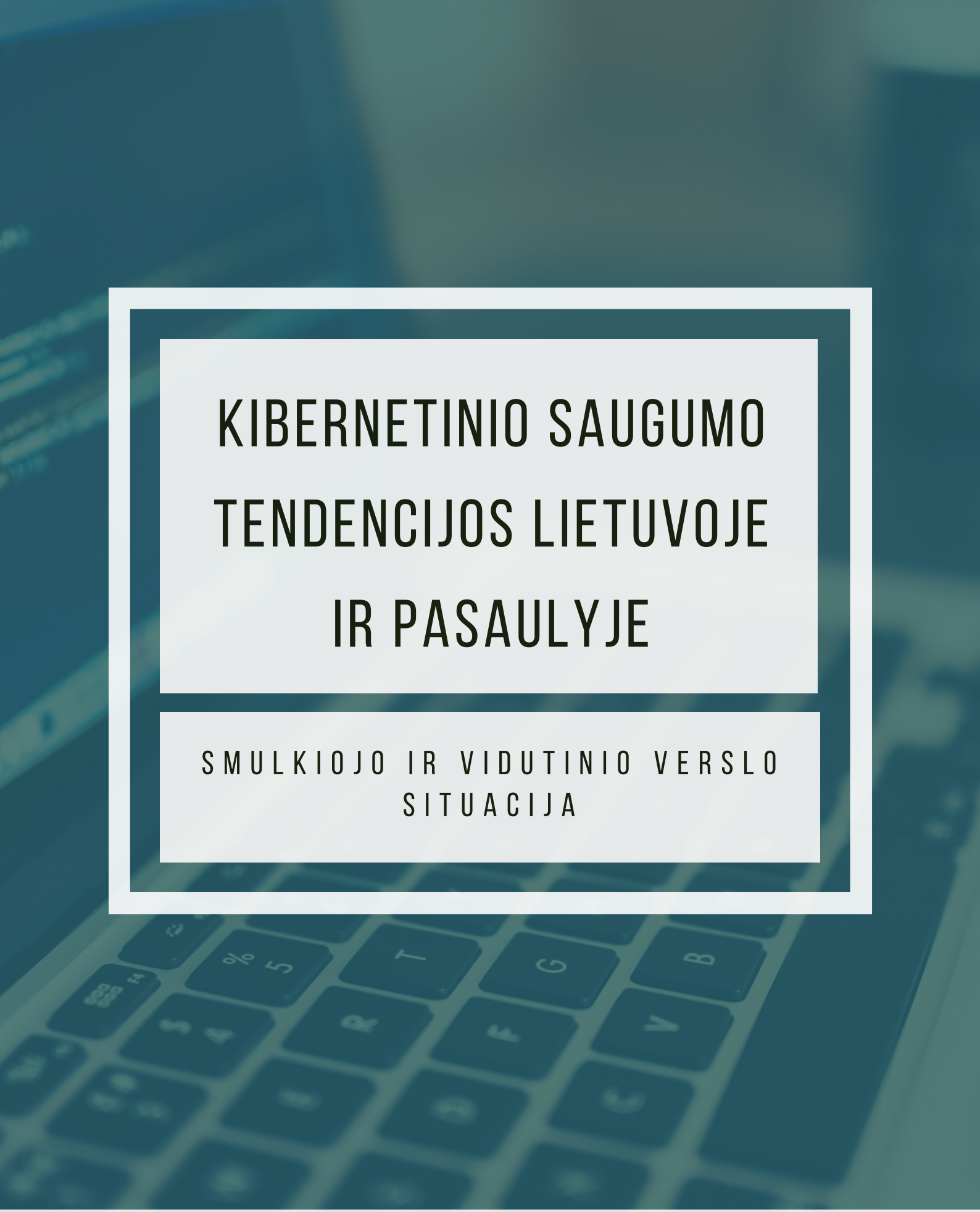


KIBERNETINIO SAUGUMO TENDENCIJOS LIETUVOJE IR PASAULYJE

SMULKIOJO IR VIDUTINIO VERSLO SITUACIJA

GABRIELĖ BILEVIČIŪTĖ
JUSTAS KIDYKAS
RŪTA BEINORIŪTĖ

SPALIS, 2019

PAGRINDINĖS SĄVOKOS

KIBERNETINIS SAUGUMAS

visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.

KIBENETINIS INCIDENTAS

įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

KIBERNETINĖ ERDVĖ

aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą.

Vartojamos sąvokos ir paaiškinimai atitinka Kibernetinio saugumo įstatyme apibrėžtas sąvokas.

KIBERNETINIO SAUGUMO POLITIKA LIETUVOJE

KIBERNETINIO SAUGUMO PRINCIPAI

Kibernetinio saugumo įstatyme įvardijami šie kibernetinio saugumo **principai**:

1) **kibernetinės erdvės nediskriminavimo** – teisės aktų nuostatos yra taikomos, o gėriai yra saugomi vienodai tiek fizinėje, tiek kibernetinėje erdvėje;
2) **kibernetinio saugumo rizikos valdymo** – taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;
3) **kibernetinio saugumo proporcingumo** – taikomos teisinės, organizacinės ir techninės kibernetinio saugumo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina;
4) **viešojo intereso viršenybės** – taikomos kibernetinio saugumo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;
5) **standartizacijos ir technologinio neutralumo** – įgyvendinant kibernetinio saugumo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;
6) **subsidiarumo** – už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinei kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

