VILNIAUS UNIVERSITETO
KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

Finansų technologijų studijų programa
Kodas 6211BX022

EDVINAS VENCEVIČIUS

MAGISTRO BAIGIAMASIS DARBAS

SLAPTAŽODŽIO NUTEKĖJIMO RIZIKOS VERTINIMO METODAS

Kaunas 2024

VILNIAUS UNIVERSITETO
KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

EDVINAS VENCEVIČIUS

MAGISTRO BAIGIAMASIS DARBAS

SLAPTAŽODŽIO NUTEKĖJIMO RIZIKOS VERTINIMO METODAS

Leidžiama ginti

Magistrantas_____
(parašas)

Darbo vadovas_____

(parašas)

Doc. dr. Kęstutis Driaunys_____
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data
Registracijos Nr.

Kaunas 2024

TURINYS

TURINYS

SANTRUMPŲ SĄRAŠAS

2FA/MFA – Dviejų veiksnių autentifikacija (angl. Two-Factor/ Multi-Factor Authentication).

GUI – Grafinė sąsaja (angl. Graphical User Interface).

IEC – Tarptautinė elektrotechnikos komisija (angl. International Electrotechnical Commission).

ISO – Tarptautinė standartizacijos organizacija (angl. International Organization for Standardization).

ISS – Tarptautinė kosminė stotis (angl. International Space Station).

MD5 – Pranešimų maišos funkcija (angl. Message Digest Algorithm 5).

PIMS – Asmens informacijos valdymo sistema (angl. Personal Information Management Systems).

PSD2 – Antroji mokėjimo paslaugų direktyva (angl. Payment Services Directive 2).

SCA – Stipri kliento autentifikacija (angl. Strong Customer Authentication).

URL – Vienodas išteklių lokatorius-adresas (angl. Uniform Resource Locator).

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

Vencevičius Edvinas (2024). A Method for Assessing the Risk of Password Leakage. MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics.

SANTRAUKA ANGLŲ KALBA
SUMMARY

Nowadays risk of password loss is increasing drastically among Financial technology sector. According to the IBM Security Report 2023, the average cost of a data breach in financial institutions in 2023 was $4.45 million, a 15% increase over three years. Considering the fact that today password remains the most popular type of protection and recent statistics prove that 2FA/MFA is still not 100% used among individuals, this raises the necessity of password loss risk assessment.

The analysis of various scientific articles and statistical portals showed, that risk management framework has a good theoretical basis, however lacks clear and coincise pratical methodologies and tools for password loss risk assessment. Existing „password strenght“ type of tools are proved to be not efficient enough, due to their limitation and basic implementation. The purpose of this master thesis is to fill the existing gap and create a new method which would incorporate 3 main risk assessment steps: risk identification, risk calculation, risk management.

The new Method for Assessing the Risk of Password Leakage was created focusing on several main password leakage risk factors: password strenght, password reuse, multi-factor authentication and social engineering-phishing influence. Using two datasets of user responses (younger individuals <25 and older individuals aged 25-45), a practical risk assessment was made for both cases. Results show that model clearly emphasises the importance of this topic, as data results show existing medium-high password loss risk levels among both group individuals. Younger individuals tend to reuse passwords, and do not update passwords frequent enough, also the lack of cybersecurity knowledge is among risk factors. On the other hand, older individuals aged 25-45 are more exposed to lack of 2FA/MFA authentication. The results of using this new method proves the existing password loss risk problem among current generation, thus raises the concern and necessity of conducting future experiments with larger datasets.

ĮVADAS

Temos aktualumas

Kibernetinių atakų ir duomenų pažeidimų visame pasaulyje vis daugėja. Net organizacijoms stengiantis kovoti su kibernetiniais nusikaltėliais nuolat randama naujų būdų, kaip pasiekti ir išnaudoti jautriuosius asmenų duomenis (Stuart, 2023). Kibernetinės atakos daro vis didesnį poveikį, nes žmonės dabar didžiąją savo gyvenimo dalį gyvena internete, o tai reiškia, kad korporacijos, vyriausybės ir kitų tipų organizacijos renka vis daugiau asmeninių duomenų – be pasirinkimo galimybės. Bankų ir finansų sektorius visada buvo pagrindinis kibernetinių grėsmių taikinys dėl kritinio jų tvarkomos informacijos pobūdžio. Didėjant priklausomybei nuo technologijų ir skaitmeninės transformacijos, Fintech sektorius susiduria su dar labiau sudėtingesnėmis kibernetinių nusikaltėlių grėsmėmis (Darem, Alhashmi, Alkhaldi, Alashjaee, Alanazi, Ebad, 2023). Anot IBM Security Report 2023 ataskaitos, vidutinė duomenų pažeidimo kaina finansinėse įmonėse 2023 m. buvo 4,45 mln. JAV dolerių, o tai yra 15% padidėjimas per trejus metus. Taip pat pastebėta, kad 13% atvejuose pradinis atakos vektorius buvo pavogti arba kompromituoti prisijungimo duomenys.

Slaptažodžiai šiandien yra dažniausiai naudojamas vartotojo autentifikavimo metodas, nes kelis dešimtmečius iki šiol vis dar laikomas populiariausias dėl dažno ir paprasto naudojimo. Nauji tyrimai, metinės ataskaitos ir nacionalinės kibernetinių grėsmių ataskaitos ir toliau įrodo, kad žmonės vis dar naudoja mažiau nei pageidaujamus slaptažodžių įpročius, pvz., pakartotinai naudoja slaptažodžius, dalijasi jais su kuo nors kitu ir naudoja paprastus, nuspėjamus slaptažodžius ir bendrai vis dar yra linkę nepaisyti slaptažodžių higienos keliose paskyrose (Brende, Mansson, 2022).

Remiantis „Verizon Data Breach Investigations Report“ (VDIR, 2022), daugiau nei 80 % atakų sukelia silpni arba pakartotinai naudojami slaptažodžiai. Kitaip tariant, keturi iš penkių pažeidimų iš dalies siejami su silpnų, pakartojamų ar pavogtų slaptažodžių naudojimu (Anuj, 2024). Tuo tarpu „Keeper Security“ atliktas pasaulinis tyrimas atskleidė, kad 75 % vartotojų nesivadovauja ekspertų patarimais ir toliau naudoja silpnus slaptažodžius. (Mercado, Varela, 2024). 70 % silpnų slaptažodžių galima nulaužti greičiau nei per 1 sekundę, naudojant paprastas brutalios jėgos atakas (Blanton 2024), o atsižvelgiant į tai, kad per pastaruosius kelis metus buvo nulaužta daugiau nei 24 milijardai slaptažodžių, tai yra labai svarus ir dėmesio reikalaujantis elementas (Stouffer, 2023). Savo ruožtu, remiantis „Google“ 2023 metais atlikta apklausa, maždaug tik 45% interneto vartotojų yra įjungę 2FA bent vienoje savo paskyroje. Remiantis 2021 metų duomenimis, tik 32%

bankininkystės ir finansų sektoriaus darbuotojų naudojosi 2FA/MFA (Flynn, 2023). Šiandien šis skaičius sparčiai auga. Remiantis JumpCloud duomenimis, 87% įmonių, kuriose dirba daugiau nei 10 000 darbuotojų, naudoja MFA (McDade, Iannini, 2024). Tačiau tai vis dar negarantuoja visiško 100% vartotojų įsipareigojimo dviejų veiksnių autentifikacijai, ir šiandien Lietuvos Fintech rinkoje vis dar nėra įrodymo, kad 2FA/MFA yra paplitęs visur.

Ši problema kelia didelį susirūpinimą Fintech sektoriui, kadangi Fintech produktai yra didelių duomenų rinkėjai – jie reguliariai renka asmeninius duomenis (pvz., vartotojų vardus, vietos įrašus, banko sąskaitų duomenis ir el. pašto adresus) ir neskelbtinus duomenis (pvz., informaciją, susijusią su etnine kilme, rase, religiniais įsitikinimais, kredito informacija ir kita), o dažniausiu atveju, slaptažodžio nutekėjimas yra kelias į visų svarbių duomenų vagystę. Didžiulis informacijos kiekis padidina jos jautrumą, nes laikui bėgant FinTech įmonė gali sukurti labai išsamų privataus interneto vartotojo „portretą“ (Adeyoju, 2020). Pastarasis 2024-ųjų Finansų technologijų įmonės „Finastra“, kuri bendradarbiauja su 45 iš 50 geriausių pasaulio bankų, didelio masto informacijos vagystės incidentas, kurio metu pradėta pardavinėti daugiau nei 400 gigabaitų pavogtų duomenų, dar kartą įrodo, kad tai yra labai svarbaus mąsto klausimas (Krebson Security, 2024). Taigi, privačių interneto vartotojų slaptažodžių saugumo praktikos vengimas gali privesti prie visų šių duomenų praradimo ir didelių piniginių nuostolių. Nemažiau svarbu ir tai, kad žmonės yra linkę kartoti savo elgesį, įskaitant 2FA autentikacijos vengimą, silpno slaptažodžio ir kibernetinio saugumo aktualumo nebuvimą. Tokiu būdu, įpročiai iš privačios erdvės yra perduodami į darbo aplinką, kas taip pat tiesiogiai prisideda prie pavojaus jau organizaciniame Fintech lygmenyje.

Problemos ištyrimo lygis

Pasirinkta tema apie slaptažodžio nutekėjimo rizikos vertinimo metodą yra nepakankamai ištirta, ypač dėl struktūrizuotos ir nuoseklios informacijos, pritaikomos privatiems interneto vartotojams Fintech kontekste, trūkumą. Dabartinės metodikos daugumoje atvejų yra sukurtos labai bendro pobūdžio ir nėra orientuotos į rizikos skaičiavimo ir mažinimo veiksnius, taip pat neatsižvelgia į teorinę rizikos vertinimo perspektyvą. Tokiu būdu, nėra metodo, kuris prisitaikytų prie privačių interneto vartotojų specifiškų rizikos veiksnių dėl slaptažodžio nutekėjimo.

Apie duomenų nutekėjimo rizikos vertinimo teorinę perspektyvą kalba Agencia Espanola Proteccion Datos (AEPD 2021), ir European Union (ENISA, 2024). Kiekviena institucija apibrėžia

eilę žingsnių ar procedūrų, skirtų nustatyti, įvertinti ir sumažinti rizikas, susijusias su asmeninių duomenų praradimo rizika. Agencia Espanola Proteccion Datos (2021) supaprastina rizikos vertinimo procesą į tris pagrindines stadijas. Pabrėžiama rizikos veiksnių, susijusių su asmeninių duomenų tvarkymu, identifikavimas ir analizė. Tuo tarpu, European Union (ENISA, 2024) pateikiama išsamesnė analizė, apimanti penkis skirtingus žingsnius rizikos vertinimui, specifiškam duomenų tvarkymo operacijoms. Siūloma aiškiai apibrėžti ir kontekstualizuoti vertinamą tvarkymo operaciją, taip pat vertinti galimus duomenų praradimo ar nutekėjimo padarinius. Galiausiai atliekamas bendras rizikos lygio vertinimas, informuojant apie tinkamas saugumo priemones, skirtas efektyviai mažinti nustatytas rizikas.

Atlikta autorių Wang D., Shan, X., Dong, Q., Shen, Y., Jia, C. (2023) „No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters“ analizė įrodė, kad šiandien egzistuojantys slaptažodžio saugumo skaičiavimo įrankiai yra nekorektiški ir neatsižvelgia į specifinius kintamuosius, kurie statistiškai remiantis, prisideda prie slaptažodžių nutekėjimo rizikos.

Darbo problema

Kaip sukurti slaptažodžio nutekėjimo rizikos vertinimo metodą privatiems interneto vartotojams?

Darbo objektas

Slaptažodžio nutekėjimo rizikos vertinimo metodas (metodika).

Darbo tikslas

Sukurti slaptažodžio nutekėjimo rizikos vertinimo metodą privatiems interneto vartotojams.

Darbo uždaviniai

1. Išnagrinėti esamas bendro pobūdžio teorines rizikos vertinimo sampratas, rizikos sąvokas bei vertinimo rekomendacijas.
2. Išnagrinėti egzistuojančius slaptažodžių nutekėjimo rizikos vertinimo įrankius.

3. Išnagrinėti bei pagrįsti ISO-27001 organizacijos saugumo metodikos pritaikomumą privatiems interneto vartotojams ir atrasti galimus dėsningumus tolimesniam metodo (metodikos) kūrimui.
4. Sukurti slaptažodžio nutekėjimo rizikos vertinimo metodą (metodiką) privatiems interneto vartotojams.
5. Panaudoti sukurtą metodą praktikoje suprogramuojant programinio pobūdžio rizikos vertinimo metodą ir išanalizuoti bei palyginti jo rezultatus bei efektyvumą su tikraisiais apklausos duomenimis tarp skirtingo amžiaus vartotojų.

Darbo struktūra

Pirmoje darbo dalyje „Slaptažodžio nutekėjimo rizikos teoriniai aspektai“ nagrinėjama rizikos vertinimo samprata, susijusios koncepcijos ir analizuojama visa rizikos vertinimo proceso eiga. Išsamiai pristatomas rizikos vertinimo procesas slaptažodžio nutekėjimo lygmenyje – išanalizuojamas rizikos identifikavimo slaptažodžiui grėsmės, pristatoma teorinė rizikos skaičiavimo metodika bei rizikos mažinimo veiksniai. Aptariama ISO-27001 organizacijos saugumo metodika ir jos pritaikymo galimybės, dėsningumai privatiems interneto vartotojams bei apibūdinama kiekvieno rizikos vertinimo žingsnio svarba.

Antroje darbo dalyje „Slaptažodžio nutekėjimo rizikos vertinimo metodas“ detaliau išnagrinėjamas egzistuojantis slaptažodžio stiprumo skaičiavimo įrankis, aptariami jo trūkumai, galimi patobulinimai. Pristatomas siūlomo metodo sprendimas, klausimynas, rizikos reikšmės bei skaičiavimai.

Trečioje darbo dalyje „Slaptažodžio nutekėjimo rizikos vertinimo eksperimentas“ pristatomas praktinis metodo (metodikos) programinis įrankis (kodas) naudojant “Python” programavimo kalbą. Taip pat pristatomas ir išanalizuojami realių duomenų (apklausos vartotojų) masyvai, atliekamas praktinis metodo testavimas su duomenimis, įvertinamas pritaikomumas bei palyginami rezultatai. Galiausiai, darbo pabaigoje yra pateikiamos gautos išvados. Apsvarstomos tolimesnės metodo tobulinimo, interpretavimo galimybes.

Darbe naudoti literatūros šaltiniai

Teorinėje dalyje daugiausiai buvo remiamasi užsienio autorių moksliniais darbais susijusiais su rizikos sąvoka ir jos vertinimo proceso samprata. Taip pat buvo naudotasi už saugumą atsakingų Europos valstybinių organizacijų sukurtų rizikos vertinimo metodikų turiniu.

Darbo tyrimai ir metodai

Atliekant slaptažodžio nutekėjimo rizikos vertinimo metodo teorinio aspekto analizę darbe bus naudojami toliau pateikiami tyrimo metodai: literatūros (straipsnių) analizė, sintezė. Taip pat bus kuriamas iškeltos problemos metodikos sprendimas.

Darbo teorinė reikšmė

Buvo atlikta slaptažodžio nutekėjimo rizikos vertinimo šaltinių analizė, leidusi apibrėžti esminius rizikos vertinimo proceso etapus, suprasti visą sampratą bei atrasti esamus trūkumus.

Išanalizuotas egzistuojantis slaptažodžio stiprumo skaičiavimo klausimynas bei pagrįstas ISO-27001 standartų pritaikomumas privatiems interneto vartotojams padėjo įžvelgti tobulinimo galimybes ir pateikė pagrindą metodo prototipo kūrimui.

Darbo praktinė reikšmė

Buvo sukurta nauja plataus pobūdžio struktūrizuota ir statistiškai bei moksliškai pagrįsta metodika, apimanti svarbiausius kintamuosius, prisidedančius prie slaptažodžio nutekėjimo grėsmės, taip pat rizikos vertinimo svoriai bei skaičiavimo formules.

Sukurtas naujasis metodas buvo programiškai suprogramuotas programėlės pavidalu „Python“ kalba.

Darbo struktūra ir apimtis

Darbą sudaro įvadas, 3 pagrindinės dalys, išvados. Pagrindinė darbo medžiaga aprašyta 68 puslapiais, įskaitant 3 lenteles, 27 paveikslus, 1 priedą. Panaudotos literatūros sąrašą sudaro 44 šaltiniai.

1. SLAPTAŽODŽIO NUTEKĖJIMO RIZIKOS TEORINIAI ASPEKTAI

1.1. Rizikos vertinimo samprata

Remiantis Ispanijos Duomenų Apsaugos Agentūra (Agencia Espanola Proteccion Datos, 2021), rizikos vertinimas yra pagrindinis bet kurios organizacijos, taip pat privačių vartotojų, procesų elementas, jis yra neatsiejama bet kurio subjekto, projekto ar žmogaus veiklos valdymo dalis. Rizikos vertinimas, arba kitaip valdymas – tai galimų (tikimybių), pasekmių (poveikių), kurių veikla gali turėti saugotinų prekių ar elementų (turto) rinkiniui, kontrolė. Rizikos vertinimui yra reikalinga analizė, tai yra kritinis ir objektyvus proceso suvokimas, svarbu sprendimus paversti konkrečiais veiksmais, kurių dėka būtų sumažinta žala.

Fintech konteksto lygmenyje, rizika yra suvokiama kaip grėsmė, kylanti atliekant vartotojų finansinius sandorius ir prekiaujant finansų ar kriptovaliutų rinkose. Kitaip tariant, technologinių naujovių keliamas pavojus atsiranda naudojantis finansinėmis paslaugomis. Be to, Fintech rizika gali būti apibrėžiama kaip bet kokie galimi gedimai, trūkumai ir netinkamas technologijos naudojimas, kuris trikdo vartotojų finansinius sandorius (Hoque, 2023). Šiandien yra plačiai aktualizuojamas susirūpinimas dėl neskaidrumo ir duomenų tvarkymo netinkamo naudojimo, kai asmenims paprastai trūksta išminties, matomumo ir kontrolės, kalbant apie duomenų interpretaciją, kas juos analizuoja, perduoda, saugo ar kitaip apdoroja ir naudoja (Janssen, Singh, 2022). Ko pasekoje, atsižvelgiant į didėjantį viešąjį diskursą su duomenimis susijusiais klausimais bei rizikos vertinimu, taip pat labai svarbu paminėti terminą PIMS (angl. Personal Information Management Systems) – koncepcija, kurios tikslas yra geriau informuoti vartotojus ir suteikti jiems daugiau galimybių, susijusių su jų duomenų tvarkymu bei pavojaus identifikavimu.

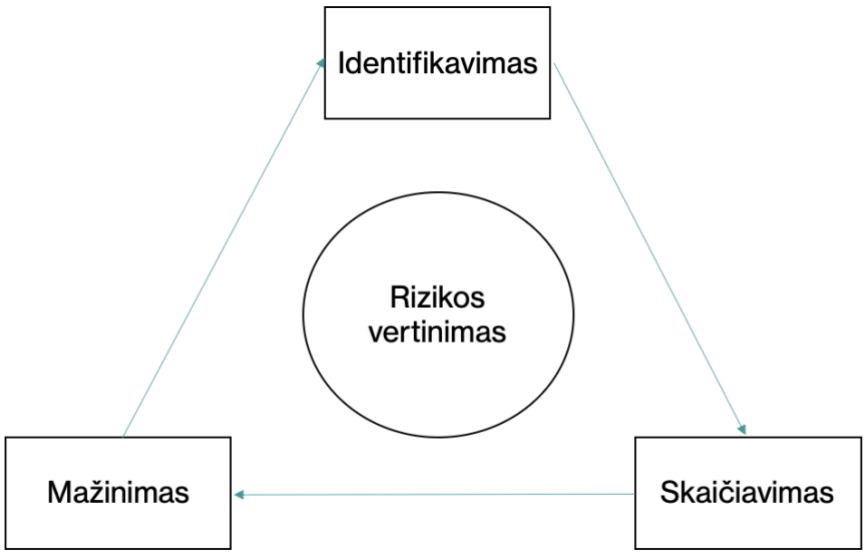
Pasak Europos duomenų apsaugos priežiūros institucijos (European Data Protection Supervisor, 2016), PIMS yra laikoma rizikos vertinimo proceso dalis. Tai yra sistemos, padedančios asmenims labiau kontroliuoti savo asmens duomenis. PIMS leidžia asmenims tvarkyti savo asmens duomenis saugiose, vietinėse ar internetinėse saugojimo sistemose ir dalytis jais kada ir su kuo jie pasirenka. Pagal PIMS koncepciją, privatūs interneto vartotojai tampa asmeninės informacijos tikraisiais savininkais. Tai gali sukelti paradigmos pokytį tvarkant asmens duomenis, o tai gali turėti socialinių ir ekonominių pasekmių.

1.2. Rizikos vertinimo procesas

BDAR (Bendrasis duomenų apsaugos reglamentas) nenustato vieno konkretaus praktinio-metodologinio požiūrio į rizikos valdymą. Šiuo atžvilgiu BDAR palieka laisvę šio rizikos valdymo teisėms ir laisvėms integruoti su kitais organizacijos rizikos valdymo ištekliais, politika ir valdymu. Apskritai BDAR taip pat nereikalauja jokių aiškų formalumo reikalavimų rizikos valdymo vykdymui, nepažeidžiant pirmiau minėtų atskaitomybės įsipareigojimų (European Data Protection Supervisor, 2016). Įprastai yra laikomasi praktikos, kad pirmiausia reikėtų sutelkti dėmesį į bendrą rizikos valdymo praktiką. Vėliau galima sutelkti dėmesį į konkrečius veiksmus ar procesus, kurie padės valdyti Fintech riziką (Hoque, 2023). Natūraliai rizikos valdymas Finansų technologijų sektoriuje yra skirstomas į tris pagrindinius etapus: rizikos ir jos poveikio nustatymas ir identifikavimas. Toliu seka aprašomas rizikos proceso skaičiavimas, susijęs su prioritetų nustatymu ir įgyvendinimu. Trečiame etape vyksta nuolatinio vertinimo procesas ir rizikos valdymo, mažinimo įgyvendinimo priemonės (Stoneburner, Goguen, Feringa, 2002).

Rizikos vertinimas gali būti klasifikuojamas dviem lygiais, tai yra įgimtu rizikos lygiu ir likutinės rizikos lygiu, naudojant tuos pačius vertinimo kriterijus kiekvienam vertinimui. Įgimta rizika yra „blogiausio atvejo“ scenarijus. Tai apima rizikos tikimybės ir poveikio įvertinimą, jei nėra jokių valdymo kontrolės intervencijų. Šis vertinimo lygis suteikia perspektyvą, kokios rizikos pasekmės gali kilti įstaigai jos nevaldomoje būsenoje. Antrasis būdas yra susijęs su likutinės rizikos nustatymu. Likutinė rizika yra viskas, kas lieka po esamų kontrolės intervencijų. Paprastai vadovybė įsteigia pakankamą kontrolę, kad sumažintų riziką iki iš anksto nustatyto lygio, kaip nurodo optimalus rodiklis. Likutinė rizika yra kritinis rodiklis, parodantis, ar esamos kontrolės priemonės yra veiksmingos sumažinant riziką iki priimtino lygio (Public Sector Risk Management Framework, 2010).

