MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

AURIMAS ŠIDLAUSKAS

Kibernetinio saugumo valdymas

VARTOTOJŲ ELEKTRONINIŲ DUOMENŲ APSAUGOS YPATUMAI

Magistro baigiamasis darbas

Darbo vadovas –

Prof. dr. Tadas Limba

Vilnius, 2017

MYKOLAS ROMERIS UNIVERSITY

FACULTY OF ECONOMICS AND BUSINESS

AURIMAS ŠIDLAUSKAS

Cyber Security Management

USERS ELECTRONIC DATA PROTECTION FEATURES

Master Thesis

Supervisor: Prof. Dr. T. Limba

Vilnius, 2017

TURINYS

LENTELĖS

PAVEIKSLAI (I)

PAVEIKSLAI (II)

PRIEDAI

ĮVADAS

Temos aktualumas ir ištirtumas. Augantis technologijų naudojimas skatina imtis įvairiausių saugumo priemonių siekiant apsaugoti vartotojų elektroninius duomenis.

Informacijos saugumas (sauga) suprantamas kaip informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams (Kiškis, Petrauskas, Rotomskis ir Štitilis, 2006). Duomenys gali būti sugadinti, kuomet duomenimis pasinaudoja žmonės kurie neturėjo teisėtos prieigos prie tų duomenų (Dulaney ir Easttom, 2014). Ilgą laiką išskirtinai vyravę techniniai informacijos saugumo klausimai tebėra aktualūs, tačiau pastebima akivaizdi informacijos saugumo mokslinių tyrimų problematikos slinktis link platesnio, vis daugiau aspektų apimančio vadybinio požiūrio. Šiuo metu plačiausiai taikomų informacijos saugumo valdymo priemonių (metodikų, standartų, modelių) raidos analizė leidžia konstatuoti augančią taikomų priemonių turinio asimiliaciją, tačiau stebint nuolat kylančias informacijos saugumo problemas (pavyzdžiui, informacijos saugumo incidentų gausėjimą), aiškėja, kad esamos priemonės nėra pakankamos informacijos saugumui valdyti (Jastiuginas, 2012).

Informacinių sistemų audito ir kontrolės asociacija plečia įgytas žinias ir įgūdžius srityse, susijusiose su informacine sauga, kokybės užtikrinimu ir kontrole, ruošia kibernetinės saugos kvalifikacijos sertifikacijas. Internetinio saugumo centras (angl. *Center for Internet Security*) įžvalgus ne pelno siekiantis subjektas, naudojantis pasaulinės informacinių technologijų (toliau - IT) bendruomenės galią apsaugoti privačias ir visuomenines organizacijas nuo kibernetinių grėsmių. Internetinio saugumo centro teikiamos kritinės saugos kontrolės priemonės (toliau - CIS) yra naudojamos visame pasaulyje ir pripažintos geriausiomis, siekiant suvaldyti IT sistemų atakas. Šios patikrintos gairės nuolat tobulinamos ir atnaujinamos.

Elektroninis saugumas paprastai suprantamas kaip apsauga nuo neteisėtos prieigos prie informacijos, jos panaudojimo, keitimo, manipuliavimo, praradimo. Bendrąja prasme saugumas - tai būsena, kai negresia joks pavojus. Tačiau absoliutaus saugumo pasiekti neįmanoma, bet tinkamai parinktos ir taikomos saugumo priemonės gali sumažinti rizikos laipsnį ir praradimų mastus.

Temos naujumas. Duomenų saugumas nėra naujiena, dėl įvairių priežasčių norima išsaugoti duomenų konfidencialumą, vientisumą ir prieinamumą, tačiau apsaugos priemonės kinta ir tobulėja. Duomenų (informacijos) saugumas – tai visuotinis, nenutrūkstamas procesas kuris reikalauja nuolatinio tobulėjimo, prisitaikant prie besikeičiančių technologijų.

Mokslinė problema. Nesirūpinama elektroninių duomenų apsauga, išskirtos kompleksinės saugumo dalys: naudojami prasti (silpni) slaptažodžiai, neatsakingai dalinamasi privačia informacija

socialiniuose tinkluose su trečiosiomis šalimis, neatnaujinama operacinė sistema, nedaromos atsarginės duomenų kopijos, nenaudojama antivirusinė programinė įranga ir t.t.

Darbo objektas – vartotojų elektroninių duomenų apsaugos priemonių taikymo ypatumai.

Darbo tikslas – išanalizuoti vartotojų elektroninių duomenų saugumo ypatumus, bei pasiūlyti rekomendacijas, kurios padėtų sumažinti duomenų praradimo, neteisėto pasinaudojimo rizikas.

Darbo uždaviniai:

1. Išanalizuoti vartotojų elektroninių duomenų apsaugos ypatumų teorinius aspektus.
2. Pateikti „Windows 10“ operacinės sistemos ir „Facebook“ vartotojų autentifikavimo funkcijas.
3. Atlikti kiekybinį tyrimą, kuriuo siekiama sužinoti Lietuvos interneto vartotojų nuomonę kokios pagrindinės duomenų saugos problemos ir kokie jų sprendimo būdai.

Duomenų rinkimo metodai ir šaltiniai. Buvo remtasi literatūros analize, statistinių duomenų analize, atlikta interneto vartotojų apklausa. Darbe atliktos teorinė aprašomoji, sisteminė, lyginamoji analizės. Mokslinės literatūros ir statistinių duomenų analize buvo siekiama išanalizuoti priemones didinančias vartotojų elektroninių duomenų apsaugą. Atliktas kiekybinis tyrimas, kuriuo siekiama sužinoti Lietuvos interneto vartotojų nuomonę apie elektroninių duomenų saugos ypatumus. Darbe buvo remtasi D. Štitilis, E. Dulaney, J. Easttom, J. Andress, S. Jastiuginas, S. Oriyano ir kitų autorių moksliniais darbais. Taip pat 2016 metų nacionalinio kibernetinio saugumo būklės ataskaita, kritinės kontrolės saugos priemonių rekomendacijomis.

Darbo struktūra. Darbą sudaro 3 dalys. Pirmoje darbo dalyje nagrinėjami vartotojų elektroninių duomenų apsaugos teoriniai aspektai: „CIA triada“, saugaus slaptažodžio sudarymo sistema, atakos prieš slaptažodžius, kritinės kontrolės priemonės Antroje darbo dalyje pateikiama praktinio apsaugos priemonių taikymo analizė: „Windows 10“ operacinės sistemos vartotojo autentifikavimo funkcijos, asmens duomenų saugumas „Facebook“ socialiniame tinkle. Trečioje dalyje nagrinėjamas atliktas tyrimas, kurio tikslas – sužinoti vartotojų nuomonę, kokios apsaugos priemonės naudojamos siekiant apsaugoti duomenis ir išvengti kibernetinių incidentų; ar atsakingai dalinamasi privačiais duomenimis „Facebook“ socialiniame tinkle.

Darbo praktinis reikšmingumas. Darbe atlikta ir išanalizuota interneto vartotojų apklausa. Išsamiai aprašytos ir vaizdine medžiaga atvaizduotos „Windows 10“ operacinės sistemos ir „Facebook“ vartotojų autentifikavimo funkcijos. Šia informacija galima remtis stiprinant saugos priemones, siekiant išvengti incidentų susijusių su duomenų praradimu, pakeitimu ir neteisėtu panaudojimu.

1. VARTOTOJŲ ELEKTRONINIŲ DUOMENŲ APSAUGOS TEORINIAI ASPEKTAI

1.1. „CIA triada“ analizė

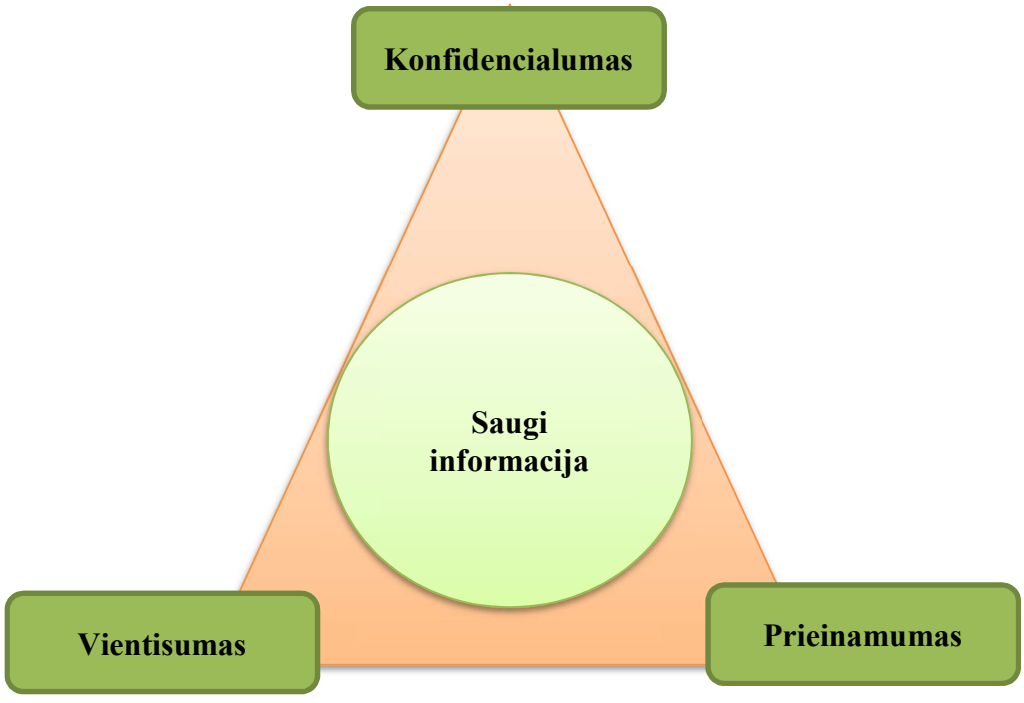
Technologijoms besiveržiant į mūsų gyvenimą, duomenų kiekiai didėja ir vis svarbesniu klausimu tampa, kaip apsaugoti savo duomenis. Duomenys tai yra informacija, kurią kompiuteris – priima, apdoroja, vaizduoja ir kaupia. Duomenys skirstomi į vaizdus, tekstus, skaičius, simbolius ir ženklus. Duomenys virsta informacija, kai tam tikram subjektui jie tampa suprantami. Dažnai duomenys ir informacija laikomi sinonimais.

Elektroninė informacija – informacinėje sistemoje tvarkomi duomenys, dokumentai ir informacija (Kibernetinio saugumo aplinka Lietuvoje, 2015).

Informacijos saugumas yra apibrėžiamas kaip saugoma informacija ir informacinės sistemos nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikimų, modifikavimo ar sunaikinimo (Andress, 2011).

Iš esmės, tai reiškia, kad mes norime apsaugoti mūsų duomenis ir sistemas nuo tų, kurie neteisėtai, netinkamai siekia jais pasinaudoti.

„CIA triada“ – tai trys pirminės informacijos saugumo koncepcijos, kurias sudaro konfidencialumas, vientisumas ir prieinamumas (Graham, Howard ir Olson, 2011).



1 Pav. CIA triados modelis

Šaltinis: „sudaryta autoriaus“

Trys „CIA triados“ koncepcijos:

1. Konfidencialumas – užtikrina, kad tam tikri duomenys prieinami tik tiems žmonėms, kuriems jie skirti;
2. Vientisumas – užtikrina, kad duomenys nebuvo koreguojami nesankcionuotų vartotojų;
3. Prieinamumas – užtikrina, kad įgalioti asmenys gautų prieigą prie duomenų ir jų naudojimo reikiamu laiku, per tam tikrą laikotarpį.

Konfidencialumas prarandamas kai informacija yra nuskaitoma arba kopijuojama asmens, neturinčio tam įgaliojimų. Konfidencialumas užtikrina, kad informacija bus prieinama tik autorizuotiems (įgaliotiems) vartotojams. Konfidencialumas dažnai gali būti asmeninio susitarimo reikalas, jeigu kitaip nenumato įstatymas. Įstatymai, ginantys intelektinės nuosavybės teises versle, remiasi koncepcija:

1. Informacija turi būti slapta, prieinama tik tiems asmenims, kurie darbe tiesiogiai su ja dirba;
2. Informacija turi turėti komercinę vertę, kad ji būtų laikoma slapta;
3. Įmonės savininkas ar vadovas turi imtis atsakingų žingsnių, kad išlaikytų informaciją paslaptyje (Kšivickienė, 2010).

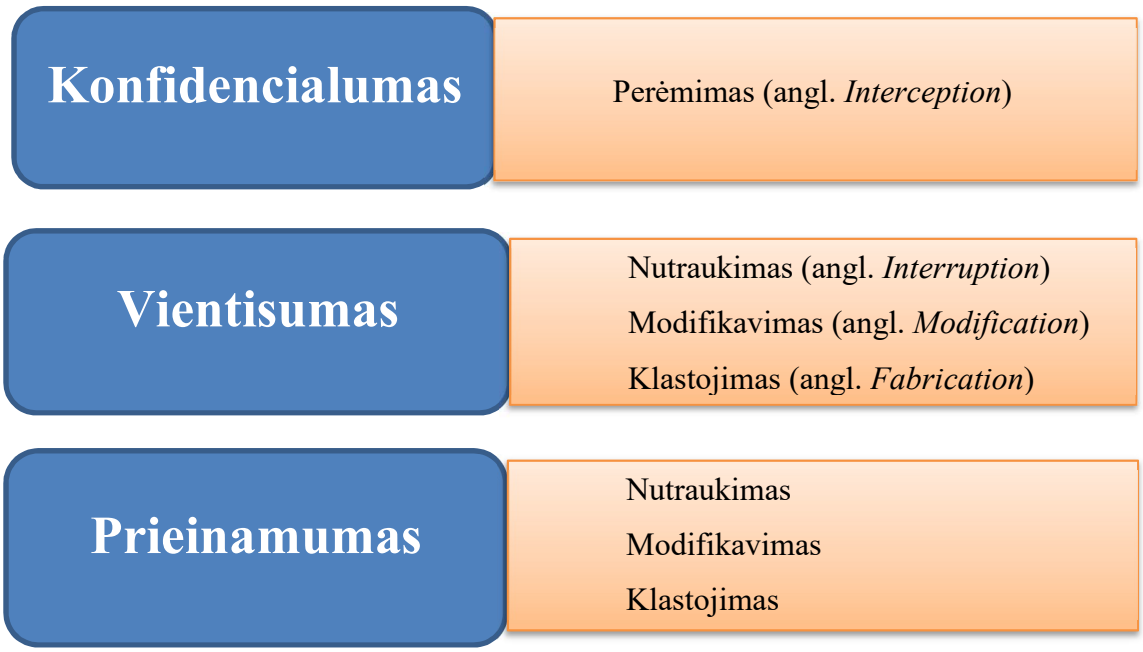
Kai kurioms informacijos rūšims konfidencialumas yra labai svarbi savybė, pvz. slaptažodžiai, asmeniniai privatūs duomenys, komercinė paslaptis ir pan.. Įvairių tipų informacija reikalauja skirtingo konfidencialumo ir konfidencialumo poreikis laikui bėgant gali kisti.

Vientisumas yra duomenų ar tam tikro ištekliaus tikrumas, patikimumas, o užtikrinant vientisumą svarbu apsaugoti duomenis nuo klaidingo ar nesankcionuoto jų pakeitimo. Vientisumas apima duomenų ir jų šaltinio vientisumą. Duomenų šaltinio vientisumo savybė dažnai vadinama autentiškumu. Pavyzdžiui, naujienų portale įkeliamas straipsnis tam tikra tema ir nurodoma, kad šaltinis „PSO“ (Pasaulio sveikatos organizacija), tačiau tikrasis šaltinis Lietuvos veterinarijos gydytojų asociacija. Tokiu būdu straipsnio informacija išlaiko vientisumą, tačiau pažeidžia šaltinio vientisumo kategoriją. Kai informacija yra pakeičiama nenumatytu būdu, tai vadinama vientisumo praradimu. Tai reiškia, kad informacija buvo pakeista be leidimo, ar tai atsitiktų dėl žmogaus klaidos, ar dėl sąmoningo įsikišimo. Vientisumas yra ypač svarbi saugumo ir finansinių duomenų savybė, pvz., jei atliekama pinigų pervedimo operacija iš vieno banko į kitą, pinigų pervedimo suma 1000 eurų, tai tokia pinigų suma turi išlikti iki pat finansinės operacijos pabaigos ir nepakisti. Vientisumo pažeidimo kontrolės metodai skirstomi į dvi klases: prevencijos ir aptikimo (atskleidimo). Prevencijos mechanizmai stengiasi išlaikyti duomenų vientisumą, blokuoja nesankcionuotą bandymą pakeisti duomenis. Pažeidimų aptikimo mechanizmai paprasčiausiai registruoja pažeidimus ir pateikia pranešimus, kad duomenų vientisumas pažeistas. Šie mechanizmai gali analizuoti sistemos įvykius (vartotojo ir sistemos veiksmus) ir taip nustatyti problemas. Vientisumą galima skirtyti į statinį (informacijos objektų nekintamumas) ir dinaminį (korektiškas veiksmų atlikimas). Todėl

dinaminio vientisumo kontrolė būtina, pvz., analizuojant finansinių operacijų srautus siekiant išvengti pažeidimų ir nusikalstamos veiklos. Vientisumas yra labai svarbus informacijos aspektas tais atvejais, kai informacija yra tam tikrų veiksmų pagrindas. Vientisumo sąvoka taip pat taikoma programinei įrangai ir jos konfigūravimui, tai yra reikšminga, nes gali būti pirmas žingsnis įvykdyti sėkmingą ataką prieš sistemos prieinamumą arba konfidencialumą. Pažeistų sistemų ir sugadintų duomenų klausimas turi būti sprendžiamas nedelsiant siekiant įvertinti tolesnį pažeidimų arba žalos potencialą.

Prieinamumas saugumo požiūriu reiškia, kad kažkas gali uždrausti prieigą prie informacijos ar paslaugos, padarydamas ją neprieinamą. Taigi informacija gali būti ištrinta arba kitaip tapti neprieinama. Tokiu atveju įvyksta informacijos prieinamumo praradimas. Tai reiškia, kad žmonės, kurie turi įgaliojimus prieiti prie informacijos, negali jos pasiekti. Informacinės sistemos kuriamos (įsigyjamos), kad teiktų tam tikras informacines paslaugas. Todėl daugelis išskiria prieinamumą kaip svarbiausią informacijos saugumo kategoriją. Ypač tai akivaizdu įvairiose valdymo informacinėse sistemose (gamybos, transporto ir kt.), taip pat sistemose aptarnaujančiose daugelį vartotojų (banko paslaugos, bilietų pardavimas, oro skrydžių tvarkaraščiai, turizmo agentūros ir kt.). Prieiga prie tinklo yra svarbi visiems, kieno veikla priklauso nuo priėjimo prie tinklo arba atskirų paslaugų teikiamų tinklo (Kompiuterių tinklų saugumo terminų aiškinamasis žodynas, 2013).

Siekiant pakenkti duomenų konfidencialumui, vientisumui ir prieinamumui susiduriama su įvairiausių rūšių atakomis, žinodami ataką poveikį, mes galime įvertinti kokia grėsmė gali kilti ir kokių priemonių imtis jai sumažinti. Vienu metu gali būti naudojamos iškart kelios atakos, taip pat svarbu jų intensyvumas.



2 Pav. Atakų kategorijos

Šaltinis: Andress, 2011

Atakų kategorijos:

1. Perėmimas – leidžia neteisėtiems vartotojams naudotis mūsų duomenimis, programomis ar sistemos aplinka. Perėmimas yra nesankcionuoti veiksmai su duomenimis kurie apima – žiūrėjimą, kopijavimą, pasiklausymą ir skaitymą. Tinkamai įvykdyta perėmimo ataka gali būti labai sunkus aptikta;
2. Nutraukimas – laikinai arba pastoviam laikui sustabdo prieigą prie duomenų;
3. Modifikavimas – neteisėtas duomenų (failų) pakeitimas arba programinės įrangos konfigūravimas;
4. Klastojimas – melagingos (žalingos) informacijos kūrimas ir platinimas (Andress, 2011).

Pagal „CIA triadą“ įvardijama, kad informacijos saugumo tikslas – užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą.

Norint išvengti nepageidaujamo poveikio kuris gali sukelti tam tikras pasekmes – konfidencialumui, vientisumui, prieinamumui, naudojami metodai apsisaugoti nuo tų nepageidaujamų pasekmių.

1 lentelė. „CIA triados“ praradimo pasekmės ir kontrolės metodai

Būtina sąlyga	**Poveikis ir galimos pasekmės**	**Kontrolės metodai**
Konfidencialumas: Apsauga nuo nesankcionuoto informacijos atskleidimo	Konfidencialumo praradimas gali sukelti šias pasekmės: • Neteisėtas privačios informacijos atskleidimas • Praradimas visuomenės pasitikėjimo • Praradimas konkurencinio pranašumo • Teisinis ieškinys prieš įmonę • Poveikis nacionaliniam saugumui	Konfidencialumas gali būti išsaugotas naudojant šiuos būdus: • Prieigos kontrolė • Bylų leidimai • Šifravimas
Vientisumas: Informacijos tikslumas ir išsamumas pagal verslo vertę ir lūkesčius	Vientisumo praradimas gali sukelti šias pasekmės: • Netikslumas • Klaidingi sprendimai • Sukčiavimas	Vientisumas gali būti išsaugotas naudojant šiuos būdus: • Prieigos kontrolė • Prisijungimas • Elektroninis parašas • Maiša (angl. *Hash*) • Šifravimas

1 lentelės tęsinys

Prieinamumas: Galimybė prieiti prie informacijos ir išteklių, kai to reikia	Prieinamumo praradimas gali sukelti šias pasekmės: • Funkcionalumo praradimas • Produktyvumo praradimas • Trikdžiai tikslams	Prieinamumas gali būti išsaugotas naudojant šiuos būdus: • Dubliavimas • Atsarginės kopijos • Prieigos kontrolė

Šaltinis: „Sudaryta autoriaus pagal Isaca: Cybersecurity Fundamentals Study Guide, 2015“

Vien techninių priemonių neužtenka norint užtikrinti informacijos saugą. Informacijos saugumo valdymas apima tris dimensijas:

1. Strateginė – administravimas, organizavimas, valdymas, laikymasis - standartų, teisinių priemonių ir gerųjų praktikų;
2. Žmogiškoji – saugumo kultūra, kompetencija, mokymai, psichologiniai aspektai;
3. Technologinė – techninės ir programinės įrangos priemonės.

Istoriškai elektroninės informacijos sauga buvo paremta tam tikrais svarbiausiais principais, kurių aktualumas išlieka iki šiol:

1. *Suvokimo principas*. Siekiant užtikrinti elektroninės informacijos saugą, reikia suvokti apsisaugojimo priemonių nuo galimos grėsmės elektroninei informacijai naudojimo būtinybę;
2. *Atsakomybės principas*. Kiekvienas elektroninės informacijos naudotojas turi suvokti savo atsakomybę ir funkcijas saugant elektroninę informaciją. Elektroninės informacijos saugą informacinėse sistemose turi užtikrinti valstybės institucijos vadovas, o ją įgyvendinti privalo saugos įgaliotiniai;
3. *Reagavimo principas*. Elektroninei informacijai kyla įvairi grėsmė, todėl būtina laiku aptikti saugos incidentus ir užkirsti kelią, be to valstybės institucijos viduje nuolat keistis informacija apie elektroninei informacijai kylančią grėsmę ir kovos su ja priemones;
4. *Demokratiškumo principas*. Elektroninės informacijos sauga turi būti įgyvendinama ir derėti su esminėmis demokratiškos visuomenės vertybėmis (pvz., laisve skleisti ir gauti informaciją);
5. *Rizikos įvertinimo principas*. Siekiant nustatyti esamą elektroninės informacijos saugos lygį ir parinkti būtinas elektroninės informacijos saugos priemones, būtina periodiškai įvertinti elektroninės informacijos saugos pavojus informacinėse sistemose;
6. *Elektroninės informacijos saugos kultūros ugdymo principas*. Siekiant užtikrinti elektroninės informacijos saugą, būtina ypač dėmesingai mokyti nuolatinius elektroninės informacijos

naudotojus elektroninės informacijos saugos ir taip ugdyti elektroninės informacijos saugos kultūrą valstybės institucijose;

7. *Elektroninės informacijos saugos priemonių projektavimo ir diegimo principas*. Elektroninės informacijos sauga turi būti kuriama kartu su informacine sistema. Elektroninės informacijos sauga turi būti pamatinis visų informacinės sistemos paslaugų elementas, kuriam būtina užtikrinti nuolatinį lėšų, neviršijančių pačios elektroninės informacijos vertės, skyrimą (Štitilis ir kt., 2016).

Pagrindinis informacijos saugumo valdymo objektas yra informacija, o informacijos saugumo valdymo tikslais – „CIA triada“. Informacijos saugumui aktualius veiksnius sujungia strateginė, žmogiškoji ir technologinė informacijos saugumo valdymo dimensijos. Informacija yra didžiausias turtas ir svarbiausias saugumo objektas.

Sekančioje temoje aptarsime saugaus slaptažodžio sudarymo sistemos ypatybes, kadangi slaptažodis daugeliu atvejų yra naudojamas užtikrinti „CIA triadą“.

1.2. Saugaus slaptažodžio sudarymo sistemos analizė

Šiuolaikiniame informacinių technologijų pasaulyje vis dažniau susiduriama su sistemų ir duomenų saugumo problemomis. Informacija yra didelė vertybė, kuri esant poreikiui, gali būti apsaugota nuo nesankcionuoto naudojimosi galimybės. Prieigos kontrolės pagrindinis uždavinys yra kontroliuoti, kurie subjektai turi teisę prisijungti prie konkrečių sisteminių resursų, tai yra įgyvendinama atliekant autentifikavimą.

Autentifikavimas – tai įrodymas, kad tam tikras asmuo turi tam tikrą tapatybę ir (arba)yra įgaliotas vykdyti tam tikrą veiklą. (Europos duomenų apsaugos teisės vadovas, 2014).

Autentifikavimas – tai asmens tapatybės patvirtinimas vienoje ar kitoje e. paslaugas teikiančioje interneto svetainėje. Šis patvirtinimas reikalingas siekiant, kad paslaugos būtų teikiamos būtent tam asmeniui (Vartotojo autentifikavimas svetainėje).

Subjekto autentifikacija – tai procesas, kai vienas subjektas (tikrintojas) įsitikina kito subjekto (pareiškėjo) tapatybe su tam tikra garantija. Šis įsitikinimas užtikrinamas reikalaujant iš pareiškėjo pateikti jo tapatybę patvirtinančius įrodymus. Subjektas tvirtina, kad jis turi tam tikrą tapatybę ir atlieka autentifikavimą, kai vienokiu ar kitokiu būdu įrodo tikrintojui, kad pateikta tapatybė tikrai priklauso jam. Procesas, kai pareiškėjas tvirtina, kad jis turi tam tikrą tapatybę, vadinamas identifikacija (Vitkus, 2010).