PAGRINDINIAI AKTORIAI

nustato kibernetinio saugumo politikos strateginius tikslus ir jiems pasiekti būtinas priemones

- **Lietuvos Respublikos Vyriausybė**

formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą

- **Krašto apsaugos ministerija**
- **Vidaus reikalų ministerija**
- **Nacionalinis kibernetinio saugumo centras**
- **Ryšių reguliavimo tarnyba**
- **Valstybinė duomenų apsaugos inspekcija**
- **Policijos departamentas prie LR VRM**

kibernetinio saugumo politiką pagal kompetenciją įgyvendina

- **Vidaus reikalų ministerija**
- **Nacionalinis kibernetinio saugumo centras**
- **Ryšių reguliavimo tarnyba**
- **Valstybinė duomenų apsaugos inspekcija**
- **Policijos departamentas**

LIETUVOS KIBERNETINIO SAUGUMO STRATEGIJA

TIKSLAI

1. STIPRINTI VALSTYBĖS KIBERNETINĮ SAUGUMĄ IR KIBERNETINIŲ GYNYBOS PAJĖGUMŲ PLĖTRĄ
2. UŽTIKRINTI NUSIKALSTAMŲ VEIKŲ KIBERNETINĖJE ERDVĖJE PREVENCIJĄ, UŽKARDYMĄ IR TYRIMĄ
3. SKATINTI KIBERNETINIO SAUGUMO KULTŪRĄ IR INOVACIJŲ PLĖTRĄ
4. STIPRINTI GLAUDŲ VIEŠOJO IR PRIVATAUS SEKTORIŲ BENDRADARBIAVIMĄ
5. STIPRINTI TARPTAUTINĮ BENDRADARBIAVIMĄ IR UŽTIKRINTI TARPTAUTINIŲ ĮSIPAREIGOJIMŲ KIBERNETINIO SAUGUMO SRITYJE VYKDYMĄ.

Antrasis ketvirtojo tikslo uždavinys – didinti viešojo bei **mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo brandą.** Šis uždavinys bus įgyvendinamas skatinant viešojo bei mažo ir vidutinio privataus sektorių atstovus tikrintis kibernetinio saugumo būklę, taisyti kibernetinio saugumo spragas.

Strategijoje įsipareigojama **kurti priemones,** skirtas viešojo bei mažų ir vidutinių privataus sektorių atstovų **kibernetinio saugumo būklei gerinti.** Siekiama, kad 2021 m. būtų bent keturios, o 2023 m. bent šešios tokios priemonės.

Šaltinis: Nacionalinė kibernetinio saugumo strategija, 2018 m.

LIETUVOS KIBERNETINIO SAUGUMO SITUACIJOS APŽVALGA

2018 m. Nacionalinis kibernetinio saugumo centras Lietuvoje užregistravo **53 183** kibernetinius incidentus, kurie palyginus su 2017 m. tapo pažangesniais ir sunkiau aptinkamais. Pažeidžiamų interneto įrenginių skaičius išaugo 21 proc.

Lietuvos 2018 m. kibernetinio saugumo grėsmės ir tendencijos, palyginti su 2017 m.

Didėjo	Socialinė inžinerija
Išliko didelė	Kenkimo PĮ paplitimas
Išliko didelė	Pažeidžiamos interneto svetainės
Nauja	Įrenginių saugumo spragos
Didėjo	Elektroninių ryšių tinklų žvalgyba
Nauja	Rangovų ir ar PĮ (ne)patikimumas
Mažėjo	Elektroninių paslaugų trikdymas

Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus

SOCIALINĖ INŽINERIJA

2018 m. buvo užregistruota 25 proc. daugiau socialinės inžinerijos metodais paremtų kibernetinių nusikaltimų nei 2017 m.

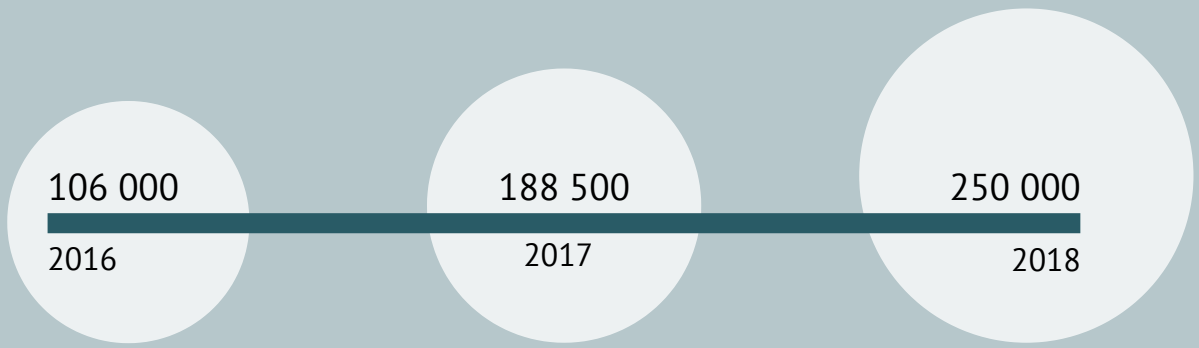
Socialinės inžinerijos metodais paremti kibernetiniai incidentai susiję su manipuliavimu naudotojų veiksmais internete ir apgaule. Jų metu vyksta informacijos rinkimas, platinama kenkimo PĮ, išnaudojami pažeidžiamumai.

Kokie tai incidentai?