Rizika gali būti vertinama kiekybiniu arba kokybiniu pagrindu. Kiekybinis įvertinimas geriausiai tinka rizikai, susijusiai su skaitinėmis funkcijomis. Pavyzdžiui, tai būtų finansinių nuostolių rizika, nes ją galima kiekybiškai įvertinti. Kiekybiniai metodai paprastai suteikia daugiau tikslumo ir yra naudojami sudėtingesnėje veikloje. Kokybinis vertinimas taikomas tada, kai rizika nėra tinkama kiekybiškai įvertinti. Tokiais atvejais pasitelkiamos subjektyvesnės priemonės, iš kurių svarbiausia yra ekspertinis vadovybės sprendimas (Public Sector Risk Management Framework, 2010).



1 pav. Rizikos vertinimo eiga

Šaltinis: Sudaryta autoriaus

1.2.1. Rizikos identifikavimas

Nors BDAR pateikia minimalių reikalavimų, kuriuos reikia valdyti nustatant rizikos veiksnius, sąrašą, reikia pažymėti, kad nereikėtų apsiriboti tik taisyklėse aiškiai įvardytų rizikos veiksnių šalinimu. Rizikos valdymas turi nustatyti ir įvertinti tuos rizikos veiksnius, kurie kyla dėl konkretaus atvejo, atsižvelgiant į jo pobūdį, apimtį ar mastą arba jo siekiamus tikslus, nepamirštant tų, kurie kyla iš dabartinio ir būsimo tvarkymo konteksto (Agencia Espanola Proteccion Datos, 2021). Grėsmė yra galimybė tam tikram grėsmės šaltiniui sėkmingai panaudoti tam tikrą pažeidžiamumą. Pažeidžiamumas yra silpnybė, kurią galima netyčia suaktyvinti arba tyčia išnaudoti. Grėsmės šaltinis nekelia pavojaus, kai nėra pažeidžiamumo, kurį būtų galima panaudoti. Nustatant grėsmės tikimybę, reikia atsižvelgti į grėsmės šaltinius, galimus pažeidžiamumus ir esamas kontrolės priemones (Agencia Espanola Proteccion Datos, 2021). Motyvacija ir ištekliai įvykdyti ataką daro žmones potencialiai pavojingais grėsmės šaltiniais. Sistemos įsilaužimų istorijos apžvalgos, saugumo pažeidimų ataskaitos, incidentų ataskaitos ir pokalbiai su sistemos administratoriais, pagalbos tarnybos darbuotojais ir vartotojų bendruomene informacijos rinkimo metu padės nustatyti žmonių grėsmių šaltinius, kurie gali pakenkti IT sistemai ir jos duomenims ir kurie gali kelti susirūpinimą, kai yra pažeidžiamumas (Stoneburner, Goguen, Feringa, 2002). Tai ne

kas mažiau svarbu ir kalbant apie privačių vartotojų riziką prarasti slaptažodžius, kadangi tiek organizacijos, tiek privačių vartotojų užpuolimo atvejai yra panašūs ir kenkėjai turi labai panašius tikslus.

Vienas iš svarbiausių Fintech rizikos kategorijų ir rūpesčių yra duomenų privatumas. Duomenų privatumo rizika visų pirma yra susijusi su klientų duomenų vagystėmis, kurios šiais laikais yra viena opiausių problemų. Dėl įsilaužimo į klientų duomenis, tokius kaip asmens tapatybės informacija, banko sąskaitos ir kortelių informacija, tiek Fintech vartotojai, tiek įmonės nuolat praranda pinigus. Dėl sparčiai augančios Fintech įmonių plėtros taip pat kyla susirūpinimas dėl duomenų privatumo. Kadangi slaptažodžiai tiesiogiai prisideda prie jautrių duomenų nutekėjimo, bei kadangi šiame darbe fokusuojamasi į privačių vartotojų slaptažodžio nutekėjimo aspektą Fintech kontekste, toliau bus analizuojami pagrindiniai slaptažodžio praktikos bei atakų dėmenys.

Yra išskiriami keturi pagrindiniai slaptažodžių įpročių veiksniai, kuriuos sudaro mažas slaptažodžio ilgis, lengvai atspėjamų slaptažodžių žodynas, pakartotinis slaptažodžio naudojimas ir antrojo faktoriaus autentifikavimo trūkumas. Jie yra nurodyti kaip svarbiausi kintamieji slaptažodžio praradimo rizikai. Ankstesnis tyrimas parodė, kad 81 % duomenų pažeidimų įvyksta dėl silpnų slaptažodžių; tai paprastai siejama su vartotojo aplaidumu (Dastane, Johari, Bakon, 2020). Ankstesniame vartotojų tyrime, kuriame dalyvavo 294 dalyviai, pranešama, kad 30 % jų buvo pažeista arba pažeista bent viena jų paskyra dėl prasto arba silpno slaptažodžio ilgio. Pastebėta, kad paprasti žodyno žodžiai lengvai nulaužiami arba pažeidžiami naudojant įrankius su žodyno sąrašu. Todėl rekomenduojama į slaptažodžius įterpti spec. simbolius ar skaičius, pavyzdžiui angliškas žodis „Winter“ į „W1nt3r“. Apibendrinant galima teigti, kad įprastas slaptažodžių žodynas, kuris laikomas silpnu, yra tokie pavyzdžiai kaip daiktavardžių, gimtadienių datų, šeimos, naminių gyvūnų vardų ar net sukakties datos vartojimas.

Minėti autoriai atliko tyrimą apie interneto vartotojų naudojamus slaptažodžius ir apskaičiavo, kad 43 % slaptažodžių buvo panaudoti pakartotinai. Slaptažodžių pakartotinio naudojimo keliose svetainėse ir jo silpnos praktikos, sukeliančios saugumo ar asmens duomenų pažeidimus, tyrimas buvo atliktas lyginant 21 geriausio JAV universiteto slaptažodžių pakartotinį naudojimą (Dastane, Johari, Bakon, 2020). Kitas pavyzdys – atvejo tyrimas apie pavogtus ir nutekintus iš konkurento Pietų Korėjos organizacijos narių prisijungimo duomenis, naudotus

nelegaliai prekybai vykdyti, kainavo 22 mln. USD nuostolį. Yra laikomasi sampratos apie dažno slaptažodžio pakartotinio naudojimo įtaką ir poveikį asmens pažeidžiamumui dėl duomenų pažeidimo. Anksčiau buvo žinomi pažeidimai, susiję ne tik su vartotojais, bet ir su organizacijomis, dėl kurių buvo nuspręsta pereiti prie antrojo veiksnio autentifikavimo. „Duo Security“ pranešė, kad tokios organizacijos ar paslaugų teikėjai, kaip „Bitly“, „Twitter“, „Buffer“, „Hootsuite“, „Tumblr“ ir daugelis kitų, pradėjo teikti antrojo veiksnio autentifikavimą ne tik savo vidiniams vartotojams, bet ir klientams (Dastane, Johari, Bakon, 2020). Nepaisant patrauklių 2FA saugumo pranašumų, jo poveikis vartotojo patirčiai šiandien lieka ne iki galo aiškus. Ankstesni 2FA tyrimai davė rezultatų, kurie gali pasirodyti prieštaringi. Nors yra keliama išvada, kad 2FA yra visiškai netinkamas naudoti, kiti nustato, kad kai kurie 2FA metodai iš tikrųjų yra labai tinkami naudoti, pavyzdžiui SMS žinutės gavimas. Tačiau galutinė nuomonė išlieka ta, kad kibernetiniam užpuolikui yra žymiai sunkiau pažeisti paskyrą ir pavogti slaptažodį, apsaugotą antruoju autentifikavimo veiksniu (Reese, Smith, Dutson, Armknecht, Cameron, Seamons, 2019).

Brute Force ataka – šio tipo atakos metu taikomos visos galimos slaptažodžių kombinacijos, kad būtų nulaužtas slaptažodis. Brutalios jėgos ataka paprastai siekiama nulaužti užšifruotus teksto formos slaptažodžius. Ankstyvosiose Linux sistemose slaptažodžiams saugoti buvo naudojamos MD5 šifravimo schemos. Operacinėje sistemoje yra slaptažodžių failas, kuriame yra vartotojo slaptažodžiai su vartotojo vardais. Jei failą pavogs užpuolikas, slaptažodis gali būti lengvai prarastas. Pradinio slaptažodžio faile nėra, bet jis yra užšifruotas žinutės santraukos (ang. MD5) algoritmu. Gali pasirodyti, kad užšifruotas slaptažodis yra saugus, tačiau iš tikrųjų jis taip pat yra pažeidžiamas brutalios jėgos atakų. Tam užpuolikas pirmiausia konvertuoja visus slaptažodžių derinius į savo MD5 šifravimą. Brutalios jėgos atakos užima labai daug laiko, nes šifravimo paieška iš visų galimybių užima daug laiko. Pavyzdžiui, vartotojas įveda slaptažodį iš 8 simbolių ir visi simboliai yra mažosios raidės, tuomet, norint nulaužti slaptažodį naudojant brute force ataką, reikia (26)8 kombinacijų, kas yra lygu 208827064576 kartai. Jei vienam kompiuteriui reikia vienos sekundės, kad patikrinti 1000 slaptažodžių, tuomet bendras laikas bus 208827064576 / 1000 = 208827064,576 sekundžių, tai yra 58007,52 valandos. Tai rodo, kad brute force ataka yra efektyvi naudojant trumpesnius slaptažodžius (Raza, Haider, Iqbal, 2012).

Klavišų registratoriai (ang. Keyloggers), kaip ir daugelis Trojos arklių, yra sukurti taip, kad imituotų teisėtą programinę įrangą ir apeitų antivirusinius ar kenkėjiškų programų skaitytuvus. Dar blogiau, privilegijų lygis, kuriuo klavišų registratoriai vykdo, yra aukštesnis nei įprastos kenkėjiškos

programos. Dėl šios funkcijos klavišų registratorių beveik neįmanoma aptikti ir pašalinti. Trojos arklys „Keylogger“ seka klaviatūra įvestus klavišų paspaudimus, įrašo ekrano veiklą ir nuskaito konkrečių dokumentų sistemas bei siunčia informaciją atgal įsilaužėliui. Nors klavišų registratorių taikymas nėra neteisėtas, jų naudojimas dažniausiai yra susijęs su kenkėjiška veikla, iš kurių viena – informacijos rinkimas: kiekvieno klavišo paspaudimo registravimas ir įrašymas iš tikslinės sistemos klaviatūros. Tai yra paprastas procesas, kurio metu užpuolikai gali pavogti neskelbtiną informaciją, pvz., mokėjimo kortelių duomenis, socialinio draudimo numerius ir vairuotojo pažymėjimo duomenis, taip pat dviejų veiksnių autentifikavimo kodus bei, žinoma, slaptažodžius (Bhardwaj, Goundar, 2020).

Žodyno atakos (ang. Dictionary attack) yra daug greitesnis nei pagrindinis Brute Force metodas. Dauguma atliekamų prijungimų užtrunka tik iki 15 minučių (Bosnjak, 2018). Daugelis vartotojų paprastai rašo slaptažodžius, susijusius su paukščių vardais, pažįstamomis vietomis, žinomų aktorių vardais. Šie slaptažodžiai gali būti vertinami pagal žodyno ataką. Užpuolikas sudaro dažniausiai vartojamų žodžių, kurie galėjo būti naudojami kaip slaptažodis, žodyną. Tada užpuolikas taiko visus šiuos žodžius, kad nulaužtų slaptažodį. Nors žodyno ataka yra greitesnė nei Brute Force ataka, ji taip pat turi tam tikrų apribojimų, t. y. ataka yra ribota žodžių ir kartais ji negali nulaužti slaptažodžio, nes išlieka galimybė, kad slaptažodžio, kurį reikia nulaužti, gali nebūti pačiame žodyne (Thai, Tanaka, 2022).

Nemažiau svarbus veiksnys, turintis įtakos slaptažodžio nutekėjimui, yra socialinės inžinerijos ir fišingo atakos. Sukčiai naudojasi šia galimybe ir kad apgauti savo aukas pasitelkiant socialinės inžinerijos metodais. „Įtikinėjimas“ apibrėžiamas kaip žmonių bendravimo procesas, kuriuo siekiama pakeisti asmens elgesį, įsitikinimus ar vertybes įvykiams, idėjoms, objektams ir kitiems žmonėms, naudojant žodinius žodžius, rašymą ar vaizdines priemones informacijai ir jausmams perteikti. Atsižvelgiant į tai, kaip vykdoma socialinės inžinerijos ataka, galima išskirti tris tipus: socialiniai išpuoliai – vykdomi prieš žmones bendraujant su auka ir žaidžiant jų emocijomis. Tokios atakos pavyzdys yra suasmenintas sukčiavimas ietimis, prieš kurį atliekama bendruomenės žvalgyba, technologijomis pagrįstos atakos – tai atakos, vykdomos internetu, pvz., socialiniuose tinkluose, svetainėse, kuriose renkama slapta informacija, pvz., prisijungimo duomenys, slaptažodžiai, banko sąskaitos duomenys, kredito kortelės duomenys ir kt. fiziškai pagrįstos atakos, t.y. fiziškai atliekami veiksmai, pvz. eidamas per šiukšliadėžę, kad gautų vertingų dokumentų. Viena iš populiaresnių socialinės inžinerijos atakų pavyzdžių yra naršymas per petį. Tai yra alternatyvus

„šnipinėjimo“ pavadinimas, kai užpuolikas šnipinėja vartotojo judesius, kad gautų slaptažodį. Šio tipo atakos metu užpuolikas stebi vartotoją; kaip jis įveda slaptažodį, t. y. kokius klaviatūros klavišus vartotojas paspaudė (ang. Shoulder Surfing) (Borowiec, Demidowski, Pecka, Jonarska, 2023).

Nuorodų manipuliavimas atliekamas apgaule nukreipiant vartotoją spustelėti nuorodą į netikrą svetainę. Tai galima padaryti per daug skirtingų kanalų, įskaitant el. laiškus, tekstinius pranešimus ir socialinę žiniasklaidą. Vienas iš būdų – subdomenų naudojimas. URL hierarchija visada eina iš dešinės į kairę. Remiantis „Yahoo Mail“ pavyzdžiu, teisinga nuoroda turėtų būti mail.yahoo.com – kur „Yahoo“ yra pagrindinis domenas, o „Mail“ yra subdomenas. Sukčiuotojas gali pabandyti apgauti naudodamas apgaulingą nuorodą yahoo.mail.com, kuri nuves vartotoja į puslapį su pagrindiniu pašto domenu ir Yahoo subdomenu. Kitas būdas – Paslėpti URL. Taip yra, kai sukčiaujantysis paslepia tikrąjį sukčiavimo svetainės URL po paprastu tekstu, pvz., „Spustelėkite čia“ arba „Prenumeruoti“. Kai kuriais atvejais sukčiai netgi gali parodyti teisėtą URL, kuris iš tikrųjų nukreipia į netikėtą svetainę (Deloitte, 2019).

1.2.2. Rizikos skaičiavimas

Finansų technologijų sektoriuje Rizikos skaičiavimas – tai rizikos atsiradimo tikimybės ir galimo tokios rizikos poveikio įstaigai nustatymas. Nustačius pagrindines ir įtakingas rizikas, visos rizikos turėtų būti suskirstytos į kategorijas ir įtrauktos į prioritetų sąrašą, kad būtų galima išsiaiškinti, kurios rizikos yra pirmoje vietoje ir jas reikia skubiai išspręsti (Hoque, 2023). Atsižvelgiant į nustatytų rizikos veiksnių rinkinį ir su jais susijusį rizikos lygį, bendram rizikos lygiui įvertinti gali būti taikomos skirtingos metodikos. Esant skirtingiems rizikos veiksniams, būtina išaiškinti, kaip šie veiksniai, vertinant atskirai, gali sąveikauti vienas su kitu, analizuojant jų bendras priklausomybes ir poveikį arba egzistuojančias tarpusavio sąveikas (Agencia Espanola Proteccion Datos, 2021). Galutinis rizikos nustatymas gaunamas padauginus grėsmės tikimybės ir grėsmės poveikio įvertinimus. Bendri rizikos įvertinimai gali būti nustatyti remiantis įvestimis iš grėsmės tikimybės ir grėsmės poveikio kategorijų. Atsižvelgiant į reikalavimus ir pageidaujamo rizikos vertinimo detalumą, kiekvienas gali naudoti skirtingus metodus. Tai gali apimti labai mažą arba labai didelę grėsmės tikimybę ir labai mažą arba labai didelį grėsmės poveikį, kad būtų sukurtas labai mažas arba labai didelis rizikos lygis. „Labai aukštas“ rizikos lygis gali pareikalauti

galimo sistemos išjungimo arba visų IT sistemų integravimo ir testavimo pastangų įmonėse (Stoneburner, Goguen, Feringa, 2002).

Šiai dienai rizikos skaičiavimo etapui slaptažodžio nutekėjimo atvejui galima priskirti tokias platformas kaip „NordPass“, „Haveibeenpwned.com“, „Security.org“. Šių įrankių/metodikų klausimynas veikia analizuojant įvesto slaptažodžio charakteristikas ir lyginant jas su duomenų bazėse saugomais kompromituotų slaptažodžių sąrašais. Tokiu būdu yra naudojami algoritmai, kurie tikrina slaptažodžio ilgį, simbolių įvairovę (didžiosios ir mažosios raidės, skaičiai, specialūs simboliai) ir nuspėjamumą. Pavyzdžiui, platforma įvertina, ar slaptažodis atitinka įprastus modelius (pvz., „123456“ ar „password“) arba asmeninius kintamuosius (pvz., gimimo datas). Savo ruožtu „Have I Been Pwned“ tikrina slaptažodį pagal didžiulę kompromituotų slaptažodžių duomenų bazę, naudojant šifravimą, siekiant vartotojo privatumo apsaugos. Tai leidžia vartotojui sužinoti, ar slaptažodis jau buvo nutekintas ankstesniuose duomenų pažeidimuose, nesukeliant papildomo privatumo pažeidimo.

Žvelgiant į rizikos skaičiavimo matematinę perspektyvą bendrąja prasme yra laikomasi tokio principo:

Rizikos balas yra skaitinė vertė, nurodanti galimą neigiamo įvykio sunkumą ir tikimybę. Šis balas padeda organizacijoms nustatyti rizikos prioritetus, o tai leidžia paskirstyti išteklius ir įgyvendinti veiksmingas kontrolės priemones, skirtas apsisaugoti nuo kritinės rizikos. Iš esmės rizikos balas sudėtingus rizikos matmenis paverčia paprastu skaičiumi, kurį lengva interpretuoti. Norint suprasti ir apskaičiuoti rizikos balą, svarbu atsižvelgti į du pagrindinius komponentus: rizikos tikimybę ir rizikos poveikį (Bonnie, 2024).

Rizikos tikimybė: šis komponentas įvertina rizikos tikimybę. Tikimybę galima išmatuoti naudojant skaitines reikšmes, tokias kaip 1–5, procentus arba kokybinius deskriptorius (pvz., reta, tikėtina, beveik garantuota). Įprastai norint nustatyti rizikos tikimybę organizacijos lygmeniu, reikia atsižvelgti į istorinius duomenis, pasikonsultuoti su vidaus ekspertais, išnagrinėkite pramonės tendencijas ir įvertinkite esamų kontrolės priemonių stiprumą.
Rizikos poveikis: šiame komponente atsižvelgiama į rizikos įvykio pasekmes, jei jis įvyktų. Norint įvertinti poveikį, reikia įvertinti galimus finansinius nuostolius, žalą reputacijai ir teisines bei

atitikties pasekmes. Kaip ir tikimybę, poveikį galima kiekybiškai įvertinti naudojant skaitines vertes arba kokybinius deskriptorius, nuo minimalaus iki labai aukšto.

Šis pagrindinis skaičiavimas leidžia organizacijoms greitai peržiūrėti įvairias rizikas, kad būtų lengviau palyginti ir nustatyti prioritetus. Didesnis rizikos balas, žinoma, rodo didesnį rizikos lygį, kai reikia skubiau ją sumažinti (Bonnie, 2024).

Rizikos balas = (tikimybė) × (poveikis)

Tai padeda organizacijoms lengvai palyginti rizikas ir nustatyti, kaip paskirstyti išteklius optimalioms reagavimo į riziką strategijoms. Svarbu paminėti, kad nors ši rizikos skaičiavimo strategija yra bendro pobūdžio ir fokusuojasi į organizacijas, jos pritaikymas slaptažodžio nutekėjimo atvejui asmeninio vartotojo kontekste taip pat aktualus ir pritaikomas (Bonnie, 2024).

1.2.3. Rizikos mažinimas

Trečiajame etape finansų institucijos turi parengti efektyvius rizikos mažinimo planus ir procedūras. Vienas iš svarbiausių finansų institucijų uždavinių yra sukurti veiksmingus kovos su sukčiavimu metodus. Be to, siekiant stebėti išorines rizikos situacijas, tokias kaip atsirandantys elektroniniai nusikaltimai ar nelegalios nuosavybės tendencijos, finansų institucijos turėtų būti pasirengusios parengti veiksmingus rizikos mažinimo planus (Hoque, 2023). Nustačius rizikos veiksnius ir apskaičiavus rizikos lygį, svarbu sumažinti riziką iki priimtino lygio (Agencia Espanola Proteccion Datos, 2021). Šiame proceso etape pateikiamos kontrolės priemonės, kurios galėtų sumažinti arba pašalinti nustatytas rizikas, atsižvelgiant į veiklą. Rekomenduojamų kontrolės priemonių tikslas – sumažinti IT sistemos ir jos duomenų rizikos lygį iki priimtino lygio.

Kontrolės rekomendacijos yra rizikos vertinimo proceso rezultatai ir suteikia indėlį į rizikos mažinimo procesą, kurio metu įvertinamos rekomenduojamos procedūrinės ir techninės saugumo kontrolės priemonės, nustatomi prioritetai ir įgyvendinami reikalingi sprendimai (Stoneburner, Goguen, Feringa, 2002). Slaptažodžio nutekėjimo rizikos mažinimo procesas remiasi gerųjų slaptažodžio valdymo praktikų laikymosi. Šiai dienai egzistuoja daug patarimų bei straipsnių, kaip apsisaugoti užtikrinti slaptažodžio tinkamą valdymą ir saugumą (ang. Password management).

Kaip teigia Tam, Glassmanan ir Vandenwauver (2010), pirmiausia svarbu, daugiau nei tik informuoti vartotojus apie paskyros, kurios slaptažodį jie turi tvarkyti, svarbą. Reikia leisti jiems suprasti ir neigiamas prasto slaptažodžių valdymo pasekmes. Vartotojai turi jausti asmeninius nuostolius, jei paskyros slaptažodis yra nutekinamas.

