojai techninėmis ir organizacinėmis priemonėmis turi užtikrinti, kad tiek sistemų naudotojų ar privilegijuotas teises turinčių naudotojų, tiek duomenų valdytojo interneto svetainės lankytojų naudojami prisijungimo slaptažodžiai atitiktų reikiamą saugumo lygį ir tam tikrą kompleksiškumo lygį. Atsakomybės už silpnų slaptažodžių naudojimą perkėlimas darbuotojams ar lankytojams nepanaikina atsakomybės duomenų valdytojui, nes, remiantis socialinės inžinerijos praktika, darbuotojai ir lankytojai yra silpnoji vieta, todėl duomenų valdytojas turi imtis tinkamų techninių ir organizacinių priemonių, kurios užtikrintų, kad būtų sumažinta rizika, kylanti dėl darbuotojų ir lankytojų veiksmų.

Duomenų valdytojams taikomi reikalavimai, susiję stiprių ir saugių slaptažodžių nustatymu

Mobiliąsias aplikacijas naudotojai gali atsisiųsti ne tik iš mobiliųjų aplikacijų platformų bet ir tiesiogiai iš internetinių svetainių, todėl siekiant geriau užtikrinti duomenų saugumą, duomenų valdytojams būtų aktualu susipažinti su EDAV[3] gairėmis, EDAV pavyzdžiais dėl ADSP, EDAV atvejų santrauka, Gairėmis ir VDAI parengta rekomendacija: Įsilaužimai į interneto svetaines – kaip reikėtų elgtis, Eleni Kosta asmens duomenų saugumo pažeidimo nagrinėjimo santrauka. Taip pat rekomenduotina susipažinti su NKSC[4] parengtais informaciniais biuleteniais: dar kartą apie slaptažodžius ir kitas kibernetinio saugumo priemones ir slaptažodžių stiprumas, sudėtingumas ir sauga.

BDAR 32 straipsnyje 1 dalyje yra įtvirtintas reikalavimas duomenų valdytojui ir duomenų tvarkytojui, t. y. 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.

Gairėse yra pateikiami reikalavimai, kurie padeda duomenų valdytojams, atsižvelgus į rizikos vertinimą, imtis tinkamų techninių ir organizacinių priemonių. Toliau šioje rekomendacijoje aptariami reikalavimai, kurie padės duomenų valdytojams užtikrinti duomenų saugumą per stiprių ir saugių slaptažodžių prizmę. Papildomai atkreipiamas dėmesys, kad duomenų valdytojui priemonėmis užtikrinus sistemų naudotojų ir interneto svetainių lankytojų stiprių ir saugių slaptažodžių naudojimą, tai neužtikrins visiško asmens duomenų saugumo, tačiau padės sumažinti riziką.

Duomenų valdytojui atlikus rizikos vertinimą ir nustačius žemą rizikos lygį:

1. Gairių 1 punktas – asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas. Duomenų valdytojas turi aprašyti sistemų naudotojų (įskaitant privilegijuotas teises turinčius naudotojus) ir / ar interneto svetainės lankytojų prisijungimų slaptažodžiams taikomus reikalavimus.

[3] Europos duomenų apsaugos valdyba.
[4] Nacionalinis kibernetinio saugumo centras

2. Gairių 86 punktas – slaptažodis sudaromas atsižvelgus į tam tikrą kompleksiškumo lygį. Atkreiptinas dėmesys, kad duomenų valdytojui nesiimant tinkamų techninių priemonių, kurios užtikrintų, kad naudotojų ir lankytojų naudojami slaptažodžiai atitiktų tam tikrą kompleksiškumo lygį, kyla rizika, kad slaptažodžiai bus lengvai atspėjami, pasinaudojant slaptažodžių parinkinėjimo (angl. *Brute Force*) kibernetine ataka. Duomenų valdytojas privalo užtikrinti, kad slaptažodžiai būtų sunkiai atspėjami, per slaptažodžio sudėtingumą ir ilgį.[5]

3. Gairių 87 punktas – prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. Duomenų valdytojas turi užtikrinti, kad naudotojai ir lankytojai negalėtų susikurti ir naudoti slaptažodžių, kurie yra nesaugūs ir silpni.