Slaptažodžių žvejyba (angl. *Phishing*), viliojimas (angl. *Baiting*), apgaulingų elektroninių laiškų siuntimas, suklastotų interneto svetainių kūrimas, susisiekimas telefonu ir kt.

TENDENCIJOS LIETUVOJE

Socialinės inžinerijos tendencijos 2016 – 2018 m. Lietuvoje.

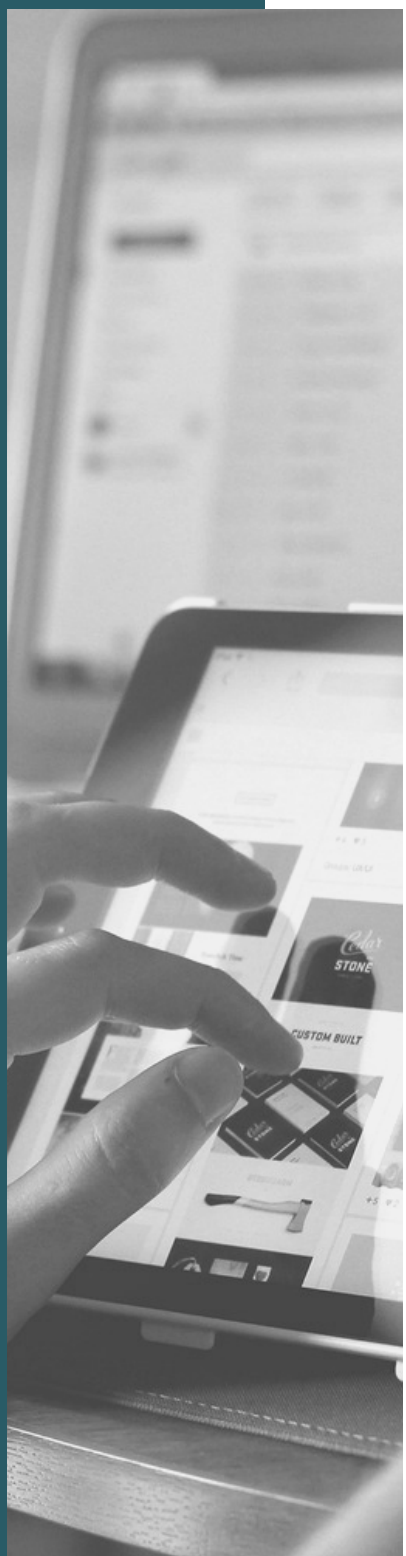


Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus

ĮGŪDŽIŲ STOKA

„Vis dar per mažai dėmesio skiriama darbuotojams šviesti ir sąmoningumui didinti. Deja, ir toliau yra laikomasi nuomonės, kad kibernetinis saugumas yra informacinių technologijų specialistų kompetencijos ir techninės įrangos klausimas“.

- Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus



Socialiniais metodais paremtų kibernetinių incidentų priežastis yra **kibernetinio saugumo ir IT įgūdžių stoka**. Tokie incidentai yra ypač svarbūs verslo įmonėms, kurios patiria finansinę žalą ar praranda konfidencialią informaciją.

„Samsung“ atlikta apklausa parodė, kad **30 proc.** respondentų, patyrusių kibernetines atakas nenutuokia, kaip įsilaužėliai pasiekė jų asmeninius duomenis ir net **daugiau nei 60 proc. nežino,** kokių veiksmų imtis, jei įsilaužta į jų įrenginius ar paskyras, rašoma pranešime žiniasklaidai.

Lietuvos kibernetinio saugumo strategijoje taip pat pažymima, kad nuo kibernetinių incidentų negalima apsisaugoti net ir taikant visas esamas technines kibernetinio saugumo priemones. Dėl to svarbu, kad **privataus sektorių atstovai rūpintųsi savo darbuotojų kibernetinės kultūros kėlimu.**

Šaltiniai: Samsung (2019): „Esate tikras, kad niekada nepatyrėte kibernetinės atakos? Pasitikrinkite, ar tikrai“.; Nacionalinė kibernetinio saugumo strategija, 2018 m.

INTERNETO SVETAINĖS

„Kibernetinio saugumo, verslo subjektai deramai neįvertina potencialios žalos, kurią patirtų dėl kibernetinio incidento, nevertina savo interneto svetainių, kaip svarbaus informacinio turto, reikalingo jų veiklai, taip pat neįvertina to, kad dalyje interneto svetainių yra saugomi asmens duomenys“.

- Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus

52%

INTERNETO SVETAINIŲ

yra pažeidžiamos, pagal 2018 m. Lietuvos interneto svetainių turinio valdymo sistemų (TVS) tyrimo rezultatus.

9%

ŠIŲ INTERNETO SVETAINIŲ

turi itin didelių pažeidžiamumų. Didžiausia pažeidžiamumo grėsmė kyla toms interneto svetainėms, kurios turi „Wordpress“, „Joomla“ TVS.

Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 m.