Yra išskiriami keletas slaptažodžių valdymo veiksmų:

• Pirmą kartą pasirenkant kompiuterio slaptažodį

• Slaptažodžio keitimas

• Leisti kam nors kitam naudoti savo slaptažodį

• Užklijuoti slaptažodį matomoje vietoje

• Slaptažodžio bendrinimas su šeima, draugais ar bendradarbiais

Pirmieji du slaptažodžių valdymo veiksmai (slaptažodžio pasirinkimas pirmą kartą ir slaptažodžio keitimas) yra įprasti, tačiau neutralūs veiksniai. Toks elgesys yra neutralus. Greičiau tai, kaip vartotojas pasirenka ir keičia slaptažodį, lemia, ar elgesys yra geras, ar blogas. Kiti trys slaptažodžių valdymo veiksmai (leisti kam nors kitam naudoti slaptažodį, priklijuoti slaptažodį matomoje vietoje ir dalytis slaptažodžiu su šeima, draugais ar bendradarbiais) yra elgesys, kurio reikia vengti (Tam, Glassmanan, Vandenwauver, 2010). Apibendrinant galima teigti, jog blogas slaptažodžių valdymas yra patogus. Vartotojų pažintiniai gebėjimai (t. y. atmintis) riboja jų naudojimąsi stipriais slaptažodžiais (Gehringer, 2002) bei didesnis vartotojų švietimas apie neigiamas blogo slaptažodžių valdymo pasekmes paskatintų gerą slaptažodžių elgesį.

Kitos slaptažodžio saugumo praktikos apima tokių taisyklių laikymosi kaip:

1. Nenaudoti nuoseklių skaičių ar raidžių.
1234, qwerty, jklm, 6789 ir kt. yra vieni pirmųjų slaptažodžių, kuriuos išbandys sukčiai. Panašiai brute force programinė įranga paprastai tikrina nuoseklius skaičius ir raides, nes jie taip dažnai naudojami (Terranovasecurity, 2024).

2. Į slaptažodį neįtraukti savo gimimo metų arba gimimo mėnesio/dienos
Kibernetiniai nusikaltėliai gali lengvai rasti šią informaciją sekdami vartotojo socialinės medijos paskyras. Tas pats pasakytina apie lengvai randamą asmeninę informaciją, pvz., naminių gyvūnėlių vardus, adresus ir darbdavių vardus.

3. Naudoti bent dvylikos raidžių, skaičių ir simbolių derinį
Kuo ilgesnis slaptažodis ir kuo daugiau simbolių jame naudojama, tuo sunkiau jį atspėti. Pavyzdžiui, M0l#eb9Qv? sujungia didžiąsias ir mažąsias raides su skaičiais ir simboliais, sudarydamas unikalų slaptažodį, kurio neįmanoma išvesti.

4. Slaptažodyje arba slaptažodžio frazėje sujungti skirtingus nesusijusius žodžius
Dėl šios praktikos kibernetiniams nusikaltėliams sunkiau atspėti slaptažodį. Svarbu nenaudoti frazių iš populiarių dainų, filmų ar televizijos laidų. Norint sukurti stipresnį slaptažodį, svarbu naudoti tris ar keturis ilgesnius žodžius. Pavyzdžiui, 9Sp!dErscalKetobogGaN.

5. Nevartoti vardų ar žodžių, esančių žodyne
Svarbu pakeisti raides skaičiais arba simboliais, kad slaptažodį būtų sunku atspėti. Arba sąmoningai naudoti rašybos klaidas slaptažodžio ar slaptažodžio frazėje.

6. Slaptažodžiams saugoti naudoti slaptažodžių tvarkyklę
Rekomenduojama nesirašyti slaptažodžių ir nelaikyti jų kompiuteryje esančiame dokumente. Svarbu įsitikinti, kad naudojamas slaptažodžių tvarkyklės įrankis, kurį suteikė IT / palaikymo komanda, kad saugoti visus profesinius ir asmeninius slaptažodžius. Daugelyje slaptažodžių tvarkytuvų taip pat yra patogus slaptažodžių generatorius, todėl nereikės kiekvieną kartą kurti naujo.

7. Nenaudoti savo slaptažodžių pakartotinai
Kiekvienam įrenginiui, programai, svetainei ir programinei įrangai reikalingas unikalus ir stiprus slaptažodis arba PIN kodas. Tik vienas pakartotinai naudojamas slaptažodis gali pradėti grandininę reakciją, kuri gali pakenkti visoms paskyroms (Terranovasecurity, 2024).

Slaptažodžio nutekėjimo apsisaugojimui dėl „Phishing“ ir socialinės inžinerijos veiksnių, visų pirma, labai svarbus yra interneto vartotojų mokymas ir švietimas, kad jie galėtų lengvai įvertinti sukčiavimo pranešimus ir atlikti tinkamus veiksmus. Netechniniai žmonės priešinasi mokymuisi, nes jiems trūksta sąmoningumo ir konservatyvaus mąstymo. Todėl praktika turėtų būti ginčytina.

Remiantis tyrimu, kai kurie mokslininkai sutiko, kad vartotojų švietimas yra naudingas. Šiais laikais žmonės neturi daug laiko skaityti straipsnių ar nuorodų apie tai, kaip apsisaugoti nuo sukčiavimo atakų, todėl, kad tai būtų suprantamiau, galima paskatinti vartotojų susidomėjimą, pavyzdžiui, vaizdo įrašo dėka, trumpu filmu ar reklama arba net įvairiomis žiniasklaidos priemonėmis (Gautam, Sharma, Kumar, 2021).

1.3. Rizikos vertinimas ISO-27001 kontekste

1.3.1. ISO-27001 standartų apžvalga

Bėgant laikui ISS standartai ir sistemos vaidino pagrindinį vaidmenį skleidžiant šiandien labai reikalingus holistinius – techninius, organizacinius ir valdymo metodus. Tarp jų ISO/IEC 27001 yra labiausiai žinomas ir yra trečias pagal paplitimą ISO sertifikatas visame pasaulyje (Culot, Podrecca, Nassimbeni, Sartor, 2021). Šiandien akademinė bendruomenė ISO/IEC 27001 standartą vis dar traktuoja kaip lyderiaujančią techninę temą. Nors, anot autorių Culot G., Podrecca M., Nassimbeni G. ir Sartor M. (2021), reikia peržiūrėti ir atnaujinti visą ISO-27001 dėl sparčiai keičiamo ir labiau susieto pasaulio bei dėl atsirandančių technologinių galimybių ir su tuo susijusius iššūkius, šiandien geresnės alternatyvos nėra, todėl tokių standartų analizė yra itin svarbi slaptažodžių nutekėjimo kontekste.

Nepaisant to, ISO 27001 yra visame pasaulyje pripažintas informacijos saugos valdymo standartas, suteikiantis sistemingą požiūrį į jautrios įmonės informacijos valdymą, siekiant užtikrinti, kad ji išliktų saugi. Šis standartas ypač svarbus Fintech įmonėms, nes jos tvarko didelius jautrių finansinių duomenų kiekius. Atitiktis su ISO 27001 ne tik padidina duomenų saugumą, bet ir sustiprina atitiktį įvairiems pasauliniams finansiniams reglamentams (Edwards, 2024).

Oficialioje ISO 27001 dokumentacijoje yra pateikiama 14 pagrindinių punktų, kurie yra svarbūs kiekvienos organizacijos saugumo kontekste ir kurių būtina laikytis, norint užtikrinti saugų procesą bei virtualią aplinką:
A.5 INFORMACIJOS SAUGUMO POLITIKA;
A.6 INFORMACIJOS SAUGUMO ORGANIZAVIMAS;
A.7 ŽMOGIŠKŲJŲ IŠTEKLIŲ SAUGUMAS;

A.8 TURTO VALDYMAS;
A.9 PRIEIGOS KONTROLĖ;
A.10 KRIPTOGRAFIJA;
A.11 FIZINĖ IR APLINKOS SAUGA;
A.12 OPERACIJŲ SAUGUMAS;
A.13 TINKLO SAUGA;
A.14 SISTEMOS ĮSIGIJIMAS, KŪRIMAS IR PRIEŽIŪRA;
A.15 SANTYKIAI SU TIEKĖJAIS;
A.16 INFORMACIJOS SAUGUMO INCIDENTŲ VALDYMAS;
A.17 INFORMACIJOS SAUGUMO ASPEKTAI VERSLO PERSPEKTYVOJE;
A.18 ATITIKTIS;

1.3.2. ISO-27001 pritaikomumas slaptažodžio nutekėjimo atvejui

Nors ISO-27001 punktai fokusuojasi į Fintech organizacijų veiklą, kai kurių iš jų pritaikymas asmeniniams vartotojams taip pat įmanomas analizuojamajame kontekste. Tam svarbu apžvelgti kiekvieną standartą ir susieti juos su slaptažodžio nutekėjimo grėsmėmis, kurios būtų aktualios privatiems interneto vartotojams.

A.5 INFORMACIJOS SAUGUMO POLITIKA – A.5.1 Informacijos saugumo valdymo kryptis. Tikslas – teikti valdymo kryptį ir paramą informacijos saugumui pagal verslo reikalavimus ir atitinkamus įstatymus bei reglamentus (ISO 27001). Šis standartas neturi aktualumo darbo analizės kontekste, kadangi nėra sąsajos tarp verslo reikalavimų ir įstatymų bei privačių interneto vartotojų veiksmų.

A.6 INFORMACIJOS SAUGUMO ORGANIZAVIMAS – A.6.1 Vidinė organizacija. Tikslas – sukurti valdymo sistemą, kuri inicijuotų ir kontroliuotų informacijos saugumo įgyvendinimą ir veikimą organizacijoje. A.6.2 Mobilieji įrenginiai ir nuotolinis darbas. Tikslas – užtikrinti nuotolinio darbo ir mobiliųjų įrenginių naudojimo saugumą (ISO 27001). Kitaip nei pirmuoju atveju, ši kategorija įgauna aktualumą, kadangi papildomos saugumo priemonės, kad būtų galima valdyti mobiliųjų įrenginių keliamą riziką bei bendrai turėti saugumo planą ir veikimą yra

svarbu ypač dėl to, kad tiek slaptažodžių vagystė, tiek “Phishing” ir Soc. Inžinerijos atakos siekiant nulaužti slaptažodį dažniausiai yra vykdomos per kompiuterinius įrenginius.

A.7 ŽMOGIŠKŲJŲ IŠTEKLIŲ SAUGUMAS – A.7.1 Prieš įsidarbinant. Tikslas – užtikrinti, kad darbuotojai suprastų savo pareigas ir būtų tinkami pareigoms, kurioms jie yra skirti. A.7.2 Darbo metu. Tikslas – užtikrinti, kad darbuotojai žinotų ir vykdytų savo įsipareigojimus informacijos saugumui. A.7.3 Darbo sutarties nutraukimas ir pakeitimas. Tikslas – apsaugoti organizacijos interesus keičiant ar nutraukiant darbo santykius (ISO 27001). Apžvelgiant pastarąjį standartą galima teigti, kad bendroji idėjos esmė – suprasti savo veiksmus, žinoti bei saugoti savo interesus yra labai svarbus aspektas kiekvienam privačiam interneto vartotojui saugantis nuo slaptažodžio nutekėjimo grėsmės.

A.8 TURTO VALDYMAS – A.8.1 Atsakomybė už turtą. Tikslas – nustatyti organizacijos turtą ir apibrėžti atitinkamas apsaugos pareigas. A.8.2 Informacijos klasifikavimas. Tikslas – užtikrinti, kad informacija būtų tinkamai apsaugota, atsižvelgiant į jos svarbą organizacijai. A.8.3 Socialinių tinklų tvarkymas tikslas – užkirsti kelią neteisėtam socialinėse medijose saugomos informacijos atskleidimui, keitimui, pašalinimui ar sunaikinimui (ISO 27001). Lygiai taip pat kaip organizacija, privatūs interneto vartotojai privalo užtikrinti savo prietaisų (turto) saugumą, taip pat neskleisti jautrios bei su prisijungimais susijusios informacijos socialinėse medijose.

A.9 PRIEIGOS KONTROLĖ – A.9.1 Verslo reikalavimai prieigos kontrolei. Tikslas – apriboti prieigą prie informacijos ir informacijos apdorojimo priemonių. A.9.2 Vartotojo prieigos valdymas. Tikslas – užtikrinti autorizuotą vartotojo prieigą ir užkirsti kelią neteisėtai prieigai prie sistemų ir paslaugų. A.9.3 Vartotojo pareigos. Tikslas – užkirsti kelią neteisėtai prieigai prie sistemų ir programų (ISO 27001). Šis standartas pabrėžia didelę svarbą užtikrinti darbo vietos saugumą ir neleisti kitiems neteisėtai prisijungti prie privataus interneto vartotojo paskyros.

A.10 KRIPTOGRAFIJA – A.10.1 Kriptografinės kontrolės. Tikslas – užtikrinti tinkamą ir veiksmingą kriptografijos naudojimą, siekiant apsaugoti informacijos konfidencialumą, autentiškumą ir (arba) vientisumą (ISO 27001). Šiuo standartu organizacijos yra raginamos implementuoti kriptografijos/šifravimo metodikas savo darbo ribose, nors tai turi didelio aktualumo ir privataus interneto vartotojo atveju, tai gali būti sudėtinga ir brangu įgyvendinti.

A.11 FIZINĖ IR APLINKOS SAUGA – A.11.1 Saugi aplinka. Tikslas – užkirsti kelią neteisėtai fizinei prieigai, žalai ir trukdymui organizacijos informacijai ir informacijos apdorojimo priemonėms. A.11.2 Įranga. Tikslas – užkirsti kelią turto praradimui, sugadinimui, vagystei ar sugadinimui ir organizacijos veiklos sutrikimams (ISO 27001). Panašiai kaip ir 8 punktas, šis standartas taip pat turi didelės svarbos – užtikrinti fizinę saugią vartotojo aplinką.

A.12 OPERACIJŲ SAUGUMAS – A.12.1 Veiklos procedūros ir atsakomybė. Tikslas – užtikrinti teisingą ir saugią informacijos apdorojimo įrenginių veiklą. A.12.2 Apsauga nuo kenkėjiškų programų. Tikslas – užtikrinti, kad informacija ir informacijos apdorojimo įrenginiai būtų apsaugoti nuo kenkėjiškų programų. A.12.3 Atsarginė kopija. Tikslas – apsaugoti nuo duomenų praradimo. A.12.4 Stebėjimo įranga. Tikslas – fiksuoti įvykius ir generuoti įrašus. A.12.5 Operacinės programinės įrangos valdymas. Tikslas – užtikrinti veikiančių sistemų vientisumą. A.12.6 Techninio pažeidžiamumo valdymas. Tikslas – užkirsti kelią techninių spragų išnaudojimui. A.12.7 Informacinių sistemų audito svarstymai. Tikslas – sumažinti audito veiklos poveikį veikiančioms sistemoms (ISO 27001). Kalbant apie šį ISO-27001 standartą, galima teigti, jog jis dalinai tinkamas privačių interneto vartotojų atvejui, kadangi užtikrinti saugią įrenginių veiklą, turėti apsaugą nuo kenkėjiškų programų (antivirusinė) bei atsarginę kopiją – labai svarbus žingsnis. Kita vertus, įsidiegti stebėjimo sistemas yra brangu ir nevisiškai aktualu, kadangi privačių interneto vartotojų veikla neprilygsta organizacijos dydžio procesams. Audito klausimas taip pat praranda aktualumą.

A.13 TINKLO SAUGA – A.13.1 Tinklo saugumo valdymas. Tikslas – užtikrinti informacijos apsaugą tinkluose ir pagalbinėse informacijos apdorojimo priemonėse. A.13.2 Informacijos perdavimas. Tikslas – palaikyti organizacijos viduje ir su bet kokiais išoriniais subjektais perduodamos informacijos saugumą (ISO 27001). Tinklo saugumas yra vienas iš svarbiausių klausimų kalbant apie duomenų (slaptažodžio) saugojimą.

A.14 SISTEMOS ĮSIGIJIMAS, KŪRIMAS IR PRIEŽIŪRA – A.14.1 Informacinių sistemų saugumo reikalavimai. Tikslas – užtikrinti, kad informacijos saugumas būtų neatsiejama informacinių sistemų dalis per visą gyvavimo ciklą. Tai taip pat apima reikalavimus informacinėms sistemoms, kurios teikia paslaugas viešaisiais tinklais. A.14.2 Saugumas plėtros ir palaikymo procesuose. Tikslas – užtikrinti, kad informacijos saugumas būtų sukurtas ir įgyvendintas informacinių sistemų kūrimo ciklo metu. A.14.3 Bandymo duomenys. Tikslas – užtikrinti testavimui

naudojamų duomenų apsaugą (ISO 27001). Šis standartas taip pat kaip ir 12, neturi pakankamo aktualumo dėl per didelio įgyvendinimo kaštų.

A.15 SANTYKIAI SU TIEKĖJAIS – A.15.1 Informacijos saugumo politika tiekėjų santykiams. Tikslas – užtikrinti tiekėjams prieinamo organizacijos turto apsaugą. A.15.2 Tiekėjo paslaugų teikimo valdymas. Tikslas – išlaikyti sutartą informacijos saugumo ir paslaugų teikimo lygį pagal tiekėjų sutartis (ISO 27001). Tiekėjų klausimas taip pat nėra aktualus privačių interneto vartotojų perspektyvoje.

A.16 INFORMACIJOS SAUGUMO INCIDENTO VALDYMAS – A.16.1 Informacijos saugumo incidentų valdymas ir komunikacijos apie saugumo įvykius ir trūkumus tobulinimas. Tikslas – užtikrinti nuoseklų ir veiksmingą požiūrį į informacijos saugumo incidentų valdymą, įskaitant komunikaciją apie saugumo įvykius ir trūkumus (ISO 27001). Šis aspektas svarbus iš to požiūrio taško, kad informacijos dokumentavimas gali būti naudingas siekiant perduoti informaciją kitiems šeimos nariams bei, žinoma, prisiminti pačiam vartotojui. Tačiau tai yra taip pat rizika.

A.17 INFORMACIJOS SAUGUMO ASPEKTAI VERSLO PERSPEKTYVOJE – A.17.1 Informacijos saugumo tęstinumas. Tikslas – informacijos saugumo tęstinumas turi būti įtrauktas į organizacijos veiklos tęstinumo valdymo sistemas (ISO 27001). Šis punktas neturi aktualumo, kadangi verslo klausimas yra mažai susijęs su privačių interneto vartotojų veiklomis.

A.18 ATITIKTIS – A.18.1 Teisinių ir sutartinių reikalavimų laikymasis. Tikslas – išvengti teisinių, įstatyminių, reguliavimo ar sutartinių įsipareigojimų, susijusių su informacijos saugumu, ir bet kokių saugumo reikalavimų pažeidimų. A.18.2 Informacijos saugumo apžvalgos. Tikslas – užtikrinti, kad informacijos saugumas būtų įgyvendintas ir eksploatuojamas pagal organizacijos politiką ir procedūras (ISO 27001). Paskutinis ISO-27001 standartas turėtų būti paminėtas, kadangi interneto erdvėje privatūs vartotojai taip pat gali pažeisti įstatymą, todėl svarbu laikytis teisinių reikalavimų bei užtikrinti, kad dalijimasis informacija yra legalus.

Apibendrinant galima teigti, kad ISO-27001 standartų aktualumas išlieka, kadangi pateikiama informacija ir patarimai yra kibernetinio saugumo pagrindai, kurių svarbu laikytis tiek organizacijoms, tiek privatiems interneto vartotojams, siekiant sumažinti kibernetinės žalos riziką esant slaptažodžio nutekėjimui.

2. SLAPTAŽODŽIO NUTEKĖJIMO RIZIKOS VERTINIMO METODAS

2.1. Egzistuojančio rizikos vertinimo metodo analizė

Plačiau žvelgiant į šiandien egzistuojančias slaptažodžio nutekėjimo rizikos vertinimo metodikas, galima išskirti tam tikrus svarius trūkumus. Visų pirma, tiek Fintech sektoriuje, tiek bendrai rinkoje neegzistuoja rizikos metodas, kuris apimtų visus tris rizikos vertinimo etapus ir juos sujungtų: rizikos identifikavimą, rizikos skaičiavimą bei rizikos mažinimą. Ankstesniame skyriuje minėti įrankiai „NordPass“, „Haveibeenpwned.com“ arba „Security.org“ apsiriboja pačio slaptažodžio stiprumo įvertinimu, neatsižvelgiant tokius kintamuosius, kaip, pavyzdžiui pakartotinis slaptažodžio naudojimas kitose platformose, slaptažodžių tvarkyklės, 2FA naudojimas, slaptažodžio keitimo praktika, bendros slaptažodžio saugumo žinios bei kiti socialinės inžinerijos aspektai. Šie įrankiai taip pat nepateikia rekomendacijų rizikos mažinimui, o kitos egzistuojančios rekomendacijos nebūtinai atitinka vartotojo situaciją ir yra labai bendro pobūdžio. Iš to iškyla abejotinas egzistuojančio metodo patikimumas, kadangi dėl nepakankamo konteksto slaptažodžiui vertinti, ganėtinai abstrakčios grįžtamosios informacijos interneto vartotojams gali atsirasti pernelyg didelis pasitikėjimas, kuris paskatins papildomai nesirūpinti slaptažodžio saugumu.

Tokių slaptažodžio stiprumo skaičiavimo (rizikos skaičiavimo) įrankių tikslumo analizę atliko autoriai Wang D., Shan, X., Dong, Q., Shen, Y., Jia, C. (2023) „No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters“. Buvo pastebėta, kad esami slaptažodžių stiprumo vertinimo įrankiai turi didelių neatitikimų įvairiuose scenarijuose, todėl sunku visuotinai įvertinti jų tikslumą. Pagrindinė problema – lankstumo nebuvimas: skirtingiems scenarijams reikalingi skirtingi vertinimo kriterijai, o šiandien egzistuojantys įrankiai tam nėra visiškai pritaikyti. Apibendrinant galima teigti, jog šiandien matomas aiškus nuoseklios rizikos vertinimo sistematikos nebuvimas, kuomet kiekvienas rizikos vertinimo etapas nėra sujungtas į vieną dedamąją, o egzistuojančios metodikos apsiriboja savo siaurumu bei konteksto trūkumu, todėl gali būti laikomos tik kaip pagalbinės priemonės. Atsižvelgiant į tai, yra būtina sukurti naują, išsamų struktūrizuotą metodą, kuris paskatintų vartotojus laikytis svarbiausių slaptažodžio saugumo praktikų.

2.2.Siūlomas rizikos vertinimo metodas

Formuojant naująjį plataus mąsto metodą, buvo atsižvelgta į keletą svarbių faktorių. Pirmiausiai, rizikos identifikavimas atliekamas suformuojant detalų klausimyną, siekiant padėti vartotojui identifikuoti pagrindines spragas ir trūkumus slaptažodžių valdymo kontekste. Rizikos identifikavimo klausimai ir jų svorių pasirinkimas yra pagrindžiamas moksline literatūra ir statistiniais duomenimis.