Autentifikavimo proceso metu yra nustatoma, ar vartotojas yra tas asmuo kuriuo jis dedasi esąs. Vartotojas yra autentifikuojamas pagal:

1. Tai ką jis žino. Pareiškėjui suteiktas slaptažodis arba asmeninis identifikacijos kodas (PIN);

2. Tai ką jis turi. Šiam įvesties tipui priklauso tiek fiziniai įrenginiai (pvz. banko kortelė, telefonas), tiek programinė įranga;
3. Tai kas jis yra. Šiai kategorijai priskiriamas įvesties tipas, vadinamas biometrika. Naudojami pirštо antspaudai, balsas, akies rainelės vaizdas.

Skirtingose sistemose, programose gali būti naudojami skirtingi autentifikacijos būdai, arba jų iš vis gali ir nebūti. Sistemose, kuriose informacija yra labai griežtai saugoma naudoja aukšto lygio autentifikaciją, užtikrinančią, kad tik tam teisę turintys asmenys galėtų prieiti prie šių duomenų. Tačiau jei informacija nėra labai svarbi, tuomet gali būti panaudoti patys primityviausi autentifikacijos būdai arba jų gali iš vis nebūti. Slaptažodžiu paremta autentifikacija yra vienas iš populiariausių autentifikacijos būdų. Tačiau jis yra mažiausiai saugus būdas autentifikuoti. Asmuo yra autentifikuojamas kai jis įveda į tam tikras vietas savo prisijungimo vardą ir slaptažodį, kurį jis vienas težino. Tuomet jo įvesti duomenys yra tikrinami sistemos duomenų bazėje, ir jei ten tokie yra, vartotojas yra autentifikuojamas.

Slaptažodis – ženklų seka, žinoma tik paslaugos teikėjui ir jos vartotojui, pagal kurią paslaugos teikėjas patikrina į jį besikreipiančio asmens tapatybę. Slaptažodis sudaromas iš raidžių, skaitmenų ir kitų ženklų (Lučinskij, Poderskis ir Tumėnas, 2007).

Vartotojų slaptažodžiais yra pagrįsta dauguma autentifikacijos formų bei bylų ir duomenų apsaugos metodų. Kadangi tinkamai autentifikuotas prisijungimas dažnai neregistruojamas, arba jei ir registruojamas, paprastai nekelia įtarimo, sukompromitavus slaptažodį galima tyrinėti sistemą iš vidaus praktiškai be pavojaus būti aptiktam. Užpuolikas gauna pilną priėjimą prie visų šio vartotojo resursų, turi žymiai didesnes galimybes pasiekti kitas paskyras, gretimus kompiuterius ir galbūt netgi gauti administratoriaus privilegijas (Informacija ir komunikacija: Saugumo svarba).

Viena empirinių tyrimų sritis yra slaptažodžiai, kurie atlieka pagrindinį vaidmenį reguliuojant prieigą prie slaptos informacijos ir internetinių paslaugų (elektroninio pašto sistemos, internetinės saugyklos, socialiniai tinklai). Įrodymai rodo, kad paprastai naudojami labai paprasti slaptažodžiai, pvz., 0000, admin, 1234. Silpni slaptažodžiai yra viena iš priežasčių kodėl žmonės patiria kibernetinio saugumo riziką. Slaptažodžių politika siekiama užtikrinti, kad vartotojai būtų saugesni (Cybersecurity in the European Digital Single Market, 2017).

Saugaus ir kriptografine prasme stipraus slaptažodžio pasirinkimas yra ne tik labai svarbus, bet ir būtinas norint apsaugoti savo privatumą ir duomenis.

Rekomendacijos norint sukurti saugų slaptažodį:

1. Visų pirma jūsų slaptažodis neturėtų būti trumpesnis nei 6 simbolių. Šiuo metu 6 simbolių deriniai yra patys populiariausi, todėl siekdami apsaugoti pačius svarbiausius duomenis, tokius kaip el. banko sąskaitos ar asmeninė informacija, naudokite mažiausiai 8–10 simbolių ilgio slaptažodžius.

2. Slaptažodį pasistenkite sukurti iš kuo daugiau skirtingų raidžių, skaičių ir simbolių. Nepamirškite ir mažųjų bei didžiųjų raidžių, kurios taip pat turi daug įtakos slaptažodžio saugumui. Kuo įvairesnis jis bus, tuo sunkiau bus atspėjamas kompiuteriu.
3. Nenaudokite visur to paties slaptažodžio. Siūlome susikurti mažiausiai tris: vieną (galima ir paprastesnį, lengviau įsimenamą) eilinėms svetainėms, kuriose nesaugomi jokie jūsų duomenys, o tiesiog tik reikalinga registracija, kad gautumėte daugiau galimybių ar naudos, antrą – vidutinės svarbos prisijungimams, pavyzdžiui, svetainėms, kuriose pateikiate savo asmeninę informaciją: telefono numerius, adresą, tikrą vardą ir pavardę, ir trečią (pati saugiausią, ilgiausią) –svarbiausioms vartotojo sąskaitoms: el. bankininkystei, el. paštui, el. parduotuvei bei kitoms panašaus pobūdžio svetainėms (Muzikevičiūtė, 2014).

Google rekomendacijos kaip sukurti sudėtingą slaptažodį ir užtikrinti paskyros saugą:

1. *Kiekvienoje svarbioje paskyroje naudokite unikalų slaptažodį*. Kiekvienoje svarbioje paskyroje, pvz., el. pašto ir internetinės bankininkystės paskyrose, naudokite kitokį slaptažodį. Rizikinga naudoti tuos pačius slaptažodžius. Jei kažkas sužinos vienos jūsų paskyros slaptažodį, gali būti, kad tas asmuo pasieks jūsų asmens informaciją ar kitas internetines paslaugas, pvz., apsipirkimo ar bankininkystės.
2. *Slaptažodyje naudokite raidžių, skaičių ir simbolių derinį.* Kai kurdami slaptažodį naudojate skaičius, simbolius ir didžiųjų bei mažųjų raidžių derinį, tokį slaptažodį sunkiau atspėti. Pavyzdžiui, aštuonių simbolių slaptažodį, sudarytą iš skaičių, simbolių ir mažųjų bei didžiųjų raidžių yra sunkiau atspėti, nes toks slaptažodis turi 30 000 kartų daugiau galimų kombinacijų nei aštuonių simbolių slaptažodis tik iš mažųjų raidžių.
3. *Nenaudokite asmens informacijos ar dažnai vartojamų žodžių kaip slaptažodžio***.** Sukurkite unikalų slaptažodį, kuris nebūtų susijęs su asmens informacija ir kuriame būtų naudojamas raidžių, skaičių ir simbolių derinys. Pavyzdžiui, galite pasirinkti atsitiktinį žodį ar frazę ir įterpti raidžių bei skaičių pradžioje, viduryje ir pabaigoje, kad būtų dar sudėtingiau atspėti (pvz., „s0kol@d4S“). Naudokite paprastų žodžių ar frazių, pvz., „slaptazodis“ ar „ileiskitemane“, klaviatūros šablonų, pvz., „qwerty“ ar „qazwsx“, ar nuoseklių šablonų, pvz., „abcd1234“, nes atspėti ar iššifruoti slaptažodį bus lengviau.
4. *Slaptažodžius laikykite saugioje vietoje***.** Nepalikite užrašų su įvairių svetainių slaptažodžiais kompiuteryje ar ant stalo, kur kiti žmonės gali lengvai juos pavogti ir pasinaudoję jais pažeisti jūsų paskyrą. Jei nuspręsite išsaugoti slaptažodžius kompiuterio faile, sukurkite tokį failo pavadinimą, kuris neatskleistų, kas jame saugoma. Jei jums sudėtinga prisiminti kelis slaptažodžius, naudokite patikimų slaptažodžių tvarkytuvę. Būtinai skirkite kelias minutes ir peržiūrėkite atsiliepimus ir nuomones apie slaptažodžių tvarkytuvės paslaugas.

Ko reikėtų vengti sudarant slaptažodį:

1. Nesirinkite slaptažodžio, skelbiamo viešai ar pavyzdžio pavidalu. pvz., slaptazodis, password ar examplepassword;
2. Nenaudokite slaptažodžio, kurį naudojate jau daugelį metų;
3. Nenaudokite slaptažodžio, kurį žino tretieji asmenys;
4. Nenaudokite slaptažodžio, susidedančio iš asmeninės informacijos (vardai, gimtadieniai, datos);
5. Nenaudokite klaviatūros šablonų, pvz., qwerty, wasd, zxcvb ar nuoseklių skaičių, pvz., 12345, 09876;
6. Neatskleiskite savo slaptažodžių kitiems bei neįvedinėkite jų kažkam stebint;
7. Nesiųskite slaptažodžių el. paštu ar nesakykite jų girdint kitiems (Slaptažodžiai ir jų saugojimas, 2017).

Nesilaikant šių rekomendacijų didėja rizika tapti hakerių aukomis, slaptažodis gali būti pasisavintas. Internete yra daug svetainių kuriose galima pasitikrinti slaptažodžio stiprumą ir per kiek laiko jis gali būti atspėtas. Svetainėje „Kaspersky Lab: Secure Password Check“ įvertinus stiprius slaptažodžius kurie buvo kuriami laikantis saugaus slaptažodžio rekomendacijų ir nesaugius slaptažodžius (trumpus, lengvai įsimenamus) gauname tokius rezultatus:

2 lentelė. Slaptažodžių saugumo vertinimas

Eil. Nr.	Silpni slaptažodžiai	Atspėjimo trukmė	Stiprūs slaptažodžiai	Atspėjimo trukmė
1	Terminator	37 sekundės	20‘sTerm1nator!!	8 metai
2	Psychopath	2 minutės	Psy-cho*path	200 metų
3	Katinas	9 min	Ka/*ti/*nas	33 metai
4	Aurimas	8 valandos	Au(rimas)!!	33 metai
5	Internetas1	12 dienų	!n-ter/netas	400 metų
6	123ligonis	18 dienų	1Li/go/nis1	33 metai

Šaltinis: „Sudaryta autoriaus pagal Kaspersky Lab: Secure Password Check“

Matome (žr. 2 lentelę), kad saugaus slaptažodžio rekomendacijų slaptažodžiai yra nesaugūs, nes per trumpą terminą gali būti atspėti.

Slaptažodžiai gali būti sudaryti iš skaičių, raidžių (didžiųjų ir mažųjų) ir specialių simbolių, galima paskaičiuoti kokia tikimybė yra atspėti slaptažodį. Kuo didesnis kiekis slaptažodžio kombinacijų, tuo sunkiau jį atspėti.

Slaptažodžių sudarymo pavyzdžiai:

1. PIN kodo slaptažodis yra sudarytas iš keturių skaitmenų. Iš viso turime dešimt skaitmenų 0, 1, 2, 3,4, 5, 6, 7, 8, 9 iš kurių galime panaudoti, bet kokia tvarka keturis skaitmenis (skaitmenys gali kartotis). Slaptažodžio kombinacijų tikimybė 10 * 10 * 10 * 10 = 10000.
2. Turime slaptažodį sudarytą iš keturių mažųjų raidžių (a – z). Iš viso yra 26 raides abėcėlėje, neskaičiuojant lietuviškų raidžių. Sudarant slaptažodį raidės gali kartotis. Slaptažodžio kombinacijų tikimybė 26 * 26 * 26 * 26 = 456976. Jeigu slaptažodį sudaro šešios mažosios raidės, kombinacijų tikimybė lygi 26 * 26 * 26 * 26 * 26 * 26=308915776.
3. Turime slaptažodį sudarytą iš aštuonių mažųjų raidžių (a – z) arba didžiųjų raidžių (A – Z). Slaptažodžio kombinacijų tikimybė 52 * 52 * 52 * 52 * 52 * 52 * 52 * 52 = 53459728531456.
4. Turime slaptažodį sudarytą iš aštuonių mažųjų raidžių (a – z) arba didžiųjų raidžių (A – Z), skaitmenų (0 – 9) ir specialių simbolių (~`!@#$%^&*()_-+={[}]|\:;”’<,>.?/) Slaptažodžio kombinacijų tikimybė 94 * 94 * 94 * 94 * 94 * 94 * 94 * 94 = 6095689385410816.

Mokslininkai Joseph Bonneau et al. straipsnyje „Slaptažodžių ir netobulo autentifikavimo evoliucija“ rašo , kaip vengti slaptažodžių pakartotinio naudojimo. Skirtingi slaptažodžiai užtikrina, kad „nulaužtas“ slaptažodis vienoje svetainėje nebus tinkamas panaudoti prisijungiant kitoje svetainėje, tačiau turint daug slaptažodžių vartotojams kyla bėdų juos prisiminti. Vartotojams patariama skirtingus slaptažodžius naudoti svarbiose svetainės paskyrose ir nustoti nerimauti dėl menkavertės vertės svetainių paskyrų.

Slaptažodžiams atsiminti galima naudoti slaptažodžių tvarkykles kurios yra populiariausiose interneto naršyklėse arba specializuotą programinę įrangą kuri slaptažodžius saugo „debesyse“ (angl. *Clouds*), pvz. „LastPass“. Šio metodo privalumai ir trūkumai:

3 lentelė. Slaptažodžių tvarkyklių privalumai ir trūkumai

Privalumai	**Trūkumai**
Nereikia prisiminti visų slaptažodžių	Piktavalis neteisėtai gavęs prieigą prie vartotojo naršyklės gali pasinaudoti joje esančiais slaptažodžiais ir įgis galimybę prisijungti prie vartotojo paskyrų
	Visiems slaptažodžiams naudojama viena sistema
	Slaptažodžius turi trečioji šalis

Šaltinis: „Sudaryta autoriaus pagal The Password Security Checklist“

JAV Nacionalinio standartų ir technologijos instituto buvęs darbuotojas Billas Burras kuris yra laikomas slaptažodžių kūrimo ekspertu, 2017 metais išplatino pranešimą spaudai, kad piktavaliams „nulaužti“ yra sunkiausia ilgus slaptažodžius. Jis rekomenduoja sudarinėti ilgus

slaptažodžius kurie susideda iš kelių žodžių, tai galėtų būti kokia nors lengvai įsimenama frazė (Statt, 2017).

Svetainėje „Kaspersky Lab: Secure Password Check“ įvertinus atsitiktinius ilgus slaptažodžius gauname tokius rezultatus:

4 lentelė. Ilgų slaptažodžių saugumo vertinimas

Eil. Nr.	Ilgi slaptažodžiai	Slaptažodžių ženklų skaičius	Atspėjimo trukmė
1	Arklyseinanamo	14	13000 metų
2	Raganosskraidodanguje	20	10000000 metų
3	Killthemalltonightbaby	22	10000000 metų
4	Baltakavasupienu	16	10000000 metų
5	Juodablackspalva	16	105000 metų
6	Metalmuzikaramina	17	520000 metų

Šaltinis: „Sudaryta autoriaus pagal Kaspersky Lab: Secure Password Check“

Kuo ilgesnis ir iš skirtingų ženklų sudarytas slaptažodis, tuo mažesni šansai, kad jis bus atspėtas kokios nors atakos metu.

Sekančioje temoje aptarsime kokias atakas piktavaliai naudoja norėdami išgauti vartotojų slaptažodžius.

1.3. Atakos prieš slaptažodžius

Piktavaliai įvairiomis atakomis siekia išgauti slaptažodžius ir dažniausiai silpnoji saugumo vieta yra vartotojas, kuris naudoja ne pakankamai stiprius slaptažodžius.

Žemiau pateiktoje lentelėje (žr. 5 lent.) matome kokio tipo gali būti atakos. Kai kurios atakos gali būti kelių tipų.

5 lentelė. Atakų tipai

Pasyvi tinklo ataka	Atliekamas tinklo srauto tebėjimas (šnipinėjamas) nekontaktuojant su auka ir nebandant įsilaužti į jo sistemą
Aktyvi tinklo ataka	Atliekami slaptažodžių spėjimai vienas po kito siekiant įsibrauti į sistemą
Ataka neprisijungus	Ataka vykdoma aukos sistemoje, pasinaudojama slaptažodžio saugojimo pažeidžiamumu

5 lentelės tęsinys

Netechninė ataka	Atakos nereikalauja jokių techninių žinių, o remiasi vagystėmis, apgaule ir vartotojų patiklumu

Šaltinis: „Sudaryta autoriaus remiantis Oriyano, 2016“

Populiariausios atakos prieš slaptažodžius.

Grubios jėgos ataka (angl. *Brute force attack*) – tai bandymai atspėti vartotojo prisijungimo duomenis prie informacinės sistemos, įvedinėjant atsitiktines simbolių sekas ir dažnai naudojamas kombinacijas. Tam naudojami įvairūs programiniai įrankiai, kurie, priklausomai nuo sistemos apsaugos lygio, suteikia galimybę atlikti iki kelių tūkstančių spėjimų per minutę. Įsibrauti į sistemą yra paprasta, jeigu žinomas jos prisijungimo adresas, o sugalvotas paskyros slaptažodis yra nesudėtingas arba labai panašus į prisijungimo vardą („Brute force“ atakos).

Grubios jėgos atakos kelia grėsmę vartotojų paskyroms ir apkrauna tinklapį su nepageidaujamu duomenų srautu. Nors šias atakas aptikti yra lengva, tačiau jų išvengti yra sunku. Pvz.: dauguma http (užklausimo - atsakymo protokolas, jungiantis klientą ir serverį) grubios jėgos įrankių gali nukreipti užklausas per atvirus įgaliotuosius serverius. Tuomet kiekviena ataka atkeliauja iš skirtingų IP (interneto protokolų) adresų, todėl tokių atakų negalima nutraukti užblokuojant konkretų IP adresą. Viską dar labiau apsunkina tai, kad grubios jėgos programinė įranga kiekvieną kartą mėgina vis skirtingą vartotoją, todėl užblokuoti kurį nors iš jų, dėl neteisingai parašyto slaptažodžio, tampa neįmanoma.

Apsaugos būdai nuo brutalios jėgos atakų:

1. Paskyrų užrakinimas po tam tikro skaičiaus neteisingų slaptažodžių bandymų. Paskyrų blokavimas gali trukti tam tikrą laikotarpį, pvz., vieną valandą arba paskyros gali likti užrakintos iki administratorius jį rankiniu būdu atrakins. Paskyros blokavimas ne visada yra geriausias sprendimas, nes piktavaliai gali piktnaudžiauti saugumo priemone ir užblokuoti šimtus vartotojų paskyrų;
2. Naudojimas įrenginių slapukus. Tai suteiks galimybę užrakinti autentifikavimo bandymus iš žinomų ir nežinomų naršyklių ar įrenginių atskirai;
3. Blokavimas IP adreso iš kurio buvo mėginama prisijungti daug kartų. Šios išeitis trūkumas tas, kad galima netyčia užblokuoti dideles vartotojų grupes, kurios naudoja tą patį įgaliotąjį serverį, pvz. interneto paslaugų tiekėją ar didelę įmonę. Dauguma tinklapių neblokuoja IP po vieno nepavykusio prisijungimo, dažniausiai reikia suklysti bent tris kartus;
4. Neteisingo prisijungimo atveju neatskleisti kurie duomenys buvo netinkami – prisijungimo vardas ar slaptažodis;

5. Po vieno ar dviejų nepavykusių prisijungimo bandymų paprašyti naudotojo ne tik vartotojo vardo ir slaptažodžio, bet ir atsakyti į slaptą klausimą;
6. Naudoti ženklų atpažinimo testą (angl. *Captcha*). Šio testo paskirtis – atskirti ar vartotojas yra žmogus, ar kompiuteris siūlant atpažinti deformuotų ženklų eilutę. Ženklų atpažinimo testas yra vienas iš geriausių būdų apsisaugoti nuo grubios jėgos atakos, tačiau būtinybė įvesti papildomus duomenis vargina vartotoją. Taigi vartotojui duoti suvesti saugos kodą reiktų, jei iš pirmo karto nepavyko atlikti autentifikacijos;
7. Ypatingos saugos atveju leisti prisijungti tik iš tam tikrų IP adresų;
8. Paskyros blokavimas tam tikrą laikotarpį po nepavykusio prisijungimo. Didžiausias grubios jėgos atakų trūkumas yra sugaištamas laikas. Prailginant šį laiką galima iš dalies sustiprinti apsaugą prieš šias atakas. Šiuo atveju galima dirbtinai įterpti net kelių sekundžių vėlavimus prieš tikrinant slaptažodį, vartotojams tai nesukels didelio nepatogumo (Blocking Brute Force Attacks, 2017).

Sąlygos, kurioms esant galima įtarti grubios jėgos ataką:

1. Daug nepavykusių prisijungimo bandymų iš to paties IP adreso;
2. Bandymas prisijungti su keliais vartotojų vardais iš vieno IP adreso;
3. Prisijungimai prie vienos vartotojo paskyros iš daug skirtingų IP adresų (Brute Force Attack, 2013).

Jei visi vartotojai naudotų sudėtingus slaptažodžius, grubios jėgos atakos didelės grėsmės nekeltų, tačiau yra vartotojų kurie renkasi trumpus ir lengvai įsimenamus slaptažodžius, todėl patartina imtis papildomų saugumo priemonių. Vartotojas šioje apsaugos sistemos grandyje yra silpnoji vieta.

Žodyno ataka (angl. *Dictionary attack*) – tai bandymai atspėti vartotojo prisijungimo duomenis prie informacinės sistemos, įvedinėjant žodžius arba žodžių derinius pasinaudojant ribotu žodynu. Žodyno ataka pasiteisina tik tuo atveju, jei slaptažodis yra tikrasis žodyno žodis arba žodžių derinys, todėl tokio pobūdžio atakos bejėgės prieš stiprius slaptažodžius, kuriuose naudojami skaičiai ar kiti simboliai.

Skiemens ataka (angl. *Syllable attack*) – tai yra junginys brutalios jėgos ir žodyno atakos. Ši ataka naudinga, kai vartotojo pasirinktas slaptažodis nėra standartinis žodis ar frazė.

Hibridinė ataka (angl. *Hybrid attack*) – šis slaptažodžio užpuolimo būdas grindžiamas žodyno ataka, bet su papildomais veiksmas procese. Išbandytus slaptažodžiai žodynų atakos metu dalinai pakeičiami tam tikrais simboliais arba pridedama koks nors skaitmuo, pvz. Sl@ptaž0dis arba Slaptažodis1 (Oriyano, 2016).

Taisyklėmis paremta ataka (angl. *Rule-Based attack*) – tai programavimo pagrindu sukurta išplėstinė ataka kurios metu slaptažodžiai gali būti įvairiai modifikuojami. Piktavalis daro prielaidą,

kad vartotojas sukūrė slaptažodį naudodamas informaciją, kurią užpuolikas anksčiau laiko žinojo, pvz. frazes ir skaitmenis, kuriuos vartotojas gali turėti tendenciją naudoti. Šis atakos metodas apima grubios jėgos, žodynų ir skiemenų išpuolių naudojimą (Rule-based Attack).

Iš anksto apskaičiuoto algoritmo ataka (angl. *Pre-Computed Hash attack*) – slaptažodžiai koduojami kriptografijos algoritmais (angl. H*ashes*), žinodamas algoritmą piktavalis gali atkurti slaptažodį. Internete galima rasti dideles duomenų bazes kuriose nurodytos standartinių algoritmų reikšmės.

„**MITM" ataka** (angl. *Man In The Middle*) – tarp dviejų sąveikaujančių šalių įsiterpia trečias asmuo – užpuolikas. Tokiu atveju užpuolikas turi galimybę ne tik perimti siunčiamus pranešimus, bet ir juos keisti, blokuoti ar siųsti naujus, žalingus pranešimus realiu laiku. MITM tipo atakos dažniausiai naudojamos, kai vyksta apsikeitimas viešais raktais , užpuolikas pateikia savo viešą raktą, taip apgaudamas sistemą ir prieidamas prie užšifruotų duomenų (Gumauskas, 2015).

Atsakomosios atakos (angl. *Replay attack*) – manipuliuojama interneto protokolo paketu, kuriame yra autentifikavimo duomenys su siuntėjo adresu. Toks protokolas persiunčiamas gaunamajai sistemai (Štitilis et al., 2009).

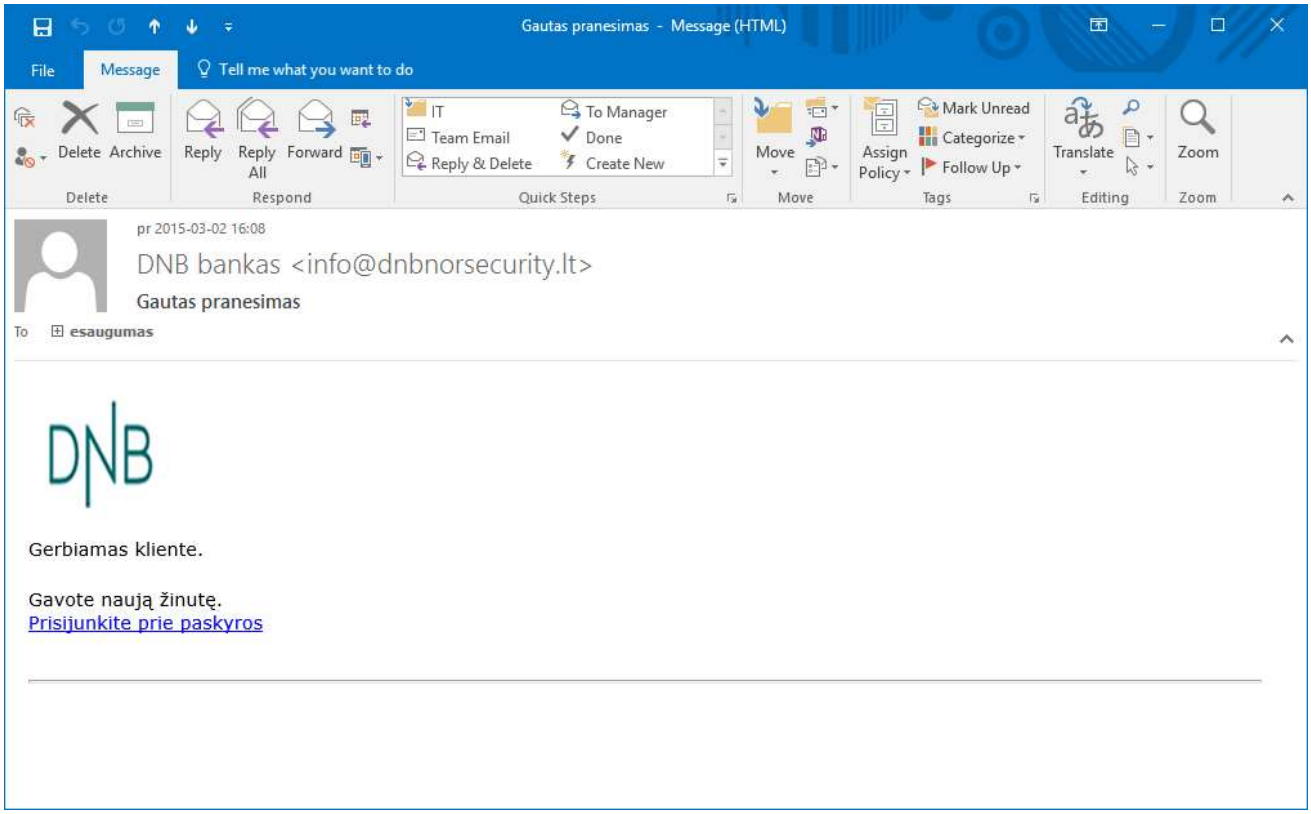
Slaptažodžio spėjimo ataka (angl. *Password Guessing attack*) Password – remiantis vartotojo nuspėjamumu bandoma atspėti jo slaptažodį.