SMULKIOJO IR VIDUTINIO VERSLO KIBERNETINIO SAUGUMO SITUACIJA LIETUVOJE

Labai mažų, mažų ir vidutinių įmonių samprata:

Įmonės tipas	Darbuotojų skaičius	Finansiniai duomenys atitinka bent viena iš šių sąlygų	
		Metinės pajamos neviršija, mln. EUR	Turto balansinė vertė neviršija, mln. EUR
Vidutinė įmonė	Mažiau kaip 250	50	43
Maža įmonė	Mažiau kaip 50	10	10
Labai maža įmonė	Mažiau kaip 10	2	2

Lietuvos Respublikos Ekonomikos ir inovacijų ministerijos duomenys

99,8%

VISŲ ĮMONIŲ LIETUVOJE

sudaro mažosios ir vidutinės įmonės

3 iš 4

LIETUVIŲ DIRBA

smulkaus ir vidutinio dydžio įmonėse

68,5%

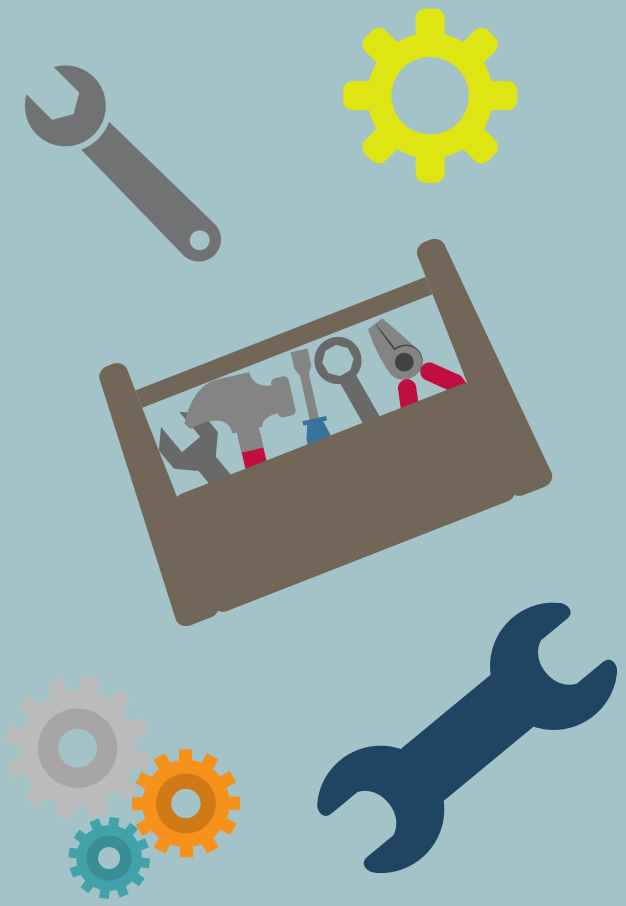
BVP DALIS

sukuriama smulkiojo ir vidutinio verslo įmonių

Šaltiniai: Statistikos departamentas, Europos Komisijos „Europos smulkiojo verslo akto“ ataskaita

KIBERNETINIO SAUGUMO PRIEMONIŲ NAUDOJIMAS

Statistikos departamento atliktas „Informacinių technologijų naudojimas įmonėse 2019 m.” tyrimas rodo, kad **smulkiojo ir vidutinio verslo (SVV) įmonės yra mažiau pasiruošusios atremti kibernetines grėsmes**. Vidutiniškai smulkios įmonės (10-49 darbuotojai), **36 proc. mažiau nei didelės įmonės** (250+ darbuotojai) naudojo bent vieną kibernetinio saugumo / e. saugos priemonę.



1 RIZIKŲ VERTINIMAS

Smulkios įmonės 44 proc. mažiau nei didelės įmonės vykdė IT rizikų vertinimą

2 SLAPTAŽODIS

Smulkios įmonės 29 proc. mažiau nei didelės įmonės naudojo griežtą tapatumo patvirtinimo slaptažodį.

3 TESTAVIMAS

E. saugos testavimą vykdė tik 24 proc. smulkių įmonių, tuo tarpu 58 proc. didelių įmonių vykdė tokį testavimą.

4 DARBUOTOJŲ MOKYMAS

Privalomus e. saugos mokymus darbuotojams turėjo tik 18 proc. smulkių ir 29 proc. vidutinių įmonių, o tuo tarpu tokius mokymus turėjo net 43 proc. didelių įmonių.

Statistikos departamento duomenys. „Informacinių technologijų naudojimas įmonėse 2019 m.”

5 IT MOKYMAI

IT mokymus darbuotojams organizavo tik 8 proc. smulkių įmonių ir net 52 proc. didelių įmonių.

6 DARBUOTOJŲ INFORMAVIMAS

Sudarant sutartį apie e. saugą darbuotojus informavo tik 57 proc. smulkių ir vidutinių įmonių.

KIBERNETINIO SAUGUMO PASLAUGŲ KAINOS

Įvairūs Lietuvoje siūlomi kibernetinio saugumo / e. saugos priemonių sprendimai (*šių paslaugų teikėjai - įmonės, įstaigos ar asmenys nėra įvardijami*).

242 EUR

Tiek per metus kainuoja **vidutinio apsaugos lygio priemonių paketas** SVV

750 EUR

Kibernetinio saugumo **pagrindų mokymai** (2 dienos, 1 asm.)

nuo
700 EUR

Kibernetinio saugumo **žinių mokymai** (2 val., iki 35 asm.)

120 EUR

Seminaras apie kibernetinio **saugumo reikalavimus** įmonėms bei organizacijoms (4,5 val., 1 asm.)

100 EUR

Reguliari **sistemų priežiūra** (5 val. per mėnesį)

~180 EUR

Per metus už **kompiuterių priežiūrą** 24/7 (už darbo vietą per mėnesį). Kaina per mėnesį nuo 15 EUR.