RIZIKOS IDENTIFIKAVIMAS:

Slaptažodžių stiprumas

1. Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?
2. Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?
3. Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?
4. Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?
5. Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. How Secure is My Password arba Pentester.com)?
6. Ar savo slaptažodžius keičiate rečiau nei kartą per metus?

Pakartotinis slaptažodžių naudojimas

7. Ar naudojate tą patį slaptažodį skirtingose paskyrose?
8. Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?
9. Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?

Remiantis „Verizon Data Breach Investigations Report“ (VDIR, 2022), daugiau nei 80 % atakų sukelia silpni arba pakartotinai naudojami slaptažodžiai. Kitaip tariant, keturi iš penkių pažeidimų iš dalies siejami su silpnų, pakartojamų ar pavogtų slaptažodžių naudojimu (Anuj, 2024). Remiantis Google Online Security Survey 2019 bei Sean Blanton 2024 statistiniu straipsniu, galima matyti, jog

pakartotinis slaptažodžių naudojimo įprotis tarp interneto vartotojų išlieka aktualus. Teigiama, kad 60 % asmenų pakartotinai naudoja slaptažodžius keliose svetainėse. Silpni slaptažodžiai yra nemažiau aktualus veiksnys. Tuo tarpu „Keeper Security“ atliktas pasaulinis tyrimas atskleidė, kad 75 % vartotojų nesivadovauja ekspertų patarimais ir toliau naudoja silpnus slaptažodžius. (Mercado, Varela, 2024). 70 % silpnų slaptažodžių galima nulaužti greičiau nei per 1 sekundę, naudojant paprastas brutalios jėgos atakas (Blanton, 2024), o atsižvelgiant į tai, kad per pastaruosius kelis metus buvo nulaužta daugiau nei 24 milijardai slaptažodžių, tai yra labai svarus ir dėmesio reikalaujantis elementas (Stouffer, 2023).

"NordPass" bei "NordStellar" atliktas 2022 metų tyrimas „Top 200 Populiariausi Slaptažodžiai“, kuriame buvo išanalizuota 2,5 B duomenų bazės, surinkta iš įvairių viešai prieinamų šaltinių, įskaitant tamsiojo interneto šaltinius, kurio metu analizuojant kenkėjiškos programinės įrangos pavogtus slaptažodžius arba duomenų nutekėjimo metu atskleistus slaptažodžius, buvo pastebėta, kad populiariausi nutekinti slaptažodžiai yra labai tipiško pobūdžio su nuspėjamaisiais kintamaisiais, be specialiųjų simbolių ir esantys trumpo ilgio. Lietuvos atveju, populiariausi slaptažodžiai išlieka:

Populiariausi slaptažodžiai Lietuvoje Lentelė 1

Reitingas	**Slaptažodis**	**Laikas iki nulaužimo**	**Panaudojimo skaičius**
1	qwerty123	<1 sekundę	1408
2	qwerty1	<1 sekundę	1234
3	123456	<1 sekundę	1087
4	123456789	<1 sekundę	810
5	lopas123	17 minučių	513

Šaltinis: „NordPass“

Iš to peršasi išvada, kad „Slaptažodžių stiprumas“ kategorija išlieka antras pagal rizikingumą veiksnys, prisidedantis prie slaptažodžių nutekėjimo grėsmės, o „Pakartotinis slaptažodžių naudojimas“ statistiškai užima trečiąją vietą.

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas

10. Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?
11. Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?
12. Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?

Įgyvendinant gerą saugumo praktiką, pvz., naudojant antrojo veiksnio autentifikavimą (2FA/MFA) prisijungiant ir reikalaujant modernių autentifikavimo protokolų, galima užkirsti kelią daugeliui slaptažodžių nutekėjimo atakų. Remiantis „Microsoft Security“ 2024 metų tyrimu bei pateikta ataskaita, teigiama, kad 99,9 % pažeistų ir nutekintų paskyrų neturi 2FA/MFA, todėl jos yra lengviausiai pažeidžiamos dėl slaptažodžių vagystės, soc. inžinerijos ir fišingo sukčiavimų bei pakartotinio slaptažodžio naudojimo (Microsoft, 2024).

Kita vertus, nors 2FA/MFA aktualumas ir patikimumas yra statistiškai pagrįstas, tai nėra privačių interneto vartotojų prioritetas. Remiantis „Google“ 2023 metais atlikta apklausa, maždaug tik 45% interneto vartotojų yra įjungę 2FA bent vienoje savo paskyroje. Tai rodo ženklų padidėjimą nuo 33 % 2017 m. Žvelgiant plačiau, 55 % technologijų išmanančių vartotojų savo paskyrose įgalino 2FA. Tarp amžiaus grupių didžiausias 2FA vartojimo procentas yra 25–35 metų amžiaus grupėje – 48 % (Elad, 2023).

Be to, papildomas saugumo naudojimas Fintech sektoriuje taip pat įgauna aktualumo.
Šifruota blokų grandinė, dviejų ir trijų faktorių autentifikavimas buvo plačiai priimtas – Finansų technologijų industrijos bando supaprastinti sandorių procesą, pašalinant potencialiai nesaugius procesus visoms dalyvaujančioms šalims. Geriausias pavyzdys yra mobilioji paslauga, pvz., „Venmo“ arba „CashApp“, leidžianti vartotojams mokėti vieni kitiems 24 valandas per parą, iš karto siunčiant grynuosius pinigus į pageidaujamą banko sąskaitą. ES Mokėjimo paslaugų direktyva

(PSD2) taip pat nustato griežtus tikrinimo reikalavimus taikant procesą, vadinamą „stipriu klientų autentifikavimu“ (SCA), siekiant dar labiau kovoti su sukčiavimu internete (Bateman 2024). Atsižvelgiant į tai, „Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas“ kategorija buvo pasirinkta kaip antra pagal reikšmingumą kuriamo metodo klausimyne.

Socialinės inžinerijos ir fišingo rizika

13. Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?
14. Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?
15. Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?

Slaptažodžių nutekėjimai dėl socialinės inžinerijos (fišingo) atakų, statistiškai žvelgiant, išlieka žemiau už dviejų veiksnių autentikacijos bei slaptažodžių stiprumo bei pakartotinio naudojimo veiksnius, tačiau taip pat išlieka svarbūs. Remiantis Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos (NKSC), dažniausiai Lietuvoje pasitaikančius kibernetinių incidentų tipus, viena pirmaujančių kategorijų nesikeičia jau kelerius metus iš eilės – tai socialinės inžinerijos metodai, bandant įvairiais būdais iš žmonių išvilioti prisijungimus prie jų elektroninių paskyrų ar kitus jautrius duomenis. 2023 metų pirmą pusmetį buvo fiksuota 265 tokio tipo atvejų ir tai sudarė beveik trečdalį (31 proc.) visų per pirmus šešis metų mėnesius fiksuotų kibernetinių incidentų. Tuo tarpu 2022 metais NKSC CERT-LT iš viso užregistravo 4 080 kibernetinių incidentų. Daugiausiai incidentų, kaip ir prieš metus, buvo susiję su kenkimo programinės įrangos platinimu (1795), socialinės inžinerijos atakomis, kuriomis siekta išvilioti įvairius jautrius duomenis (ang. Phishing) (1005), nepageidaujamų laiškų ir klaidinančios informacijos platinimu (524). Taigi galima teigti, jog soc. inžinerijos tipo atakos siekiant išvilioti/nutekinti slaptažodžius procentiškai yra mažesnioji dalis ir nepersveria pirmų dviejų kategorijų veiksnių.

Pereinant prie antrojo metodo etapo – rizikos skaičiavimo, pirmiausia suskaičiuojami keturių kategorijų rizikos svorių matmenys, remiantis statistiniais duomenimis. Kiekvienos kategorijos procentinės vertės svorio įvertinimui naudojama teorinėje dalyje pristatyta rizikos skaičiavimo formulė: Rizikos balas = (tikimybė) × (poveikis)

RIZIKOS SKAIČIAVIMAS:

Slaptažodžių stiprumas

Tikimybė = 0.75, remiantis Keeper Security 2024 pasauliniu tyrimu, kad 75 % vartotojų nesivadovauja ekspertų patarimais ir toliau naudoja silpnus slaptažodžius.

Poveikis = 0.80, remiantis VDIR 2022, kad 80 % atakų sukelia silpni arba pakartotinai naudojami slaptažodžiai.

Slaptažodžio stiprumo rizika = 0.75 * 0.80 = 0.6

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas

Tikimybė = 0.55, remiantis Google Survey 2023 statistika, kad tik 45% vartotojų naudoja dviejų veiksnių autentifikavimą, tuomet tikimybė kad vartotojai nenaudoja 2FA yra 55%.

Poveikis = 0.99, Microsoft Security 2024 ataskaita, kad 99% slaptažodžio pažeidimų įvyksta neturint 2FA autentifikacijos.

Antrojo veiksnio autentifikacijos (2FA/MFA) rizika = 0.55 * 0.99 = 0.5445

Pakartotinis slaptažodžių naudojimas

Tikimybė = 0.60, remiantis Sean Blanton 2024, kad 60 % asmenų pakartotinai naudoja slaptažodžius keliose svetainėse.

Poveikis = 0.80, remiantis VDIR 2022, kad 80 % atakų sukelia silpni arba pakartotinai naudojami slaptažodžiai.

Pakartotinis slaptažodžių naudojimas rizika = 0.60 * 0.80 = 0.48

Socialinės inžinerijos ir fišingo rizika

Tikimybė = 0.31, remiantis NKSC 2023, kad 31% visų atakų yra socialinės inžinerijos pobūdžio atakos.

Poveikis = 0.70, remiantis tuo, kad socialinės inžinerijos atakos padariniai, kai ataka sėkminga, garantuoja slaptažodžio nutekėjimą. Kita vertus, šiam rodikliui trūksta apibrėžtumo, kadangi socialinės inžinerijos atakų sėkmė priklauso nuo žmogaus veiksmų (Bluebridge, 2019), ji nėra tokia automatiška kaip silpnų, pakartotinų slaptažodžių ar 2FA trūkumo atveju.

Socialinės inžinerijos ir fišingo rizika = 0.31 * 0.70 = 0.217

Matematinis rizikos svorių kiekvienai kategorijai priskyrimas:

Bendras rizikos rodiklis = 0.5445 + 0.6 + 0.48 + 0.217 = 1.8415

Slaptažodžio stiprumo svoris = 0.6 / 1.8415 = 0.3258213 = 32.58%

Antrojo veiksnio autentifikacijos (2FA/MFA) svoris = 0.5445 / 1.8415 = 0.295683 = 29.57%

Pakartotinio slaptažodžių naudojimo svoris = 0.48 / 1.8415 = 0.260657 = 26.07%

Socialinės inžinerijos ir fišingo svoris = 0.217 / 1.8415 = 0.1178387 = 11.78%

Siekiant suskaičiuoti slaptažodžio nutekėjimo riziką pagal vartotojo pateiktus atsakymus klausimyne tam tikroje kategorijoje, visų riziką keliančių atsakymų suma padalinama iš visų klausimų skaičiaus kategorijoje :

Tikimybė (kategorijoje) = Suma riziką keliančių atsakymų / Klausimų skaičius kategorijoje

Galutinė slaptažodžio nutekėjimo rizika apskaičiuojama sudauginus kategorijos svorius su rizikos skaičiavimo pagal kategoriją kintamaisiais:

Galutinė rizika = sum(Kategorijos svoris * Tikimybė kategorijoje)

RIZIKOS MAŽINIMAS:

Implementuojant rizikos mažinimo etapą kuriamajame metode, yra siekiama vartotojui pateikti slaptažodžio nutekėjimo rizikos mažinimo rekomendacijas, priklausomai nuo vartotojų atsakymų į klausimus. Rizikos mažinimo veiksniai ir patarimai bus pateikiami remiantis tuo, kuri rizikos vertinimo kategorija yra „silpniausia“ bei koks bendras vartotojo rizikos balas. Galutiniame žingsnyje GUI grafinės sąsajos pagalba siekiama pateikti vartotojui langa su informacinio pobūdžio tekstu:

„Jūsų slaptažodžio nutekėjimo rizika yra [procentinė vertė]. Silpniausia vieta [kategorija].
Rekomenduojama laikytis žemiau pateiktų rekomendacijų:
[patarimai]“

Slaptažodžių stiprumas

1. Ar jūsų slaptažodis trumpesnis nei 12 simbolių?
   → *Naudokite ilgesnius, bent 12–16 simbolių slaptažodžius.*
2. Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?
   → *Venkite lengvai atspėjamų ar populiarių žodžių bei frazių. Naudokite slaptažodžių tvarkyklę.*
3. Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?
   → *Naudokite specialių simbolių, skaičių, didžiųjų ir mažųjų raidžių kombinacijas.*
4. Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?
   → *Niekada nesidalinkite slaptažodžiais su kitais asmenimis.*
5. Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. How Secure is My Password arba Pentester.com)?
   → *Reguliariai, bent kartą per mėnesį tikrinkite slaptažodžių nutekėjimo incidentų duomenis.*
6. Ar savo slaptažodžius keičiate rečiau nei kartą per metus?
   → *Keiskite slaptažodžius bent kartą į metus arba dažniau.*

Pakartotinis slaptažodžių naudojimas

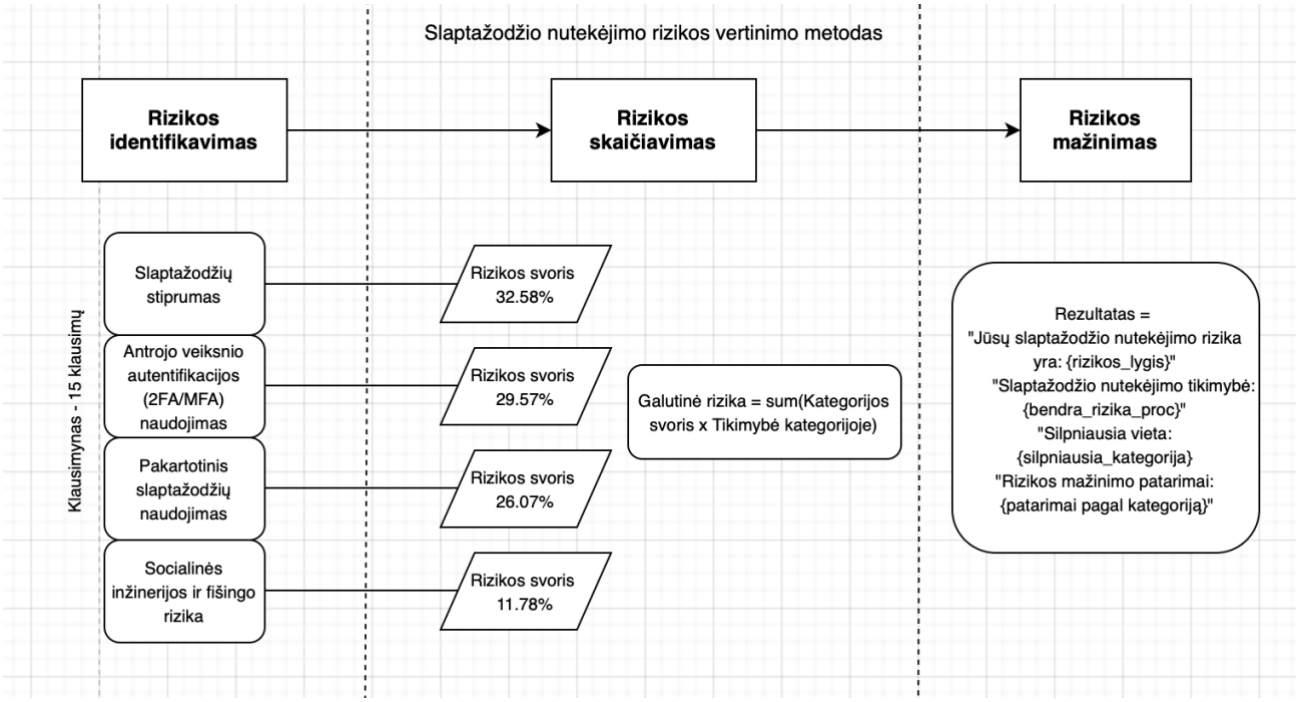
7. Ar naudojate tą patį slaptažodį skirtingose paskyrose?
   → *Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę.*
8. Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?
   → *Finansinėms paskyroms naudokite stiprius ir unikalius slaptažodžius, kad jie būtų nepriklausomi nuo kitų paskyrų.*
9. Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?
   → *Venkite viešai saugoti savo slaptažodžius.*

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas

10. Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?
    → *Naudokite 2FA visose paskyrose, naudojant autentifikacijos programėles (pvz. „Google Authenticator“).*
11. Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?
    → *Įsitikinkite, kad visos svarbiausios paskyros naudoja 2FA autentikaciją, pvz. autentifikacijos programėles arba SMS kodus.*
12. Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz. SMS, biometriniai duomenys ir kita?
    → *Nevenkite naudoti skirtingų 2FA metodų.*

Socialinės inžinerijos ir fišingo rizika

13. Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?
    → *Prieš spustelėdami nuorodą, patikrinkite jos URL, išanalizuokite situaciją bei įsitikinkite, jog siuntėjas yra teisėtas. Naudokite naršyklės plėtinius, skirtus fišingo prevencijai.*
14. Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?
    → *Niekada nesidalinkite slaptažodžiais telefonu ar el. paštu. Oficialios organizacijos tokios informacijos niekada neprašys.*
15. Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos riziką ir fišingą?
    → *Dalyvaukite švietime apie kibernetinių atakų, soc.inžinerijos ir fišingo riziką.*



2 pav. Slaptažodžio nutekėjimo rizikos vertinimo metodas

Šaltinis: Sudaryta autoriaus

3. SLAPTAŽODŽIO NUTEKĖJIMO RIZIKOS VERTINIMO EKSPERIMENTAS

3.1. Rizikos vertinimo eksperimento paruošimas su „Python“

Siekiant implementuoti viso metodo pritaikomumą į kompiuterizuotą programą, buvo nuspręsta kurti ją dalimis:

- Kategorijų ir klausimų, svorių infrastruktūros kūrimas;
- Vizualaus Tkinter GUI programos dizaino kūrimas;
- Klausimų ir kategorijų praktinis atvaizdavimas;
- Rizikos matematinis skaičiavimas;
- Rezultatų atvaizdavimas;

Sekantis žingsnis apima svorio koeficientų pasirinkimą. Kaip buvo siūlomo sprendimo dalyje, svorių pasirinkimas buvo atliktas remiantis statistine analize. Tokiu būdu, kategorijų skirstymas yra:

Rizikos vertinimo kategorijų skirstymas Lentelė 2

Rizikos vertinimo kategorija	Svoris (procentine išraiška)
Slaptažodžių stiprumas	32.58%
Antrojo veiksnio autentifikacija (2FA/MFA)	29.57%
Pakartotinis slaptažodžių naudojimas	26.07%
Socialinės inžinerijos ir fišingo rizika	11.78%

Šaltinis: Sudaryta autoriaus

Toliau yra atliekamas rizikos skaičiavimas ir rezultatų interpretavimas pagal atsakytus klausimus. Programa eina ciklu (for) per kiekvieną rizikos kategoriją ir jos svorį. Jeigu atsakymas į klausimą yra neigiamas (keliantis riziką), tuomet 1 (vertė/skaičius) yra pridedamas prie suma_atsakymų tusčio sąrašo, kuris palaipsniui pildosi su neigiamais atsakymais. Tokiu būdu naudojant (if) klausimai yra išskirstomi, taip pat surenkamas bendras klausimų skaičius. Prie to paties yra apskaičiuojama „silpniausia vartotojo kategorija“ bei yra pridedami patarimai prie blogai atsakytų klausimų. Vėliau, remiantis pristatyta rizikos skaičiavimo formule, yra apskaičiuojama kiekvienos kategorijos rizika bei galutinė vartotojo riziką slaptažodžio nutekėjimui.

```
def nustatyti_rizikos_lygi(self, procentai):
    if procentai <= 20:
        return "Maža"
    elif 21 <= procentai <= 50:
        return "Vidutinė"
    else:
        return "Didelė"

def skaiciuoti_rizika(self):
    bendra_rizika = 0
    silpniausia_kategorija = None
    max_rizika = 0
    visi_patarimai = []

    for kategorija, svoris in svoriai.items():
        suma_atsakymų = 0
        klausimu_skaicius = len(klausimai[kategorija])
        patarimai_kategorijai = []

        for i, klausimas in enumerate(klausimai[kategorija]):
            atsakymas = self.atsakymai[kategorija][i].get()
            if klausimas["safe"]:
                suma_atsakymų += 1 - atsakymas
                if atsakymas == 0:
                    patarimai_kategorijai.append(klausimas["patarimas"])
            else:
                suma_atsakymų += atsakymas
                if atsakymas == 1:
                    patarimai_kategorijai.append(klausimas["patarimas"])

        tikimybe = suma_atsakymų / klausimu_skaicius
        kategorijos_rizika = svoris * tikimybe
        bendra_rizika += kategorijos_rizika

        if kategorijos_rizika > max_rizika:
            max_rizika = kategorijos_rizika
            silpniausia_kategorija = kategorija

        visi_patarimai.extend(patarimai_kategorijai)

    bendra_rizika_proc = bendra_rizika * 100
    rizikos_lygis = self.nustatyti_rizikos_lygi(bendra_rizika_proc)
```

3 pav. Rizikos skaičiavimo ir atsakymų tikrinimo kūrimas

Šaltinis: Sudaryta autoriaus

Galu gale, vartotojui pateikiamas rezultatas ir rizikos mažinimo etapas – procentinė slaptažodžio nutekėjimo rizika ir rizikos lygis, pagrindinė „silpniausia vieta“, į kurią svarbiausia atkreipti dėmesį bei visi riziką mažinantys veiksniais, remiantis neigiamai atsakytais klausimais. Savo ruožtu paskutinė if __name__ == “__main__”; dalis yra atsakinga už viso rizikos vertinimo metodo paleidimą, grafinės sąsajos lango sukūrimą, klasės objektų inicijavimą bei įvykių ciklo startą.