Duomenų vagystės ataka (angl. *Phishing*) – tai tokia sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius bei kitus konfidencialius duomenis.

Dažniausiai tokio pobūdžio atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Vėliau tokiu būdu gauta informacija gali būti panaudota vykdant nusikalstamas veikas: neteisėtus prisijungimus prie informacinių sistemų, pinigų vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis kortelėmis (Phishing).

Paprastai ataka pradedama nuo elektroninio pašto laiškų, atrodančių taip, lyg jie būtų siunčiami banko ar kitos rimtos organizacijos. Laiško siuntėjo laukelyje esantis adresas dažniausiai būna netikras (falsifikuotas). Pavyzdžiui, laiške gali būti pranešama, kad sustabdytas vartotojo sąskaitos galiojimas, ir nurodoma, kad kol jis neužpildys tam tikrų duomenų pateiktoje anketoje, jo sąskaitos galiojimas nebus atnaujintas. Arba neva keičiantis aptarnavimo sistemai ar jos konfigūracijai reikia atnaujinti prisijungimo duomenis, todėl prašoma juos pateikti ir t.t. (Kaip veikia „phishing"?, 2017).

Žemiau pateiktame paveikslėlyje (žr. 3 pav.) galime pamatyti „Phishing“ laiško pavyzdį, kuriame vaizduojamas falsifikuotas „DNB“ banko elektroninis laiškas.



3 pav. „Phishing“ „DNB“ banko laiško pavyzdys

Šaltinis: „ „Phishing“ laiško pavyzdys“

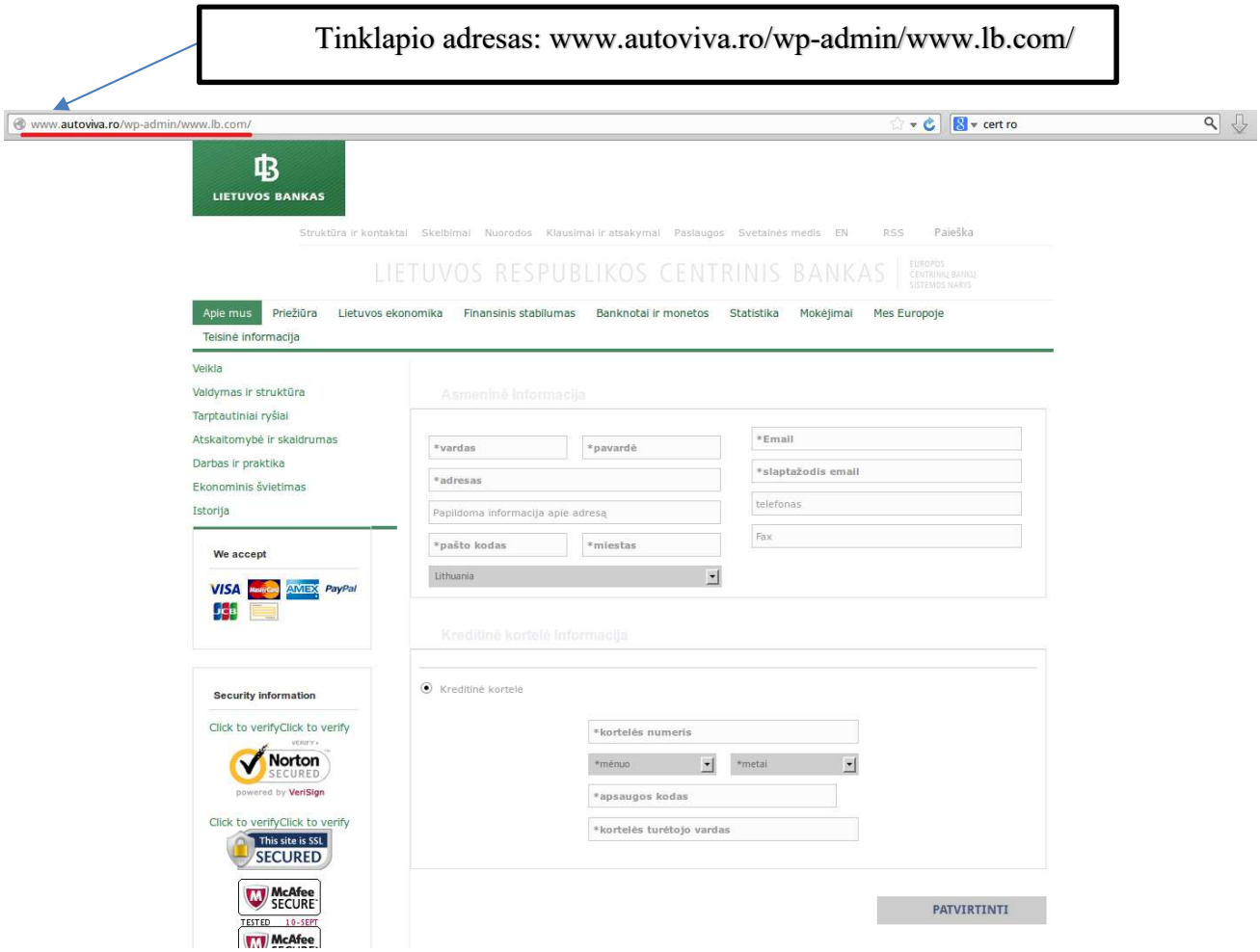
Laiškas taip pat gali turėti priedus su kenkėjiška programine įranga, atidarius, tokį priedą įsilaužėliai gali gauti prieigą į vartotojo sistemą.

Dažniausiai naudojami scenarijai:

1. Atsitiktiniams žmonėms išsiunčiamas elektroninis laiškas (toliau e. laiškas) banko vardu, kurio forma bei grafinis apipavidalinimas atrodo įtikinamai. Paprastai tokiame e. laiške yra parašyta prasimanyta priežastis kodėl vartotojas dėl vienokių ar kitokių priežasčių turėtų paspausti nurodytą nuorodą ir prisijungtų prie elektroninės bankininkystės. Vartotojas paspaudęs tokią nuorodą, patenka į suklastotą banko svetainę. Tokios svetainės dizainas gali nesiskirti nuo realios bankinės sistemos, tačiau tikrai skirsis jos interneto adresas – galbūt viena raide, galbūt vienu skaičiumi ar simboliu. Tokia svetainė nenaudos saugaus https (saugus užklausos - atsakymo protokolas, jungiantis klientą ir serverį) ryšio bei neturės galiojančio, banko vardu išduoto SSL (elektroninis dokumentas, padedantis klientams nustatyti svetainės tapatybę ir užšifruoti tarp kliento ir serverio siunčiamą informaciją.) sertifikato. Kitas žingsnis – prisijungimui bus reikalaujama ne vieno kodų kortelės kodo, bet,

tikėtina, visų. Taip yra todėl, kad net ir žinodami jūsų vartotojo vardą bei slaptažodį, nusikaltėliai negali prisijungti prie jūsų banko sąskaitos neturėdami jūsų kodų kortelės duomenų. Bankai prašo vartotojų įvesti vieną iš daugelio kodų bandant prisijungti prie elektroninės bankininkystės, o banko sistemos prašomas kodas bendru atveju parenkamas atsitiktiniu būdu - tai neleidžia nusikaltėliams nuspėti, kokio kodo reikės prisijungimui, todėl paprasčiausias sprendimas jų atžvilgiu paprašyti vartotojų įvesti visus kodus.

Žemiau pateiktame paveikslėlyje (žr. 4 pav.) galime pamatyti „Phishing“ tinklapio pavyzdį, kuriame vaizduojamas falsifikuotas „Lietuvos“ banko tinklapis.



4 pav. Lietuvos banko „Phishing“ tinklapio pavyzdys

Šaltinis: „ „Phishing“ tinklapio pavyzdys“

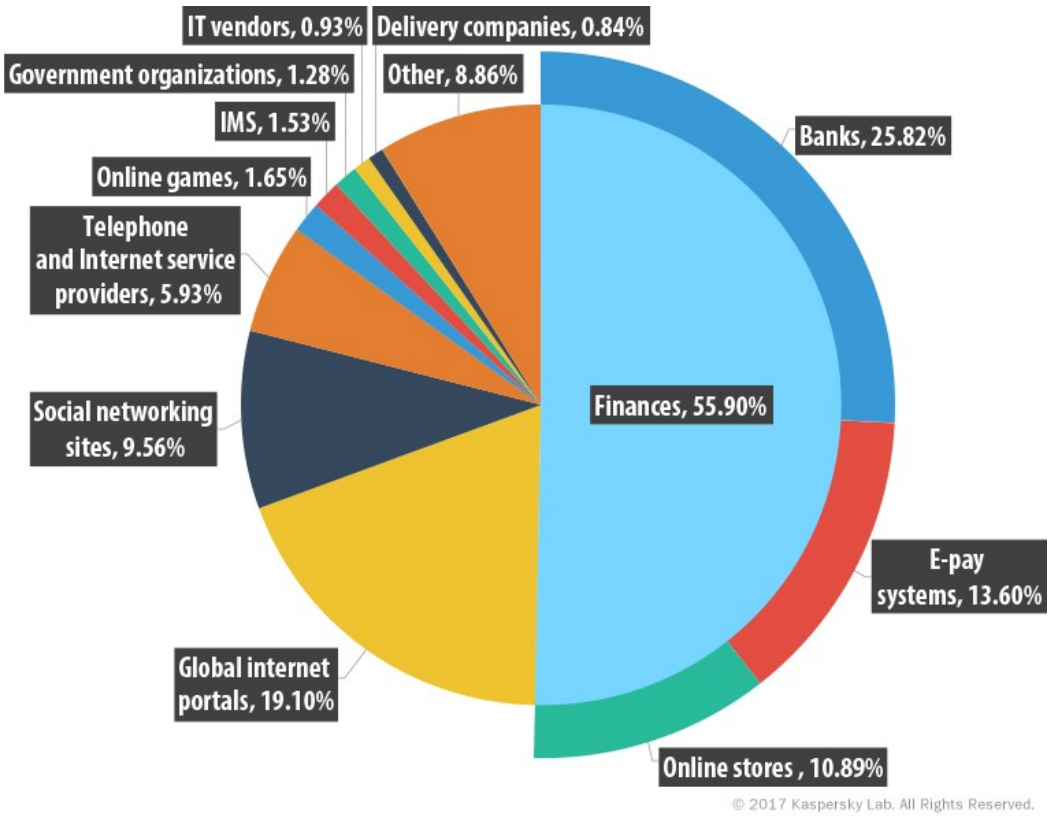
2. Atsitiktiniams žmonėms banko vardu išsiunčiamas įtikinamai atrodantis e. laiškas, kurio forma bei grafinis apipavidalinimas atrodo įtikinamai. E. laiške bus suformuluotas pretekstas prašymui, pvz., kvietimas dalyvauti klientų apklausoje. Norėdamas sudalyvauti apklausoje, vartotojas turi paspausti nuorodą, esančią e. laiške bei prisijungti prie suklastotos elektroninės bankininkystės sistemos tinklalapio. Scenarijus yra panašus į prieš tai esantį, tačiau, jo mintis

yra tokia – „dalyvavimui apklausoje“ reikia prisijungti prie banko, tam jūsų prašoma įvesti vartotojo vardą, slaptažodį bei vieną kodą iš kodų kortelės. Toks prisijungimas lyg ir nesukelia įtarimų, tačiau šio scenarijaus metu, suklastotas tinklalapis fone perduoda šiuos prisijungimo duomenis realiai banko sistemai. Vėliau būtų atvaizduojama „apklausa“, o atsakius į jos klausimus, jūsų būtų paprašyta įvesti dar vieną kodą iš kodų kortelės tam, kad būtų patvirtinamas jūsų dalyvavimas „apklausoje“. Viskas atrodo kaip realus darbas su banko sistema - vienas kodas prisijungimui, kitas kodas „dalyvavimui patvirtinti“, tačiau iš tikrųjų, antruoju kodu yra paprasčiausiai patvirtinamas pinigų pervedimas į kitą, nusikaltėlių kontroliuojamą, sąskaitą ir fone perduodamas realiai banko sistemai įvykdyti.

3. Atsitiktiniams žmonėms platinamos žinutės socialiniuose tinkluose arba susirašinėjimo programose. Žinutėje būna nurodyta nuoroda ir pretekstas jai paspausti. Pretekstas žinutėje priklauso nuo organizacijos kategorijos - finansinės paslaugos, elektroninė parduotuvė ir t.t.. Paspaudus nuorodą vartotojas bus nukreiptas suklastotą puslapį. Suklastotuose puslapiuose gali būti prašoma vartotojo, priklausomai nuo organizacijos kategorijos, įvesti:
    - Asmeninius duomenis– vardą, pavardę, adresą, telefoną, e. paštą ir t.t.;
    - Prisijungimo duomenis – vartotojo vardą ir slaptažodį, specialius prisijungimo kodus;
    - Banko kortelės duomenis – sąskaitos numerį, kortelės išdavimo ir galiojimo datą, kortelės patvirtinimo arba patvirtinimo vertės kodą (CVV/CVC).

„Phishing“ atakos neapima vien piktybinių laiškų, gaunamų tik per elektroninio pašto dėžutes pvz., „Gmail“, „Yahoo“ ir t.t.. „Phishing“ atakoms naudojamos visokio pobūdžio žinutės, platinamos socialiniuose tinkluose ar tiesioginio susirašinėjimo programose. Dauguma „phishing“ laiškų siuntėjų nežino tikslaus adresato. Sukčiai išsiunčia tūkstančius vienodo turinio žinučių ir tikisi, jog keli ar keliolika vartotojų „užkibs ant kabliuko“. Beasmenės žinutės tampa vienu iš pirmųjų pavojaus signalų. Atsakingi ir savo darbą išmanantys administratoriai nesiunčia tokių žinučių kaip „Gerbiamas kliente“ ar „Mielas pirkėjau“. Dažniausiai taip daro kibernetiniai sukčiai, apsimesdami banko, draudimo ar kitų svarbių įstaigų atstovais.

2017 metų pirmo ketvirčio „Kaspersky Lab“ atlikto tyrimo (žr. 5 pav.) organizacijų kategorijų diagramoje matome, kad daugiausiai „phishing“ atakų patiria finansinės organizacijos – 55,90%. Antroje vietoje yra visuotiniai interneto portalai (nespecializuoti), atakos sudaro 19.10%. Trečioje vietoje yra socialiniai tinklai, kuriuose „phishing“ atakų mąstas 9,56%.



5 pav. Organizacijų kategorijos kurias paveikė „Phishing“ atakos

Šaltinis: „Spam and phishing in Q1 2017“

6 lentelė. Pavojaus signalai įspėjantys apie „phishing“ ataką

Nr.	Pavojaus signalas
1	Beasmenė žinutė
2	Žinutė iš paslaugų teikėjo kurio paslaugomis niekada nesinaudojote
3	Laiške nurodytos neaiškios nuorodos
4	Laiške prisegti neaiškūs priedai (failai)
5	Įtartinas tinklapio adresas
6	Nenaudojamas „https“ protokolas

Šaltinis: „sudaryta autoriaus"

„**Spear–phishing“ ataka** – sudėtingesnė nei reguliari „phishing“ ataka, piktavaliai analizuoja potencialių aukų asmeninę informaciją ir pagal ją formuojamas „phishing“ laiškas. Tokie laiškai yra sunkiai identifikuojami naudojant „phishing“ filtrus.

Socialinė inžinerijos ataka – netechnologinis būdas įsilaužti į sistemą ar tinklą. Tai sistemos vartotojų apgavimo procesas, kai šie įtikinami atlikti veiksmus, naudingus programišiui, pavyzdžiui, suteikti informacijos, kuri padėtų įveikti ar apeiti saugumo mechanizmus. Socialinę inžineriją svarbu suprasti, nes programišiai šį metodą gali taikyti atakuodami žmogiškąjį sistemos elementą ir

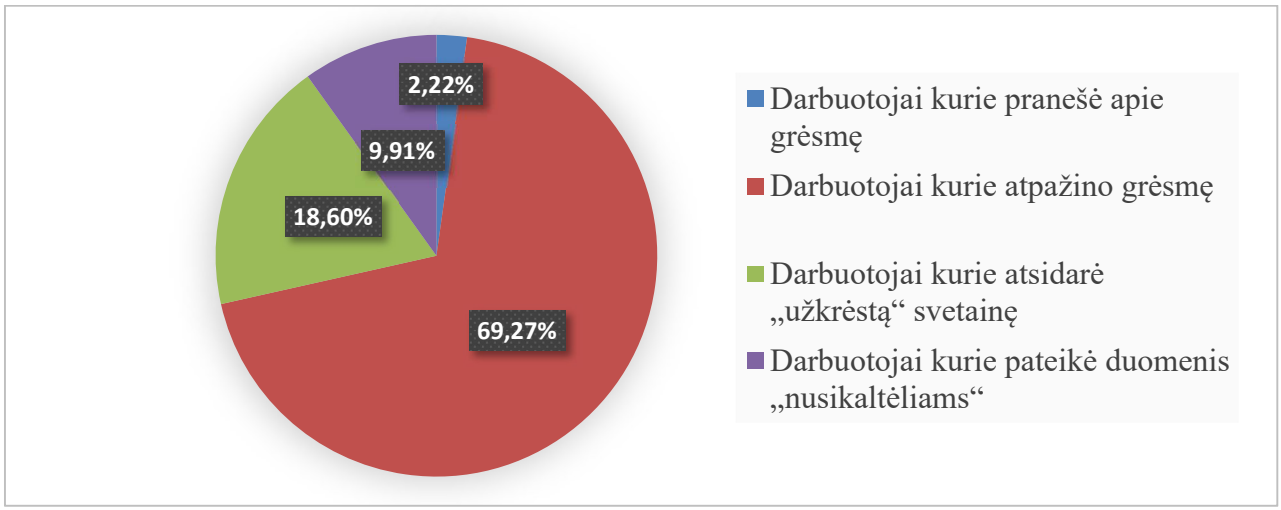
pergudrauti technines saugumo priemones. Šiuo metodu informacija gali būti renkama prieš ataką ar atakuojant. Socialinis inžinierius paprastai naudojasi telefonu ar internetu, kai bando apgauti žmones ir priversti juos atskleisti informaciją arba padaryti ką nors, kas prieštarauja organizacijos saugumo politikai. Socialiniai inžinieriai išnaudoja natūralų žmogaus polinkį pasitikėti kito žmogaus žodžiu, o ne ieško kompiuterio apsaugos spragų. Taigi vartotojai yra silpnoji vieta (Čenys ir Juknius, 2011).

Socialinės inžinerijos atakų tipai:

1. Socialinė inžinerija, kuri remiasi žmonėmis. Būdingas bendravimas su žmonėmis siekiant išgauti reikiamą informaciją, pavyzdžiui - apsimetama darbuotoju arba vartotoju, skambinama telefonu, žvilgčiojama per petį, naršoma šiukšlėse;
2. Socialinė inžinerija, kuri remiasi kompiuteriais. Bandoma išgauti norimą informaciją naudojantis programine įranga, pavyzdžiui - elektroninių laiškų priedai, netikri internetiniai puslapiai.

Atsižvelgiant į smarkiai augančią socialinės inžinerijos metodais pagrįstų kibernetinių atakų tendenciją, 2016 metų pabaigoje NKSC organizavo pratybas, kuomet kompiuteriais dirbančių darbuotojų pašto dėžutes pasiekė išgalvoti elektroniniai laiškai, siūlantys apsilankyti neegzistuojančios įmonės tinklalapyje. Šiomis pratybomis buvo siekiama įvertinti organizacijos darbuotojų įgūdžius pastebėti apgaulingus elektroninius laiškus ir reakciją į incidentą, o išanalizavus pratybų rezultatus – patikslinti organizacijos kompiuterių naudotojų švietimo kibernetinio saugumo klausimais programą. Nors didžioji dalis darbuotojų atpažino grėsmę, beveik trečdalis jų pasidavė socialine inžinerija pagrįstai kibernetinei atakai: apsilankė „užkrėstoje“ svetainėje ir (arba) pateikė duomenis „nusikaltėliams“ (2016 metų nacionalinio kibernetinio saugumo būklės ataskaita, 2017).

Kompiuterių naudotojų gebėjimai atpažinti žalingus laiškus atvaizduoti diagramoje (žr. 6 pav.).



6 pav. Kompiuterių naudotojų gebėjimai atpažinti žalingus laiškus

Šaltinis: „Sudaryta autoriaus pagal 2016 metų nacionalinio kibernetinio saugumo būklės ataskaita“

NKSC (Nacionalinio kibernetinio saugumo centro) vertinimu, didelė naudotojų dalis nesugeba įvertinti galimų savo veiksmų pasekmių ir nėra pasirengę atsisakyti jiems nemokamai siūlomų „dovanų“. Dėl to būtina nuolat šviesti darbuotojus, gerinti jų kibernetinio saugumo žinias, laiku perspėti apie kibernetinėje erdvėje tykančius pavojus ir grėsmių tendencijas.

Sekančioje temoje aptarsime 20 kritinės kontrolės priemonių, kurios padeda užtikrinti vartotojų asmens duomenų saugumą ir sumažinti kibernetinių incidentų riziką.

1.4. Kritinės kontrolės priemonės

Kritinės kontrolės priemonės (angl. *Critical Security Controls*) yra rekomenduojamų praktiškų saugumo priemonių rinkinys, kuris padeda organizacijoms atremti labiausiai paplitusias ir pavojingiausias kibernetines atakas.

Šis nemokamas, tarptautiniu mastu pripažįstamas ir naudojamas priemonių rinkinys yra sudarytas ir patvirtintas tarptautinės kibernetinio saugumo ekspertų bendruomenės. Kritinės saugos kontrolės priemonės nėra tiesiog dar vienas sąrašas priemonių, kurias organizacijos turėtų įgyvendinti. Tai - nuoseklus ir pagal svarbą suskirstytas priemonių rinkinys, kuris remiasi ir papildo kitas kibernetinio saugumo metodikas, tokias kaip NIST (Nacionalinis standartų ir technologijos institutas) kibernetinio saugumo metodika, US-CERT (JAV Reagavimo į kompiuterinio saugumo incidentus grupė) rekomendacijos bei kitos tarptautinės strategijos (5 kritinės saugos kontrolės priemonės norint išvengti 85 proc. kibernetinio saugumo spragų, 2015).

CIS informuoja apie faktinius išpuolius ir veiksmingą gynybą, atspindi bendrąsias ekspertų žinias (analitikų, technologų, pažeidžiamumo testuotojų, programuotojų ir kt.) daugelyje sektorių. CIS sąraše pateikiami geriausi gynybos būdai, siekiant užkirsti kelią kibernetiniams išpuoliams ar stebėti juos (The CIS Critical Security Controls for Effective Cyber Defense, 2016).

Kritinių saugos kontrolės priemonių tikslas – organizacijos informacijos saugumo stiprinimas. Kritinės kontrolės priemonės sumažina kibernetinio incidento riziką.

Kibernetinis incidentas – įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

CIS kontrolės priemonės vertinamos IT specialistų visame pasaulyje. Jas nuolat peržiūri ir atnaujina tarptautinė kibernetinio saugumo ekspertų bendruomenė, remdamasi realių atakų prieš privatųjį ir viešąjį sektorių duomenimis ir jų analize.

Žemiau pateiktoje lentelėje matome dvidešimt kritinės kontrolės priemonių.

7 *lentelė*. 20 kritinės kontrolės priemonių

Nr.	Kritinės kontrolės priemonė
1	Leistinų ir neatpažintų įrenginių inventorizavimas (angl. *Inventory of Authorized and Unauthorized Devices*)
2	Leistinos ir neleistinos naudoti programinės įrangos identifikavimas (angl. *Inventory of Authorized and Unauthorized Software*)
3	Techninės ir programinės įrangos saugios konfigūracijos mobiliuosiuose įrenginiuose, darbo vietos ar tarnybinėse stotyse numatymas (angl. *Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers*)
4	Nenutrūkstamas sistemų pažeidžiamumo vertinimas ir saugumo spragų taisymas (angl. *Continuous Vulnerability Assessment and Remediation*)
5	Naudojimosi administratoriaus teisėmis kontrolė (angl. *Controlled Use of Administrative Privileges*)
6	Audito žurnalų įrašų stebėjimas, analizė ir saugojimas (angl. *Maintenance, Monitoring and Analysis of Audit Logs*)
7	Elektroninio pašto ir naršyklių apsauga (angl. *Email and Web Browser Protections*)
8	Apsauga nuo kenkimo programų (angl. *Malware Defenses*)
9	Tinklo prievadų, protokolų ir paslaugų naudojimo apribojimai (angl. *Limitation and Control of Network Ports, Protocols and Services*)
10	Duomenų atkūrimo pajėgumas (angl. *Data Recovery Capability*)
11	Saugios tinklo įrenginių, tokių kaip saugasienės, maršruto parinktuvai, komutatoriai, konfigūracijos numatymas (angl. *Secure Configurations for Network Devices such as Firewalls, Routers and Switches*)
12	Tinklo perimetro apsauga (angl. *Boundary Defense*)
13	Duomenų apsauga (angl. *Data Protection*)
14	Prieigos kontrolė, paremta principu „būtina žinoti“ (angl. *Controlled Access Based on the Need to Know*)
15	Belaidės prieigos kontrolė (angl *Wireless Access Control*)
16	Naudotojų paskyrų stebėjimas ir kontrolė (angl. *Account Monitoring and Control*)

17	Saugumo srities gebėjimų vertinimas ir reikiamų mokymų numatymas (angl. *Security Skills Assessment and Appropriate Training to Fill Gaps*)
18	Taikomųjų programų saugumas (angl. *Application Software Security*)
19	Reagavimas į incidentus ir jų valdymas (angl. *Incident Response and Management*)
20	Bandymai įsilaužti ir „raudonųjų komandų“ pratybos (angl. *Penetration Tests and Red Team Exercises*)

Šaltinis: Nacionalinis kibernetinio saugumo centras, 2015

Apsaugos priemonių efektyvumas priklauso nuo to kaip joms pavyksta sumažinti riziką. Rizika mažinama dviem būdais: apsisaugojimas nuo atakos (išvengimas) ir pasekmių, po sėkmingos atakos, mažinimas (pastebėjus - atakos stabdymas, žalos įvertinimas). Kadangi atakos profilį numatyti yra sudėtinga, rekomenduojama taikyti keletą apsaugos priemonių, kurios būtų derinamos tarpusavyje. Toks saugumo priemonių sistemos kūrimo principas yra vadinamas gilia, nuoseklia gynyba (angl. *Defense-in-depth*).

20 kritinės kontrolės priemonių:

1. Leistinų ir neatpažintų įrenginių inventorizavimas. Aktyvus valdymas (inventorizavimas, stebėjimas ir taisymas) visų įrenginių esančių tinkle, kad prieiga būtų suteikiama tik leistiniems įrenginiams, o neatpažinti arba pažeidžiami neturėtų tokios galimybės.