40 EUR/val.

Darbo vietų techninės ir programinės **įrangos tvarkymas, testavimas**

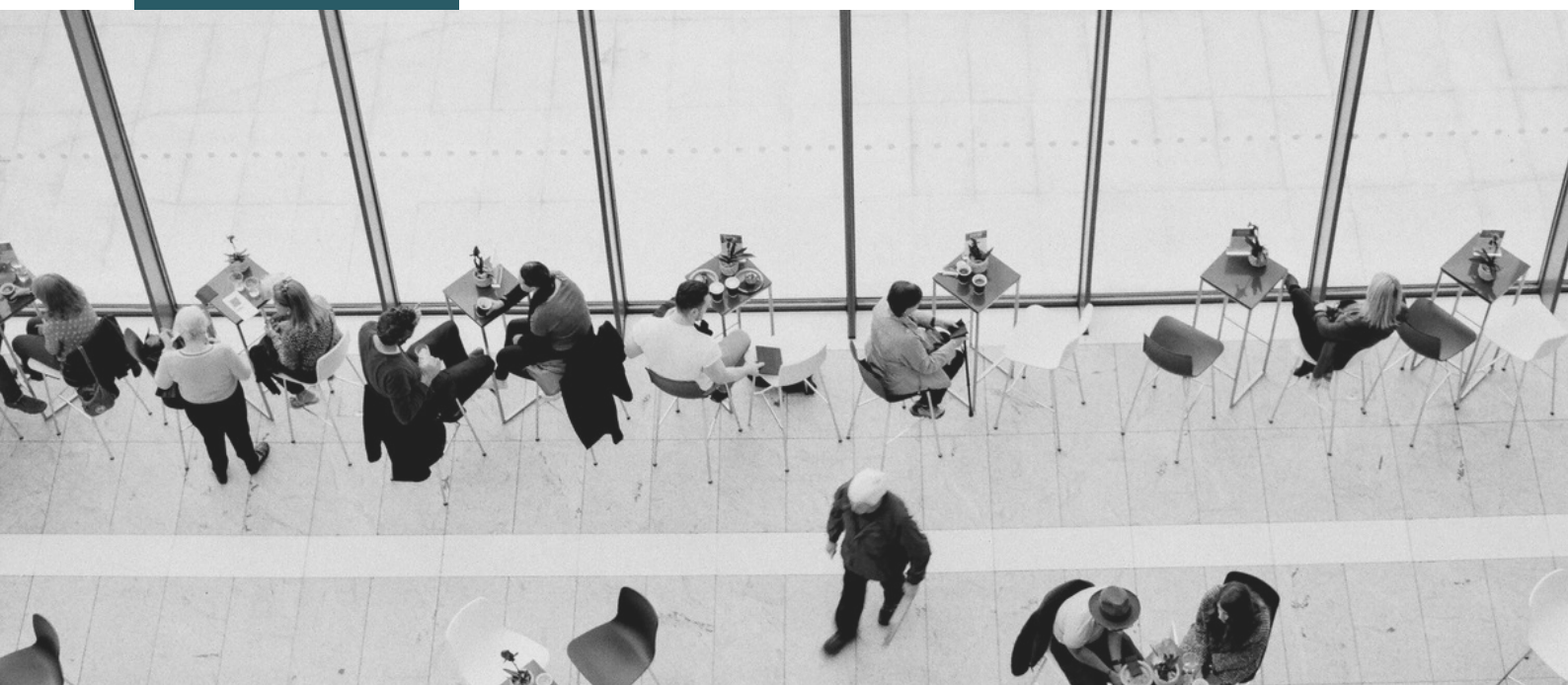
20 EUR

IT specialisto atvykimas į kliento darbo vietą Vilniaus mieste

SVV KIBERNETINIO SAUGUMO TENDENCIJOS PASAULYJE

Kibernetinės atakos jau ne pirmus metus atsiduria tarp dažniausiai vykdomų nusikaltimų. Tokios nusikalstamos veikos kibernetinėje erdvėje, kaip rodo „PwC“ kompanijos 2018 m. atlikto Pasaulio ekonominių nusikaltimų tyrimas, daro **didžiausią žalą privačiam sektoriui ir turi didelį neigiamą poveikį pasaulio ekonomikai**. Smulkaus bei vidutinio verslo įmonės yra vienos pagrindinių programišių taikinių. Nepaisant, kad atakos prieš SVV (ypač smulkiąsias) įmones gana retai pasiekia žiniasklaidos antraštes, beveik pusė visų kibernetinių atakų yra nukreiptos prieš smulkiojo ir vidutinio verslo įmones – „Cisco“ įmonės tyrimas teigia, kad per 2018 metus net **53 proc. tokių įmonių patyrė kibernetinius pažeidimus** [1].

[1] „Cisco Cybersecurity Report: Special Edition SMB“ (Cisco, 2018)



KODĖL SVV NĖRA PASIRENGĘS?

KIBERNETINIO SAUGUMO PRIEMONIŲ TRŪKUMAS

47 % SVV įmonių nežino kaip reikėtų apsisaugoti nuo kibernetinių atakų ir tik trečdalis jų (33 %) jaučiasi visiškai pasiruošusios atremti kibernetinio saugumo atakas [2]. Mažų įmonių kibernetinio saugumo priemonės dažnai yra nepakankamos [3], o atakai jau įvykus smulkesnės įmonės neturi užtektinai žmogiškųjų ir techninių išteklių incidento suvaldymui ir situacijos atstatymui [4].