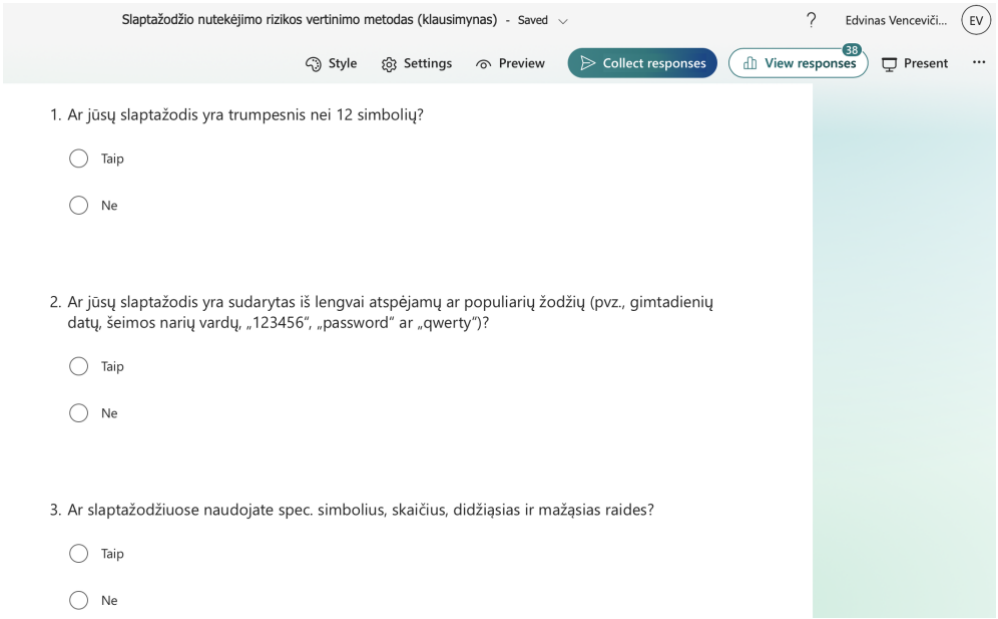
```
        rezultatas = f"Jūsų slaptažodžio nutekėjimo rizika yra: {rizikos_lygis}\n"
        rezultatas += f"Slaptažodžio nutekėjimo tikimybė: {bendra_rizika_proc:.2f}%\n\n"
        rezultatas += f"Silpniausia vieta: {silpniausia_kategorija}\n\nRizikos mažinimo patarimai:\n"
        rezultatas += "\n".join(f"- {patarimas}" for patarimas in visi_patarimai)

        messagebox.showinfo("Rezultatas", rezultatas)

if __name__ == "__main__":
    root = tk.Tk()
    app = RizikosVertinimas(root)
    root.mainloop()
```

4 pav. Galutinių rizikos vertinimo metodo rezultatų pateikimas

Šaltinis: Sudaryta autoriaus

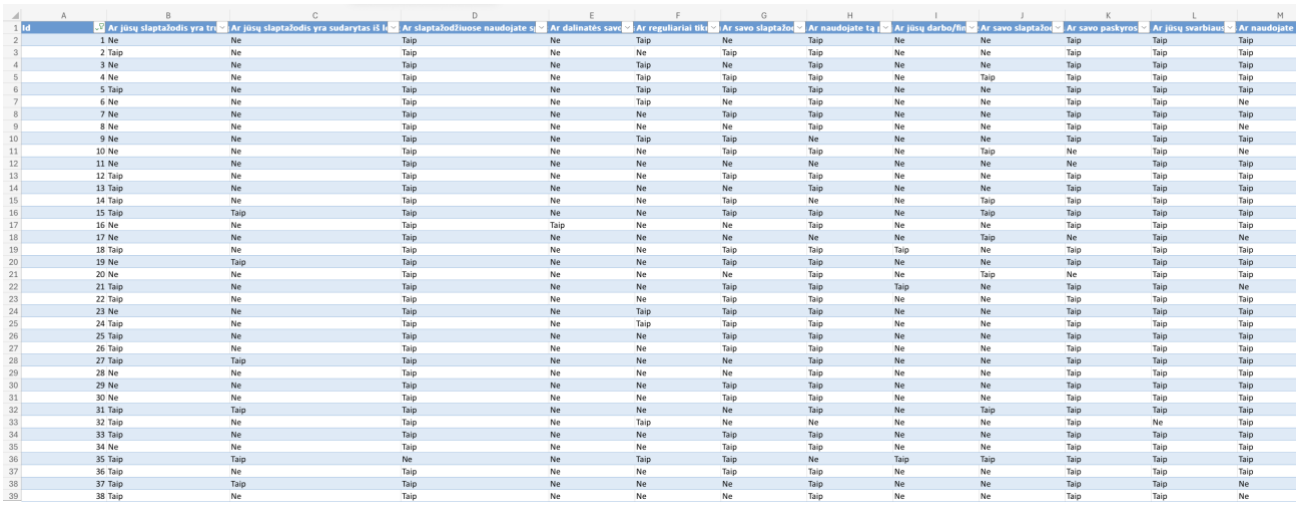
3.2. Duomenų rinkimas rizikos vertinimo eksperimentui

Siekiant atlikti sukurto rizikos vertinimo metodo eksperimentą su realiais duomenimis, buvo nuspręsta sukurti anoniminę Google Forms apklausą pagal privačių interneto vartotojų dviejų amžių grupes, tai yra vartotojai iki 25 metų bei 25–45 metų grupės vartotojai. Apklausoje buvo surašyti visi klausimai iš keturių jau žinomų slaptažodžio nutekėjimo grėsmių kategorijų: Slaptažodžių stiprumas, Antrojo veiksnio autentifikacija (2FA/MFA), Pakartotinis slaptažodžių naudojimas, Socialinė inžinerija ir Fišingas. Su šia apklausa buvo siekiama surinkti kuo daugiau atsakymų, siekiant plačiai ištestuoti metodą ir išanalizuoti kuo daugiau skirtingų rizikos scenarijų lygius ir bei atrasti dėsningumus tarp skirtingo amžiaus grupių, tokiu būdu įsitikinti metodo funkcionalumu ir pritaikomumu praktikoje. Iš viso buvo surinkta 55 vartotojų atsakymai, 38 iš jų priklauso pirmajam duomenų rinkiniui (iki 25 metų), o likę 17 priklauso antrajam duomenų rinkiniui (25–45 metų). Šių atvejų analizė bus atliekama Rizikos vertinimo eksperimento skyriuje.



5 pav. Apklausos rezultatų rinkimas su Google Forms

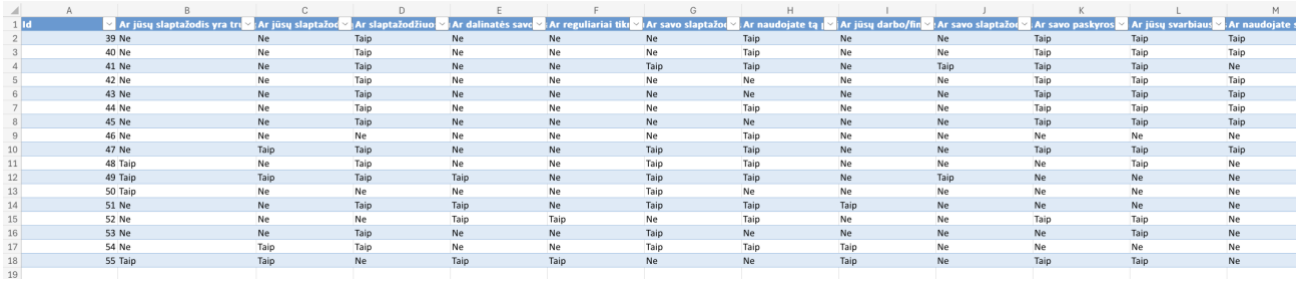
Šaltinis: Sudaryta autoriaus



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Id	Ar jūsų slaptažodis yra tr	Ar jūsų slaptažodis yra sudarytas iš l	Ar slaptažodžiuose naudojate s	Ar dalinatės savo	Ar reguliariai tik	Ar savo slaptažo	Ar naudojate tą	Ar jūsų darbo/fin	Ar savo slaptažo	Ar savo paskyros	Ar jūsų svarbiaus	Ar naudojate
2	1	Ne	Ne	Taip	Ne	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Taip
3	2	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
4	3	Ne	Ne	Taip	Ne	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Taip
5	4	Ne	Ne	Taip	Ne	Taip	Taip	Taip	Ne	Taip	Taip	Taip	Taip
6	5	Taip	Ne	Taip	Ne	Taip	Taip	Taip	Ne	Ne	Taip	Taip	Taip
7	6	Ne	Ne	Taip	Ne	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne
8	7	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
9	8	Ne	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne
10	9	Ne	Ne	Taip	Ne	Taip	Taip	Ne	Ne	Ne	Taip	Taip	Taip
11	10	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Taip	Ne	Taip	Ne
12	11	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne	Ne	Ne	Taip	Taip
13	12	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
14	13	Taip	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
15	14	Taip	Ne	Taip	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip	Taip
16	15	Taip	Taip	Taip	Ne	Ne	Taip	Taip	Ne	Taip	Taip	Taip	Taip
17	16	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
18	17	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne	Taip	Ne	Taip	Ne
19	18	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Taip	Ne	Taip	Taip	Taip
20	19	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
21	20	Ne	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Taip	Ne	Taip	Taip
22	21	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Taip	Ne	Taip	Taip	Ne
23	22	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
24	23	Ne	Ne	Taip	Ne	Taip	Taip	Taip	Ne	Ne	Taip	Taip	Taip
25	24	Taip	Ne	Taip	Ne	Taip	Taip	Taip	Ne	Ne	Taip	Taip	Taip
26	25	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
27	26	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
28	27	Taip	Taip	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
29	28	Ne	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
30	29	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
31	30	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
32	31	Taip	Taip	Taip	Ne	Ne	Ne	Taip	Ne	Taip	Taip	Taip	Taip
33	32	Taip	Ne	Taip	Ne	Taip	Ne	Ne	Ne	Ne	Taip	Ne	Taip
34	33	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
35	34	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
36	35	Taip	Taip	Ne	Ne	Taip	Taip	Ne	Taip	Taip	Taip	Taip	Taip
37	36	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
38	37	Taip	Taip	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne
39	38	Taip	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne

6 pav. Pirmojo duomenų rinkinio atsisiuntimas

Šaltinis: Sudaryta autoriaus



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Id	Ar jūsų slaptažodis yra tr	Ar jūsų slaptažoc	Ar slaptažodžiuo	Ar dalinatės savc	Ar reguliariai tik	Ar savo slaptažo	Ar naudojate tą	Ar jūsų darbo/fin	Ar savo slaptažo	Ar savo paskyros	Ar jūsų svarbiaus	Ar naudojate
2	39	Ne	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
3	40	Ne	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
4	41	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Taip	Taip	Taip	Ne
5	42	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne	Ne	Taip	Taip	Taip
6	43	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne	Ne	Taip	Taip	Taip
7	44	Ne	Ne	Taip	Ne	Ne	Ne	Taip	Ne	Ne	Taip	Taip	Taip
8	45	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne	Ne	Taip	Taip	Taip
9	46	Ne	Ne	Ne	Ne	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne
10	47	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip
11	48	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne	Ne	Ne	Taip	Ne
12	49	Taip	Taip	Taip	Taip	Ne	Taip	Taip	Ne	Taip	Ne	Ne	Ne
13	50	Taip	Ne	Ne	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Ne	Ne
14	51	Ne	Ne	Taip	Taip	Ne	Taip	Taip	Taip	Ne	Ne	Ne	Ne
15	52	Ne	Ne	Ne	Taip	Taip	Ne	Taip	Ne	Ne	Taip	Taip	Ne
16	53	Ne	Ne	Taip	Ne	Ne	Taip	Ne	Ne	Ne	Ne	Taip	Ne
17	54	Ne	Taip	Taip	Ne	Ne	Taip	Taip	Taip	Ne	Ne	Ne	Ne
18	55	Taip	Taip	Ne	Taip	Taip	Ne	Ne	Taip	Ne	Taip	Taip	Ne
19													

7 pav. Antrojo duomenų rinkinio atsisiuntimas

Šaltinis: Sudaryta autoriaus

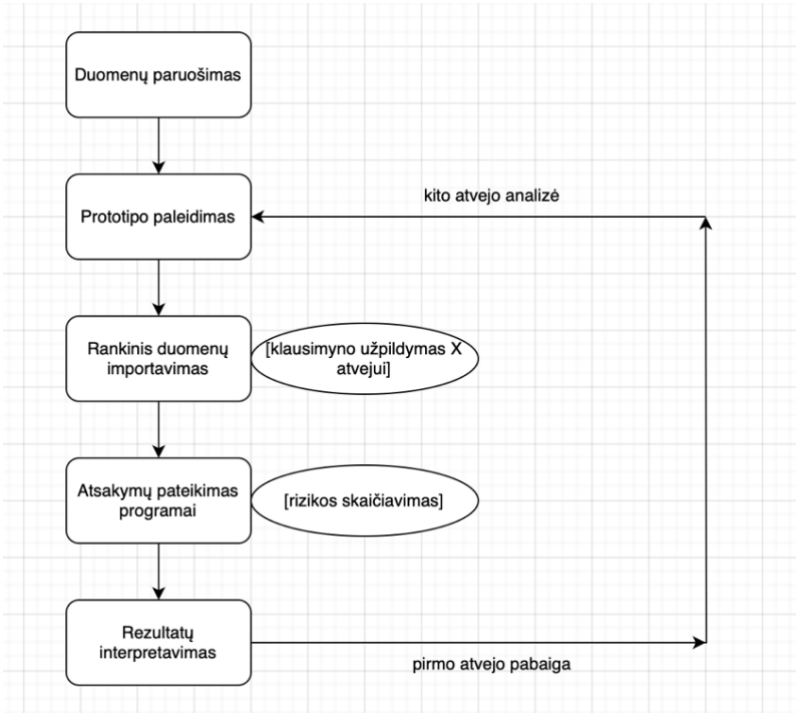
Klausimas	Atsakymas
Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?	Ne
Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?	Ne
Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?	Taip
Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?	Ne
Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?	Taip
Ar savo slaptažodžius keičiate rečiau nei kartą per metus?	Ne
Ar naudojate tą patį slaptažodį skirtingose paskyrose?	Taip
Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?	Ne
Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?	Ne
Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?	Taip
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?	Taip
Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?	Taip
Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?	Taip
Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?	Ne
Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?	Taip

8 pav. Apklausos duomenų atvaizdavimas su “Python” pagal vartotojo ID

Šaltinis: Sudaryta autoriaus

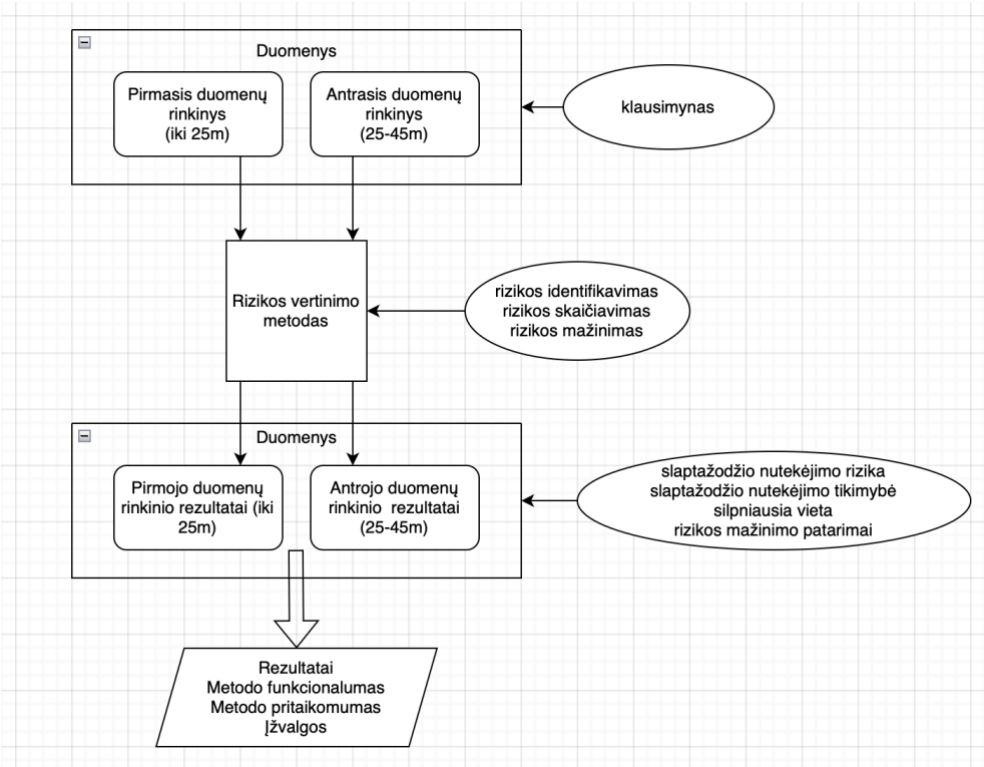
3.3. Rizikos vertinimo eksperimento eiga

Eksperimento atlikimui buvo nuspręsta laikytis toliau pateikto plano: Pirmiausia, kaip buvo minėta praeitame skyriuje, surinktų dviejų duomenų rinkiniai buvo vizualiai “išvalyti”, ištrinant nereikalingus stulpelius arba eilutes, siekiant palengvinti tolimesnio duomenų “importavimo” (atsakymų pateikimo metodui) žingsnį. Galutinai paruošus duomenis yra paleidžiama programinė įranga autoriaus kompiuterio “komandinėje eilutėje” - terminale. Siekiant praktiškai pavaizduoti slaptažodžio nutekėjimo rizikos vertinimo metodo praktišką pritaikomumą, yra atliekama keletas vartotojų atvejų analizės atskirai. Suvedus pirmojo vartotojo iš apklausos gautų atsakymų rezultatus į programinės įrangos kompiuterinę programą kiekvienai kategorijai, pasirenkamas galutinis žingsnis - rizikos vertinimo/skaičiavimo etapas. Atlikus tai, yra išanalizuojami pateikti metodo (metodikos) rezultatai, siekiant įvertinti pačios programos veikimą bei rezultatų validumą. Atlikus kiekvieno vartotojo/atvejo eksperimentinę analizę, bus pateikti rizikos vertinimo metodo eksperimento rezultatai. Vėliau taip pat bus atliekama bendra visų duomenų palyginamoji analizė remiantis metodu.



9 pav. Rizikos vertinimo metodo architektūra

Šaltinis: Sudaryta autoriaus



10 pav. Rizikos vertinimo eksperimento procesas

Šaltinis: Sudaryta autoriaus

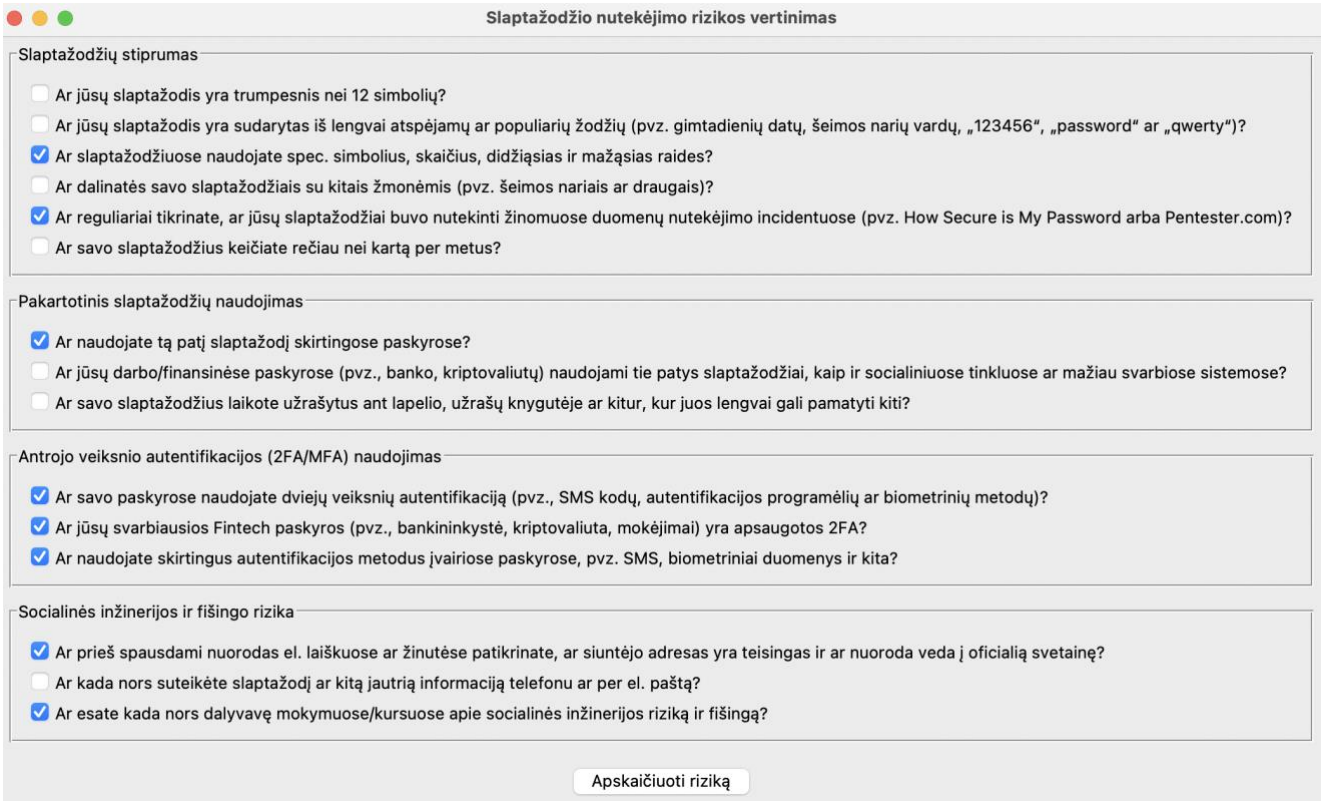
Pirmojo duomenų rinkinio eksperimentas I

Remiantis pirmojo apklausos vartotojo (Id = 1) atsakymais, yra paleidžiamas slaptažodžio nutekėjimo rizikos vertinimo metodas ir įvedami pateikti duomenys.

Klausimas	Atsakymas
Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?	Ne
Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?	Ne
Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?	Taip
Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?	Ne
Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?	Taip
Ar savo slaptažodžius keičiate rečiau nei kartą per metus?	Ne
Ar naudojate tą patį slaptažodį skirtingose paskyrose?	Taip
Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?	Ne
Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?	Ne
Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?	Taip
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?	Taip
Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?	Taip
Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?	Taip
Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?	Ne
Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?	Taip

11 pav. Pirmojo atvejo klausimyno analizė

Šaltinis: Sudaryta autoriaus



12 pav. Pirmojo atvejo slaptažodžio nutekėjimo rizikos vertinimas

Šaltinis: Sudaryta autoriaus

13 pav. Pirmojo atvejo slaptažodžio nutekėjimo rizikos vertinimo rezultatas

Šaltinis: Sudaryta autoriaus

Pirmojo atvejo eksperimentas parodė teigiamus rezultatus. Atliktą slaptažodžio nutekėjimo rizikos vertinimo metodą galimą išskaidyti plačiau į tris pagrindines dalis:

Rizikos identifikavimas – buvo atliktas remiantis atsakytais vartotojo klausimais. Rezultatas rodo, kad svarbiausias slaptažodžio nutekėjimo riziką skatinantis veiksnys yra pakartotinis slaptažodžių naudojimas.