Kriminalinės ar kitos suinteresuotos grupės nuolat skenuoja viešąją adresų erdvę siekdamos aptikti pažeidžiamus įrenginius (neatnaujinta programinė įranga, nauji nesukonfigūruoti įrenginiai), kuriuos galėtų išnaudoti. „BYOD“ (angl. *Bring your own device*) technologijų populiarėjimas sukelia dar didesnę riziką prijungti prie tinklo įrenginius, kurie yra nesaugūs. Net trumpam prijungtas įrenginys prie sistemos gali sukelti pavojų (Damkus, 2017).

Svarbu įdiegti automatizuotą tinklo dalyvių aptikimo įrankį, kuris atliktų preliminarią sistemų, prijungtų prie organizacijos tinklo, inventorizaciją. Tik žinomi įrenginiai gali būti prijungiami prie sistemos.

2. Leistinos ir neleistinos naudoti programinės įrangos identifikavimas. Aktyvus valdymas visos programinės įrangos esančios tinkle, kad būtų įdiegta ir naudojama tik autorizuota programinė įranga, o neleistina ir nevaldoma programinė įranga negalėtų būti įdiegiama arba naudojama.

Piktavaliai, stengdamiesi patekti į sistemą, ieško pažeidžiamos programinės įrangos, kurią būtų galima nuotoliniu būdu išnaudoti. Piktavaliai platina specialiu būdu parengtus žalingus failus ar nuorodas į užkrėstas svetaines. Kai nenusimąsčiusios aukos (vartotojai) pasiekia šį turinį, piktavaliai dažnai įdiegiant žalingą kodą ar programinę įrangą į vartotojo kompiuterį, kuris suteikia ilgalaikę sistemos kontrolę. Kai kurie piktavaliai gali naudoti „Nulinė diena“ (angl. *„Zero day“*)

pažeidžiamumą t. y. pažeidžiamumas kuriam programinės įrangos gamintojas dar nėra išleidęs jokio pataisymo (CIS Control 2 Inventory of Authorized and Unauthorized Software).

Nebūtinos darbui programinės įrangos veikimas sistemoje padidina riziką, jog ji bus neatnaujinta. Svarbu reguliariai vykdyti nežinomos programinės įrangos paiešką, ją aptikus pašalinti.

3. Techninės ir programinės įrangos saugios konfigūracijos mobiliuosiuose įrenginiuose, darbo vietos ar tarnybinėse stotyse numatymas. Naujos įrangos nustatymai yra specialiai pritaikyti „lengvai integracijai į tinklą“, o ne saugumui užtikrinti, todėl naudojami standartiniai slaptažodžiai (kuriuos galima sužinoti pagal įrenginio gamintoją), supaprastintos kontrolės priemonės, senesni protokolai, palikti atviri prievadai (angl. *ports*) ir servisai, instaliuota daug nereikalingų paprogramių ir įskiepių. Piktavaliai, žinodami šias potencialias įrangos ydas, pirmiausiai mėgina piktnaudžiauti prasta konfigūracija, siekdami prieiti prie tinklo įrenginių, programinės įrangos ar paslaugų.

Svarbu numatyti ir užtikrinti saugios konfigūracijos operacinės sistemos naudojimą: nereikalingų naudotojo paskyrų pašalinimą, nereikalingų servisų išjungimą, atnaujinimų diegimą, nereikalingų tinklo prievadų uždarymą ugniasienės naudojimą (angl. *firewall*) Administravimo teisės turi būti griežtai ribojamos ir suteikiamos tik žmonėms, kurie turi atitinkamų žinių ir yra įpareigoti dirbti su sistemų konfigūracijos pakeitimais. Tai padėtų valdyti neleistinos programinės įrangos diegimą ir naudojimą (The CIS Critical Security Controls for Effective Cyber Defense, 2016).

4. Nenutrūkstamas sistemų pažeidžiamumo vertinimas ir saugumo spragų taisymas. Kibernetinės gynybos specialistai turi stebėti naujausią informaciją susijusią su sistemų ir programinės įrangos atnaujinimais, tačiau „puolantieji“ (besistengiantys išnaudoti pažeidžiamumus) taip pat turi prieigą prie šios informacijos. Po pranešimų apie aptiktas spragas prasideda lenktynės, kuriose dalyvauja „puolantieji“, programinės įrangos gamintojai (besistengiantys sukurti ir išplatinti saugumo atnaujinimus) ir „gynėjai“ (besistengiantys įvertinti riziką, išbandyti saugumo priemones ir atnaujinti sistemas). Organizacijos neieškančios sistemos pažeidžiamumų, dirbančios su aptiktomis spragomis, rizikuoja sistemų saugumu (Damkus, 2017).

5. Naudojimosi administratoriaus teisėmis kontrolė. Administratorius yra asmuo, kuris gali atlikti keitimus kompiuteryje, kurie turės įtakos kitiems kompiuterio vartotojams. Administratoriai gali keisti saugos parametrus, įdiegti programinę įrangą ir aparatūrą, pasiekti visus failus kompiuteryje ir keisti kitų vartotojų paskyras. Norėdami prisijungti kaip administratorius, turite turėti kompiuteryje vartotojo paskyrą, kurios tipas administratorius (Kaip įeiti administratoriaus teisėmis?).

Piktavaliai gali išnaudoti naudotojus, kurie įprastiniam darbui naudojasi administratoriaus teises turinčiomią paskyrą. Pagrindinis tai leisiantis padaryti aspektas – visos naudotojo programos taip pat naudojasi aukšto lygmens leidimais, todėl failas kuris atidaromas iš atsiųsto elektroninio laiško arba perkeltas iš tinklapio, turi galimybę pasinaudoti programų ar operacinės sistemos pertekliniais leidimais (įterpti kenksmingą kodą, aktyvuoti reikiamas paslaugas ir pan.). Kitas būdas

pasinaudoti administratoriaus privilegijomis yra silpnų slaptažodžių atspėjimas-„nulaužimas“ arba programinių klaidų išnaudojimas (The CIS Critical Security Controls for Effective Cyber Defense, 2016).

Svarbu užtikrinti, kad administratoriaus privilegijos būtų griežtai kontroliuojamos ir suteikiamos tik esant būtinybei. Administratoriaus privilegijas turinčių paskyrų slaptažodžiai turi atitikti sudėtingus sudarymo reikalavimus (žiūrėti 1.2 temą).

6. Audito žurnalų įrašų stebėjimas, analizė ir saugojimas. Saugumo įrašų nekaupimas arba jų neanalizavimas leidžia piktavaliams sėkmingai vykdyti numatytus veiksmus apsisaugant nuo tyrėjų. Be audito įrašų darymo ataka gali tęstis be galo ilgai, o žala gali būti neatstatoma. Be tinkamai ir periodiškai atliekamos saugumo įrašų peržiūros galima apskritai neaptikti sėkmingų atakų.

7. Elektroninio pašto ir naršyklių apsauga. Svarbu naudoti- patikimą ir visada atnaujintą naršyklę, tinkamai sukonfiguruotą ir neturėti nepatikimų įskiepių. Populiariausios naršyklės naudojasi duomenų bazėmis kuriose yra pateiktas kenkėjiškų svetainių sąrašas, tai gali apsaugoti vartotoją nuo labiausiai paplitusių grėsmių. Vartotojai naršydami internete ir atidarinėdami elektroninių paštu atsiųstas nuotodas turėtų saugotis duomenų vagystės atakų (angl. *phishing*).

8. Apsauga nuo kenkimo programų. Kenkėjiška programa – tai bet kokio tipo programinė įranga, skirta - informacijos pasisavinimui, sistemos keitimui (modifikavimui) ar kompromitavimui (Oriyano, 2016).

Kenkėjiška programa gali greitai plisti ir keistis. Atakos vektoriumi gali tapti bet kas: įrenginiai, elektroniniai laiškai, tinklapiai, tinklo paslaugos, naudotojo veiksmai, informacijos laikmenos ir t.t. Modernus kodas sugeba vengti ir slėptis nuo apsaugos priemonių, jas pulti ar atjungti.

Turi būti taikomos automatinės apsaugos priemonės – antivirusinė ir antišnipinėjimo programinė įranga, ugniasienė, kurios visą laiką stebėtų veikiančių sistemų darbą. Sistemos nustatymuose būtina numatyti, jog draudžiama automatiškai paleisti įdėtos laikmenos ar prijungto įrenginio vykdomuosius failus (angl. *autorun*).

2016 metais pastebėta, kad lyginat su 2015 metais, Lietuvoje kelis kartus padidėjo bandymai įsilaužti į organizacijų tinklus pasinaudojant kompiuterių naudotojų naivumu ir jiems siunčiamuose laiškuose esančiomis nuorodomis nukreipti juos į užkratą turinčias svetaines, iš kurių šis užkratas automatiškai užkrečia naudotojų kompiuterius. Toks užkrato infiltravimo būdas yra itin efektyvus, tad artimiausioje ateityje ši metodika bus ir toliau naudojama piktavalių (2016 metų nacionalinio kibernetinio saugumo būklės ataskaita, 2017).

9. Tinklo prievadų, protokolų ir paslaugų naudojimo apribojimai. Piktavaliai ieško nuotoliniu būdu pasiekiamų tinklo paslaugų, kurios būtu pažeidžiamos ir jomis būtų galima pasinaudoti. Daugelis programinės įrangos paketų diegiant automatiškai įjungia daugelį paslaugų (angl. *services*),

kurios yra programinio paketo dalis, apie tai papildomai neinformuodami naudotojų ar administratorių.

Svarbu užtikrinti, kad kiekvienoje sistemoje būtų leidžiama veikti tik numatytiems (kurie yra reikalingi) protokolams, prievadams ir paslaugoms. Visos paslaugos turėtų būti reguliariai atnaujinamos, o nereikalingi sistemos komponentai šalinami.

10. Duomenų atkūrimo pajėgumas. Sėkmingos atakos rezultatas – vartotojų programinės įrangos ir konfigūracijos pokyčiai. Kibernetiniai nusikaltėliai gali sunai sunaikiniti arba pakeisti (jei buvo pažeistas duomenų vientisumas) informaciją. Jei vartotojas ar organizacija neturi patikimo ir greito būdo atkurti prarastą informaciją, jų gali laukti dideli finansiniai nuostoliai ir kiti nemalonumai išnaudojimas (The CIS Critical Security Controls for Effective Cyber Defense, 2016).

Svarbu užtikrinti galimybę daryti atsargines duomenų kopijas reguliariai. Jautrių duomenų kopijos turėtų būti daromos kuo dažniau. Siekiant kuo greitesnio sistemos darbo atkūrimo, gali būti daromos operacinės sistemos, aplikacijų ir duomenų kopijos. Taip pat svarbu reguliariai išbandyti padarytas duomenų kopijas ir užtikrinti, kad atsarginės kopijos yra tinkamai apsaugotos fizinio saugumo ir šifravimo priemonėmis.

11. Saugios tinklo įrenginių, tokių kaip saugasienės, maršruto parinktuvai, komutatoriai, konfigūracijos numatymas. Naujai įsigyta įranga būna pritaikyta lengvam jos prijungimui prie tinklo ir naudojimui, o ne saugumui. Toje įrangoje leidžiamas perteklinis skaičius paslaugų ir prievadų, sukurtos gamyklinės paskyros su standartiniais slaptažodžiais, nereikalingos ar reklaminės programinės įrangos diegimas. Piktavaliai gali nesunkiai sužinoti tinklo įrangos duomenis ir mėginti pasinaudoti standartiniais jos nustatymais. Tai gali tapti kritine saugumo spraga, jei įrenginiai nebuvo tinkamai paruošti. Pasinaudojus saugumo spragomis galima gauti neteisėtą prieigą prie tinklo resursų, nukreipti duomenų srautą per norimus įrenginius, perimti siunčiamus duomenis (Damkus, 2017).

12. *Tinklo perimetro apsauga*. Piktavaliai stengiasi aptikti ir išnaudoti prastai apsaugotas nutolusias sistemas, kurių perimetro apsaugos įrenginiai neuždraudžia neleistinos veiklos. Prasta perimetro apsauga gali reikšti, jog organizacijos duomenys, laikomi tarnybinėse ar darbo stotyse, gali būti pasisavinti ar pakeisti, o tinklo paslaugos išnaudotos neleistiniems veiksmams atlikti (Oriyano, 2016).

13. Duomenų apsauga. Duomenų saugumas – sudėtingas klausimas, kurio sprendimui reikalingas šifravimo, vientisumo apsaugos ir duomenų praradimo technologijų kombinavimas. Netinkamai apsaugoti duomenys gali būti prarasti perdavimo ar saugojimo metu, pavogtų ar pamestų įrenginių atveju, perdavimo trečiųjų šalių sistemoms būdu, dėl naudotojų klaidų ar saugumo politikų trūkumo. Organizacijos nesugebėjimas kontroliuoti jos kuriamos informacijos gali reikšti didžiulius nuostolius.

14. Prieigos kontrolė, paremta principu „būtina žinoti“. Organizacijos gali skirti nepakankamai dėmesio kritinės ir įprastinės informacijos ar prieigos identifikavimui ir atskyrimui. Jautrios sistemos (pvz., „SCADA“ – užtikrinančios fizinių sistemų valdymą) gali veikti toje pačioje terpėje kaip ir įprastos. Įsibrovėliams patekus į tinklą, tampa lengva sutrikdyti jautrių sistemų veiklą, pasisavinti kritinę informaciją. Tokiais atvejais, įprastinio tinklo apsaugos priemonių įveikimas reiškia ir prieigos prie fizinių sistemų valdymo praradimą. Žala gali neproporcingai išaugti.

15. Belaidės prieigos kontrolė. Itin pavojingi incidentai įvyko dėl atakuojančiųjų sėkmingo prisijungimo prie organizacijos tinklo apeinant perimetro apsaugos priemones (jungiantis per nesaugų wireless access pointą esantį organizacijos pastate). Keliaujančių organizacijos atstovų kompiuteriai apkrečiami kenksmingu kodu nesaugiuose tinkluose ar interneto kavinėse, o vėliau išnaudojami kaip „galinės durys“ (backdoor) į organizacijos tinklą. Didelį pavojų gali sukelti neleistinai prie organizacijos tinklo prijungti ir paslėpti bevieliai prieigos taškai (rogue access point). Bevielis ryšys itin pavojingas būtent dėl išnykusio poreikio fiziniam susijungimui – nesaugiu prisijungimu galima ilgai piktnaudžiauti ir gauti neribotą prieigą prie organizacijos tinklo. Užtikrinti, kad bevieliai įrenginiai, jungiami prie tinklo, atitinka patvirtintą saugumo konfigūraciją. Numatyti, jog tinklo pažeidžiamumų paieškos įrankiai atpažintų bevielio ryšio stoteles prijungtas prie fizinio tinklo. Atlikti aptiktų įrenginių analizę lyginant su leistinų įrenginių sąrašu (Damkus, 2017).

16. Naudotojų paskyrų stebėjimas ir kontrolė. Puolantieji gali aptikti ir išnaudoti anksčiau buvusias teisėtų naudotojų paskyras. Ankstesnių darbuotojų, testuotojų, pratybų dalyvių nekontroliuojamos paskyros, kurios nebuvo ištrintos ir išlaikė anksčiau joms suteiktas teises, gali būti išnaudotos gauti neteisėtai prieigai prie organizacijos tinklo ar duomenų.

Svarbu peržiūrėti sistemos paskyras ir ištrinti visas, kurios negali būti susietos su konkrečiais savininkais ar veiklos procesais (neaiškios paskirties).

17. Saugumo srities gebėjimų vertinimas ir reikiamų mokymų numatymas. Kibernetinis saugumas negali būti vertinimas vien tik techniniu pobūdžiu. Žmogiškasis faktorius turi reikšmingos įtakos visų sistemų naudojimui ir stebėjimui. Organizacijoje personalo kompetencija yra svarbi visuose lygmenyse - darbuotojai gali būti paveikti socialinės inžinerijos, administratoriai neatpažinti saugumo pažeidimo požymių, programuotojai gali palikti sisteminių klaidų, o vadovai neįvertinti saugumo poreikių ar neteisingai investuoti į saugumo priemones. Gerai paruoštas personalas itin sustiprina visas technines ir organizacines priemones taikomas organizacijoje, sumažėja kibernetinių incidentų rizika (The CIS Critical Security Controls for Effective Cyber Defense, 2016).

Svarbu įvertinti kokių žinių ir gebėjimų trūksta konkrečiai darbuotojų grupei, paruošti švietimo planą, vesti mokymus reikiamiems įgūdžiams sukurti. Nuolat papildyti mokymo programą įtraukiant naujausias grėsmes, apsaugos būdus ir kitą svarbią informaciją. Stebėti, kad numatytos naudotojų grupės reguliariai atnaujintu žinias.

18. Taikomųjų programų saugumas. Atakos gali išnaudoti pažeidžiamumus aptiktus internetinėje (angl. *web-based*) ir kitoje programinėje įrangoje.

Internetinė programinė įranga - tai bet kuri programa, turinti prieiga prie tinklo per http protokolą, o ne esanti įrenginio atmintyje (Web-Based Application).

Pažeidžiamumai gali slypėti programavimo klaidose, loginiuose sutrikimuose, reakcijose į netikėtas sąlygas. Pvz. nesugebėjimas patikrinti naudotojo įvesties dydžio; nesugebėjimas filtruoti nereikalingų, bet potencialiai piktybinių simbolių sekų iš įvesties srautų; prastas priskirtos atminties valdymas. Piktavaliai pasinaudodami šiais pažeidžiamumais gali atlikti įvairiausias atakas, populiariausios – „Buffer overflows“, „SQL injection attacks“, „Cross-site scripting“ (CIS Control 18 Application Software Security).

19. Reagavimas į incidentus ir jų valdymas. Kibernetiniai incidentai tapo kasdieniniu reiškiniu mūsų gyvenime. Jei reaguojama netinkamai, puolėjai gali padaryti daugiau žalos, pakartotinai užkrėsti sistemas, pagrobti daugiau duomenų.

Organizacijose svarbu užtikrinti, kad yra paruoštos reagavimo į incidentus procedūros, kurios apima užduočių paskirstymą personalui. Procedūros turi apibrėžti incidentų valdymo fazes. Nustatyti incidentų valdymo atsakomybę konkretiems specialistams. Rengti mokymus iš šviesti darbuotojus.

20. Bandymai įsilaužti ir „raudonųjų komandų“ pratybos. Gera gynyba reikalauja aiškios gynybos programos, techninio pasirengimo, gerų saugumo politikų įgyvendinimo ir valdymo, bei atitinkamo darbuotojų elgesio, todėl gyvenant nuolatinių pokyčių sąlygomis svarbu nuolat tikrinti savo gynybinį pajėgumą. Testavimas prasideda nuo pažeidžiamumų aptikimo ir įvertinimo. Realūs pavyzdžiai leidžia kritiškai vertinti pasirengimą atremti atakas.

Remiantis nacionalinio kibernetinio saugumo ataskaita, 2016 metais Lietuvoje įvyko keliolika rezonansinių kibernetinių išpuolių, NKSC fiksavo 3 kartus daugiau nei 2015 metais standartinėmis priemonėmis neaptinkamų kibernetinių incidentų organizacijų kompiuterių tinkluose, net 5 kartus suintensyvėjusią tinklų išorinio perimetro kibernetinę žvalgybą ir išaugusias grėsmes, susijusias su kompiuterių naudotojų apsilankymais žalingą kodą platinančiose užvaldytose interneto svetainėse. Didžioji dauguma incidentų kilo dėl elementarios kibernetinės higienos nesilaikymo, vadybos ir saugos standartų ar gerosios pasaulyje pripažintos praktikos bei naujai išleistų kibernetinio saugumo klausimus apibrėžiančių LR norminių aktų nesilaikymo. Pažymėtina, kad kaip ir 2015 metais, tik pavienės didelės organizacijos turėjo tinkamus ir pakankamus pajėgumus, galinčius valdyti kibernetiniam saugumui kylančias grėsmes.

Vartotojai pagal savo galimybes ir poreikius turėtų vadovautis rekomendacijomis norėdami užtikrinti duomenų – prieinamumą, konfidencialumą ir vientisumą.

2. PRAKTINIS APSAUGOS PRIEMONIŲ TAIKYMAS

2.1. Vartotojų autentifikavimo galimybės „Windows 10“ operacinėje sistemoje

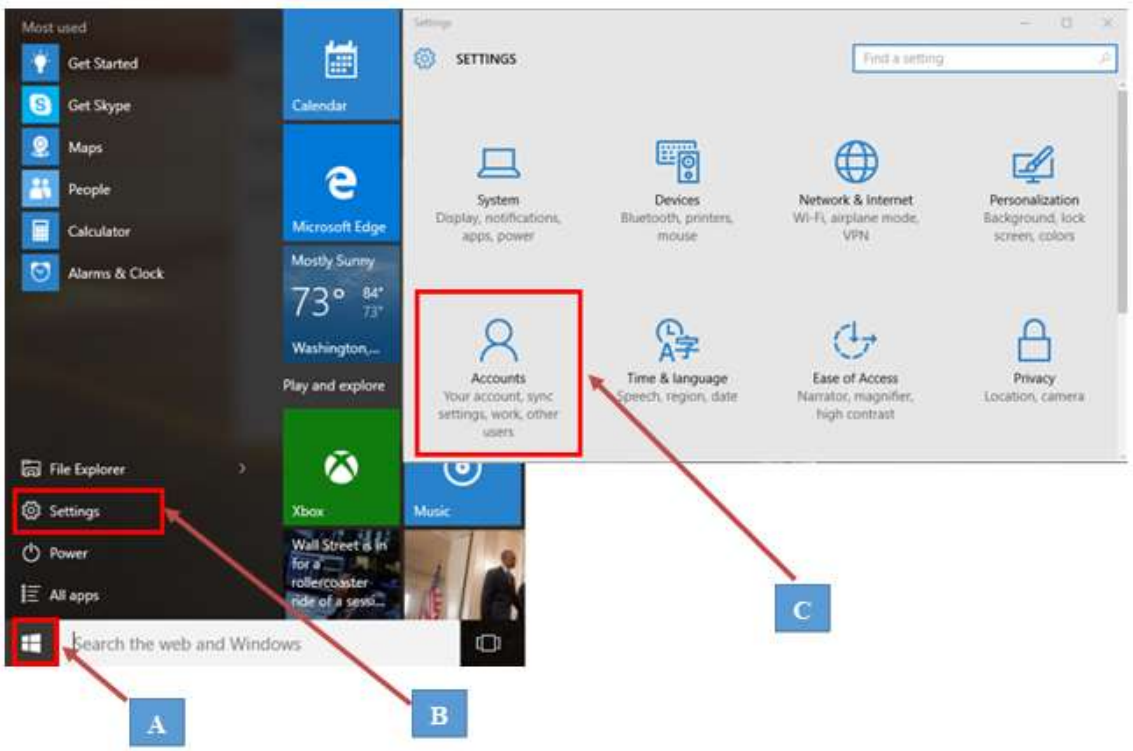
Daugelis žmonių siekdami išsaugoti savo privatumą ir nenorėdami, kad jų asmeninė informacija būtų prieinama visiems apriboja prieigą. Prieigos neturintys asmenys negalės naudotis asmeniniais duomenimis. Viena svarbiausių operacinės sistemos funkcijų yra saugumas.

„Windows 10“ operacinėje sistemoje vartotojai savo asmeninę paskyrą gali apsaugoti keliais būdais:

1. Slaptažodis;
2. PIN kodas;
3. Paveikslėlio slaptažodis;
4. „Windows Hello“ biometrinių duomenų atpažinimas.

Slaptažodis yra tradicinė ir seniausiai naudojama „Windows“ operacinėse sistemose vartotojo autentifikavimą patvirtinanti priemonė. Norint apsaugoti kompiuterį slaptažodžiu „Windows 10“ operacinėje sistemoje reikia atlikti tokius veiksmus:

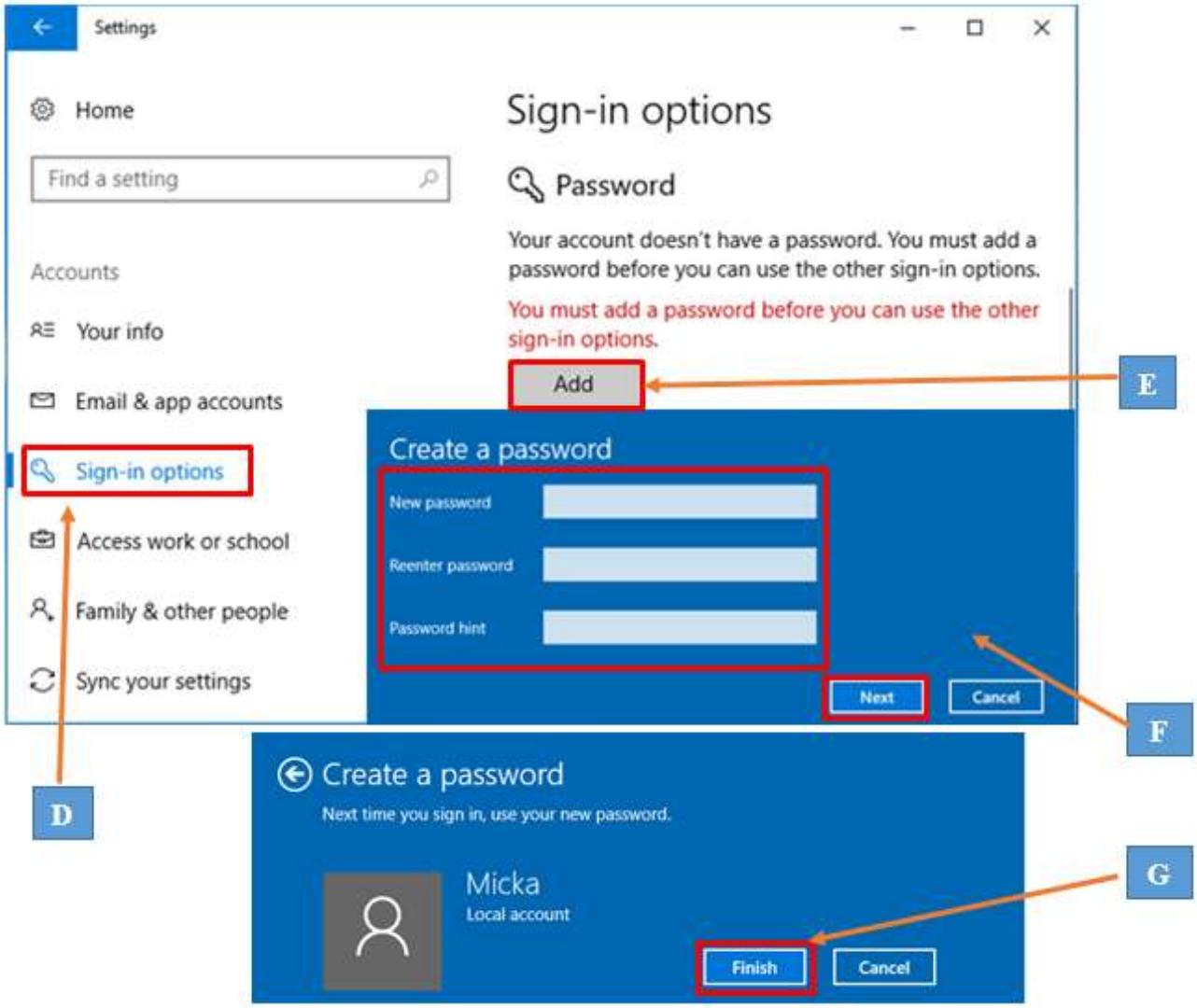
1. A) Spaudžiame „Pradžios meniu“ (angl. *Start menu*) – B) Atsiradusioje juostoje spaudžiame „Parametrai“ (angl. *Settings*) – C) Atsidariusiame „Parametrai“ lange spaudžiame „Paskyros“ (angl. *Accounts*).