RIZIKOS NEĮVERTINIMAS

51 % SVV teigia nemanančios, jog gali būti kibernetinės atakos aukomis [5]. Technologijų plėtra ir platesnis daiktų interneto (angl. *Internet of Things*) naudojimas didina pažeidžiamumo mastą bei poreikį tinklo valdymo paslaugoms. Net 42 % įmonių teigia nežinančios, kokie veiksniai lemia tai, kad įvyksta įsilaužimas ir net 60 % įmonių negali įvardyti įsilaužimo šaltinio [6]. Nepaisant didelio atakų prieš SVV įmones skaičiaus, jos **nemato kibernetinio saugumo kaip esminės rizikos veiklos tęstinumui** [7]. SVV įmonės nėra izoliuotos viena nuo kitos – dažnu atveju jos yra didelių organizacijų tiekimo grandies dalis. Dėl to, rizika išlieka ne vien SVV įmonėms, bet ir jų verslo partnerių saugumui ir jų klientų duomenų apsaugai. Jungtinės Karalystės atvejis rodo, kad tik 18 % įmonių reikalauja tiekėjų turėti ar laikytis tam tikrų kibernetinio saugumo standartų [8].

SKAITMENINIO TURTO VERTĖS NESUVOKIMAS

Verslo subjektai nesuvokia savo interneto svetainių, kaip svarbaus informacinio turto, reikalingo jų veiklos tęstinumui ir neįvertina to, kad dalyje interneto svetainių yra saugomi asmens duomenys [9]. Statistika rodo, kad **įmonės, laikančios klientų duomenis skaitmeniniu būdu, dažniau patiria kibernetines atakas** [10]. Dėl kibernetinės atakos sutrikusi įmonės ir internetinio puslapio veikla gali padaryti daug žalos, kurią sunku įvertinti. Ši žala neapsiriboja internetinio puslapio atkūrimu. Dėl veiklos sutrikimų įmonės praranda klientus, pajamas, o kai kuriais atvejais gresia baudos dėl Bendrojo duomenų apsaugos reglamento (BDAR) reikalavimų nesilaikymo. Dažnu atveju, finansiniai nuostoliai po incidento yra didesni nei momentinė įsilaužimo žala. **Svetainė nėra tik svetainė – tai yra tiltas į kitus incidentus ir kitų organizacijų tinklus.**

DABUOTOJŲ ŽINIŲ TRŪKUMAS

Daugiau nei 20 % kibernetinių incidentų privačiame sektoriuje įvyksta dėl **darbuotojų aplaidumo ar nežinojimo** (tokių incidentų skaičius kyla) [11]. Duomenų vagystės „žvejybos“ būdu (angl. *phishing*) vis dar yra vienas iš pagrindinių (ir neretai labiausiai nuostolingų) sukčiavimo internete atvejų [12]. **Net 70 % SVV įmonių teigia, kad per tris mėnesius yra užfiksuojamas bent vienas „žvejybos“ atvejis** [13]. Neužtenka technologinių sprendimų apsaugančių nuo visų grėsmių. Apklausos Jungtinėje Karalystėje rodo, kad net 43 % įmonių sutinka, kad jos yra **pažeidžiamesnės dėl nepakankamo kibernetinio sąmoningumo** lygio įmonių viduje [14].

KIBERNETINIŲ SAUGUMO PRIEMONIŲ KAINA IR KOMPLEKSIŠKUMAS

Verslas dažnai neįvertina investicijų į kibernetinio saugumo priemones naudos ir atnešamos grąžos. JK atvejis rodo, kad **33 % smulkių ir 18 % vidutinio dydžio įmonių per metus kibernetinio saugumo priemonėms neišleidžia nė svaro,** o vidutiniškai SVV įmonė išleidžia vos 200 svarų, kas yra lygu metiniam antivirusinės ar antikenkėjiškos programinės įrangos mokesčiui [15]. Be to, **kibernetinis saugumas nėra baigtinis procesas** – IT sistemų kompleksiškumas ir sąveika yra nuolat kintanti bei reikalaujanti reguliarių priemonių atnaujinimo. Bazinių kibernetinių saugumo mokymų pasiūla yra, tačiau mažesnės įmonės dažnai nemato prasmės apmokyti visų darbuotojų arba nėra linkusios skirti papildomų kaštų. Pavyzdžiui, Jungtinėje Karalystėje vos trečdalis įmonių siunčia savo darbuotojus į vidinius arba išorinius kibernetinio saugumo įgūdžių ir / arba sąmoningumo ugdymo mokymus [16].

[2] „SME Supply Chain Research“ (KPMG, 2015).
[3] „The Kaspersky Lab Global IT Risk Report“ (Kaspersky, n.d.).
[4] „Cyber Security ‘Myths’ Putting a Third of SME Revenue at Risk“ GOV.UK (Cabinet Office, Home Office, The Rt Hon Karen Bradley MP, and Ed Vaizey, 2015).
[5] „2018 State of Cybersecurity in Small & Medium Size Businesses (SMBs)“.
[6] Kelly Finnerty et al., „Cyber Security Breaches Survey 2019,“ 2019.
[7] „2018 State of Cybersecurity in Small & Medium Size Businesses (SMBs)“ (Ponemun Institute, 2018).
[8] Finnerty et al., „Cyber Security Breaches Survey 2019“.
[9] „Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus“ (Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, 2018).
[10] Finnerty et al., „Cyber Security Breaches Survey 2019“.
[11] „IBM X-Force Threat Intelligence Index 2018“ (IBM, 2018).
[12] „Nacionalinio kibernetinio saugumo būklės ataskaita už 2018metus“.
[13] „The Kaspersky Lab Global IT Risk Report“.
[14] Rebecca Klahr et al., „Cyber Security Breaches Survey 2017: Main Report,“ 2017.
[15] Finnerty et al., „Cyber Security Breaches Survey 2019“.
[16] Finnerty et al.