Rizikos skaičiavimas – buvo atliktas remiantis programinėje įrangoje sukurtais matematiniais skaičiavimais. Kadangi „Slaptažodžių stiprumas“, „Antrojo veiksnio autentifikacijos (2FA/MFA)“ bei „Socialinės inžinerijos ir fišingo rizika“ kategorijos nepridėjo rizikos taškų, tuomet rizikos skaičius tampa 8.69%:

Tikimybė = 1/3 = 0.3333

Kategorijos svoris = 0.260657

Kategorijos rizika = 0.3333 x 0.260657 = 0.086885

Galutinė rizika = 0 + 0 + 0.086885 + 0 = 0.086885

Rizikos mažinimas – buvo atliktas identifikavus rizikos veiksnius bei apskaičiavus rizikos procentą. Gale vartotojui yra pateikiama svarbiausia rekomendacija – „*Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę*“

Tokiu būdu galima teigti, kad šiame konkrečiame atvejyje slaptažodžio nutekėjimo rizikos vertinimo metodo tikslas yra paskatinti vartotoją ir toliau laikytis stiprių slaptažodžio saugumo praktikų bei pasitaisyti vienintelę spragą – pakartotinių slaptažodžių skirtingose paskyrose naudojimą, kuris yra ganėtinai reikšmingas veiksnys, tačiau pavieniui nėra kritinio pobūdžio.

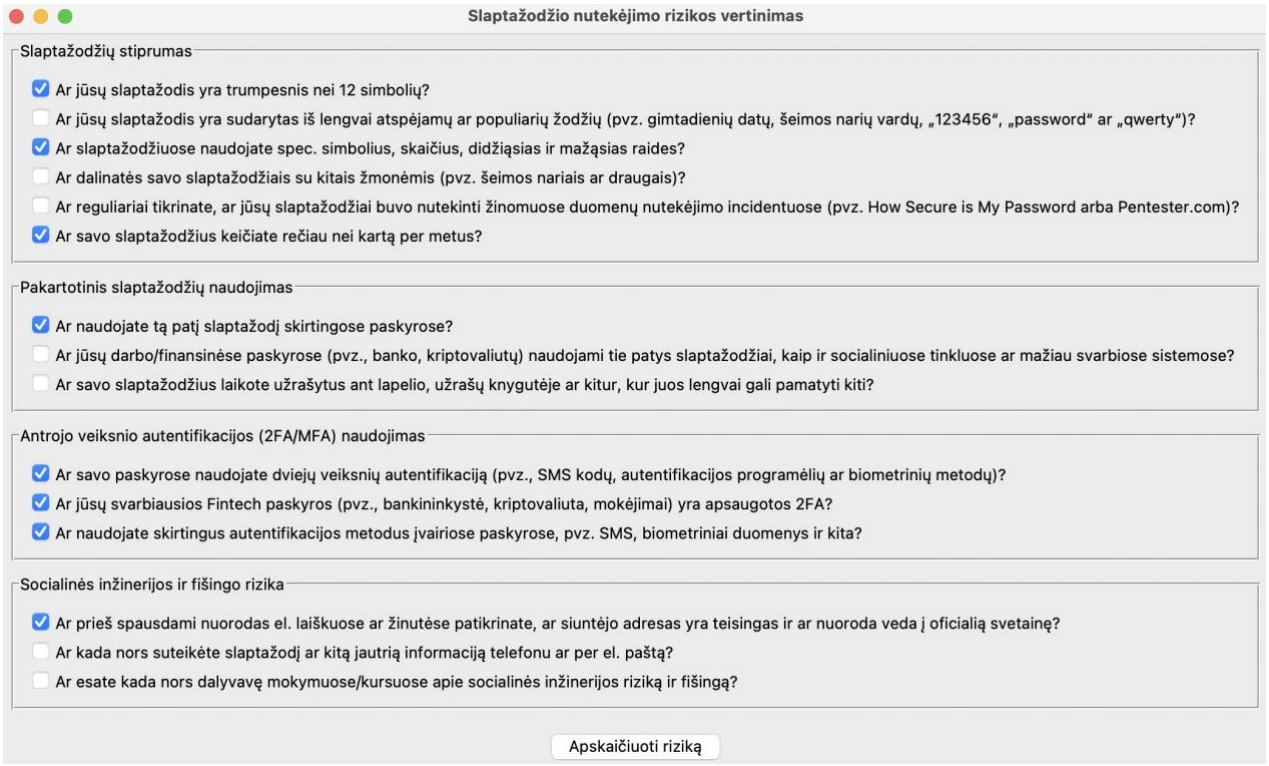
Pirmojo duomenų rinkinio eksperimentas II

Remiantis antrojo apklausos vartotojo (Id = 2) atsakymais, yra paleidžiamas slaptažodžio nutekėjimo rizikos vertinimo metodas ir įvedami pateikti duomenys.

Klausimas	Atsakymas
Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?	Taip
Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?	Ne
Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?	Taip
Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?	Ne
Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?	Ne
Ar savo slaptažodžius keičiate rečiau nei kartą per metus?	Taip
Ar naudojate tą patį slaptažodį skirtingose paskyrose?	Taip
Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?	Ne
Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?	Ne
Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?	Taip
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?	Taip
Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?	Taip
Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?	Taip
Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?	Ne
Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?	Ne

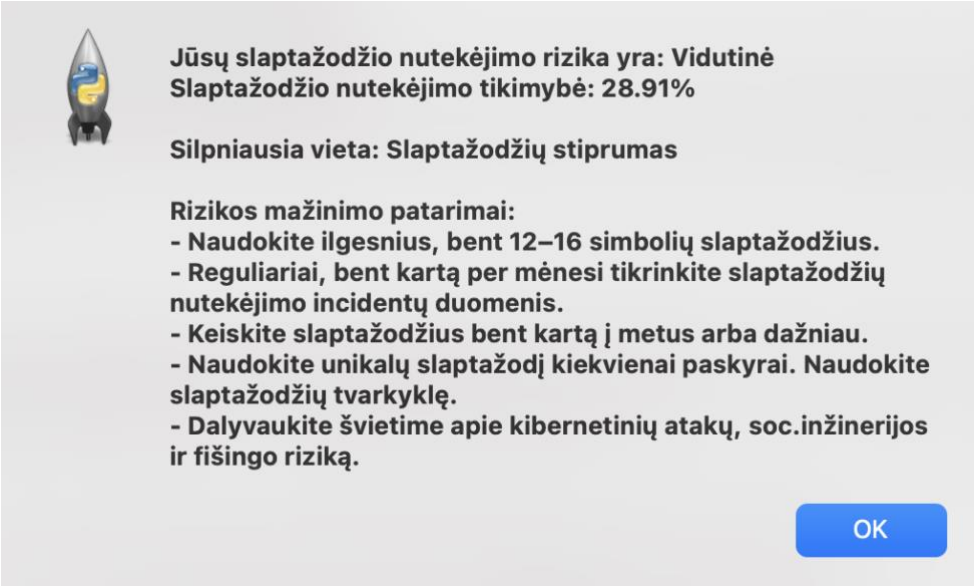
14 pav. Antrojo atvejo klausimyno analizė

Šaltinis: Sudaryta autoriaus



15 pav. Antrojo atvejo slaptažodžio nutekėjimo rizikos vertinimas

Šaltinis: Sudaryta autoriaus



16 pav. Antrojo atvejo slaptažodžio nutekėjimo rizikos vertinimo rezultatas

Šaltinis: Sudaryta autoriaus

Atlikus antrojo atvejo eksperimentą galima pastebėti kitokius rezultatus:

Rizikos identifikavimas – buvo atliktas remiantis atsakytais vartotojo klausimais. Rezultatas rodo, kad svarbiausias slaptažodžio nutekėjimo riziką skatinantis veiksnys yra slaptažodžių stiprumas. Į jį įeina trumpas slaptažodžio ilgis, retas slaptažodžių keitimas. Prie mažesnių rizikos veiksnių taip pat prisideda to paties slaptažodžio naudojimas skirtingose paskyrose bei švietimo apie fišingą ir socialinę inžineriją, trūkumas.

Rizikos skaičiavimas – buvo atliktas remiantis programinėje įrangoje sukurtais matematiniais skaičiavimais. Rizikos taškai buvo surinkti iš visų kategorijų, išskyrus „Antrojo veiksnio autentifikacija(2FA/MFA)“. Tokiu būdu slaptažodžio nutekėjimo rizika yra 28.91%:

Slaptažodžių stiprumas:

Tikimybė = 3/6 = 0.5

Kategorijos svoris = 0.3258213

Kategorijos rizika = 0.5 x 0.3258213 = 0.1629

Pakartotinis slaptažodžių naudojimas:

Tikimybė = 1/3 = 0.3333

Kategorijos svoris = 0.260657

Kategorijos rizika = 0.3333 × 0.260657 = 0.0869

Socialinės inžinerijos ir fišingo rizika:

Tikimybė = 1/3 = 0.3333

Kategorijos svoris = 0.1178387

Kategorijos rizika = 0.3333 × 0.1178387 = 0.0393

Galutinė rizika = 0.1629 + 0.0869 + 0 + 0.0393 = 0.2891

Rizikos mažinimas – buvo atliktas identifikavus rizikos veiksnius bei apskaičiavus rizikos procentą. Gale vartotojui yra pateikiama svarbiausios rekomendacijos:

„Naudokite ilgesnius, bent 12-16 simbolių slaptažodžius“;

„Reguliariai, bent kartą per mėnesį tikrinkite slaptažodžių nutekėjimo incidentų duomenis“;

„Keiskite slaptažodžius bent kartą į metus arba dažniau“;

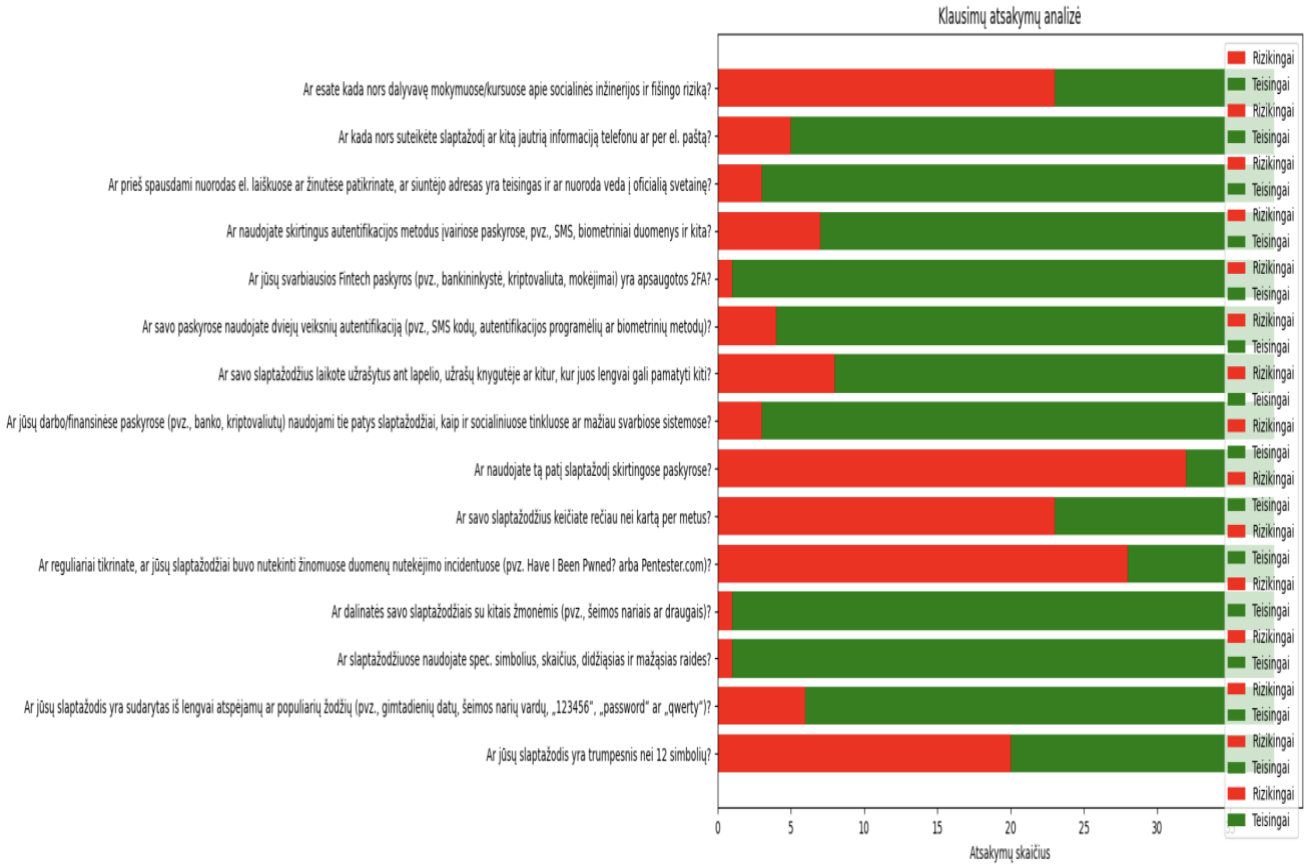
„Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę“;

„Dalyvaukite švietime apie kibernetinių atakų, soc.inžinerijos ir fišingo riziką“;

Taigi galima teigti, kad šiame konkrečiame atvejyje slaptažodžio nutekėjimo rizikos vertinimo metodo tikslas yra paskatinti vartotoją ir toliau laikytis stiprių slaptažodžio saugumo praktikų bei pasitaisyti vienintelę spragą – pakartotinių slaptažodžių skirtingose paskyrose naudojimą, kuris yra ganėtinai reikšmingas veiksnys, tačiau pavieniui nėra kritinio pobūdžio.

Pirmojo duomenų rinkinio eksperimento rezultatai

Pritaikius slaptažodžio nutekėjimo rizikos vertinimo metodą visiems pirmojo duomenų rinkinio atvejams buvo gauti rezultatai, remiantis atsakytų klausimų statistika. „Teisingai“ rodo atsakymą, nesukeliantį rizikos, tuo tarpu „Rizikingai“ byloja, kad atsakymas kelia slaptažodžio nutekėjimo riziką.



17 pav. Pirmojo duomenų rinkinio klausimų atsakymų analizė

Šaltinis: Sudaryta autoriaus

Klausimų atsakymų analizė:

Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?: Teisingai (0) - 18, Rizikingai (1) - 20

Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?: Teisingai (0) - 32, Rizikingai (1) - 6

Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?: Teisingai (0) - 37, Rizikingai (1) - 1

Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?: Teisingai (0) - 37, Rizikingai (1) - 1

Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?: Teisingai (0) - 10, Rizikingai (1) - 28

Ar savo slaptažodžius keičiate rečiau nei kartą per metus?: Teisingai (0) - 15, Rizikingai (1) - 23

Ar naudojate tą patį slaptažodį skirtingose paskyrose?: Teisingai (0) - 6, Rizikingai (1) - 32

Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?: Teisingai (0) - 35, Rizikingai (1) - 3

Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?: Teisingai (0) - 30, Rizikingai (1) - 8

Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?: Teisingai (0) - 34, Rizikingai (1) - 4

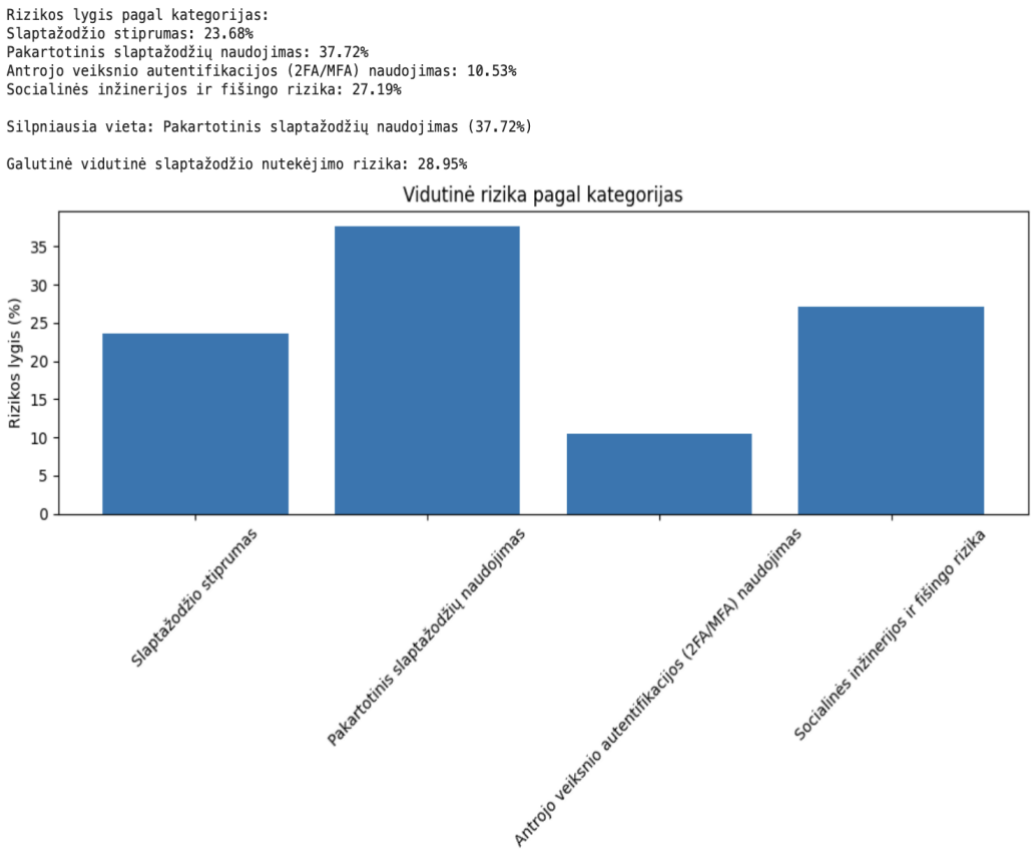
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?: Teisingai (0) - 37, Rizikingai (1) - 1

Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?: Teisingai (0) - 31, Rizikingai (1) - 7

Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?: Teisingai (0) - 35, Rizikingai (1) - 3

Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?: Teisingai (0) - 33, Rizikingai (1) - 5

Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?: Teisingai (0) - 15, Rizikingai (1) - 23



18 pav. Pirmojo duomenų rinkinio rizikos vertinimo rezultatai

Šaltinis: Sudaryta autoriaus

Statistika rodo, kad pirmojo duomenų rinkinio (iki 25m) vartotojai tam tikrose srityse pakankamai gerai supranta slaptažodžių nutekėjimo riziką. Iš 15 klausimų, 10 klausimų yra atsakyta teigiamai. Savo ruožtu, rizikingiausios tendencijos išlieka, kurios rodo, kad tam tikri specifiniai rizikos faktoriai išlieka. Didžiausią riziką keliantis klausimas susijęs su pakartotiniu slaptažodžiu naudojimu. Iš 38 vartotojų, 32 vartotojai patvirtino naudojąs tą patį slaptažodį skirtingose paskyrose, tai yra daugiau nei 84 %. Antras rizikingiausias veiksnys apima slaptažodžių keitimo praktiką. 28 vartotojai vengia tikrinti slaptažodžių nutekėjimo duomenų incidentus, tuo tarpu tik 15 iš 38 vartotojų keičia slaptažodį dažniau nei kartą per metus. Nepaisant gerų slaptažodžio stiprumo tendencijų kalbant apie spec. simbolius, skaičius ir raidžių kombinacijas, slaptažodžio ilgis išlieka problematiškas. Daugiau nei 50% vartotojų slaptažodžio ilgis nesiekia rekomenduojamų 12 simbolių. Kalbant apie dviejų veiksnių autentifikacijos (2FA/MFA) kategoriją, galima matyti, kad ji yra plačiai naudojama, tik 4 privatūs vartotojai patvirtino nenaudojąs dviejų veiksnių

autentifikacijos. Paskutinė – socialinės inžinerijos ir fišingo rizikos kategorija rodo, kad tarp jaunimo išlieka kibernetinio saugumo išsilavinimo stoka, kadangi 23 vartotojai niekada nebuvo dalyvavę mokymuose apie šių kibernetinių grėsmių pavojų, tuo tarpu 5 vartotojai prisipažino kada nors atskleidę slaptažodį telefonu ar el. paštu.

Apibendrinant pirmojo duomenų rinkinio visų atsakymų rezultatus matoma tendencija:

Rizikos lygis pagal kategorijas:

Slaptažodžio stiprumas: 23.68%

Pakartotinis slaptažodžių naudojimas: 37.72%

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas: 10.53%

Socialinės inžinerijos ir fišingo rizika: 27.19%

Silpniausia vieta: Pakartotinis slaptažodžių naudojimas (37.72%)

Galutinė vidutinė slaptažodžio nutekėjimo rizika: 28.95%

Apibendrinant galima teigti, kad pritaikius slaptažodžio nutekėjimo rizikos vertinimo metodą buvo pastebėtos pagrindinės tendencijos, kurios rodo, kad tarp jauno amžiaus vartotojų šiandien vis dar išlieka blogų slaptažodžių įpročių taikymas. Pakartotinio slaptažodžių naudojimo rodiklis beveik siekia 40%, o bendra galutinė vidutinė slaptažodžio nutekėjimo rizika yra 28.95%. Dviejų veiksnių autentifikacijos (2FA/MFA) kategorija išlieka mažiausiai rizikinga, kas ženkliai sumažina slaptažodžio nutekėjimo riziką. Kitaip tariant, metodas parodo, kad pagrindinės iki 25 metų vartotojų silpnosios vietos yra slaptažodžių pernaudojimas, retas jų atnaujinimas ir nepakankamas kibernetinio saugumo suvokimas. Tokiu būdu, galima statistiškai išskirti pagrindinius rizikos mažinimo veiksnius, aktualius pirmojo duomenų rinkinio vartotojams:

„Naudokite ilgesnius, bent 12–16 simbolių slaptažodžius“;

„Reguliariai, bent kartą per mėnesį tikrinkite slaptažodžių nutekėjimo incidentų duomenis“;

„Keiskite slaptažodžius bent kartą į metus arba dažniau“;

„Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę“;

„Dalyvaukite švietime apie kibernetinių atakų, soc.inžinerijos ir fišingo riziką“;

Antrojo duomenų rinkinio eksperimentas I

Remiantis antrojo duomenų rinkinio (25–45m) keturiasdešimt aštunto apklausos vartotojo (Id = 48) atsakymais, yra paleidžiamas slaptažodžio nutekėjimo rizikos vertinimo metodas ir įvedami pateikti duomenys.