7 pav. Paskyros nustatymų atidarymas

Šaltinis: „Sudaryta autoriaus“

2. D) Atsidariusiame „Paskyros parametrų“ lange pasirenkame „Prisijungimo parinktys“ (angl. *Sign-in options*) – E) „Prisijungimo parinktys“ skyriuje po „Slaptažodis“ (angl. *Password*) spaudžiame „Pridėti“ (angl. *Add*) – F) Atsiradusiame „Sukurti slaptažodį“ (angl. *Create a password*) lango laukelyje „Naujas slaptažodis“ (angl. *New password*) įvedame saugų slaptažodį, tuomet pakartotinai vėl įrašome tą patį slaptažodį į laukelį „vėl įvesti slaptažodį“ (angl. *Reenter password*) ir „Slaptažodžio užuomina“ (angl. *Password hint*) įvedame žodį arba žodžių junginį kuris primintų sukurtą slaptažodį, pavyzdžiui jeigu sukurtas slaptažodis „Ka!ė=dos“, slaptažodžio užuomina galėtų būti „Mėgstamiausia šventė“, ji turėtų priminti slaptažodį. Visa tai atlikus spaudžiame „Toliau“ (angl. *Next*) – G) Naujai atsiradusiame lange spaudžiame „Pabaigti“ (angl. *Finish*).



8 pav. Slaptažodžio sukūrimas

Šaltinis: „Sudaryta autoriaus“

Ankstesniame skyriuje jau aptarėme, kad svarbu laikytis saugaus slaptažodžio rekomendacijų. Slaptažodis turi būti sudarytas iš 8 - 10 ženklų, kuriuos sudaro raidžių didžiosios ir mažosios raidės, bei simboliai.

Kita „Windows 10“ operacinės sistemos vartotojo autentifikavimą patvirtinanti priemonė yra PIN kodas (Asmeninis identifikacijos numeris). PIN kodo autentifikavimo metodas yra lengviausias naudoti. Atitinkamame lange užtenka įvesti 4 PIN kodo skaitmenis. Norint galima sukurti ir sudėtingesnį PIN kodą kurį sudarytų daugiau nei keturi skaitmenys, taip pat būtų naudojami ženklai, kuriuos sudarytų raidžių didžiosios ir mažosios raidės, bei simboliai. Lengvas PIN kodas atrodytų taip „1575“, o sudėtingas „t7+98A!“.

Vienas svarbus skirtumas tarp slaptažodžio ir PIN, kad PIN yra susietas su konkrečiu įrenginiu, kuriame jis buvo nustatytas. Šis PIN yra nenaudingas vartotojui neturinčiam konkretaus įrenginio. PIN yra vietinis įrenginys. Slaptažodis perduodamas serveriui - jis gali būti perimtas perduodant arba pavogtas iš serverio. PIN kodas yra vietinis įrenginys - jis niekur neperduodamas ir nėra saugomas serveryje. Kai PIN yra sukurtas, jis nustato patikimus santykius su tapatybės teikėju ir sukuria asimetrinę raktų porą, kuri naudojama autentiškumui patvirtinti. Kai įvedate PIN kodą, jis atrakina autentiškumo patvirtinimo raktą ir naudoja raktą, norint pasirašyti užklausą, kuri siunčiama į autentifikavimo serverį.

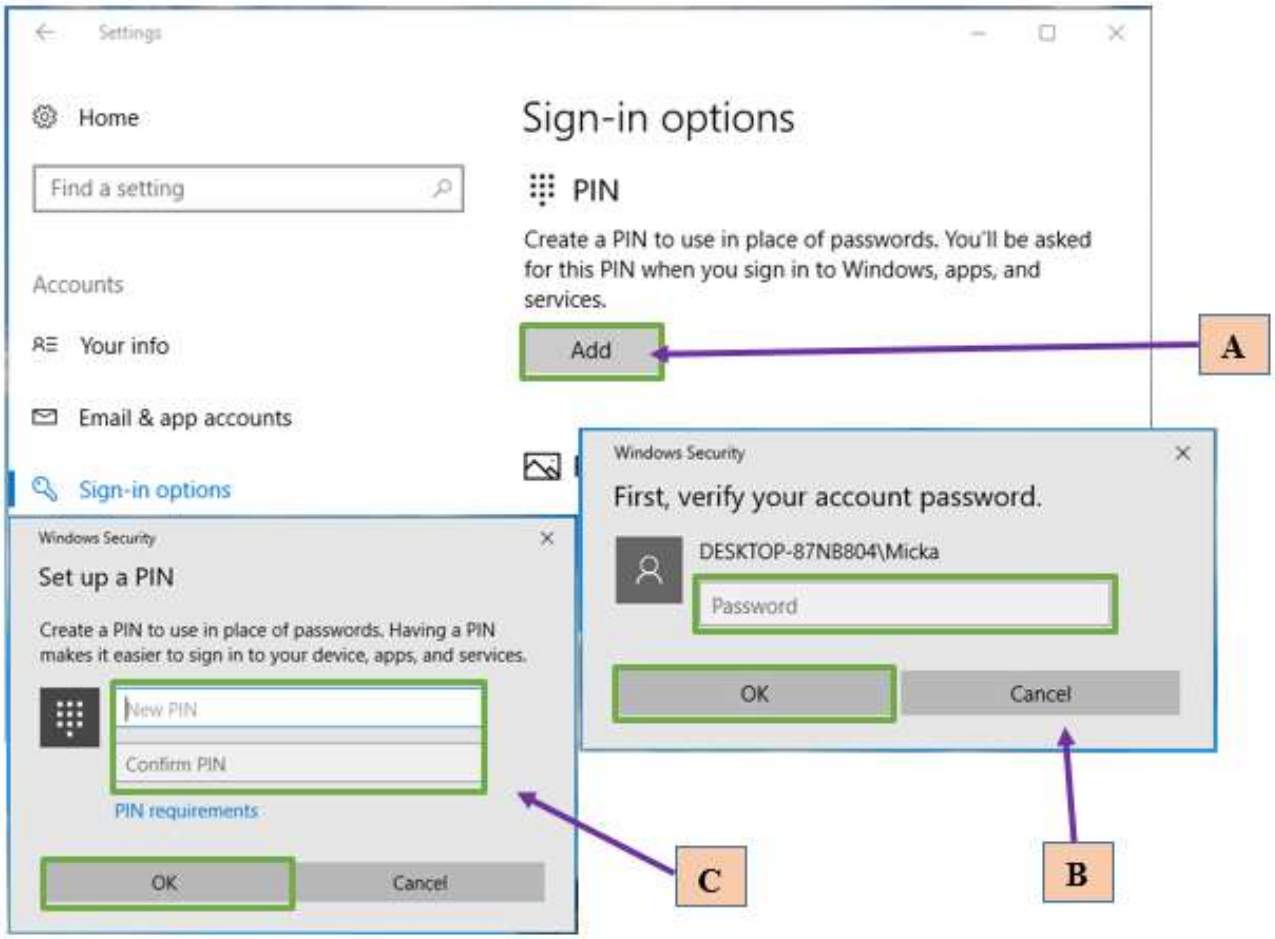
Pastaba. Norint naudotis kitomis prisijungimo galimybėmis, tokiomis kaip PIN kodu arba paveikslėlių slaptažodžiu reikia turėti susikūrus paskyros slaptažodį. Kaip tai padaryti yra aprašyta šios temos pradžioje.

Svarbu pažymėti, kad „Windows 10" PIN kodo naudojimas tai nėra slaptažodžio pakeitimas. Prisiregistravę prie „Microsoft“ paskyros nustatote savo PIN kodą naudodami savo vartotojo vardą ir slaptažodį. Tada sukuriate savo PIN kodą kaip papildomą autentifikavimą į savo „Microsoft“ paskyrą, gudrybė tame, kad PIN kodas veikia tik jūsų įrenginyje. Su fizine prieiga prie jūsų įrenginio mažai tikėtina, kad kenksmingas asmuo galės pasiekti jūsų paskyrą (Windows 10 says a PIN is more secure than a password. How?, 2015).

Norint apsaugoti kompiuterį PIN kodu „Windows 10“ operacinėje sistemoje reikia atlikti tokius veiksmus:

1. A) „Prisijungimo parinktys“ (angl. *Sign-in options*) skyriuje po „PIN“ (angl. *Personal Identification Number*) spaudžiame „Pridėti“ (angl. *Add*) – B) Atsiradusiame lange prašoma patvirtinti savo paskyros slaptažodį, įvedame savo paskyros slaptažodį ir spaudžiame „Gerai“ (angl. *OK*) – C) Naujai atsiradusiame lange įvedame savo sugalvotą PIN kodą „Naujas PIN“ (angl. *New PIN*) laukelyje, pakartotinai tą patį padarome „Patvirtinti PIN“ (angl. *Confirm PIN*) laukelyje ir spaudžiame „Gerai“ (angl. *OK*).

Pastaba. PIN kodo reikalavimuose yra nurodyta, kad PIN kodas mažiausiai gali būti keturių skaitmenų, taip pat negali visi skaitmenys kartotis arba sudaryti nuoseklios sekos, pavyzdžiui 1111, 12345 ir t.t.



9 pav. PIN kodo sukūrimas

Šaltinis: „Sudaryta autoriaus“

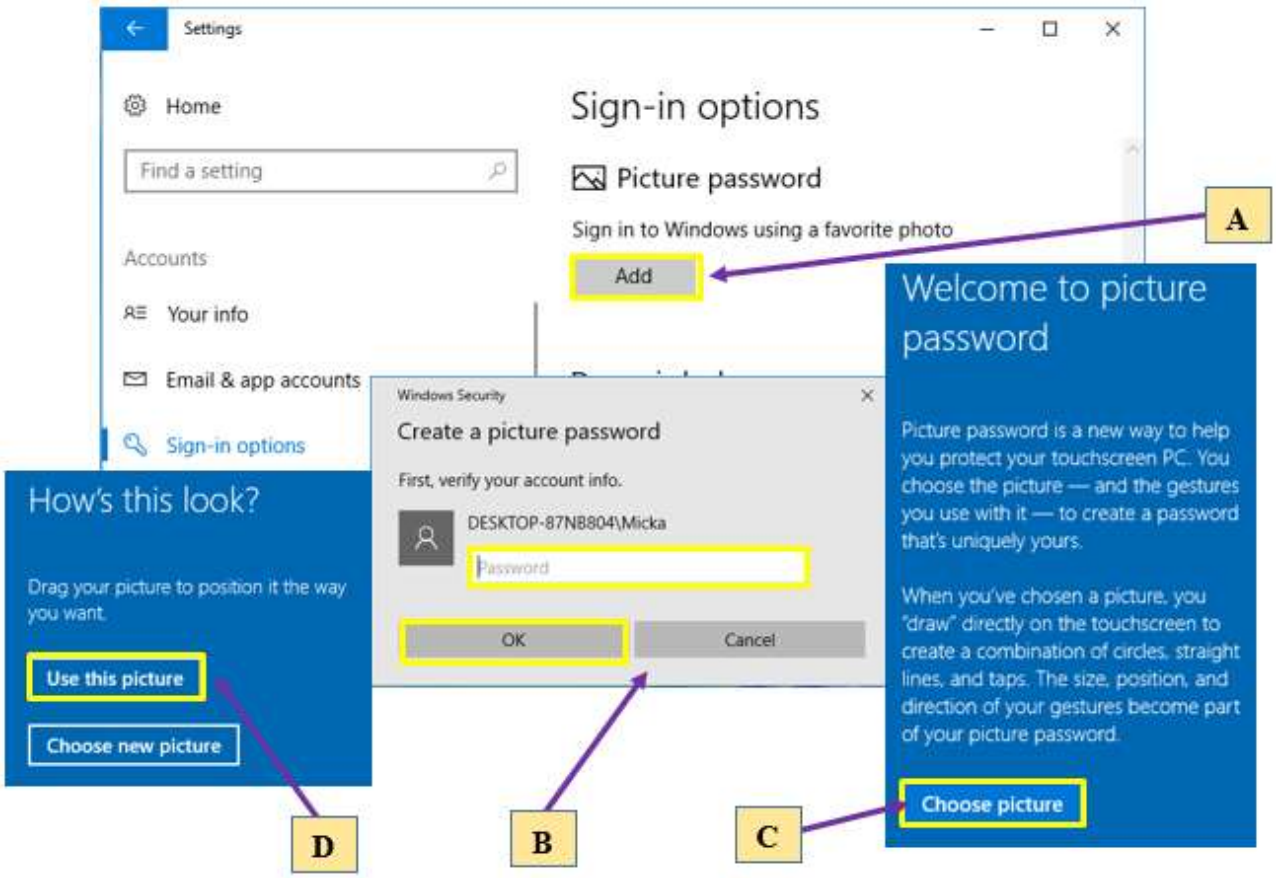
PIN kodo naudojimas yra greitesnis vartotojo autentifikavimo, nes užtenka įvesti tik keturis skaitmenis.

Sekanti „Windows 10“ operacinės sistemos vartotojo autentifikavimą patvirtinanti priemonė yra paveikslėlio slaptažodis.

Nuotraukų slaptažodis yra alternatyva įprastam slaptažodžiui arba PIN kodui kai prisijungiate prie „Windows 10“ sistemos. .Vartotojas gali prisijungti prie „Windows 10“ sistemos piešdamas figūras, paliesdamas reikiamus taškus arba atlikdamas reikiamus gestus iš anksto pasirinktoje nuotraukoje.

Norint apsaugoti kompiuterį paveikslėlio slaptažodžiu „Windows 10“ operacinėje sistemoje reikia atlikti tokius veiksmus:

1. A) „Prisijungimo parinktys“ (angl. *Sign-in options*) skyriuje po „Paveikslėlio slaptažodis“ (angl. Picture password) spaudžiame „Pridėti“ (angl. *Add*) – B) Atsiradusiame lange prašoma patvirtinti vartotojo identitetą, įvedame paskyros slaptažodį, ir spaudžiame „Gerai“ (angl. OK) – C) Naujai atsiradusiame mėlyno fono lange spaudžiame „Pasirinkti paveikslėlį“ (angl. *Choose picture*), vartotojas turi nevaržomą teisę iš savo turimų paveikslėlių (nuotraukų) pasirinkti jam patinkantį. – D) Pasirinkus norimą paveikslėlį, galime keisti jo išsidėstymo poziciją ekrane, kadangi paveikslėlis nėra absoliučiai visas atvaizduojamas ekrane. Nustačius paveikslėlio poziciją ekrane spaudžiame „Naudoti šį paveikslėlį“ (angl. *Use this picture*).



10 pav. Paveikslėlio slaptažodžio kūrimas (I)

Šaltinis: „Sudaryta autoriaus“

2. E) Mūsų pasirinktame paveikslėlyje turime užfiksuoti tris gestus. Galimos trys gestų variacijos- linija, taškas ir apskritimas. Kokius gestus naudoti pasirenka vartotojas, pavyzdžiui linija, linija ir apskritimas. Gestai gali kartotis ir būti naudojami bet kokia tvarka. Gestų išdėstymą paveikslėlyje taip pat pasirenka vartotojas. Dešinėje lango pusėje matome kelintą gestą atliekame- pirmą, antrą ar trečią. Užfiksavus tris gestus paveikslėlyje, procedūrą pakartojame dar kartą (sistema patvirtina ar tiksliai atkartojote gestus), jeigu antrą kartą nepavyko atkartoti gestų identiškų pirmajam, tuomet sistema nurodo vėl pakartoti procedūrą

kol pirmojo ir antrojo gestų užfiksavimo rezultatai sutampa. – D) Sistemai patvirtinus sėkmingą gestų užšifravimą paveikslėlyje naujai atsiradusioje lentelėje spaudžiame „Baigti“ (angl. *Finish*).

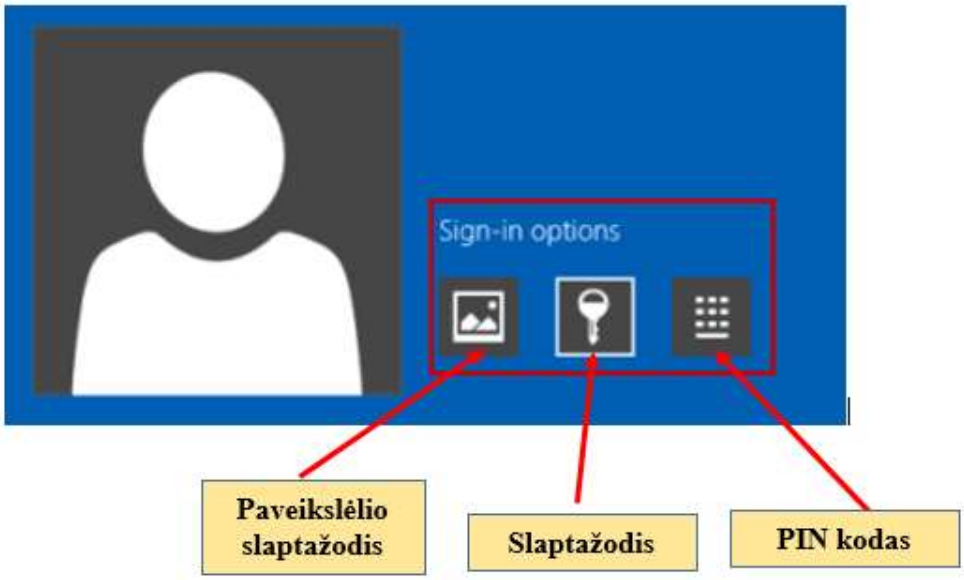
11 pav. Paveikslėlio slaptažodžio kūrimas (II)

Šaltinis: „Sudaryta autoriaus“

Paveikslėlio slaptažodžiai yra tokie pat saugūs kaip PIN kodas. Duomenys yra susieti su įrenginiu, todėl kažkas turi turėti jūsų įrenginį, kad juo galėtų panaudoti. Paveikslėlio slaptažodžio vartotojo autentifikavimo funkcija patogu naudotis įrenginiuose su jutikliniu ekranu, tuomet nebūtina naudoti kompiuterio pelės. Reikia nepamiršti, jeigu naudojate lietimui jautrų ekraną, kad piešimo gestai palieka riebalų ir kitas žymes. Tinkamoje šviesoje esant tinkamam kampui, kažkas gali sugebėti iššifruoti savo gestus, tačiau greitas ekrano nuvalymas po paveikslėlio slaptažodžio panaudojimo turėtų padėti išspręsti šį trūkumą.

Nuotraukų slaptažodžis ir PIN kodas nėra skirti papildomam saugumo lygiui. Vartotojas norėdamas prisijungti prie „Windows10“ sistemos, visada gali pasirinkti norimą autentifikavimo būdą, pavyzdžiui naudoti įprastą slaptažodį, o ne paveikslėlio slaptažodį ar PIN kodą, kurį nustatė.

Žemiau pateiktame paveikslėlyje (žr. 12 pav.) matome vartotojo autentifikavimo pasirinkimo būdus „Windows 10“ sistemoje.



12 pav. Vartotojo autentifikavimo pasirinkimo būdai „Windows 10“ sistemoje

Šaltinis: „Sudaryta autoriaus“

Vartotojai norėdami užtikrinti savo asmeninių duomenų konfidencialumą ir apriboti prieigą nuo neteisėto prisijungimo prie „Windows 10“ operacinės sistemos, naudojasi autentifikavimo funkcija. Kurį autentifikavimo metodą naudos vartotojas yra jo asmeninis pasirinkimas.

Sekančioje temoje aptarsime „Facebook“ socialinio tinklo vartotojų teisę ir galimybę viešinti savo privačius duomenis, kokios rizikos gali kilti dalinantis savo asmenine informacija su trečiaisiais asmenimis.

2.2. Asmens duomenų saugumas „Facebook“ socialiniame tinkle

Socialinis tinklas – interaktyvi interneto struktūra (interneto svetainė) vienijanti tam tikrą, bendrų interesų turinčią narių grupę, kuri ir kuria konkrečios svetainės turinį ir virtualiai bendrauja tarpusavyje, automatizuotomis konkrečios svetainės priemonėmis. Socialiniai (interneto) tinklai – paskutiniu metu aktyviai besivystanti interneto dalis, kuriai galima priskirti tiek paprastus diskusijų forumus, tiek sudėtingus visuomeninius ir (ar) komercinius interneto projektus (15min, Socialinis tinklas).

Socialinis tinklas – interneto bendruomenė, turinti bendrų interesų, kurie naudoja svetainę ar kitas technologijas, kad bendrautų vieni su kitais ir dalytųsi informacija, ištekliais ir t.t: Svetainė ar internetinė paslauga, kuri palengvina šį bendravimą (Social network, 2017).

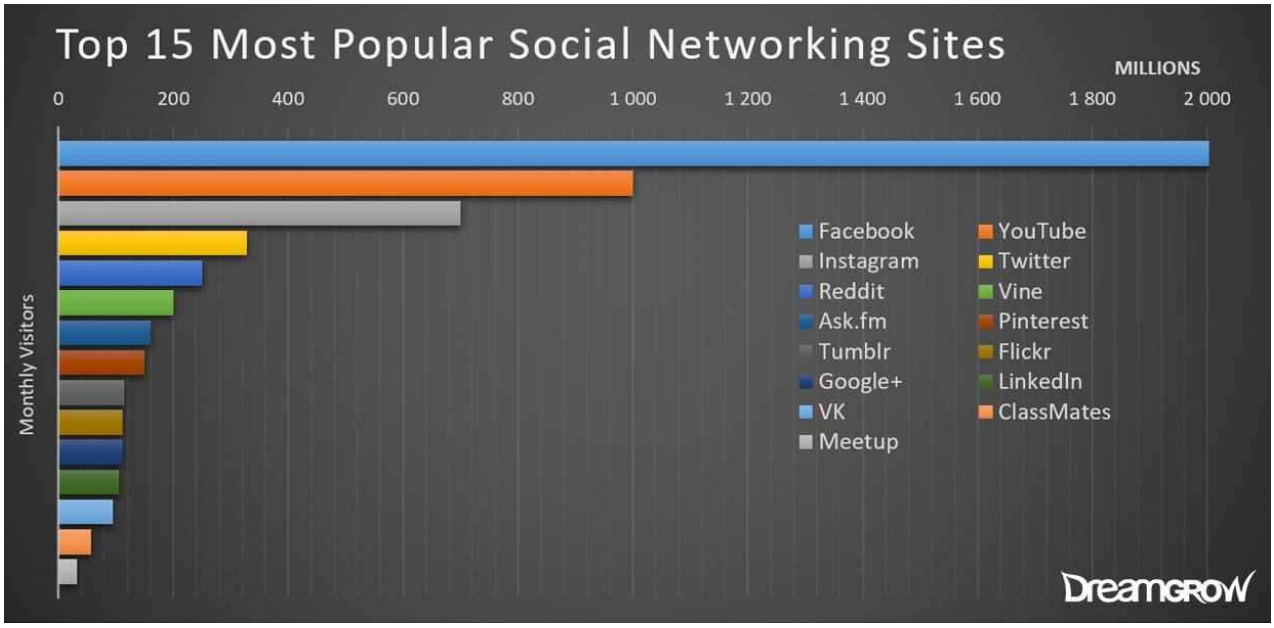
Socialinius tinklus galima apibrėžti kaip tam tikrą internetinę paskyrą, kurioje žmonės susikuria profilius, bendrauja su kitais žmonėmis, keičiasi informacija, pramogauja, žaidžia žaidimus ir kitaip dalyvauja virtualiame socialiniame gyvenime. Žmonių sukurti profiliai socialiniuose

tinkluose gali būti vieši, pusiau vieši ar privatūs, tai dažniausiai priklauso tiek nuo pačio socialinio tinklalapio reglamentuojamų taisyklių tiek ir nuo žmogaus poreikių ar jis nori būti visiems matomas, ar tik savo kontaktų sąraše esantiems žmonėms. Turbūt vienas iš didžiausių socialinių tinklų privalumų yra tai, kad jie padaro pasaulį atviresniu ir labiau sujungtu, čia pradingsta ne tik atstumai tarp žmonių, bet ir laikas, nes vartotojai gali komunikuoti su kitais žmonėmis realiuoju laiku nors jie tuo metu ir yra visai kitoje pasaulio pusėje (Zaidieh, 2012).

Pagrindinis socialinio tinklo tikslas – palaikyti ryšius tarp asmenų priklausančių tam tinklui.

Internetiniu adresu www.facebook.com randamas socialinio bendravimo tinklalapis, kuris leidžia registruotiems vartotojams kurti profilius, įkelti nuotraukas, filmuotą medžiagą. Taip pat bendrauti su kitais tinklo vartotojais asmeninėmis arba viešomis žinutėmis. Tinklalapis įkurtas 2004-aisiais vietiniu lygiu, o po dvejų metų tapo prieinamas visiems. 2012-aisiais „Facebook“ jau turėjo milijardą originalių vartotojų. Tinklalapio populiarumą lėmė jo visapusiškumas. Jame galima žaisti žaidimus, kurti dienoraščius, dalintis, bendrauti, registruoti savo gyvenimo įvykius, sekti kitus.

„Facebook“ socialinio tinklo įkūrėjas ir generalinis direktorius Markas Zuckerbergas savo „Facebook“ paskyroje 2017 metų liepos 27 dieną paskelbė „ Nuo šio ryto „Facebook“ bendruomenėje dabar oficialiai yra 2 milijardai žmonių! Siekdami sujungti pasaulį, darome pažangą, o dabar pasistenkime dar labiau suartinti pasaulį. Būti šioje kelionėje kartu su jumis yra didelė garbė“. „Facebook“ yra populiariausias socialinis tinklas pasaulyje, kurio mėnesio aktyvių vartotojų skaičius 2 milijardai. Tai reiškia, kad daugiau nei ketvirtadalis pasaulio gyventojų yra šiame socialiniame tinkle. Žemiau esančiame paveikslėlyje (žr. 13 pav.) matome pavaizduotą grafiką kuris parodo 15 populiariausių socialinių tinklų puslapių išdėstytų pagal vartotojų mėnesinį lankomumą. „Facebook“, „Youtube“ ir „Instagram“ užima lyderio pozicijas.



13 pav. 15 populiariausių socialinių tinklų

Šaltinis: Top 15 Most Popular Social Networking Sites and Apps, 2017

„Kantar TNS“ duomenimis, „Facebook“ naudojasi beveik pusė Lietuvos gyventojų (45 proc.).