KOKIA ŽALA?

Dažnu atveju kibernetinių atakų nuostoliai verslui yra sunkai nusakomi ir paskaičiuojami, tačiau ekspertai sutinka, kad bendra rizika ir su ja susiję nuostoliai ateityje tik didės. Europos kovos su elektroniniu nusikalstamumu centras (EC3) prognozuoja, kad tokių nusikaltimų skaičius vis didės, o Pasaulio ekonomikos forumo visuotinių grėsmių ataskaitoje yra skelbiama, kad kibernetinių nusikaltimų **padaroma žala pasaulinei ekonomikai 2021 metais gali siekti net 6 milijardus JAV dolerių**. Kibernetinių įsilaužimų žalos apskaičiavimai pasaulyje skiriasi, kadangi nėra vieningai sutartos metodikos nuostolių įvertinimui. Padaryta žala dažnai būna daug kartų didesnė nei išlaidos, kurių būtų reikėję siekiant užkirsti kelią tokiems išpuoliams. Didelės kompanijos apsaugai nuo tokių atakų skiria nemažai lėšų, todėl **pagrindiniais taikiniais tampa mažos įmonės.** Vienuose tyrimuose į žalos apskaičiavimą yra įtraukiami tik tiesioginiai, su laikinu veiklos sutrikimu susiję nuostoliai, tačiau kituose tyrimuose yra įtraukiamas duomenų atkūrimas, sistemų remontas ir atnaujinimas, prarastas pelnas ir galimi nauji klientai, krizinės komunikacijos išlaidos, teisinių procesų išlaidos ir baudos (pvz. dėl BDAR pažeidimų). Dėl to, skirtingų tyrimų rodikliai gerokai skiriasi.

Palyginimui, Jungtinės Karalystės vyriausybės užsakyta apklausa parodė, kad vidutinė vieno įsilaužimo kaina **smulkioms įmonėms siekia 5,430 svarų, o vidutinėms – 10,470 svarų** [17], tuo tarpu „Kaspersky“ įmonės tyrimas Jungtinėse Valstijose parodė, kad SVV įmonės dėl kibernetinių atakų vidutiniškai patiria net 149,000 dolerių nuostolių [18]. Nepaisant žalos skaičiavimo neatitikimų tarp skirtingų tyrimų, juose taip pat yra pažymima, kad įmonės negeba suvokti galimos žalos masto. Tas pats „Kaspersky“ tyrimas rodo, kad 70 % apklaustų įmonių teigia, kad kibernetinio incidento atveju nuostoliai įmonei nesiektų 25,000 dolerių, vis dėlto, įvykusių incidentų analizė rodo kur kas didesnius skaičius. Smulkesniam verslui ir 10,000 eurų nuostolis jau yra didelis smūgis, kuris gali nulemti pačios įmonės likimą [19].

Britų ekspertai pabrėžia, kad verslui dažniausiu atveju yra labai **sudėtinga ir neaišku kaip reikėtų tikslingai įsivertinti įsilaužimo žalą**, ko pasekmėje, įmonėms yra sunku įvertinti investicijų į kibernetinio saugumo priemones (net ir bazines) grąžą [20]. Bendra kibernetinių atakų žala nacionaliniu mastu irgi yra sunkiai nustatoma, kadangi tik maža dalis įmonių informuoja atitinkamas saugumo ir teisėsaugos institucijas apie įvykusias kibernetines atakas.

[17] Finnerty et al.
[18] „The Kaspersky Lab Report: The Cost of a Data Breach Continues to Grow Worldwide“ (Kaspersky, 2018).
[19] „Annual Cyber Security Assessment 2019“ (Estonian Information System Authority, 2019).
[20] Finnerty et al., „Cyber Security Breaches Survey 2019“.

MAŽOS KLAIDOS KAINUOJA DAUG

yahoo!

Įsilaužimo į „Yahoo“ metu, 2014 metais buvo nutekinta informacija iš 3 milijardų naudotojų paskyrų. Tam, jog patektų į vidinį tinklą, programišiui užteko nusiųsti elektroninį laišką su prisegtu kenkėjišku failu vienam iš kompanijos darbuotojų.

Uber

„UBER“ 2016 -ųjų spalį buvo nutekinta informacija apie 56 milijonus vairuotojų. Šis incidentas kilo, nes IT specialistas laikė slaptažodžius viešai prieinamoje „Github“ saugykloje.

EQUIFAX

2017 m. liepą įmonė „Equifox“ pranešė, jog buvo nutekinta 146 milijonų klientų asmens duomenys. Skaičiuojama, kad apie 56,200 buvo pasai, vairuotojų pažymėjimai, mokesčių mokėtojų ID numeriai. Skaičiuojama jog ši ataka galėjo kainuoti daugiau nei 600 milijonų dolerių. Silpnąją vietą programišiai rado įmonei laiku neatnaujinus „Apache Struts“ programinės įrangos. Gavus prieigą prie vidinio tinklo, piktavaliai turėjo marias laiko jautrios ir silpnai apsaugotos informacijos paieškai.