4. Gairių 88 punktas – naudotojų ir lankytojų slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. *Hash Form*). Dažnai pasitaiko, kad svetainių lankytojų prisijungimų slaptažodžiai yra saugomi neužkoduoti, įvykus kibernetiniam incidentui ir nutekinus prisijungimų duomenis, piktavaliams tampa atviri ne tik prisijungimų vardai, bet ir slaptažodžiai. Tokiais atvejais piktavaliai, pasinaudodami kredencialų brukimo (angl. *Credential Stuffing*) kibernetine ataka, bando prisijungti prie svetainių lankytojų paskyrų, naudodami nutekėjusius prisijungimo duomenis. Kitaip tariant, piktavaliai ieško lankytojų naudojamų vienodų prisijungimų skirtingose svetainėse. Sėkmingos kibernetinės atakos atveju, piktavalis gauna prieigą prie lankytojo paskyros su joje saugomais asmens duomenimis. Sėkmingos atakos atveju duomenų valdytojas turi vertinti, kad tai yra asmens duomenų saugumo pažeidimas. Todėl, kad tokių kibernetinių atakų mažėtų, būtina papildomai apsaugoti lankytojų slaptažodžius.

Duomenų valdytojui atlikus rizikos vertinimą ir nustačius vidutinį rizikos lygį, papildomai atsirandantys reikalavimai:

5. Gairių 89 punktas – turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius, taip pat turi būti užtikrinta, kad slaptažodžiai nesikartotų. Duomenų valdytojai, įgyvendinę šiame punkte nurodytus reikalavimus, kad slaptažodžiai būtų stiprūs, saugūs ir nesikartojantys, sumažins slaptažodžių parinkinėjimo (angl. *Brute Force*), kredencialų brukimo (angl. *Credential Stuffing*) ar kitų kibernetinių atakų, susijusių su slaptažodžių pažeidžiamumu, kylančią riziką.

6. Gairių 91 punktas – Privilegijuotiems naudotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas kelių veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamos ir papildomos saugumo priemonės, tokios kaip IP adreso kontrolė, virtualus privatus tinklas (angl. VPN) ir kiti atitinkami saugumo mechanizmai. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt. Atkreiptinas dėmesys, kad dažnu atveju įvykus kibernetiniam incidentui ir piktavaliui prisijungus prie sistemos su privilegijuoto naudotojo prisijungimais, duomenų valdytojas patiria gerokai didesnę žalą, nei piktavaliui

[5] 2022 m. spalio 14 d. CNIL „Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité“: https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

pasinaudojus neprivilegijuoto naudotojo prisijungimais. Tačiau dažnai pasitaiko, kad duomenų valdytojai neužtikrina privilegijuotiems naudotojams kelių veiksnių autentifikavimo taikymo, o tai yra pagrindinė priežastis, kodėl piktavaliams pavyksta pasinaudoti privilegijuotomis prieigos teisėmis. Taip pat daugeliu atveju kibernetiniai incidentai neįvyktų, jei privilegijuotiems naudotojams būtų taikomas kelių veiksnių autentifikavimas.

Duomenų valdytojui atlikus rizikos vertinimą ir nustačius aukštą rizikos lygį, papildomai atsirandantys reikalavimai:

7. Gairių 93 punktas – Prisijungimo procedūros metu neteikti pagalbos pranešimų, kurie padėtų leidimo neturinčiam naudotojui (pvz., jei nepavyksta prisijungti, sistema neturi nurodyti, kuri duomenų dalis yra teisinga ar neteisinga). Šio reikalavimo įgyvendinimas užtikrins, kad piktavaliui, bandančiam parinkti tinkamus prisijungimus ir nežinančiam prisijungimo vardo ir slaptažodžio (angl. *Brute Force*), tai padaryti bus gerokai sunkiau ir ilgiau, kadangi piktavalis turės ne tik atspėti visą prisijungimo slaptažodį, o dar ir pritaikyti jį tinkamam prisijungimo vardui.