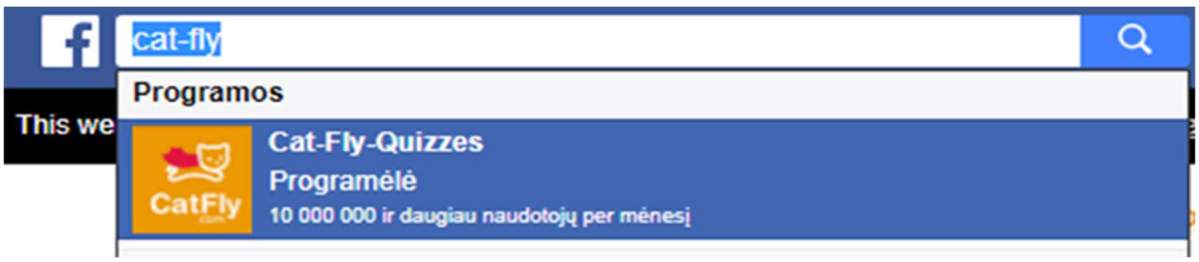
„Facebook“ socialinis tinklas yra išskirtinis, nes pakeitė žmonių bendravimo metodus, kurie apima kasdieninį asmeninį bendravimą, reklamą, pažinimą, požiūrį į santykius ir žmonių grupes. Išskirtinumas slypi tame, kad su socialinių tinklų atėjimu nyksta tradicinis žmogaus bendravimas su žmogumi. „Facebook“ tinkle dalijamasi turiniu, kuris dar prieš porą dešimčių metų būtų buvęs privatus, skirtas tik artimiausiems žmogų supančio rato nariams matyti.

Žmogus pats nusprendžia, ar jis nori registruotis socialiniame tinkle, ar ne, o užsiregistravęs – kiek privačios informacijos paviešinti. Taigi žmogus, siekdamas neatskleisti jokios privačios informacijos, turėtų iš viso nesiregistruoti socialiniuose tinkluose. Jei žmogus nusprendžia užsiregistruoti, tačiau nenori skelbti daug privačios informacijos, jis turėtų socialinio tinklo valdytojui pateikti tik minimalios apimties informaciją (Gyvenimas tinkle: liga ar trūkstamo dėmesio kompensacija?, 2013).

Dažnas atvejis kai patys vartotojai nesaugo savo duomenų ir privatumo, skelbdami neribotą kiekį, neribotos informacijos apie save ir savo aplinką.

Reikia nepamiršti, kad „Facebook“ socialinis tinklas yra platforma suteikianti galimybę veikti trečiųjų šalių programėlėms, dar vadinamomis aplikacijomis.

„Facebook“ aplikacijos – tai programos, kurios veikia „Facebook“ aplinkoje, naudoja šio socialinio tinklo funkcijas ir gali būti dviejų rūšių – tos, kurias sukūrė pats „Facebook“ – įvykiai, grupės, nuotraukos, pasiūlymai ir t.t. ir tos, kurias sukūrė trečiosios šalys. „Facebook“ socialiniame tinkle yra tūkstančiai programėlių sukurtų trečiųjų šalių. Žemiau pateiktame paveikslėlyje (žr. 14 pav.) matome programėlę „CatFly“, tai yra viktorinos (angl. Q*uiz*) tipo programėlė turinti virš dešimt milijonų aktyvių vartotojų per mėnesį.



14 pav. „CatFly“ programėlės vartotojų skaičius

Šaltinis: „Sudaryta autoriaus“

Vartotojai norintys naudotis „Facebook“ trečiųjų šalių programėlėmis turi autentifikuoti save pateikdami savo asmeninę informaciją.

Maksimalų asmeninių duomenų sąrašą sudaro:

1. Viešasis profilis (būtina);
2. Draugų sąrašas;

3. El. paštas;
4. „Pasidalinimai sienoje“ (angl. *Timeline posts*);
5. Gimtadienis;
6. Nuotraukos;
7. Pomėgiai.

Šių duomenų prašo trečiųjų šalių programėlės, duomenų sąrašas gali kisti individualiai – vienur prašoma mažiau domenų, kitur daugiau. Prašomas duomenų kiekis priklauso nuo trečiosios šalies programėlės.

Žemiau pateiktame paveikslėlyje (žr. 15 pav.) matome „CatFly“ programėlės vartotojo patvirtinimo langą, kuriame atliekamas autentifikavimas.

15 pav. Vartotojo patvirtinimas „CatFly“ programėlėje

Šaltinis: „Sudaryta autoriaus“

Neatlikus pateikiamų duomenų redagavimo trečiųjų šalių programėlės „pasiima“ maksimalų nurodytą duomenų kiekį.

„CatFly“ privatumo politikoje nurodoma, kad „Siekdami personalizuoti, tobulinti ir tęsti paslaugų naudojimą, svetainė renka, apdoroja ir naudoja vartotojo naudojamus duomenis, leidžiančius tinklalapiui įvertinti jo turinį (pvz. kokias nuorodas vartotojas spaudžia, kokią informaciją jis perduoda per el. paštą ar socialinę žiniasklaidą), naudojamas paslaugas ir bendravimo

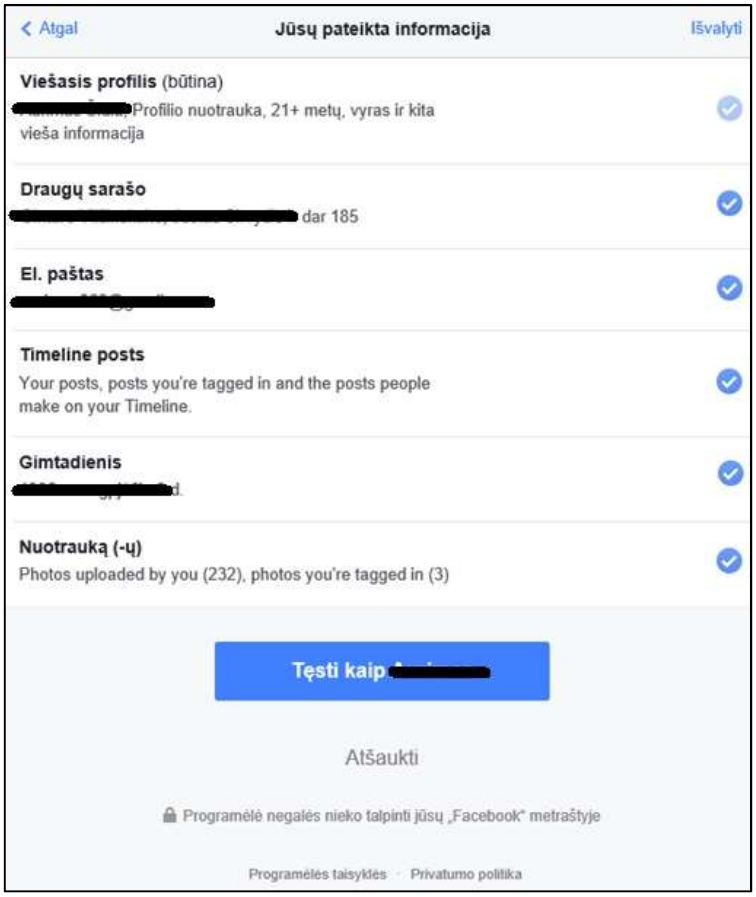
duomenis“(Privatumo politikos 2.3 p.). „Tais atvejais, kai vartotojas registruojasi ir prisijungia prie paslaugos per trečiąją šalį „Facebook“ – vartotojas suteikia tinklalapiui teisę susipažinti su visais jo „Facebook“ prieinamais duomenimis ir naudoti juos: viešąjį profilį, nuotraukas, draugų sąrašą, el. pašto adresą ir „patinka“ (angl. *Like*), komentarais, pasidalinta informacija (3.3 p) (Catfly privatumo politika, 2017).

Žemiau pateiktame paveikslėlyje „Jūsų pateikta informacija“ (žr. 16 pav.) matome „CatFly“ programėlės prašomų vartotojo duomenų sąrašą.

„CatFly“ programėlės maksimalus prašomas asmeninių duomenų sąrašas:

1. Viešasis profilis (būtina);
2. Draugų sąrašas;
3. El. paštas;
4. „Pasidalinimai sienoje“ (angl. *Timeline posts*);
5. Gimtadienis;
6. Nuotraukos;

Norint naudotis paslauga būtina pateikti viešojo profilio duomenis, kuriuos sudaro – vartotojo nuotrauka, amžius, lytis ir kita vieša informacija, kitaip trečioji šalis neteiks paslaugos.



16 pav. Vartotojo teikiamos informacijos redagavimas „CatFly“ programėlėje

Šaltinis: „Sudaryta autoriaus“

Facebook vartotojai kartais dėl neatidumo, kartais tiesiog dėl nežinojimo arba apatijos atiduoda maksimalius savo asmeninius duomenų kiekius trečiųjų šalių programėlėms.

Sutikimas su visomis svetainių sąlygomis (privatumo politika ir paslaugų teikimo taisyklėmis) išreiškiamas prisijungimu prie svetainės. Tai reiškia, kad jeigu vartotojas naudojasi svetainės paslaugomis, jis besąlygiškai sutinka su visomis nurodytomis sąlygomis.

„CatFly“ tinklapio privatumo politikoje skelbiama, kad visas turinys yra skirtas tik maloniam laiko praleidimui arba pramoginiams tikslams. Be to, pabrėžiama, kad ši paslauga nemokama. Ši svetainės nereikalauja pervesti ar kitaip sumokėti tam tikrą mokestį, tačiau, ar tai nereiškia, kad vartotojas „sumoka“, leisdamas pasinaudoti savo asmens duomenimis.

Rekomendacijos, kokių veiksmų reiktų imtis norint geriau užtikrinti savo asmenių duomenų apsaugą:

1. Nesidalinti su „Facebook“ informacija, kuri nutekinimo atveju galėtų padaryti žalos.
2. Įvertinti svetainės patikimumą prieš „atiduodant“ jai savo asmeninius duomenis naudojantis „Facebook“ autentifikavimo funkcija.
3. Perskaityti svetainės privatumo politiką ir paslaugų teikimo taisykles, prieš prisijungiant prie jos, naudojant „Facebook“ identifikacijos duomenis. Taisyklėse atkreipti dėmesį - kokiems tikslams svetainė naudoja asmeninius vartotojo duomenis, bei koks jų saugojimo/tvarkymo laikotarpis; ar asmens duomenų valdytojas užtikrina vartotojų asmens duomenų saugumą; kokios svetainės privatumo politikos ir paslaugų teikimo taisyklių keitimo sąlygos ir vartotojo informavimo būdai jas pakeitus; kokia atsakomybė tenka svetainės valdytojams dėl teikiamų paslaugų ir kokias rizikas prisiima vartotojas besinaudojantis jomis.
4. „Facebook“ autentifikacijos metu, atlikti pateikiamų asmeninių duomenų redagavimą, siekiant išvengti maksimalaus duomenų pasidalinimo su trečiaisiais asmenimis.

Nors paslaugų teikėjai nurodo vartotojų asmens duomenų rinkimo, naudojimo ir saugojimo sąlygas, bet nėra 100% saugumo garantijos, kad duomenys nebus pavogti, parduoti arba panaudoti kitais tikslais.

3. VARTOTOJŲ ELEKTRONINIŲ DUOMENŲ APSAUGOS YPATUMŲ TYRIMAS

3.1. Tyrimo metodologija

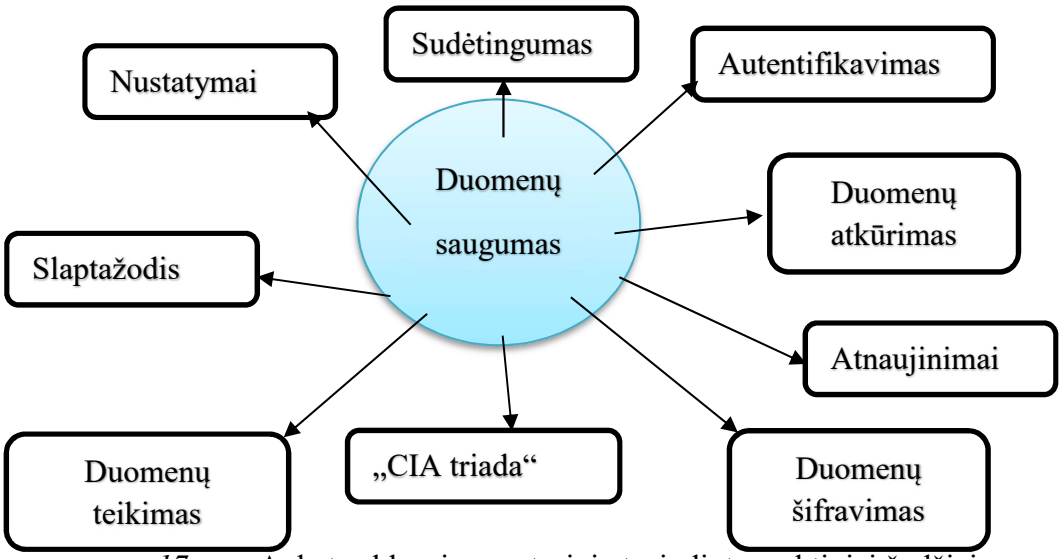
Siekiant išsiaiškinti Lietuvos interneto vartotojų nuomonę apie duomenų saugumą ir jų naudojamus apsaugos būdus, buvo pasirinktas kiekybinis tyrimas. Šis metodas labiausiai tinka apklausti didelę respondentų imtį. Apklausos, kaip pirminių duomenų rinkimo metodas, leidžia atsakyti į dažnai iškylančius klausimus: kodėl žmonės ką nors daro arba nedaro, kas patinka ir nepatinka. Apklausos padeda išsiaiškinti žmonių veiksmus lemiančias priežastis.

Tyrimo instrumentas – anketa. Anketa – klausimų, kuriuos sujungia tyrėjo siekimas ištirti kokį nors socialinį reiškinį ar procesą, visuma (Luobikienė, 2009).

Anketa yra vienas populiariausių sociologinių tyrimų metodų. Ji turi būti aiški, nedviprasmiška, patikima ir skatinti respondento norą bendradarbiauti ir kuo teisingiau atsakinėti (Kardelis, 2007).

Anketa buvo platinama per „Skype“, „Facebook“ socialinį tinklą, elektroninį paštą. Respondentai buvo asmenys, naudojantys internetą, nes internetas yra privaloma sąlyga norint gauti anketą.

Anketą sudaro 15 klausimų, kurie sudaryti remiantis magistrinio darbo teorine dalimi. Anketoje nebuvo uždavinėjami demografiniai klausimai (lytis, amžius, išsilavinimas, gaunamos pajamas), nes jos tikslas nėra nustatyti kas kokius apsaugos būdus naudoja. Klausimų turinį galima atvaizduoti pasitelkus raktinius žodžius (žr. 17 pav.)



17 pav. Anketos klausimyno turinį atspindintys raktiniai žodžiai

Šaltinis: „Sudaryta autoriaus“

Visi anketos klausimai yra orientuoti į vartotoją, kuriam rūpi duomenų saugumas.

Tyrimo imtis: Buvo naudojama svetainės Factus.lt imties dydžio skaičiuoklė, kuri remiasi Yamane ir Jadov imties skaičiavimo formulėmis. Lietuvoje gyvena 2814696 žmonės, o internetu naudojasi 75 procentai (Oficialios statistikos portalas, 2017), visi jie yra potencialios kibernetinių incidentų aukos. Pasirinktas 95 procentų tikimybės lygmuo su 5 procentų paklaida ir 2111022 Lietuvos interneto vartotojų populiacija. Apskaičiuotas reikalingas imties dydis 384 anketos. Per tyrimo laikotarpį gauta 390 anketų. Gauti anketiniai duomenys informatyvūs ir nėra atmestos nei vienos anketos, todėl galima daryti prielaidą, jog šių duomenų užtenka atlikti analizę.

Duomenys buvo apdorojami Microsoft Excel programa. Gauti tyrimo duomenys buvo apdorojami remiantis sisteminimo metodu - grupuojant atsakymus, sudarant lenteles. Naudojama aprašomoji tyrimo rezultatų analizė ir lyginamoji analizė.

Tyrimo tikslas – sužinoti vartotojų nuomonę apie duomenų saugumą ir jų naudojamus apsaugos būdus.

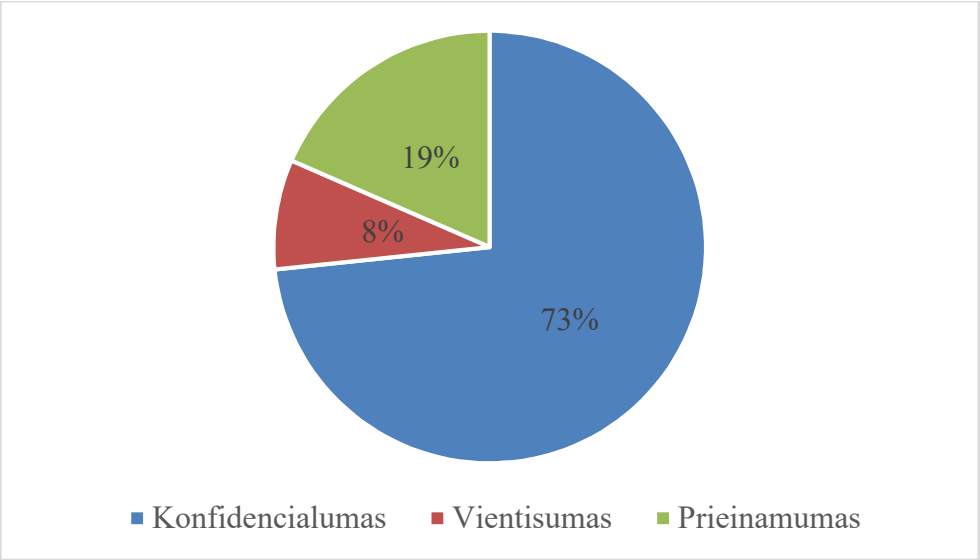
Tyrimo uždaviniai:

1. Kuri informacijos saugumo kategorija svarbiausia;
2. Kokie slaptažodžių sudarymo ir naudojimo ypatumai;
3. Koks „Facebook“ autentifikacijos funkcijos populiarumas;
4. Ar vartotojai sąmoningai dalinasi savo asmeniniais duomenimis su trečiosiomis šalimis naudodamiesi „Facebook“ socialinio tinklo autentifikacijos funkcija;
5. Kokios duomenų apsaugos priemonės dominuoja.

Tyrimo objektas – vartotojų elektroninių duomenų apsaugos priemonių taikymo ypatumai.

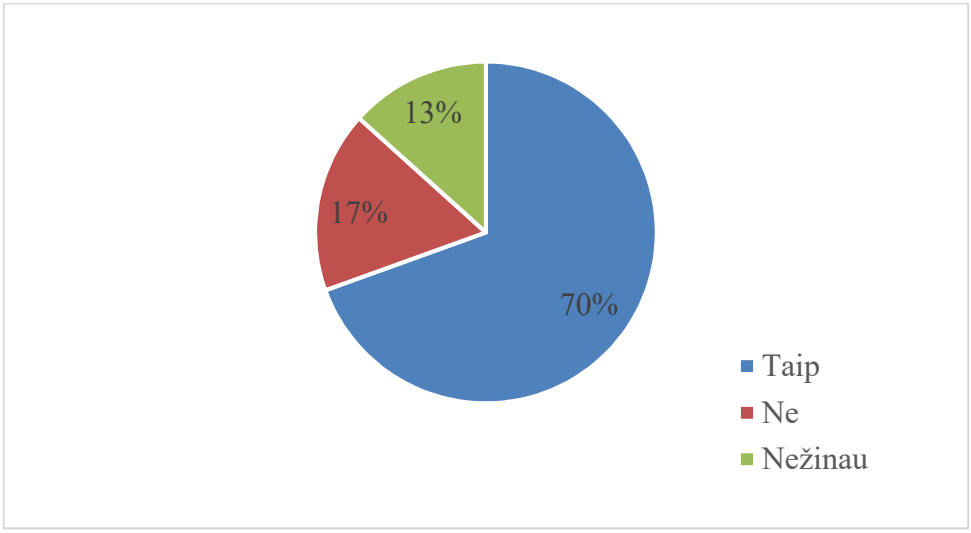
3.2. Tyrimo rezultatų analizė

1 klausimas. Kuri informacijos saugumo kategorija Jums svarbiausia? Daugiausia respondentų (73 proc.) svarbiausia saugumo kategorija įvardina vientisumą, (19 proc.) konfidencialumą ir tik (8 proc.) prieinamumą. Sprendžiant iš rezultatų, vartotojams svarbiausia, kad jų duomenys nebūtų sugadinti arba prarasti. Vien tik konfidencialumo praradimas gali būti lengvai ištaisomas pvz. apribojant prieigą nuo neteisėto prisijungimo naudojant slaptažodį. Prieinamumas dažniausiai suprantamas kaip laikinas trikdis kuomet vartotojas negali naudotis įprastomis paslaugomis. Blogiausia kas gali nutikti, pažeidus vieną saugumo kategoriją gali būti pažeidžiamos ir likusios. (žr. 18 pav.).



18 pav. Kuri informacijos saugumo kategorija Jums svarbiausia?

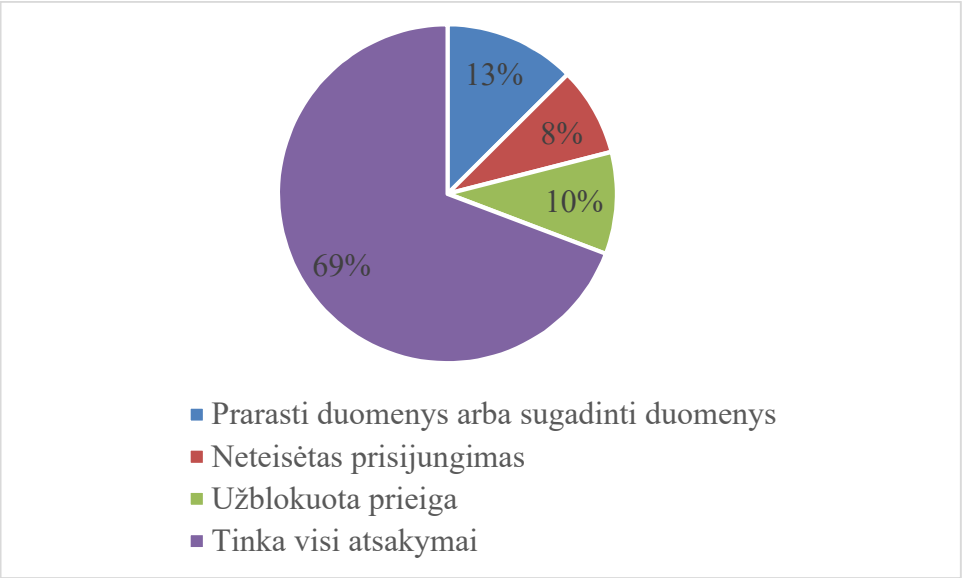
2 klausimas. Ar esate susidūrę su kibernetiniais incidentais? Didžioji dauguma vartotojų (70 proc.) teigia, kad yra patyrę kibernetinių incidentų, 17 procentų respondentų teigia nėra susidūrę ir (13 proc.) nežino. Nacionalinis kibernetinio saugumo centro (toliau - NKSC) manymu, kibernetinio saugumo lygis Lietuvoje yra nepatenkinamas. NKSC prognozuoja, kad kibernetinių incidentų nemažės, o tikslinių kibernetinių atakų skaičius vien didės (žr. 19 pav.).



19 pav. Ar esate susidūrę su kibernetiniais incidentais?

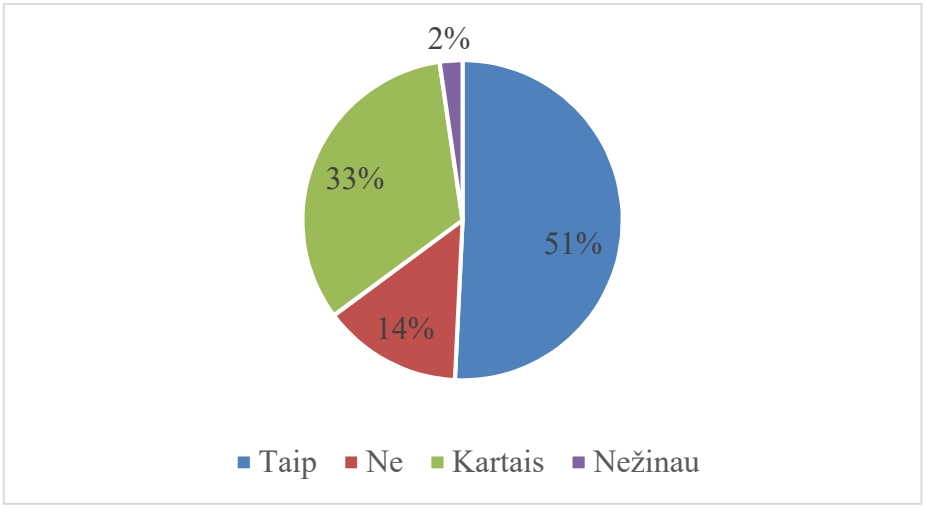
3 klausimas. Jeigu praeitame (pirmame) klausime atsakėte „taip“, tuomet kokią žalą patyrėte? Didžioji dauguma (69 proc.) yra patyrę – vientisumo, prieinamumo ir konfidencialumo pažeidimus, (13 proc.) vartotojų buvo sugadinti arba prarasti duomenys, (8 proc.) patyrė nesankcionuotą prisijungimą ir (10 proc.) vartotojų buvo užblokuota prieiga prie vienokių ar kitokių paslaugų. Įvairios organizacijos nuolatos teikia rekomendacijas kokių apsaugos priemonių reikia imtis norint išvengti kibernetinių incidentų. Dauguma priemonių yra standartinės ir daug metų nesikeičiančios, tiesiog

vartotojai dėl abejingumo arba žinių trūkumo nesiima veiksmų kurie padėtų kibernetinių incidentų riziką. (žr. 20 pav.).



20 pav. Jeigu praeitame (pirmame) klausime atsakėte „taip“, tuomet kokią žalą patyrėte?