Cituojami atvejai iš 15min. „Ko reikėtų pasimokyti iš eilinės šimtų milijonų žmonių duomenų vagystės?“

VIEŠOJI KONSULTACIJA

Siekiant parengti priemonių paketą, kuris padėtų SVV įmonėms kelti savo kibernetinio saugumo žinias ir didinti atsparumą kibernetinėms grėsmėms, bus vykdoma viešoji konsultacija. Viešosios konsultacijos tikslas – nustatyti Lietuvos SVV įmonių (darbuotojų skaičius iki 250) kibernetinio saugumo spragas ir poreikius šioje srityje bei identifikuoti potencialias SVV įmonių kibernetinio saugumo stiprinimo priemones, kurias galėtų kurti ar įgyvendinti valstybės institucijos

APKLAUSA

SVV įmonių vadovų ir darbuotojų apklausa, vykdoma internetu, siekiant išsiaiškinti šių įmonių kibernetinio saugumo spragas ir sąmoningumo stiprinimo priemonių poreikį.

Apklausa SVV įmonės (darbuotojų skaičius iki 250) **vadovams** – http://epilietis.lrv.lt/lt/formos/kibernetinis-saugumas-svv-vadovai

Apklausa SVV įmonės (darbuotojų skaičius iki 250) **darbuotojams** – http://epilietis.lrv.lt/lt/formos/kibernetinis-saugumas-svv-darbuotojai

INTERVIU CIKLAS

Interviu ciklas su viešojo, privataus ir akademinio sektoriaus ekspertais padės paruošti informacinį paketą, kuris padėtų gerinti kibernetinio saugumo supratimą SVV įmonėse.

KONSULTACIJOS TRUKMĖ

- Apklausa vykdoma iki 2019 m. gruodžio 15 d.
- Interviu ciklas vykdomas iki 2020 m. sausio 10 d.

KONTAKTAI

Gabrielė Bilevičiūtė *gabriele.bileviciute@kurklt.lt*
Justas Kidykas *justas.kidykas@kurklt.lt*
Rūta Beinoriūtė *ruta.beinoriute@kurklt.lt*

http://kurklt.lt/projektai/smulkiojo-ir-vidutinio-verslo-imoniu-kibernetinio-saugumo-samoningumo-didinimas/

LITERATŪROS SĄRAŠAS

1. „Nacionalinio kibernetinio saugumo būklės ataskaita už 2018 metus“, (Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, 2018) https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf;
2. „Ko reikėtų pasimokyti iš eilinės šimtų milijonų žmonių duomenų vagystės?“ 15min. https://www.15min.lt/mokslasit/straipsnis/technologijos/ko-reiketu-pasimokyti-is-eilines-simtu-milijonu-zmoniu-duomenu-vagystes-646-1071220;
3. Lietuvos Respublikos Ekonomikos ir inovacijų ministerija, http://eimin.lrv.lt/lt/veiklos-sritys/verslo-aplinka/smulkiojo-ir-vidutinio-verslo-politika;
4. Samsung (2019): „Esate tikras, kad niekada nepatyrėte kibernetinės atakos? Pasitikrinkite, ar tikrai" https://www.samsung.com/lt/news/local/esate-tikras-kad-niekada-nepatyrete-kibernetines-atakos-pasitikrinkite-ar-tikrai/;
5. Lietuvos Respublikos Vyriausybė, Nacionalinė kibernetinio saugumo strategija, (2018);
6. Lietuvos Respublikos Seimas, Lietuvos Respublikos kibernetinio saugumo įstatymas (2014, XII-1428);
7. „Informacinių technologijų naudojimas įmonėse 2019 m.” (Statistikos departamentas, 2019) https://osp.stat.gov.lt/informaciniai-pranesimai?sritis=7&tema=39;
8. „Europos smulkiojo verslo akto“ ataskaita (Europos komisija, 2018) https://ec.europa.eu/growth/smes/business-friendly-environment/performance-review_en;
9. „Cisco Cybersecurity Report: Special Edition SMB“ (Cisco, 2018) https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf;
10. „SME Supply Chain Research“ (KPMG, 2015) https://home.kpmg/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf;.
11. „The Kaspersky Lab Global IT Risk Report“ (Kaspersky, n.d.) https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf;
12. „Cyber Security ‘Myths’ Putting a Third of SME Revenue at Risk“ GOV.UK (Cabinet Office, Home Office, The Rt Hon Karen Bradley MP, and Ed Vaizey, 2015). https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk;
13. „2018 State of Cybersecurity in Small & Medium Size Businesses (SMBs)“. (Ponemun Institute, 2018), https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf;
14. Kelly Finnerty et al., „Cyber Security Breaches Survey 2019,“ 2019;.
15. „IBM X-Force Threat Intelligence Index 2018“ (IBM, 2018) https://www.ibm.com/security/data-breach/threat-intelligence;
16. Rebecca Klahr et al., „Cyber Security Breaches Survey 2017: Main Report,“ 2017;
17. „The Kaspersky Lab Report: The Cost of a Data Breach Continues to Grow Worldwide“ (Kaspersky, 2018) https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-report-the-cost-of-a-data-breach-continues-to-grow-worldwide;
18. „Annual Cyber Security Assessment 2019“ (Estonian Information System Authority, 2019) https://www.ria.ee/sites/default/files/contenteditors/kuberturve/ktt_aastaraport_eng_web.pdf.;