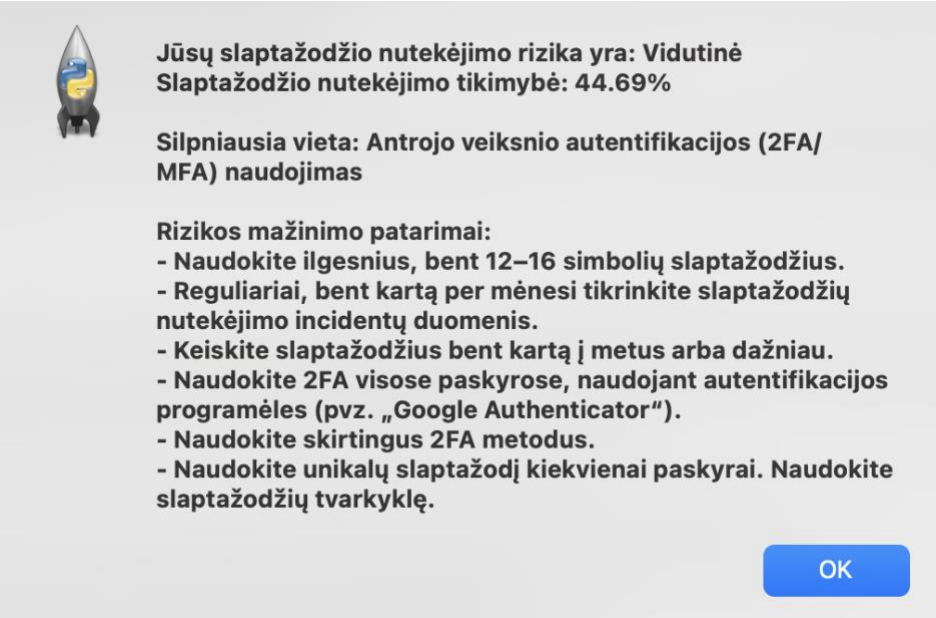
Klausimas	Atsakymas
Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?	Taip
Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?	Ne
Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?	Taip
Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?	Ne
Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?	Ne
Ar savo slaptažodžius keičiate rečiau nei kartą per metus?	Taip
Ar naudojate tą patį slaptažodį skirtingose paskyrose?	Taip
Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?	Ne
Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?	Ne
Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?	Ne
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?	Taip
Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?	Ne
Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?	Taip
Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?	Ne
Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?	Taip

19 pav. Keturiasdešimt aštunto atvejo klausimyno analizė

Šaltinis: Sudaryta autoriaus

20 pav. Keturiasdešimt aštunto slaptažodžio nutekėjimo rizikos vertinimas

Šaltinis: Sudaryta autoriaus



21 pav. Keturiasdešimt aštunto atvejo slaptažodžio nutekėjimo rizikos vertinimo rezultatas

Šaltinis: Sudaryta autoriaus

Žvelgiant į keturiasdešimt aštunto atvejo eksperimentinę analizę galima matyti specifiškesnius rezultatus.

Rizikos identifikavimas – Rezultatas rodo, kad svarbiausias slaptažodžio nutekėjimo riziką skatinantis veiksnys yra Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas, kitaip tariant – jo vengimas. Be to, taip pat galima pastebėti pavienius rizikos veiksnius iš visų kitų kategorijų, išskyrus soc.inžinerijos ir fišingą.

Rizikos skaičiavimas – buvo apskaičiuotas remiantis „Slaptažodžių stiprumas“, „Antrojo veiksnio autentifikacijos (2FA/MFA)“ bei „Pakartotinis slaptažodžių naudojimas“ kategorijos atsakymų vertėmis, ko pasekoje rizika tampa 44.69%:

Slaptažodžių stiprumas:

Tikimybė = 3/6 = 0.5

Kategorijos svoris = 0.3258213

Kategorijos rizika = 0.5 x 0.3258213 = 0.1629

Pakartotinis slaptažodžių naudojimas:

Tikimybė = 1/3 = 0.3333

Kategorijos svoris = 0.260657

Kategorijos rizika = 0.3333 × 0.260657 = 0.0869

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas:

Tikimybė = 2/3 = 0.6667

Kategorijos svoris = 0.295683

Kategorijos rizika = 0.6667 × 0.295683 = 0.1971

Galutinė rizika = 0.1629 + 0.0869 + 0 + 0.1971 = 0.4469

Rizikos mažinimas – Dėl pakankamai aukštos rizikos vartotojui yra pateikiama daug saugumo rekomendacijų:

„Naudokite ilgesnius, bent 12–16 simbolių slaptažodžius“;

„Reguliariai, bent kartą per mėnesi tikrinkite slaptažodžių nutekėjimo incidentų duomenis“;

„Keiskite slaptažodžius bent kartą į metus arba dažniau“;

„Naudokite 2FA visose paskyrose, naudojant autentifikacijos programėles (pvz. „Google Authenticator“)“;

„Naudokite skirtingus 2FA metodus“;

„Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę“;

Apibendrinant šį analizuojamą atvejį galima matyti, kad metodas aiškiai pabrėžia vidutinės rizikos egzistavimą remiantis didžiausiu riziką keliančiu veiksniu – antrojo veiksnio autentifikacija (2FA/MFA).

Antrojo duomenų rinkinio eksperimentas II

Remiantis antrojo duomenų rinkinio (25–45m) penkiasdešimto apklausos vartotojo (Id = 50) atsakymais, yra paleidžiamas slaptažodžio nutekėjimo rizikos vertinimo metodas ir įvedami pateikti duomenys.

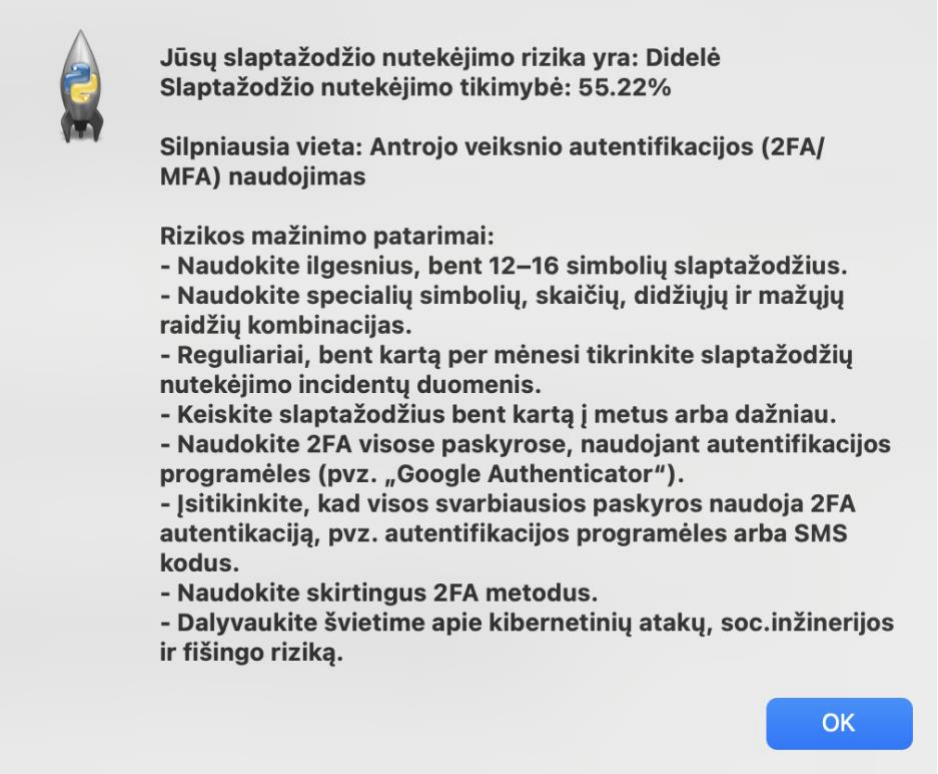
Klausimas	Atsakymas
Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?	Taip
Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?	Ne
Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?	Ne
Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?	Ne
Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?	Ne
Ar savo slaptažodžius keičiate rečiau nei kartą per metus?	Taip
Ar naudojate tą patį slaptažodį skirtingose paskyrose?	Ne
Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?	Ne
Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?	Ne
Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?	Ne
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?	Ne
Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?	Ne
Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?	Taip
Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?	Ne
Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?	Ne

22 pav. Penkiasdešimto atvejo klausimyno analizė

Šaltinis: Sudaryta autoriaus

23 pav. Penkiasdešimto atvejo slaptažodžio nutekėjimo rizikos vertinimas

Šaltinis: Sudaryta autoriaus



24 pav. Penkiasdešimto atvejo slaptažodžio nutekėjimo rizikos vertinimo rezultatas

Šaltinis: Sudaryta autoriaus

Žvelgiant į penkiasdešimto atvejo eksperimentinę analizę galima matyti dar labiau neigiamus rezultatus.

Rizikos identifikavimas – Rezultatas rodo, kad svarbiausias slaptažodžio nutekėjimo riziką skatinantis veiksnys yra taip pat Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas, tačiau pastebima ženkliai didesnė rizika dėl kitų veiksnių.

Rizikos skaičiavimas – rizikos lygis apskaičiuotas susumuojant visų keturių kategorijų rizikos veiksnius, tokiu būdų gaunant skaičių 55.22%:

Slaptažodžių stiprumas:

Tikimybė = 4/6 = 0.6667

Kategorijos svoris = 0.3258213

Kategorijos rizika = 0.6667 x 0.3258213 = 0.2172

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas:

Tikimybė = 3/3 = 1

Kategorijos svoris = 0.295683

Kategorijos rizika = 1 × 0.295683 = 0.295683

Socialinės inžinerijos ir fišingo rizika:

Tikimybė = 1/3 = 0.3333

Kategorijos svoris = 0.1178387

Kategorijos rizika = 0.3333 × 0.1178387 = 0.039

Galutinė rizika = 0.2172 + 0.295683 + 0.039 + 0= 0.5522

Rizikos mažinimas – Dėl labai aukštos rizikos vartotojui yra pateikiama daug saugumo rekomendacijų:

„Naudokite ilgesnius, bent 12–16 simbolių slaptažodžius“;

„Naudokite specialių simbolių, skaičių, didžiųjų ir mažųjų raidžių kombinacijas“;

„Reguliariai, bent kartą per mėnesi tikrinkite slaptažodžių nutekėjimo incidentų duomenis“;

„Keiskite slaptažodžius bent kartą į metus arba dažniau“;

„Naudokite 2FA visose paskyrose, naudojant autentifikacijos programėles (pvz. „Google Authenticator“)“;

„Įsitikinkite, kad visos svarbiausios paskyros naudoja 2FA autentikaciją, pvz. autentifikacijos programėles arba SMS kodus“;

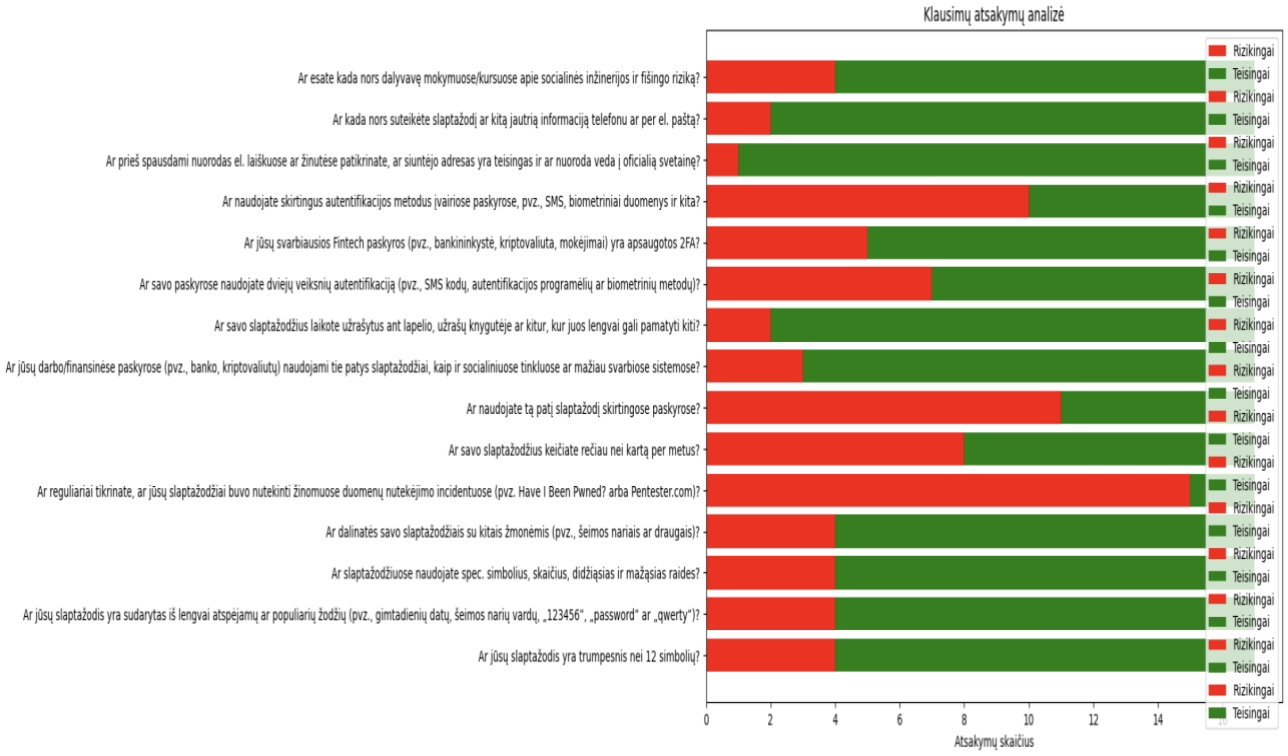
„Naudokite skirtingus 2FA metodus“;

„Dalyvaukite švietime apie kibernetinių atakų, soc.inžinerijos ir fišingo riziką“;

Apibendrinant šį analizuojamą atvejį galima matyti, kad metodas aiškiai pabrėžia didelės rizikos egzistavimą remiantis didžiausiu riziką keliančiu veiksniu – antrojo veiksnio autentifikacija (2FA/MFA) bei papildomais kitais rizikos faktoriais.

Antrojo duomenų rinkinio eksperimento rezultatai

Pritaikius slaptažodžio nutekėjimo rizikos vertinimo metodą visiems antrojo duomenų rinkinio atvejams buvo pastebėti kitokie rezultatai. Šiame atvejyje taip pat „Teisingai“ rodo atsakymą, nesukeliantį rizikos, tuo tarpu „Rizikingai“ byloja, kad atsakymas kelia slaptažodžio nutekėjimo riziką.



25 pav. Antrojo duomenų rinkinio klausimų atsakymų analizė

Šaltinis: Sudaryta autoriaus

Klausimų atsakymų analizė:

Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?: Teisingai (0) - 13, Rizikingai (1) - 4

Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz., gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?: Teisingai (0) - 13, Rizikingai (1) - 4

Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?: Teisingai (0) - 13, Rizikingai (1) - 4

Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz., šeimos nariais ar draugais)?: Teisingai (0) - 13, Rizikingai (1) - 4

Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?: Teisingai (0) - 2, Rizikingai (1) - 15

Ar savo slaptažodžius keičiate rečiau nei kartą per metus?: Teisingai (0) - 9, Rizikingai (1) - 8

Ar naudojate tą patį slaptažodį skirtingose paskyrose?: Teisingai (0) - 6, Rizikingai (1) - 11

Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?: Teisingai (0) - 14, Rizikingai (1) - 3

Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?: Teisingai (0) - 15, Rizikingai (1) - 2

Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?: Teisingai (0) - 10, Rizikingai (1) - 7

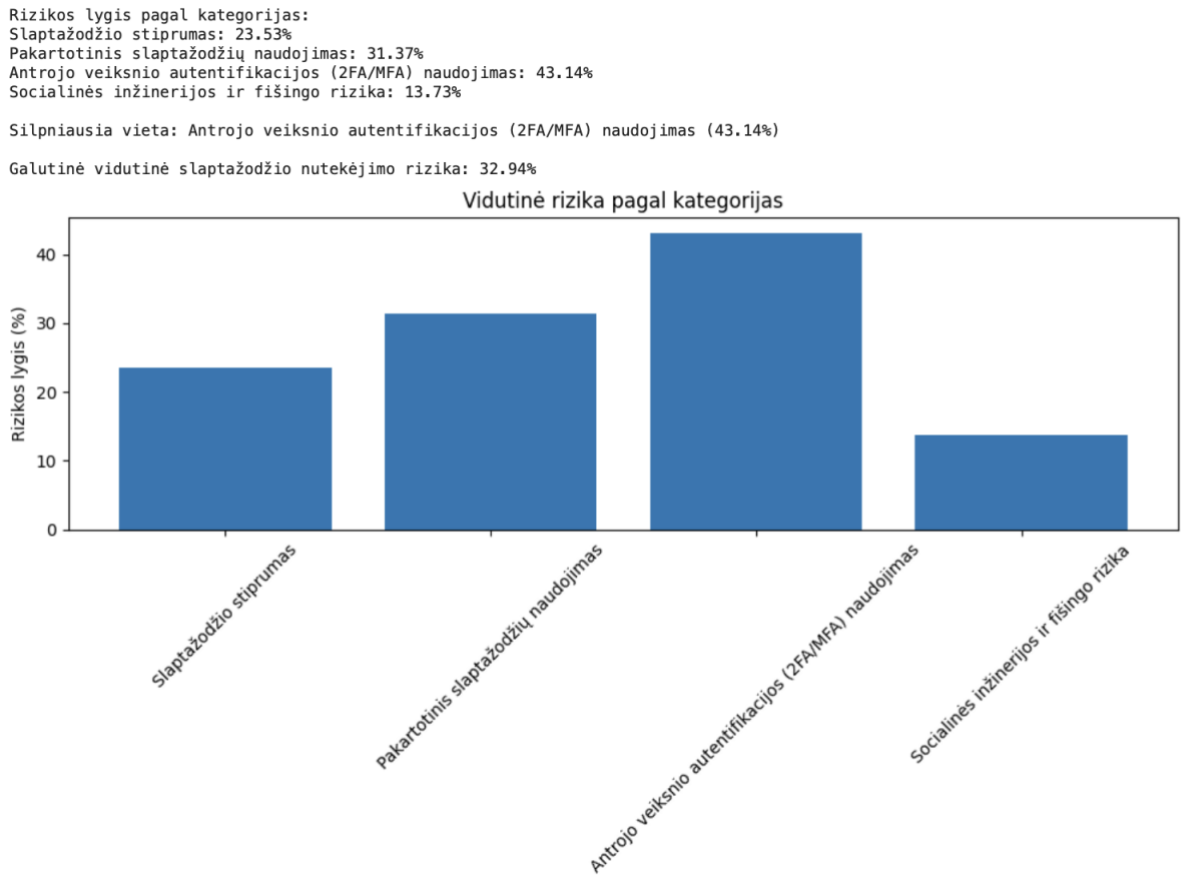
Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?: Teisingai (0) - 12, Rizikingai (1) - 5

Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz., SMS, biometriniai duomenys ir kita?: Teisingai (0) - 7, Rizikingai (1) - 10

Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?: Teisingai (0) - 16, Rizikingai (1) - 1

Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?: Teisingai (0) - 15, Rizikingai (1) - 2

Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos ir fišingo riziką?: Teisingai (0) - 13, Rizikingai (1) - 4



26 pav. Antrojo duomenų rinkinio rizikos vertinimo rezultatai

Šaltinis: Sudaryta autoriaus

Statistiškai analizuojant antrojo duomenų rinkinio (25–45m) rezultatus, yra matomi tam tikri pokyčiai, lyginant su pirmuoju rinkiniu. Nors probleminės sritys išlieka panašios, visgi antrojo duomenų rinkinio vartotojai yra mažiau supranta slaptažodžio nutekėjimo riziką. Rizikingiausias klausimas išlieka apie slaptažodžių nutekėjimo incidento duomenų tikrinimą – net 15 vartotojų iš 17 atsakė nepraktikuojąs šių dalykų. Antroje vietoje matoma prasta pakartotinė slaptažodžių naudojimo praktika bei slaptažodžių keitimas. 42% vartotojų linkę pakartotinai vartoti slaptažodžius. Nors šie rodikliai statistiškai yra mažiau rizikingesni, lyginant su pirmuoju duomenų rinkiniu (iki 25m), tai yra vis tiek nerimą keliantys skaičiai. Slaptažodžių ilgumas taip pat, palyginti su pirmuoju rinkiniu,

yra mažiau rizikingas, iš 17 vartotojų, tik 4 atsakė naudojąs trumpesnį nei 12 simbolių slaptažodį, o tai yra 23%. Kalbant apie Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimą, matomas ženklus skirtumas, lyginti su pirmuoju duomenų rinkiniu. Autentifikacija vis dar nėra pakankamai plačiai naudojama tarp vyresnio amžiaus interneto vartotojų. Statistika rodo, kad tik 59% vartotojų savo paskyrose naudoja dviejų veiksnių autentifikaciją ir tik 41% vartotojų naudoja bent kelis skirtingus autentifikacijos metodus. Tuo tarpu remiantis *„Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA?“* klausimu, galima prognozuoti, kad 29% vartotojų neturi/nenaudoja dviejų veiksnių autentifikacijos su mokėjimais ar kriptovaliutomis susijusiose Fintech paskyrose. Nepaisant to, soc.inžinerijos ir fišingo kategorija rodo labai teigiamas tendencijas. Matoma, kad ši kategorija yra stipriai mažiau rizikingesnė, kas rodo didesnį kibernetinį švietimą ir išsilavinimą tarp vyresnio amžiaus vartotojų. Net 16 iš 17 vartotojų atsakė tikrinąs žinutes ir el. laiškus dėl kenkėjiškų/pavojingų elementų. O 76% vartotojų yra bent kartą dalyvavę švietime/mokymuose apie kibernetinį fišingo ir soc.inžinerijos pavojų.