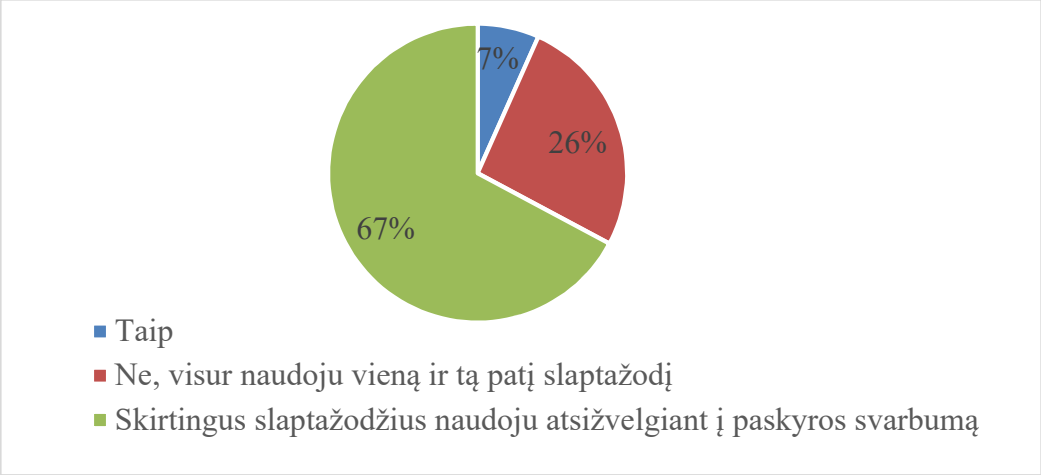
4 klausimas. Ar kurdami slaptažodį vadovaujatės saugaus slaptažodžio rekomendacijomis? Pusė vartotojų (51 proc.) nurodė, kad vadovaujasi saugaus slaptažodžio kūrimo rekomendacijomis. Trečdalis (33 proc.) vartotojų kartais, tai galima paaiškinti, jog kai kurios svetainės leidžia yra mažai reikšmingos vartotojams ir jie nemato būtinybės kurti stiprius slaptažodžius. Saugaus slaptažodžio rekomendacijomis nesinaudoja 14 procentų respondentų ir tik 2 procentai prisipažįsta nežino kokie turėtų būti slaptažodžiai. Yra daug rekomendacijų koks turėtų būti slaptažodis, bet pagrindas yra slaptažodžio ilgis ir ženklų skirtingumas (didžiosios ir mažosios raidės, skaičiai, simboliai) (žr. 21 pav.).



21 pav. Ar kurdami slaptažodį vadovaujatės saugaus slaptažodžio rekomendacijomis?

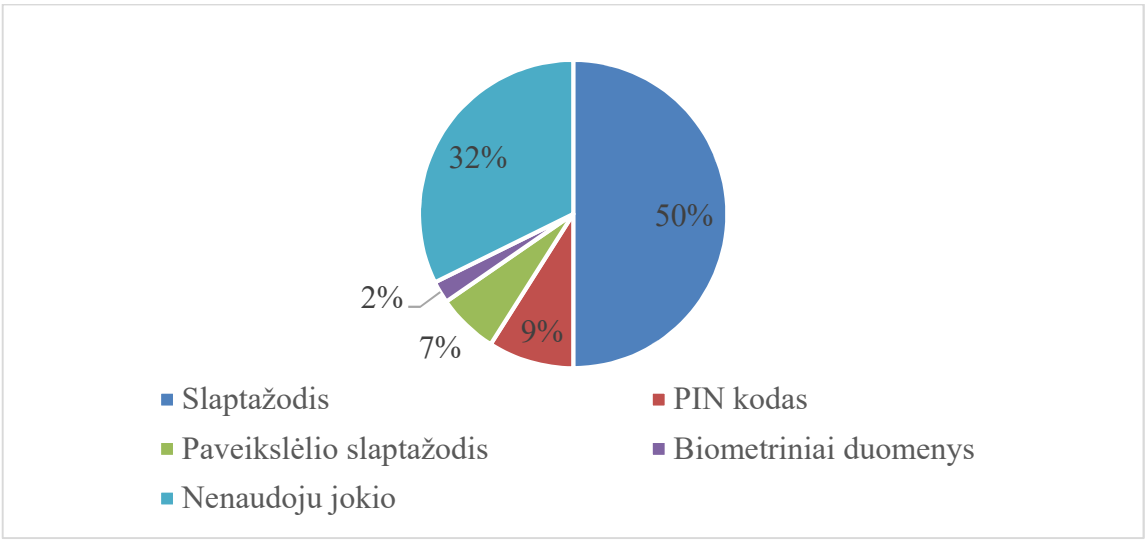
5 klausimas. Ar naudojate skirtingą slaptažodį skirtingose interneto puslapių paskyrose? 67 procentai respondentų atsakė, jog skirtingus slaptažodžius naudoja atsižvelgiant į paskyros svarbumą, tai yra logiškas sprendimas, nes nėra sukuriama begalė slaptažodžių ir mažėja rizika juos pamiršti. (7

proc.) nurodė, jog visuose internetiniuose puslapiuose naudoja skirtingą slaptažodį, tokiu atveju yra pasitelkiama į pagalbą programinė įranga arba naudojamasi labai mažai paslaugų kurių prieiga reikalauja slaptažodžio. Visur vieną ir tą patį slaptažodį naudoja (26 proc.), tokiems vartotojams kyla labai didelį rizika, kad incidento atveju neteisėtai įgytu slaptažodžiu bus pasinaudota ir kitose svetainėse (žr. 22 pav.).



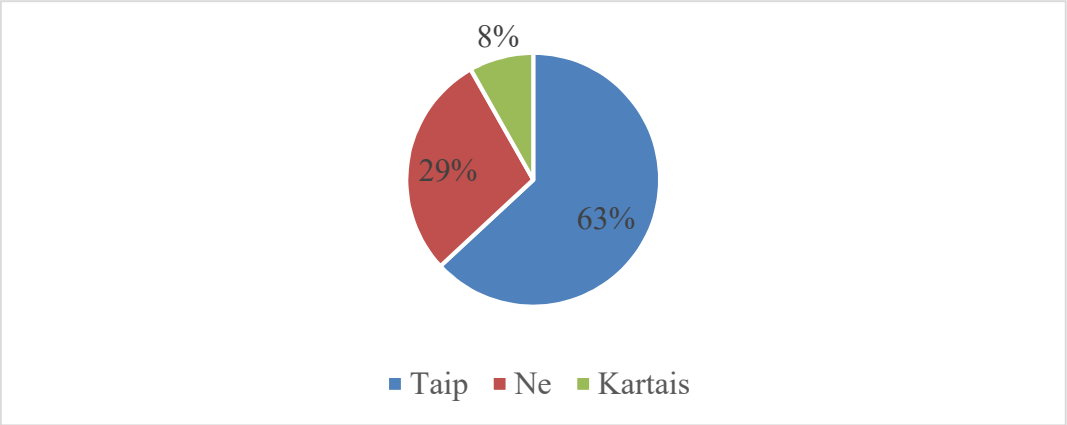
22 pav. Ar naudojate skirtingą slaptažodį skirtingose interneto puslapių paskyrose?

6 klausimas. Kuris autentifikacijos būdas priimtiniausias norint prisijungti prie „Windows 10“ operacinės sistemos? Nesinaudojantiems „Windows 10“ operacine sistema prašome ignoruoti klausimą. (50 proc.) vartotojų naudoja slaptažodį, tai vartotojo autentifikavimo priemonė, (32 proc.) nėra apsaugoję „Windows 10“ operacinės sistemos, jiems kyla didžiulė rizika, kad bus pažeistas duomenų konfidencialumas. PIN kodą naudoja (9 proc.), o paveikslėlių slaptažodį (7 proc.) respondentų, darome išvadą, kad šie autentifikavimo įrankiai nėra labai populiarūs. Autentifikavimui atlikti biometrinius duomenis naudoja tik (2 proc.) vartotojų, toks autentifikavimo būdas reikalauja specialios techninės įrangos (žr. 23 pav.).



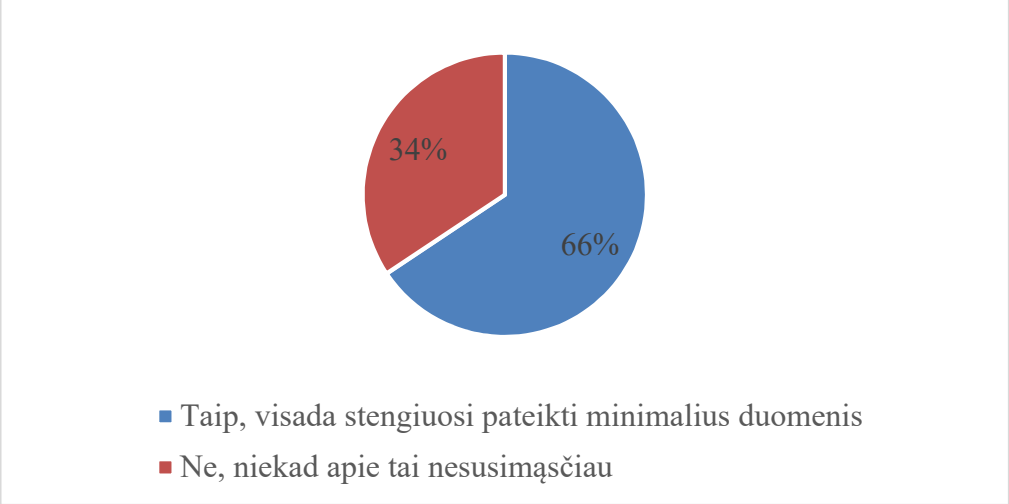
23 pav. Kuris autentifikacijos būdas priimtiniausias norint prisijungti prie „Windows 10“ operacinės sistemos? Nesinaudojantiems „ Windows 10“ operacine sistema prašome ignoruoti klausimą.

7 klausimas. Ar esant galimybei naudojatės „Facebook“ socialinio tinklo autentifikacijos funkcija, norėdami užsiregistruoti e. sistemoje? 63 procentai respondentų norėdami naudotis įvairiomis internetinėmis paslaugomis naudojasi „Facebook“ autentifikacijos funkcija, tai yra labai populiarus būdas greitai būti užregistruotu tam tikroje svetainėje. (8 proc.) kartais užsiregistruoja tam tikrose svetainėse pasinaudodami „Facebook“ socialiniu tinklu, galima daryti prielaidą, kad šie vartotojai yra ypač atsargūs ir supranta asmeninių duomenų svarbą. „Facebook“ autentifikavimo funkcija nesinaudoja, (29 proc.) respondentų, tikėtina, kad jie nesinaudoja šiuo socialiniu tinklu arba su niekuo nenori dalintis savo asmeniniais duomenimis (žr. 24 pav.).



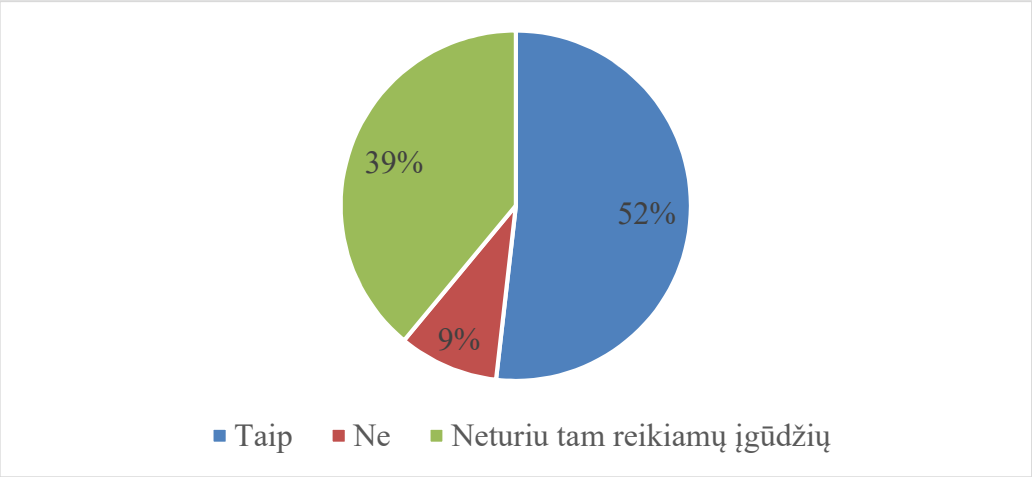
24 pav. Ar esant galimybei naudojatės „Facebook“ socialinio tinklo autentifikacijos funkcija, norėdami užsiregistruoti e. sistemoje?

8 klausimas. Jeigu praeitame (septintame) klausime atsakėte „taip“ arba „kartais“, tuomet ar atkreipėte dėmesį ir atsakingai įvertinote kokius savo asmeninius duomenis atiduodate trečiajam asmeniui? Daugiau nei pusė (66 proc.) supranta asmeninių duomenų svarbą ir stengiasi atskleisti jų kuo mažesnį kiekį. (34 proc.) vartotojų tęsdavo registravimo procesą neatlikę pateikiamų duomenų redagavimo, taip pateikdami maksimalius trečiosios šalies prašomus asmeninus duomenis. Tai reiškia tris dalykus- vartotojas labai stipriai pasitiki trečiosios šalies duomenų apsauga, vartotojas nenori turėti jokio privatumo ir dalinasi savo duomenimis su visais ir visada, vartotojas turi mažai per mažai žinių, kad galėtų įvertinti situaciją (žr. 25 pav.).



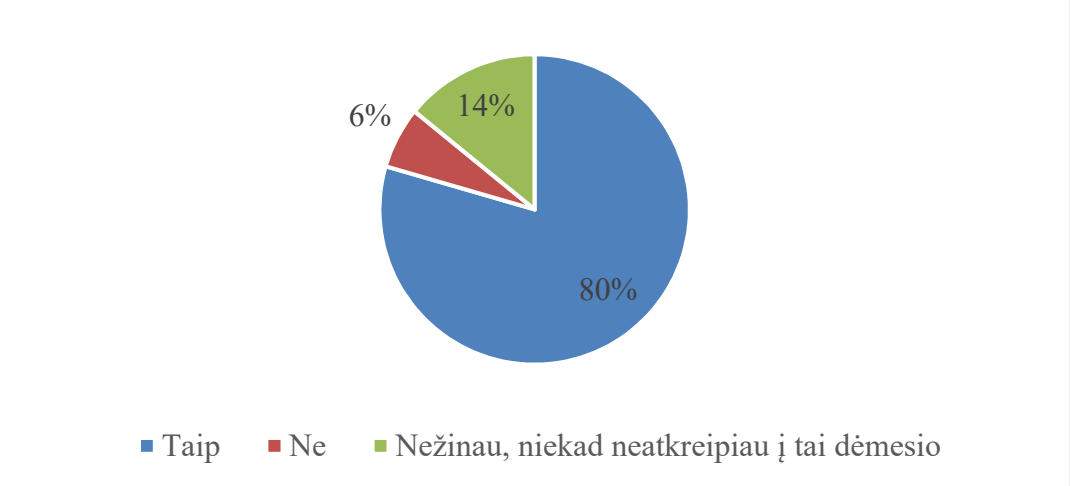
25 pav. Jeigu praeitame (septintame) klausime atsakėte „taip“ arba „kartais“, tuomet ar atkreipėte dėmesį ir atsakingai įvertinote kokius savo asmeninius duomenis atiduodate trečiajam asmeniui?

9 klausimas. Ar reguliariai atnaujinate programinę įrangą? 52 procentai respondentų, teigia reguliariai atnaujinantys programinę įrangą, 39 procentai vartotojų neatnaujina programinės įrangos ir 9 neturi reikiamų įgūdžių tai padaryti. Nacionalinis kibernetinio saugumo centras ir toliau masiškai aptinka tinkluose veikiančius kompiuterius, kurie naudoja pasenusią operacinę ir taikomąją programinę įrangą, apie kurios pažeidžiamumus, leidžiančius įsibrauti į organizacijų kompiuterių tinklus pačiais paprasčiausiais būdais yra visuotinai žinoma (žr. 26 pav.).



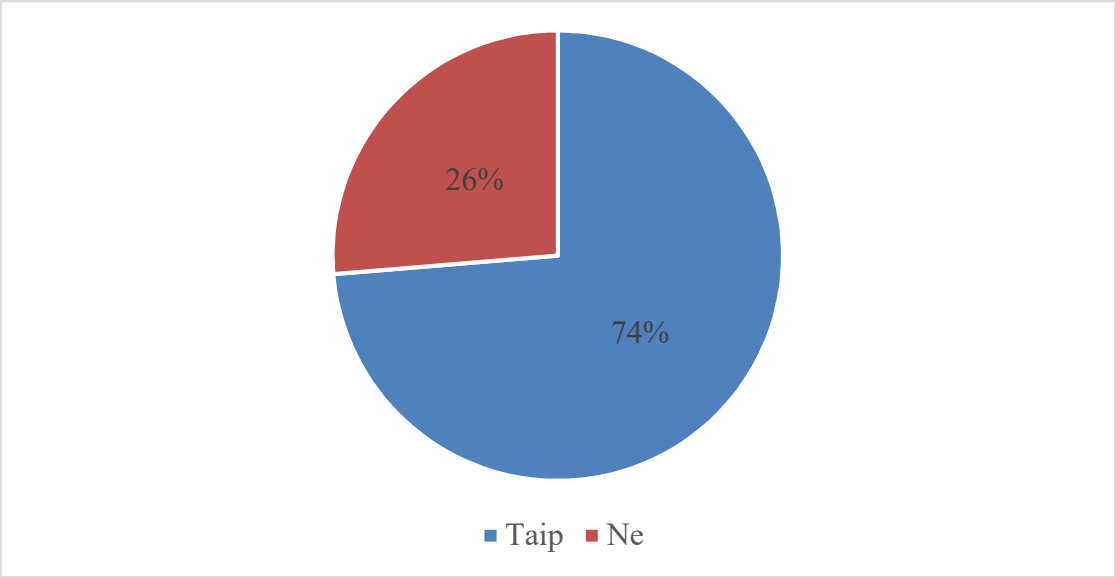
26 pav. Ar reguliariai atnaujinate programinę įrangą?

10 klausimas. Ar naudojatės operacine sistema nuolatos prisijungęs administratoriaus teisėmis? Nuolatos administratoriaus teisėmis prisijungę naudojasi 80 procentų respondentų, (14 proc.) nurodė nežinantys kokias vartotojo teises turi ir (6 proc.) vartotojų nėra prisijungę administratoriaus teisėmis. Nuolatos būnant prisijungus administratoriaus teisėmis yra rizikinga, nes kibernetinio incidento atveju nusikaltėliai gali išnaudoti įvairius sistemos procesus siekdami pasiekti savo tikslą (žr. 27 pav.).



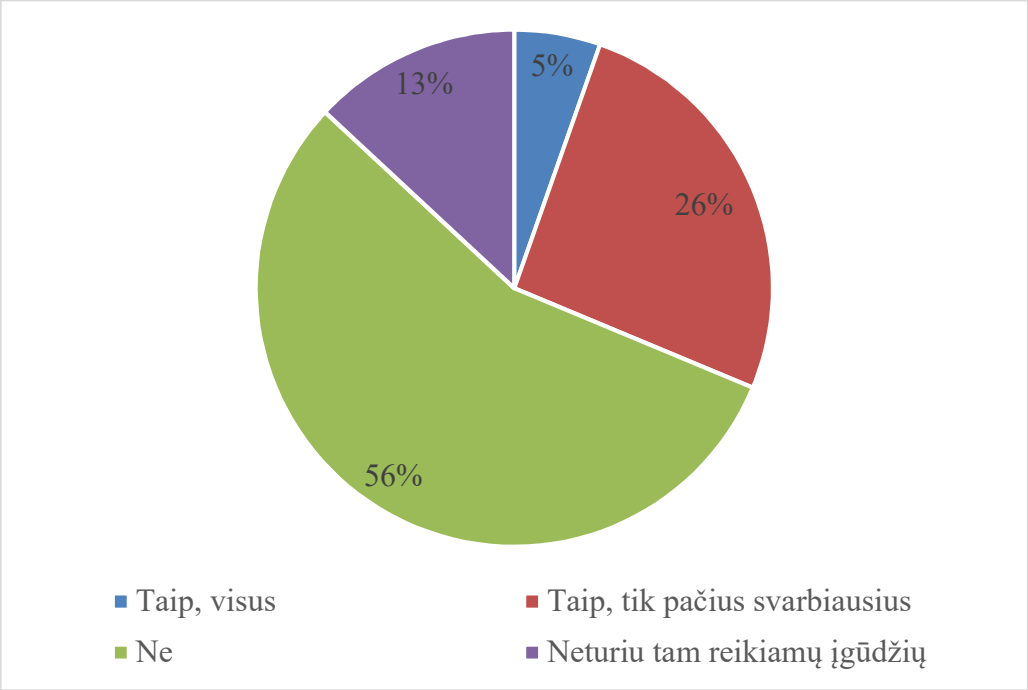
27 pav. Ar naudojatės operacine sistema nuolatos prisijungęs administratoriaus teisėmis?

11 klausimas. Ar naudojate antivirusinę programą? Beveik trys ketvirtadaliai (74 proc.) vartotojų naudoja antivirusinę programą, taip apsaugodami savo sistemą nuo kenkėjiškų programų. (26 proc.) nurodė nenaudojantys antivirusinės programinės įrangos (žr. 28 pav.).



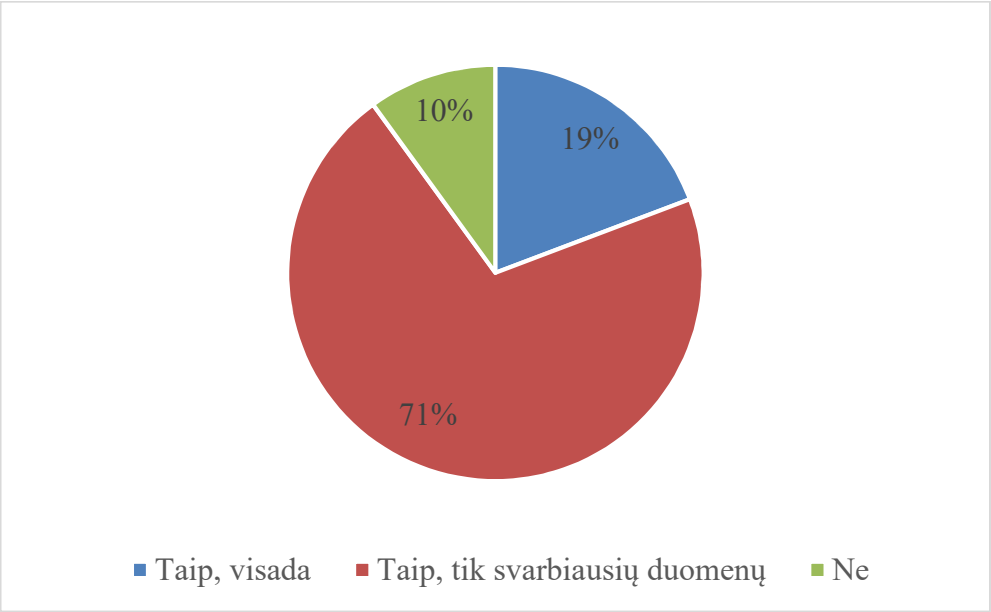
28 pav. Ar naudojate antivirusinę programą?

12 klausimas. Ar šifruojate duomenis? 56 procentai respondentų teigia, kad nešifruoja duomenų. 26 procentai vartotojų šifruoja jų nuožiūra tik pačius svarbiausius duomenis. 13 procentų neturi reikiamų įgūdžių atlikti duomenų šifravimui ir 5 procentai šifruoja absoliučiai visus savo duomenis. Egzistuoja daugybė programinės įrangos kuri suteikia galimybė šifruoti duomenis esančius stacionariuosiuose diskuose ir nešiojamosiose laikmenose (žr. 29 pav.).



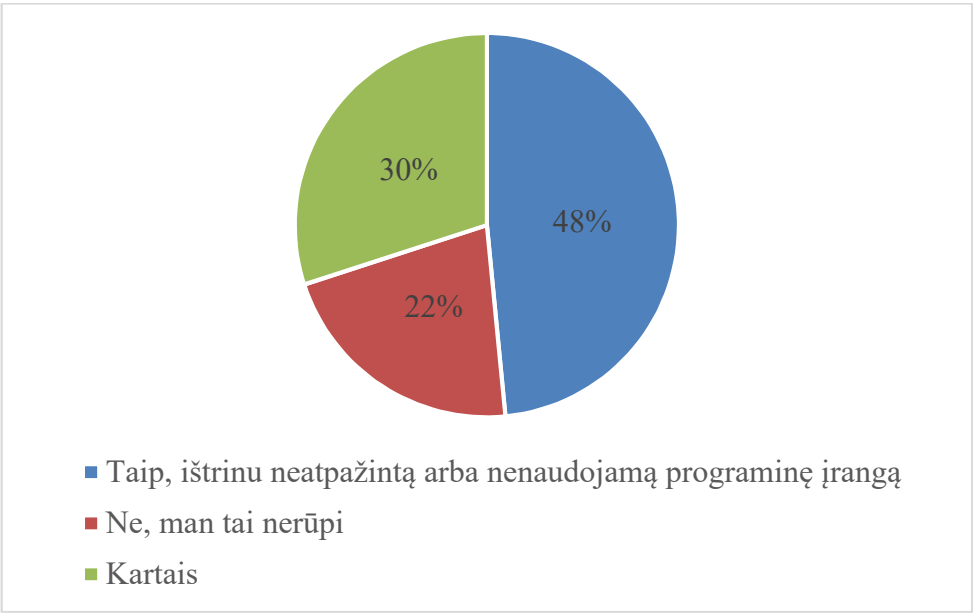
29 pav. Ar šifruojate duomenis?

13 Klausimas. Ar darote duomenų atsargines kopijas? 71 procentai respondentų teigia darantys tik pačių svarbiausių duomenų atsargines kopijas, o 19 procentai daro absoliučiai visų duomenų atsargines kopijas. Atsarginių duomenų kopijų nedaro tik 10 procentai respondentų. Šiuolaikinė programinė įranga suteikia visas galimybes realiu laiku daryti atsargines duomenų kopijas pvz., į kitą kietąjį diską (žr. 30 pav.).



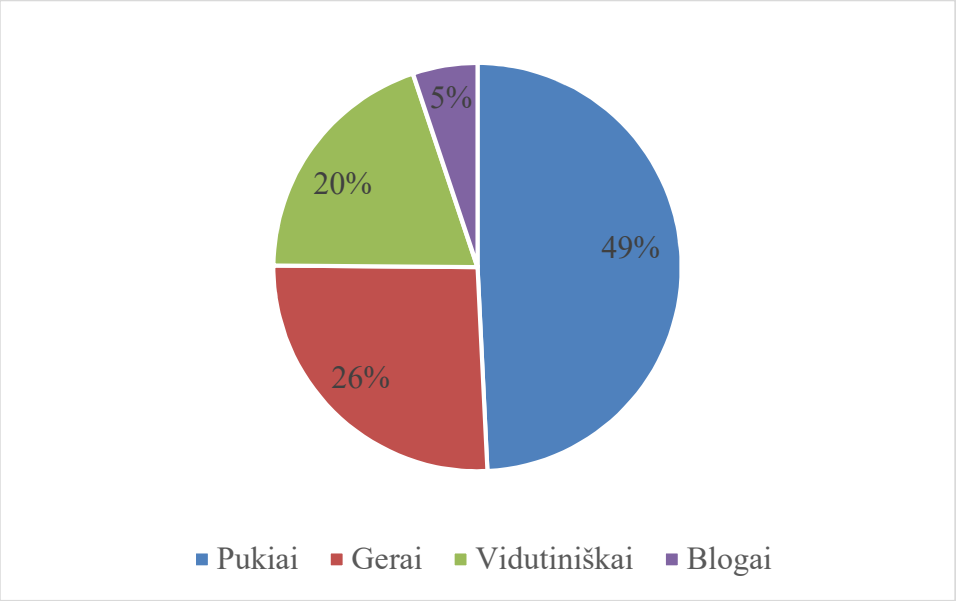
30 pav. Ar darote duomenų atsargines kopijas?