Papildomai VDAI atkreipia dėmesį, kad pastaruoju metu yra padaugėję asmens duomenų saugumo pažeidimų, kurie įvyksta sistemų naudotojams (įskaitant ir privilegijuotus naudotojus) ar svetainių lankytojams prisijungimų duomenis išsaugojus naršyklėje, per kurią jungiamasi prie svetainių, sistemų ar kt. T. y. piktavaliui perėmus naudotojo ar lankytojo darbo ar asmeniniame kompiuterio naršyklėje išsaugotus prisijungimo duomenis, piktavalis gauna prieigą ne tik prie prisijungimo duomenų, tačiau taip pat jis žino, kur gali prisijungti naudodamasis turimais prisijungimais. Tokiais atvejais piktavaliui, norinčiam prisijungti prie sistemos ar svetainės, nereikės vykdyti slaptažodžių parinkinėjimo (angl. *Brute Force*), kredencialų brukimo (angl. *Credential Stuffing*) ar kitų kibernetinių atakų. Atitinkamai duomenų valdytojų naudojamos apsaugos sistemos skirtos atpažinti galimus neteisėtus prisijungimus ir juos sustabdyti bus neveiksmingos, išskyrus atvejus, kai leidimas prisijungi prie sistemų yra leidžiamas tik ribotam naudotojų skaičiui (angl. *Whitelist*) arba yra naudojama kelių veiksnių autentifikacija.

Įvertinus Eleni Kosta asmens duomenų saugumo pažeidimo nagrinėjimo santrauką, papildomai atkreiptinas dėmesys, kad Europoje priežiūros institucijos, vertindamos asmens duomenų saugumo pažeidimus ir nustačiusios, kad asmens duomenų saugumo pažeidimas kilo dėl silpnų slaptažodžių, duomenų valdytojams teikia rekomendaciją[6], kurioje siūloma duomenų valdytojui įgyvendinant slaptažodžių politiką, laikytis toliau pateiktomis rekomendacijomis:

- Užtikrinti, kad slaptažodžiai būtų sudaryti iš ne mažiau kaip 12 simbolių, kuriuose yra bent viena didžioji raidė, viena mažoji raidė, vienas skaičius ir vienas specialus simbolis arba.
- Užtikrinti, kad slaptažodžiai būtų sudaryti iš ne mažiau kaip 8 simbolių, kuriuose yra 3 iš 4 simbolių kategorijų (t. y. didžiosios ir mažosios raidės, skaičiai ir specialieji simboliai) ir būtų taikomos papildomos priemonės pvz., prieigos prie paskyros atidėjimas arba blokavimas po kelių nesėkmingų autentifikavimo bandymų.

[6] https://www.edpb.europa.eu/system/files/2021-10/fr_2021-01_decisionpublic.pdf

- Taip pat turi būti užtikrinamas reguliarus slaptažodžių atnaujinimas (pvz., kas 6 mėnesius).

Rekomendacijos

Duomenų valdytojai, remdamiesi BDAR reikalavimais, turi užtikrinti asmens duomenų saugumą tinkamomis techninėmis ir organizacinėmis priemonėmis. Atsižvelgiant į pastebimas tendencijas, kad dažnu atveju kibernetiniai incidentai įvyksta dėl silpnų ir nesaugių slaptažodžių naudojimo, VDAI pateikia rekomendacijas duomenų valdytojams, kurios padės geriau apsaugoti asmens duomenis:

1. Vidiniuose teisė aktuose apsibrėžti reikalavimus stipriems ir saugiems slaptažodžiams ir techninėmis priemonėmis užtikrinti jų laikymąsi;
2. Užtikrinti, kad slaptažodžiai būtų ne trumpesni nei 12 simbolių, susidedantys iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių.
3. Užtikrinti, kad slaptažodžiai būtų periodiškai keičiami;
4. Užtikrinti, kad naudotojo ar lankytojo prieš tai naudoti slaptažodžiai nebūtų naudojami;
5. Užtikrinti, kad kuriami naudotojo ar lankytojų kuriami slaptažodžiai atitiktų nustatytą kompleksiškumo lygį, o neatitinkantys negalėtų būti sukuriami;
6. Slaptažodžiai turi būti saugomi užšifruoti;
7. Naudoti dviejų faktorių autentifikavimą, ypač privilegijuotiems sistemų naudotojams;
8. Techninėmis ir organizacinėmis priemonėmis užtikrinti, kad sistemų naudotojai negalėtų išsaugoti prisijungimo duomenų kompiuteriuose ar naudojamuose naršyklėse.