Tokiu būdų, apibendrinant antrojo duomenų rinkinio atsakymu rezultatus matoma tendencija:

Rizikos lygis pagal kategorijas:

Slaptažodžio stiprumas: 23.53%

Pakartotinis slaptažodžių naudojimas: 31.37%

Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas: 43.14%

Socialinės inžinerijos ir fišingo rizika: 13.73%

Silpniausia vieta: Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas (43.14%)

Galutinė vidutinė slaptažodžio nutekėjimo rizika: 32.94%

Taigi galima teigti, kad pritaikius slaptažodžio nutekėjimo rizikos vertinimo metodą antrajam duomenų rinkiniui ir palyginus rezultatus su pirmuoju rinkiniu, yra matomi akivaizdūs skirtumai. Nepaisant labai mažos rizikos socialinės inžinerijos ir fišingo kategorijoje, palyginus su pirmuoju rinkiniu, vyresnio amžiaus vartotojai susiduria su Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimo trūkumu. Ši kategorija laikoma silpniausia vieta, nes 43.14% vartotojų nesilaiko reikiamų saugumo praktikų. Slaptažodžio stiprumo ir pakartotinio slaptažodžių naudojimo tendencijos išlieka panašios. Tokiu būdu, galutinė slaptažodžio nutekėjimo rizika antrojo duomenų

rinkinio vartotojams yra didesnė nei pirmojo rinkinio – 32.94%. Tokiu būdu, metodo pritaikymas parodė ryškų skirtumą tarp slaptažodžio saugumo praktikų skirtingo amžiaus vartotojų, matoma, kad 2FA vartojimo problema išlieka kaip viena svarbiausių, kartu su pakartotiniu slaptažodžių naudojimu. Statistiškai galima išskirti pagrindinius rizikos mažinimo veiksnius, aktualius antrojo duomenų rinkinio vartotojams:

"Reguliariai, bent kartą per mėnesi tikrinkite slaptažodžių nutekėjimo incidentų duomenis";

"Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę";

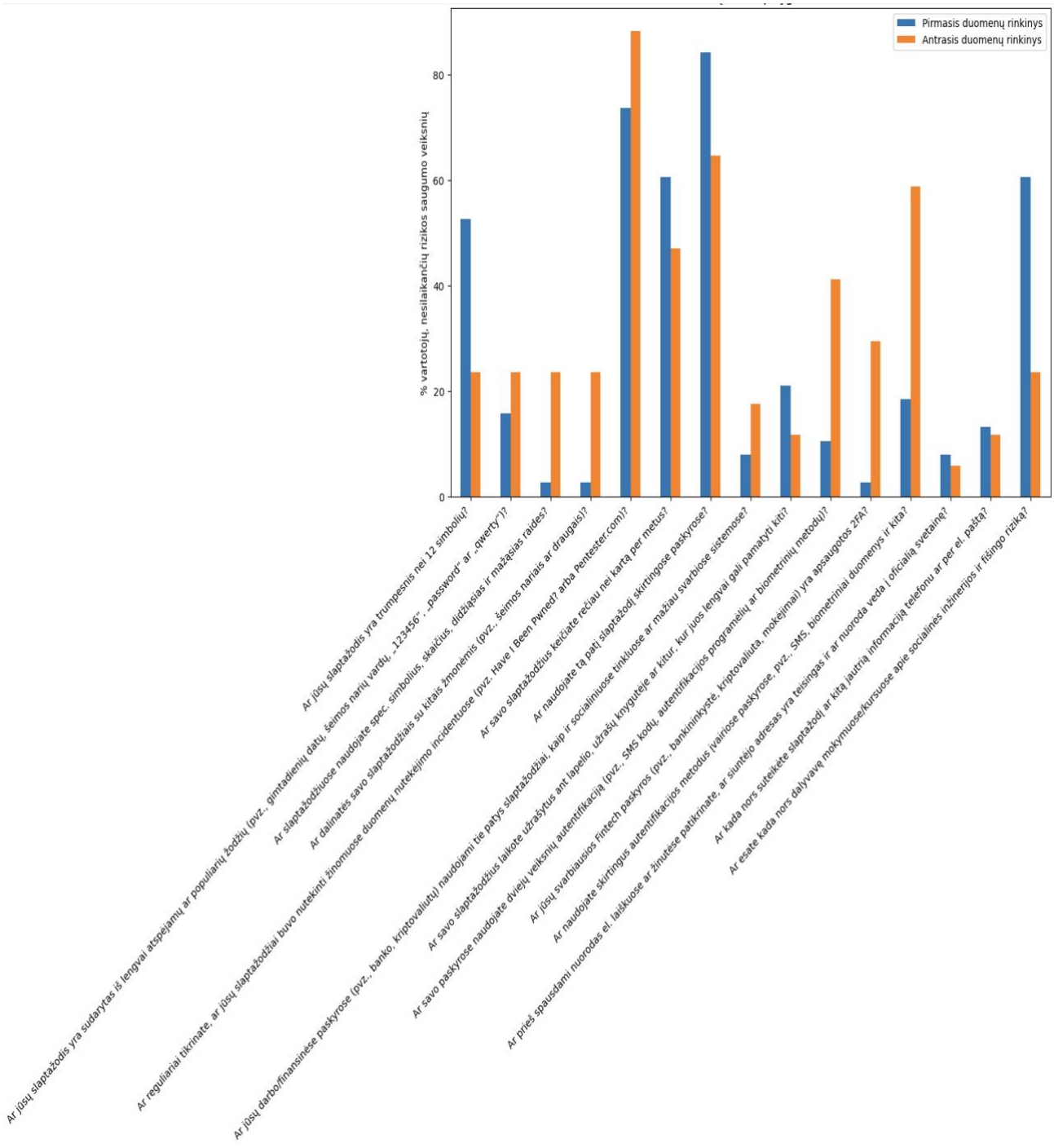
"Naudokite 2FA visose paskyrose, naudojant autentifikacijos programėles (pvz. „Google Authenticator“)";

Įsitikinkite, kad visos svarbiausios paskyros naudoja 2FA autentikaciją, pvz. autentifikacijos programėles arba SMS kodus";

"Naudokite skirtingus 2FA metodus";

Rezultatų palyginimas tarp skirtingo amžiaus vartotojų Lentelė 3

Kategorija	Pirmasis duomenų rinkinys (iki 25m)	Antrasis duomenų rinkinys (25–45m)
Slaptažodžio stiprumas	23.68%	23.53%
Pakartotinis slaptažodžių naudojimas	37.72%	31.37%
Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas	10.53%	43.14%
Socialinės inžinerijos ir fišingo rizika	27.19%	13.73%
Galutinė rizika	28.95%	32.94%
Silpniausia vieta	Pakartotinis slaptažodžių naudojimas	Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas



27 pav. Klausimų analizės palyginimas tarp dviejų duomenų rinkinių

Šaltinis: Sudaryta autoriaus

IŠVADOS

1. Remiantis atlikta moksline literatūros, ir jau egzistuojančių įrankių analize buvo sukurtas ir pristatytas slaptažodžio nutekėjimo trijų rizikos etapų vertinimo metodas, apimantis keturias slaptažodžių nutekėjimo rizikos grėsmes: slaptažodžių stiprumas, antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas, pakartotinis slaptažodžių naudojimas, socialinės inžinerijos ir fišingo rizika.
2. Remiantis Verizon Data Breach Investigations Report (VDIR 2022), Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos (NKSC 2023), Microsoft Security 2024 ataskaita, Google Survey 2023 ataskaita (LogMeOnce 2023), IBM Security Report 2023 buvo pagrįstas svorių bei reikšmių aktualumas naujam metodui. Metodo pritaikomumas buvo integruotas į Python programinę įrangą.
3. Buvo atliktas eksperimentinis tyrimas vertinant slaptažodžių nutekėjimo riziką, kurio metu buvo surinkti 55 vartotojų atsakymai, kurie buvo suskirstyti į pirmąjį duomenų rinkinį (iki 25m) ir antrąjį duomenų rinkinį (25–45m) pagal vartotojų amžiaus grupę. Metodas buvo pritaikytas visiems vartotojo atsakymams pagal skirtingus duomenų rinkinius.
4. Eksperimento rezultatai parodė, kad sukurtas ir pritaikytas metodas aiškiai identifikavo rizikos veiksnius, pateikė rizikos skaičiavimą bei rizikos mažinimo veiksnius. Metodo pritaikymo rezultatai pabrėžė egzistuojančią slaptažodžio nutekėjimo riziką tarp apklaustųjų vartotojų.
5. Eksperimento rezultatai parodė, kad pagrindinės iki 25 metų vartotojų silpnosios vietos yra slaptažodžių pernaudojimas, retas jų atnaujinimas ir nepakankamas kibernetinio saugumo suvokimas. Pakartotinio slaptažodžių naudojimo rodiklis beveik siekia 40%, o bendra galutinė vidutinė slaptažodžio nutekėjimo rizika yra 28.95%.
6. Eksperimento rezultatai parodė, kad vyresniojo amžiaus vartotojai (antrasis duomenų rinkinys) susiduria Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimo trūkumu. Ši kategorija laikoma silpniausia vieta, nes 43.14% vartotojų nesilaiko reikiamų saugumo praktikų, o galutinė slaptažodžio nutekėjimo rizika antrojo duomenų rinkinio vartotojams yra didesnė nei pirmojo rinkinio – 32.94%. Tuo tarpu kibernetinis išsilavinimas, soc.inžinerijos ir fišingo žinios išlieka kaip svarbus veiksnys, kuris mažina bendrą riziką.

PASIŪLYMAI

Siekiant išplėsti eksperimento detalumą rekomenduojama atlikti analizę su didesnio masyvo duomenimis

Siekiant dinamiškai ištestuoti ir palyginti dabartinių apklaustųjų vartotojų rezultatų pokyčius, rekomenduojama ateityje pakartoti duomenų surinkimą ir eksperimentą.

LITERATŪRA

1. Adeyoju, A. (2020). Financial Technology and Privacy: Evaluating the Approach to Consumer Data. Article in SSRN Electronic Journal. DOI: 10.2139/ssrn.3558810
2. Agencia Espanola Proteccion Datos (AEPA) (2021). Risk Management and Impact Assessment in the Processing of Personal Data. Prieiga: https://www.aepd.es/guides/risk-management-and-impact-assessment-in-processing-personal-data.pdf
3. Anuj, A. (2024). The 8 Most Common Causes of Data Breaches. Akamai. Prieiga: https://www.akamai.com/blog/security/8-most-common-causes-of-data-breaches
4. Bateman, R. (2024). 2-Factor Authentication for Payments in the EU. Prieiga: https://www.termsfeed.com/blog/2-factor-auth-eu-payments/
5. Bhardwaj, A., Goundar, S. (2020). Keyloggers: silent cyber security weapons. Article in Network Security. DOI: 10.1016/S1353-4858(20)30021-0
6. Blanton, S. (2024). 50+ Password Statistics & Trends to Know in 2024. Jumpcloud. Prieiga: https://jumpcloud.com/blog/password-statistics-trends
7. Bluebridge (2019). Populiariausi socialinės inžinerijos būdai ir kaip nuo jų apsisaugoti? Prieiga: https://bluebridge.lt/it-ziniu-centras/populiariausi-socialines-inzinerijos-budai-ir-kaip-nuo-ju-apsisaugoti/
8. Bonnie, E. (2024). Risk Analysis Calculations: 7 Ways to Determine Cybersecurity Risk Scores. Secureframe. Prieiga: https://secureframe.com/blog/risk-analysis-calculation
9. Bosnjak, L. (2018). Brute-force and dictionary attack on hashed real-world passwords. Conference: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). DOI: 10.23919/MIPRO.2018.8400211
10. Brende, H., Mansson, O. (2022). Perceived risk in online services and its effects on password strength. University of Adger. Prieiga: https://hdl.handle.net/11250/3019809
11. Culot, G., Podrecca, M., Nassimbeni, G., Sartor, M. (2021). The ISO/IEC 27001 information security management standard: a literature review and theory-based research agenda. The TQM Journal. DOI: 10.1108/TQM-09-2020-0202. Prieiga: https://www.researchgate.net/publication/350433247

12. Darem, A., Alhashmi, A., Alkhaldi, T., Alashjaee, A., Alanazi, S., Ebad, S. (2023). Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. IEEE Access. DOI: 10.1109/ACCESS.2023.3327016
13. Dastane, O., Johari, Z., Bakon, K. (2020). The Effect of Bad Password Habits on Personal Data Breach. DOI: 10.30534/ijeter/2020/538102020
14. Deloitte (2019). Understanding phishing techniques. Cyber 101. Prieiga: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf
15. Edwards, M. (2024). ISO 27001 for the Fintech Sector. Prieiga: https://www.isms.online/sectors/iso-27001-for-the-fintech-sector/
16. Elad, B. (2023). Two-Factor Authentication Statistics By Users, Industry, Adoption Rate and Benefits. Prieiga: https://www.enterpriseappstoday.com/stats/two-factor-authentication-statistics.html
17. European Data Protection Supervisor (2016). Personal Information Management Systems. Prieiga: https://www.edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en
18. European Union (ENISA) (2024). Evaluating the level of risk for a personal data processing operation. Prieiga: https://www.enisa.europa.eu/risk-level-tool/risk
19. Flynn, J. (2023). 17 ESSENTIAL MULTI-FACTOR AUTHENTICATION (MFA) STATISTICS [2023]. Zippia. Prieiga: https://www.zippia.com/advice/mfa-statistics/
20. Gautam, H., Sharma, V., Kumar, V. (2021). Phishing Prevention Techniques: Past, Present and Future. DOI: 10.1007/978-981-33-6307-6_10
21. Gehringer, E. (2002). Choosing passwords: Security and human factors. Conference: Technology and Society, 2002. (ISTAS'02). DOI: 10.1109/ISTAS.2002.1013839
22. Hoque, A. (2023). FinTech Risk Management and Monitoring. Murdoch University. DOI: 10.1007/978-3-031-18552-6_1
23. IBM Security Report (2023). IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. Prieiga: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs
24. ISO 27001 STANDARD. International Standards Organization Security Control Framework. Prieiga: https://www.cssia.org/wp-content/uploads/2020/01/ISO_27001_Standard.pdf

25. Janssen, H., Singh, J. (2022). Personal Information Management Systems. DOI: https://doi.org/10.14763/2022.2.1659
26. Krebson Security (2024). Fintech Giant Finastra Investigating Data Breach. Prieiga: https://krebsonsecurity.com/2024/11/fintech-giant-finastra-investigating-data-breach/
27. LogMeOnce (2023). Two Factor Authentication Statistics. Prieiga: https://logmeonce.com/resources/two-factor-authentication-statistics/
28. Madnick, E. Stuart. (2023). The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase. Prieiga: https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf
29. McDade, M., Iannini, L. (2024). Multi-Factor Authentication (MFA) Statistics You Need To Know In 2024. Expert Insights. Priega: https://expertinsights.com/insights/multi-factor-authentication-statistics/
30. Mercado, A., Varela, L. (2024). 10 Password Statistics that Predict Online Security Trends in 2024. Prieiga: https://www.skillademia.com/statistics/password-statistics/
31. Microsoft (2024). Security at your organization: Multifactor authentication statistics. Prieiga: https://learn.microsoft.com/en-us/partner-center/security/security-at-your-organization
32. Nacionalinis kibernetinio saugumo centras (NKSC) (2023). Nacionalinė kibernetinio saugumo būklės ataskaita už 2022 m. ir 2023 m. I-ojo ketvirčio incidentų statistika. Prieiga: https://nksc.lrv.lt/lt/naujienos/nacionaline-kibernetinio-saugumo-bukles-ataskaita-uz-2022-m-ir-2023-m-i-ojo-ketvircio-incidentu-statistika/
33. Nacionalinis kibernetinio saugumo centras (NKSC) (2023). Spalis – kibernetinio saugumo mėnuo: NKSC ir KAM atkreipia dėmesį į vieną didžiausių pavojų internetinėje erdvėje. Prieiga: https://nksc.lrv.lt/lt/naujienos/spalis-kibernetinio-saugumo-menuo-nksc-ir-kam-atkreipia-demesi-i-viena-didziausiu-pavoju-internetineje-erdveje/
34. Nordpass, Nordstellar (2022). Top 200 Populiariausi slaptažodžiai. Prieiga: https://nordpass.com/lt/most-common-passwords-list/
35. Public Sector Risk Management Framework (2010). Department: National Treasury Republic of South Africa. Prieiga: https://ag.treasury.gov.za/org/rms/rmf/Shared%20Documents/Downloads/10%20Risk%20Assessment.pdf?Mobile=1

36. Raza, M., Iqbal, M., Sharif, M., Haider, W. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. World Applied Sciences Journal. DOI: 10.5829/idosi.wasj.2012.19.04.1837
37. Reese K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. Brigham Young University, ISBN 978-1-939133-05-2. Prieiga: https://www.usenix.org/system/files/soups2019-reese.pdf
38. Stoneburner, G., Goguen, A., Feringa, A. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology Gaithersburg, Special Publication 800-30. Prieiga: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf
39. Stouffer, C. (2023). 139 password statistics to help you stay safe in 2024. Norton. Prieiga: https://us.norton.com/blog/privacy/password-statistics
40. Tam, L. Glassman, M., Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Old Dominion University. DOI: 10.1080/01449290903121386
41. Terranovasecurity (2024). How to Create a Strong Password in 7 Easy Steps. Security Awareness Training. Prieiga: https://www.terranovasecurity.com/blog/how-to-create-a-strong-password-in-7-easy-steps
42. Thai, B., Tanaka, H. (2022). An analysis of password security risk against dictionary attacks. Department of Computer Science National Defense Academy.
43. Verizon (2022). Data Breach Investigation Report. Prieiga: https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf
44. Wang D., Shan, X., Dong, Q., Shen, Y., Jia, C. (2023). No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters. Prieiga: https://www.usenix.org/system/files/sec23fall-prepub-291_wang-ding.pdf

PRIEDAI

Slaptažodžio nutekėjimo rizikos vertinimo metodo programinės įrangos kodas

```
import tkinter as tk
from tkinter import messagebox

# Klausimų bei rizikos mažinimo patarimų kūrimas
klausimai = {
    "Slaptažodžių stiprumas": [
        {"klausimas": "Ar jūsų slaptažodis yra trumpesnis nei 12 simbolių?", "safe": False, "patarimas": "Naudokite ilgesnius, bent 12–16 simbolių slaptažodžius."},
        {"klausimas": "Ar jūsų slaptažodis yra sudarytas iš lengvai atspėjamų ar populiarių žodžių (pvz. gimtadienių datų, šeimos narių vardų, „123456“, „password“ ar „qwerty“)?", "safe": False, "patarimas": "Venkite lengvai
        {"klausimas": "Ar slaptažodžiuose naudojate spec. simbolius, skaičius, didžiąsias ir mažąsias raides?", "safe": True, "patarimas": "Naudokite specialių simbolių, skaičių, didžiųjų ir mažųjų raidžių kombinacijas."},
        {"klausimas": "Ar dalinatės savo slaptažodžiais su kitais žmonėmis (pvz. šeimos nariais ar draugais)?", "safe": False, "patarimas": "Niekada nesidalinkite slaptažodžiais su kitais asmenimis."},
        {"klausimas": "Ar reguliariai tikrinate, ar jūsų slaptažodžiai buvo nutekinti žinomuose duomenų nutekėjimo incidentuose (pvz. Have I Been Pwned? arba Pentester.com)?", "safe": True, "patarimas": "Reguliariai, bent ka
        {"klausimas": "Ar savo slaptažodžius keičiate rečiau nei kartą per metus?", "safe": False, "patarimas": "Keiskite slaptažodžius bent kartą į metus arba dažniau."}
    ],
    "Pakartotinis slaptažodžių naudojimas": [
        {"klausimas": "Ar naudojate tą patį slaptažodį skirtingose paskyrose?", "safe": False, "patarimas": "Naudokite unikalų slaptažodį kiekvienai paskyrai. Naudokite slaptažodžių tvarkyklę."},
        {"klausimas": "Ar jūsų darbo/finansinėse paskyrose (pvz., banko, kriptovaliutų) naudojami tie patys slaptažodžiai, kaip ir socialiniuose tinkluose ar mažiau svarbiose sistemose?", "safe": False, "patarimas": "Finansi
        {"klausimas": "Ar savo slaptažodžius laikote užrašytus ant lapelio, užrašų knygutėje ar kitur, kur juos lengvai gali pamatyti kiti?", "safe": False, "patarimas": "Venkite viešai saugoti savo slaptažodžius."}
    ],
    "Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas": [
        {"klausimas": "Ar savo paskyrose naudojate dviejų veiksnių autentifikaciją (pvz., SMS kodų, autentifikacijos programėlių ar biometrinių metodų)?", "safe": True, "patarimas": "Naudokite 2FA visose paskyrose, naudojant
        {"klausimas": "Ar jūsų svarbiausios Fintech paskyros (pvz., bankininkystė, kriptovaliuta, mokėjimai) yra apsaugotos 2FA? ", "safe": True, "patarimas": "Įsitikinkite, kad visos svarbiausios paskyros naudoja 2FA autent
        {"klausimas": "Ar naudojate skirtingus autentifikacijos metodus įvairiose paskyrose, pvz. SMS, biometriniai duomenys ir kita?", "safe": True, "patarimas": "Naudokite skirtingus 2FA metodus."}
    ],
    "Socialinės inžinerijos ir fišingo rizika": [
        {"klausimas": "Ar prieš spausdami nuorodas el. laiškuose ar žinutėse patikrinate, ar siuntėjo adresas yra teisingas ir ar nuoroda veda į oficialią svetainę?", "safe": True, "patarimas": "Prieš spustelėdami nuorodą, p
        {"klausimas": "Ar kada nors suteikėte slaptažodį ar kitą jautrią informaciją telefonu ar per el. paštą?", "safe": False, "patarimas": "Niekada nesidalinkite slaptažodžiais telefonu ar el. paštu. Oficialios organizaci
        {"klausimas": "Ar esate kada nors dalyvavę mokymuose/kursuose apie socialinės inžinerijos riziką ir fišingą?", "safe": True, "patarimas": "Dalyvaukite švietime apie kibernetinių atakų, soc.inžinerijos ir fišingo rizi
    ]
}

# Rizikos kategorijų svorių nustatymas
svoriai = {
    "Slaptažodžių stiprumas": 0.3258213,
    "Antrojo veiksnio autentifikacijos (2FA/MFA) naudojimas": 0.295683,
    "Pakartotinis slaptažodžių naudojimas": 0.260657,
    "Socialinės inžinerijos ir fišingo rizika": 0.1178387
}
```

```
#Programos logikos kūrimas
class RizikosVertinimas:
    def __init__(self, root):
        self.root = root
        self.root.title("Slaptažodžio nutekėjimo rizikos vertinimas")
        self.atsakymai = {kategorija: [tk.IntVar() for _ in klaus] for kategorija, klaus in klausimai.items()}
        self.sukurti_langa()

    def sukurti_langa(self):
        for kategorija, klaus in klausimai.items():
            frame = tk.LabelFrame(self.root, text=kategorija, padx=10, pady=10)
            frame.pack(fill="both", expand="yes", padx=10, pady=5)
            for i, klausimas in enumerate(klaus):
                tk.Checkbutton(frame, text=klausimas["klausimas"], variable=self.atsakymai[kategorija][i]).pack(anchor="w")

        tk.Button(self.root, text="Apskaičiuoti riziką", command=self.skaiciuoti_rizika).pack(pady=10)

    def nustatyti_rizikos_lygi(self, procentai):
        if procentai <= 20:
            return "Maža"
        elif 21 <= procentai <= 50:
            return "Vidutinė"
        else:
            return "Didelė"

    def skaiciuoti_rizika(self):
        bendra_rizika = 0
        silpniausia_kategorija = None
        max_rizika = 0
        visi_patarimai = []

        for kategorija, svoris in svoriai.items():
            suma_atsakymų = 0
            klausimu_skaicius = len(klausimai[kategorija])
            patarimai_kategorijai = []

            for i, klausimas in enumerate(klausimai[kategorija]):
                atsakymas = self.atsakymai[kategorija][i].get()
                if klausimas["safe"]:
                    suma_atsakymų += 1 - atsakymas
                    if atsakymas == 0:
                        patarimai_kategorijai.append(klausimas["patarimas"])
                else:
                    suma_atsakymų += atsakymas
                    if atsakymas == 1:
                        patarimai_kategorijai.append(klausimas["patarimas"])

            tikimybe = suma_atsakymų / klausimu_skaicius
            kategorijos_rizika = svoris * tikimybe
            bendra_rizika += kategorijos_rizika

            if kategorijos_rizika > max_rizika:
                max_rizika = kategorijos_rizika
                silpniausia_kategorija = kategorija

            visi_patarimai.extend(patarimai_kategorijai)

        bendra_rizika_proc = bendra_rizika * 100
        rizikos_lygis = self.nustatyti_rizikos_lygi(bendra_rizika_proc)
```

```
        #Rezultatų pateikimas
        rezultatas = f"Jūsų slaptažodžio nutekėjimo rizika yra: {rizikos_lygis}\n"
        rezultatas += f"Slaptažodžio nutekėjimo tikimybė: {bendra_rizika_proc:.2f}%\n\n"
        rezultatas += f"Silpniausia vieta: {silpniausia_kategorija}\n\nRizikos mažinimo patarimai:\n"
        rezultatas += "\n".join(f"- {patarimas}" for patarimas in visi_patarimai)

        messagebox.showinfo("Rezultatas", rezultatas)

if __name__ == "__main__":
    root = tk.Tk()
    app = RizikosVertinimas(root)
    root.mainloop()
```