14 klausimas. Ar tikrinate kokia programinė įranga „gyvena“ Jūsų kompiuteryje? 48 procentai respondentų teigia reguliariai tikrinantys kokia programinė įranga yra jų kompiuteryje, aptikus nepageidaujamą ji pašalinama Kartais peržiūri ir pašalina nereikalingą programinę įrangą 30 procentai vartotojų ir tik 22 procentų nesiima jokių veiksmų. Nelicencijuota, pasenusi programinė įranga padidina riziką, kad bus išnaudota siekiant įvykdyti kibernetinį incidentą (žr. 31 pav.).



31 pav. Ar tikrinate kokia programinė įranga „gyvena“ Jūsų kompiuteryje?

15 klausimas. Kaip vertinate savo žinias IT saugumo srityje? 49 procentai vartotojų savo IT žinias įvertino puikiai, (26 proc.) gerai, (20 proc.) vidutiniškai ir tik (5 proc.) blogai. Kadangi tai yra kiekvieno vartojo asmeninė nuomonė, sunku daryti išvadas. IT žinios ir kibernetinis saugumas yra du neatsiejami dalykai, tik turėdami žinių sugebėsime tinkamai apsaugoti savo duomenis (žr. 32 pav.).



32 pav. Kaip vertinate savo žinias IT saugumo srityje?

Tyrimo apibendrinimas:

1. Daugumai vartotojų svarbiausia saugumo kategorija įvardina vientisumą, kad duomenys nebūtų prarasti arba sugadinti;
2. Stiprius slaptažodžius naudoja daugiau nei pusė vartotojų, dauguma svetainių vadovaujasi saugaus slaptažodžio kūrimo rekomendacijomis ir stengiasi pabrėžti slaptažodžio svarbą. Slaptažodis yra pati populiariausia vartotojo autentifikavimo priemonė;
3. „Facebook“ autentifikacijos funkcija yra naudojama daugelio vartotojų, tačiau net trečdalis jų nėra atkreipęs dėmesio kokius asmeninius duomenis atiduoda trečiajai šaliai;
4. Vartotojai neskiria pakankamai dėmesio programinės įrangos atnaujinimui. Nacionalinis kibernetinio saugumo centras ir toliau masiškai aptinka tinkluose veikiančius kompiuterius, kurie naudoja pasenusią operacinę ir taikomąją programinę įrangą, apie kurios pažeidžiamumus, leidžiančius įsibrauti į organizacijų kompiuterių tinklus pačiais paprasčiausiais būdais yra visuotinai žinoma;
5. Antivirusinę programinę įrangą naudoja dauguma vartotojų. Tai pati populiariausia saugumo priemonė siekiant apsisaugoti nuo kibernetinių incidentų;
6. Didžioji dauguma vartotojų daro duomenų atsargines kopijas, nes suvokia, kad prarastus duomenis galės atkurti ir taip išvengs didelių nuostolių.

IŠVADOS

1. „CIA triada“ – tai trys pirminės informacijos saugumo koncepcijos, kurias sudaro konfidencialumas, vientisumas ir prieinamumas. Kritinės kontrolės priemonės (angl. *Critical Security Controls*) yra rekomenduojamų praktiškų saugumo priemonių rinkinys, kurio tikslas informacijos saugumo stiprinimas ir kibernetinių incidentų rizikos mažinimas. Elektroninis saugumas paprastai suprantamas kaip apsauga nuo neteisėtos prieigos prie informacijos, jos panaudojimo, keitimo, manipuliavimo, praradimo. Prieigos kontrolė įgyvendinama atliekant autentifikavimą. Slaptažodžiu paremta autentifikacija yra vienas iš populiariausių autentifikacijos būdų. Silpni arba netinkamai naudojami slaptažodžiai padidina incidentų riziką. Slaptažodžiams išgauti, naudojamos techninės ir netechninės atakos.

2. Išsamiai aprašytos ir vaizdine medžiaga atvaizduotos „Windows 10“ operacinės sistemos ir „Facebook“ vartotojų autentifikavimo funkcijos. Vartotojai norėdami užtikrinti savo asmeninių duomenų konfidencialumą ir apriboti prieigą nuo neteisėto prisijungimo prie „Windows 10“ operacinės sistemos, naudojasi autentifikavimo funkcija, galima rinktis iš keturių autentifikacijos būdų – slaptažodis, PIN kodas, paveikslėlio slaptažodis ir biometriniai duomenys. Kurį autentifikavimo metodą naudos vartotojas yra jo asmeninis pasirinkimas. Įvairios svetainės, kurių vartotojai gali naudotis jų teikiamomis paslaugomis tik užsiregistravus, vis dažniau siūlo alternatyvią registracijos formą – vartotojo autentifikavimą pasidalinus asmeniniais duomenimis iš „Facebook“ socialinio tinklo.

3. Didžioji dauguma vartotojų teigia, kad yra patyrę kibernetinių incidentų. Nacionalinis kibernetinio saugumo centro manymu, kibernetinio saugumo lygis Lietuvoje yra nepatenkinamas ir prognozuojama, kad kibernetinių incidentų nemažės, o tikslinių kibernetinių atakų skaičius didės. Duomenų vientisumą vartotojai įvardijo svarbiausia saugumo kategorija. Vartotojai vadovaujasi saugaus slaptažodžio kūrimo rekomendacijomis, galima daryti prielaidą, nes dauguma svetainių taiko apribojimus nesaugių slaptažodžių kūrimui. Ketvirtis respondentų tą patį slaptažodį naudoja visose svetainėse, tai sudaro sąlygas, sužinojus vartotojo slaptažodį, gauti prieigą prie visų jo naudojamų paslaugų. Vartotojai reguliariai neatnaujinantys programinės įrangos ir nesinaudojantys antivirusine programa, bei prisijungę sistemoje administratoriaus teisėmis yra pažeidžiami ir rizikuoja tapti kibernetinio incidento aukomis. Daugiau nei pusė respondentų naudojasi registracijos forma – vartotojo autentifikavimu pasidalinus asmeniniais duomenimis iš „Facebook“ socialinio tinklo, tačiau net trečdalis vartotojų neįvertina ir nežino kokius konkrečius asmeninius duomenis „atiduoda“ paslaugas teikiančioms trečiosioms šalims.

REKOMENDACIJOS

1. Norint apsaugoti „CIA triadą“ naudojami kontrolės metodai:
   - Konfidencialumą apsaugo – prieigos kontrolė, bylų leidimai, šifravimas;
   - Vientisumą apsaugo – prieigos kontrolė, prisijungimas, elektroninis parašas, maiša, šifravimas;
   - Prieinamumą apsaugo – dubliavimas, atsarginės kopijos, prieigos kontrolė.
2. Sudarant slaptažodį vadovautis saugaus slaptažodžio rekomendacijomis arba naudoti ilgus (14 - 20 simbolių) slaptažodžius sudarytus iš atsitiktinių žodžių.
3. Siekiant užtikrinti asmenių duomenų apsaugą naudojantis „Facebook“ socialiniu tinklu:
   - Nesidalinti su „Facebook“ informacija, kuri nutekinimo atveju galėtų padaryti žalos;
   - Įvertinti svetainės patikimumą prieš „atiduodant“ jai savo asmeninius duomenis naudojantis „Facebook“ autentifikavimo funkcija;
   - Susipažinti su svetainės privatumo politika ir paslaugų teikimo taisyklėmis prieš prisijungiant prie jos, naudojant „Facebook“ identifikacijos duomenis ir atkreipti dėmesį kokiems tikslams svetainė naudoja asmeninius vartotojo duomenis bei koks jų saugojimo/tvarkymo laikotarpis; ar asmens duomenų valdytojas užtikrina vartotojų asmens duomenų saugumą; kokios svetainės privatumo politikos ir paslaugų teikimo taisyklių keitimo sąlygos ir vartotojo informavimo būdai jas pakeitus; kokia atsakomybė tenka svetainės valdytojams dėl teikiamų paslaugų ir kokias rizikas prisiima vartotojas besinaudojantis jomis;
   - „Facebook“ autentifikacijos metu atlikti pateikiamų asmeninių duomenų redagavimą, kad būtų išvengta maksimalaus duomenų pasidalinimo.
4. Naudoti vartotojo autentifikavimą siekiant apsaugoti „Windows“ operacinę sistemą nuo neteisėtos prieigos.
5. Vadovautis kritinės kontrolės priemonėmis – atnaujinti programinę įrangą, naudoti antivirusinę programą, nebūti prisijungus administratoriaus teisėmis, nenaudoti įtartinos programinės įrangos, šifruoti duomenis, daryti duomenų atsargines kopijas ir t.t.

LITERATŪROS SĄRAŠAS

Vadovėliai ir monografijos

1. Kiškis, M., Petrauskas, R., Rotomskis, I. ir Štitilis, D. (2006). Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universiteto leidybos centras.
2. Dulaney, E. ir Easttom, C. (2014). Comptia Security+ Study Guide: Sy0-401, 6th Edition. doi: 10.1118/978-1118875070.
3. Graham, J., Howard, R. ir Olson, R. (2011). Cyber Security Essentials. doi: 10.1201/978-1-4398-5126-5.
4. Andress, J. (2011) The basics of information security: understanding the fundamentals of infosec in theory and practice. doi: 10.1016/978-1597496537.
5. Štitilis, D., Kiškis, M., Limba, T., Rotomskis, I., Agafonov, K., Gulevičiūtė, G. ir Panka, K. (2016). Interneto ir technologijų teisė. Vilnius: Registrų centras.
6. Lučinskij, M., Poderskis, P. ir Tumėnas, P. (2007). Duomenų saugos pradmenys. Kaunas: Smaltijos leidykla.
7. Isaca: Cybersecurity Fundamentals Study Guide. (2015). doi: 10.1604/978-1604206999.
8. Scientific Advice Mechanism: Cybersecurity in the European Digital Single Market. (2017). doi: 10.2777/978-92-79-66217-1.
9. Europos taryba: Europos duomenų apsaugos teisės vadovas. (2014). Liuksemburgas: Europos Sąjungos leidinių biuras.
10. Oriyano, S. (2016). Certified Ethical Hacker Version 9 Study Guide. doi: 10.1002/978-1-119-25224-5.
11. Čenys, A. ir Juknius, J. (2011). Saugumo patikros ir etiško įsilaužimo technologijos. doi: 10.5755/978-609-433-070-4.
12. Damkus, M. (2015). Saugumo priemonių taikymas. Mokomoji medžiaga: Kibernetinio saugumo rizikų valdymas.
13. Luobikienė, I. (2009). Sociologinių tyrimų metodika: mokomoji knyga. Kaunas: Technologija.
14. Kardelis, K. (2007). Mokslinių tyrimų metodologija ir metodai: vadovėlis. Šiauliai: Lucilijus.

Moksliniai straipsniai

15. Jastiuginas, S. (2012). Integralus informacijos saugumo valdymo modelis. Informacijos mokslai, 61, 7-30.

16. Bonneau, J., Herley, C., Oorschot, P., Stajano, F. (2015). Passwords and the evolution of imperfect authentication, 58 (7), 78–87.
17. Štitilis, D. ir Laurinaitis, M. (2009). Tapatybės vagystė elektroninėje erdvėje. Informacijos mokslai, 50, 239-247.
18. Zaidieh, A. J. Y. (2012). The Use of Social Networking in Education: Challenges and Opportunities. World of Computer Science and Information Technology Journal, 2 (1), 18-21.

Teisės aktai

19. Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). Teisės aktų registras, 20553.

Kiti interneto šaltiniai

20. Valstybinio audito ataskaita: Kibernetinio saugumo aplinka Lietuvoje. (2015). Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3497 [žiūrėta 2017-01-09]
21. Kšivickienė, D. (2010, gruodžio 14). Konfidenciali informacija darbe. Prieiga per internetą: http://www.manager.lt/blog/articles/view/konfidenciali-informacija-darbe [žiūrėta 2017-01-09].
22. Kompiuterių tinklų saugumo terminų aiškinamasis žodynas. Prieiga per internetą: http://www.tinklusaugumas.lt/Confidentiality,%20Integrity,%20Availability [žiūrėta 2017-01-09]
23. Vartotojo autentifikavimas svetainėje. Prieiga per internetą: http://www.epilietis.eu/index.php/mokymas/e-paslaugos/e-parasas/119-vartotojo-autentifikavimas-svetainese [žiūrėta 2017 04 10]
24. Vitkus., P. (2010). Apsaugos inžinerija. Prieiga per internetą: http://www.elen.ktu.lt/studentai/lib/exe/fetch.php?media=apsaugos_inzinerija_2010.ppt [žiūrėta 2017 04 10]
25. Informacija ir komunikacija: Saugumo svarba. Prieiga per internetą: http://www.paltarokogimnazija.lt/Informatika/infokom20004_002.htm [žiūrėta 2017 04 10]
26. Muzikevičiūtė, D. (2014, balandžio 16).Saugaus ir įsimenamo slaptažodžio sukūrimas – išsprendžiamas galvosūkis. Prieiga per internetą: http://vakomanda.lt/saugaus-ir-isimenamo-slaptazodzio-sukurimas-issprendziamas-galvosukis [žiūrėta 2017 04 11]
27. Slaptažodžiai ir jų saugojimas. (2017, birželio 5). Prieiga per internetą: http://www.esaugumas.lt/lt/belaidzio-tinklo-saugumas/slaptazodziai-ir-ju-saugojimas.html [žiūrėta 2017 04 11]

28. Kaspersky Lab: Secure Password Check. (2017). Prieiga per internetą: https://password.kaspersky.com/ [žiūrėta 2017 04 15]
29. The Password Security Checklist. (2017, liepos 5). Prieiga per internetą: https://www.upguard.com/blog/the-password-security-checklist [žiūrėta 2017 04 15]
30. Statt., N. (2017, rugpjūčio 7). Best practices for passwords updated after original author regrets his advice. Prieiga per internetą: https://www.theverge.com/2017/8/7/16107966/password-tips-bill-burr-regrets-advice-nits-cybersecurity [žiūrėta 2017 04 15]
31. „Brute force“ atakos. Prieiga per internetą: https://www.cert.lt/rekomendacijos/brute_force_atakos.html [žiūrėta 2017 06 20]
32. Blocking Brute Force Attacks. (2017, rugpjūčio 9). Prieiga per internetą: https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks#Locking_Accounts [žiūrėta 2017 06 20]
33. Brute Force Attack. (2013, kovo 25). Prieiga per internetą: http://www.tinklusaugumas.lt/Brute%20Force%20Attack [žiūrėta 2017 06 20]
34. Rule-based Attack. Prieiga per internetą: https://hashcat.net/wiki/doku.php?id=rule_based_attack [žiūrėta 2017 06 20]
35. Gumauskas, V. (2015). Pramoninių kompiuterinių tinklų saugumo sistemų tyrimas (baigiamasis magistro projektas). Prieiga per internetą: https://epubl.ktu.edu/object/elaba:8654609/8654609.pdf [žiūrėta 2017 06 20]
36. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys. Phishing. Prieiga per internetą: https://www.cert.lt/rekomendacijos/phishing.html [žiūrėta 2017 06 20]
37. Kaip veikia „phishing“?. (2017, birželio 20). Prieiga per internetą: https://www.esaugumas.lt/lt/duomenu-vagystes-phishing/kaip-veikia-phishing/248 [žiūrėta 2017 06 25]
38. „Phishing“ laiško pavyzdys. Prieiga per internetą: https://www.esaugumas.lt/lt/duomenu-vagystes-phishing/phishing-laisku-pavyzdziai/462 [žiūrėta 2017 06 25]
39. „Phishing“ tinklapio pavyzdys. Prieiga per internetą: https://www.esaugumas.lt/lt/duomenu-vagystes-phishing/phishing-tinklalapiu-pavyzdziai/463 [žiūrėta 2017 06 25]
40. Spam and phishing in Q1 2017. Prieiga per internetą: https://securelist.com/spam-and-phishing-in-q1-2017/78221/ [žiūrėta 2017 06 25]
41. 2016 metų nacionalinio kibernetinio saugumo būklės ataskaita. (2017), Prieiga per internetą: https://kam.lt/download/57062/nksc_metine_ataskaita_uz_2016.pdf
42. Socialinis tinklas. Prieiga per internetą: https://www.15min.lt/tema/socialinis-tinklas-14336 [žiūrėta 2017 07 18]

43. Social network. (2017). Prieiga per internetą: http://www.dictionary.com/browse/social-network [žiūrėta 2017 07 18]
44. Top 15 Most Popular Social Networking Sites and Apps. (2017). Prieiga per internetą: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/ [žiūrėta 2017 07 18]
45. Gyvenimas tinkle: liga ar trūkstamo dėmesio kompensacija?. (2013). Prieiga per internetą: http://www.respublika.lt/lt/naujienos/lietuva/kitos_lietuvos_zinios/gyvenimas_tinkle_liga_ar_trukstamo_demesio_kompensacija/,print.1 [žiūrėta 2017 07 21]
46. Catfly privatumo politika. (2017). Prieiga per internetą: https://catfly.lt/privacy [žiūrėta 2017 07 21]
47. 5 kritinės saugos kontrolės priemonės norint išvengti 85 proc. kibernetinio saugumo spragų. (2015, spalio 16). Prieiga per internetą: https://www.nrdcs.lt/lt/pranesimai-ziniasklaidai/5-kritines-saugos-kontroles-priemones-norint-isvengti-85-proc-kibernetinio-saugumo-spragu/69 [žiūrėta 2017 09 10]
48. The Center for Internet Security, Critical Security Controls for Effective Cyber Defense. (2016). Prieiga per internetą: https://cybersecurity.idaho.gov/wp-content/uploads/sites/23/2016/10/CSCmaster.pdf
49. Nacionalinis kibernetinio saugumo centras. (2015). Prieiga per internetą: https://www.cisecurity.org/wp-content/uploads/2017/03/Kibernetinio-saugumo-centras-1.pdf [žiūrėta 2017 09 10]
50. CIS Control 2 Inventory of Authorized and Unauthorized Software. Prieiga per internetą: https://www.cisecurity.org/controls/inventory-of-authorized-and-unauthorized-software/ [žiūrėta 2017 09 15]
51. Kaip įeiti administratoriaus teisėmis?. Prieiga per internetą: https://support.microsoft.com/lt-lt/help/14028/windows-7-how-log-on-as-an-administrator [žiūrėta 2017 09 12]
52. Web-Based Application. Prieiga per internetą: https://www.techopedia.com/definition/26002/web-based-application [žiūrėta 2017 09 17]
53. CIS Control 18 Application Software Security. Prieiga per internetą: https://www.cisecurity.org/controls/application-software-security/ [žiūrėta 2017 10 10]
54. Windows 10 says a PIN is more secure than a password. How?. (2015, rugpjūčio 24). Prieiga per internetą: https://www.404techsupport.com/2015/08/24/windows-10-says-secure-password/
55. Respondentų skaičiuoklė. Prieiga per internetą: http://www.factus.lt/main-calculator/ [žiūrėta 2017 10 15]
56. Oficialios statistikos portalas. (2017). Prieiga per internetą: https://osp.stat.gov.lt/ [žiūrėta 2017 10 15]

Šidlauskas A. Vartotojų elektroninių duomenų apsaugos ypatumai / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. T. Limba. – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir verslo fakultetas, 2017. – 69 p.

SANTRAUKA

Darbo tikslas – išanalizuoti vartotojų elektroninių duomenų saugumo ypatumus, bei pasiūlyti rekomendacijas, kurios padėtų sumažinti duomenų praradimo, neteisėto pasinaudojimo rizikas.

Mokslinė problema. Nesirūpinama elektroninių duomenų apsauga, išskirtos kompleksinės saugumo dalys: naudojami prasti (silpni) slaptažodžiai, neatsakingai dalinamasi privačia informacija socialiniuose tinkluose su trečiosiomis šalimis, neatnaujinama operacinė sistema, nedaromos atsarginės duomenų kopijos, nenaudojama antivirusinė programinė įranga ir t.t.

Darbo objektas – vartotojų elektroninių duomenų apsaugos priemonių taikymo ypatumai.

Mokslinės literatūros ir statistinių duomenų analize buvo siekiama išanalizuoti elektroninių duomenų saugumo ypatumus. Atliktas kiekybinis tyrimas kuriuo siekiama sužinoti Lietuvos interneto vartotojų nuomonę, kokios apsaugos priemonės naudojamos siekiant apsaugoti duomenis ir išvengti kibernetinių incidentų; ar atsakingai dalinamasi privačiais duomenimis „Facebook“ socialiniame tinkle.

Išskirtas „CIA triados“ praradimo poveikis ir galimos pasekmės, bei kontrolės metodai. Nustatyta, kad vartotojai naudodamiesi „Facebook“ socialinio tinko autentifikacijos funkcija „atiduoda“ savo asmeninius duomenis trečiosioms šalims, kad galėtų naudotis jų teikiamomis paslaugomis.

Darbą sudaro 3 dalys. Pirmoje darbo dalyje nagrinėjami vartotojų elektroninių duomenų apsaugos teoriniai aspektai: „CIA triada“, saugaus slaptažodžio sudarymo sistema, atakos prieš slaptažodžius, kritinės kontrolės priemonės. Antroje darbo dalyje pateikiama praktinio apsaugos priemonių taikymo analizė: „Windows 10“ operacinės sistemos autentifikavimo funkcijos, asmens duomenų saugumas „Facebook“ socialiniame tinkle. Trečioje dalyje nagrinėjamas atliktas tyrimas, kurio tikslas - sužinoti vartotojų nuomonę, kokios apsaugos priemonės naudojamos siekiant apsaugoti duomenis ir išvengti kibernetinių incidentų; ar atsakingai dalinamasi privačiais duomenimis „Facebook“ socialiniame tinkle.

Raktiniai žodžiai: elektroninė informacija, slaptažodis, autentifikavimas, kritinės kontrolės priemonės, duomenų saugumas.

Sidlauskas A. Users electronic data protection features / Master‘s Work in Cyber Security Management. Supervisor assoc. prof. T. Limba. –Vilnius: Mykolas Romeris University, Faculty of Economics and Business, 2017. – 69 p.

SUMMARY

The aim of the work is to analyze the peculiarities of consumer electronic data security and to propose recommendations that would reduce the risk of data loss and misuse.

Scientific problem. Electronic data protection is not provided, the following elements of complex security are used: poor (passive) passwords used, irresponsible sharing of private information on social networks with third parties, non-renewal of the operating system, backup data, non-use of antivirus software, etc.

The object – users electronic data relief features.

Scientific literature and statistical analysis was used to analyze the peculiarities of electronic data security. A quantitative study was conducted to find out the opinion of Lithuanian Internet users about the security measures used to protect data and prevent cyber incidents; responsibility of sharing private data on the „Facebook“ social network.

Outstanding effects and potential consequences of the loss of “CIA triad”, and control methods. It has been determined that users use Facebook Social Network Authentication to provide their personal data to third parties in order to use their services.

Master‘s thesis consists of three parts. The first part deals with users- electronic data protection theoretical aspects: “CIA triad”, secure password creation, password cracking attacks, critical security controls. The second part of the work provides an analysis of the practical application of protective measures: „Windows 10“ operating system authentication features, personal data security on „Facebook“ social network. The third part analyze quantitative study, which aims - to find out the views of users, what kind of security measures used to protect data and prevent cyber incidents; responsibility of sharing private data on the „Facebook“ social network.

Key words: electronic information, password, authentication, critical security controls, data security.

PRIEDAI

1 priedas. Tyrime panaudota anketa

Laba diena. Aš, Mykolo Romerio universiteto Kibernetinio saugumo valdymo magistrantūros studijų studentas, atlieku tyrimą „Vartotojų elektroninių duomenų apsaugos ypatumai".

Tyrimo tikslas – sužinoti Lietuvos interneto vartotojų nuomonę, kokios apsaugos priemonės naudojamos siekiant apsaugoti duomenis ir išvengti kibernetinių incidentų; ar atsakingai dalinamasi privačiais duomenimis „Facebook" socialiniame tinkle.

Tyrimo metu gauta informacija bus pateikta apibendrinta forma. Šioje anketoje Jūsų pateikti duomenys viešai nebus skelbiami. Maloniai prašome Jūsų atsakyti į pateiktus klausimus.

Pažymėkite atsakymą apibraukdami tinkamą variantą.

1. Kuri informacijos saugumo kategorija Jums svarbiausia?
   - Konfidencialumas
   - Vientisumas
   - Prieinamumas

2. Ar esate susidūrę su kibernetiniais incidentais?
   - Taip
   - Ne
   - Nežinau

3. Jeigu praeitame (pirmame) klausime atsakėte „taip", tuomet kokią žalą patyrėte?
   - Prarasti duomenys arba sugadinti duomenys
   - Neteisėtas prisijungimas
   - Užblokuota prieiga
   - Tinka visi atsakymai

4. Ar kurdami slaptažodį vadovaujatės saugaus slaptažodžio rekomendacijomis?
   - Taip
   - Ne
   - Nežinau

5. Ar naudojate skirtingus slaptažodžius skirtingose interneto puslapių paskyrose?
    - Taip
    - Ne, visur naudoju vieną ir tą patį slaptažodį
    - Skirtingus slaptažodžius naudoju atsižvelgiant į paskyros svarbumą

6. Jeigu naudojatės „Windows 10“ operacine sistema, kuris autentifikacijos būdas priimtiniausias?
    - Slaptažodis
    - PIN kodas
    - Paveikslėlio slaptažodis
    - Biometriniai duomenys
    - Nenaudoju jokio

7. Ar esant galimybei naudojatės „Facebook“ socialinio tinklo autentifikacijos (tapatybės patvirtinimo) funkcija, norėdami užsiregistruoti e. sistemoje?
    - Taip
    - Ne
    - Kartais

8. Jeigu praeitame (septintame) klausime atsakėte „taip“ arba „kartais“, tuomet ar atkreipėte dėmesį ir atsakingai įvertinote kokius savo asmeninius duomenis atiduodate trečiajam asmeniui?
    - Taip, visada stengiuosi pateikti minimalius duomenis
    - Ne, niekad apie tai nesusimąsčiau

9. Ar reguliariai atnaujinate programinę įrangą?
    - Taip
    - Ne
    - Neturiu tam reikiamų įgūdžių

10. Ar naudojatės operacine sistema nuolatos prisijungęs administratoriaus teisėmis?
    - Taip
    - Ne
    - Nežinau, niekad neatkreipiau į tai dėmesio

11. Ar naudojate antivirusinę programą?
    - Taip
    - Ne

12. Ar šifruojate duomenis?
    - Taip, visus
    - Tik pačius svarbiausius
    - Ne
    - Neturiu tam reikiamų įgūdžių

13. Ar darote duomenų atsargines kopijas?
    - Taip, visada
    - Taip, tik svarbiausių duomenų
    - Ne

14. Ar tikrinate kokia programinė įranga „gyvena“ Jūsų kompiuteryje?
    - Taip, ištrinu neatpažintą arba nenaudojamą programinę įrangą
    - Ne, man tai nerūpi
    - Kartais

15. Kaip vertinate savo žinias IT saugumo srityje?
    - Puikiai
    - Gerai
    - Vidutiniškai
    - Blogai