# KIBERNETINIS SAUGUMAS IR VERSLAS

## KĄ TURĖTŲ ŽINOTI KIEKVIENAS ĮMONĖS VADOVAS

2020

Kurk Lietuvai

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

KRAŠTO APSAUGOS MINISTERIJA

# KIBERNETINIS SAUGUMAS IR VERSLAS

## KĄ TURĖTŲ ŽINOTI KIEKVIENAS ĮMONĖS VADOVAS

2020

# Įvadas

Kibernetiniai nusikaltimai tampa vis didesniu rūpesčiu verslui visame pasaulyje. Ne išimtis ir Lietuva – net 3 iš 4 smulkiojo ir vidutinio verslo (SVV) vadovų sutinka, kad kibernetinis saugumas yra svarbus jų įmonei. Skirtingi tyrimai rodo, kad SVV įmonės yra mažiausiai pasiruošusios atremti šias grėsmes ar spręsti atsirandančias saugumo spragas, o tuo neretai pasinaudoja kibernetiniai nusikaltėliai. Dėl kintančių verslo poreikių, kai vis daugiau užduočių patikima automatizuotiems IT sprendimams ir įmonių veikla tampa vis labiau priklausoma nuo skaitmeninės informacijos, kyla vis didesnė rizika tapti pažeidžiamiems kibernetinėje erdvėje.

2019 metų „Kurk Lietuvai“ programos dalyvių Krašto apsaugos ministerijoje vykdyto projekto „Smulkiojo ir vidutinio verslo įmonių kibernetinio saugumo sąmoningumo didinimas“ metu atlikta apklausa parodė, kad 74 proc. Lietuvos SVV įmonių jaučiasi nepasiruošusios arba nežino, ar yra pasiruošusios atremti kibernetines atakas. Po atlikto tyrimo ir interviu ciklo su kibernetinio saugumo ekspertais nustatyta, kad pažeidžiamiausias privačiame sektoriuje yra smulkusis šalies verslas.

Kibernetinis saugumas po truputį tampa neatsiejama verslo gyvybingumo ir plėtros dalimi. Kibernetinio incidento padariniai SVV gali būti itin skaudūs, kartais net lemtingi verslo pranašumui ar tęstinumui. Tik užtikrindama savo verslo ir klientų informacijos saugumą įmonė galės išlikti ir augti ateityje. Kibernetinio saugumo užtikrinimas tampa pažangios, konkurencingos ir socialiai atsakingos įmonės, kuri kuria bei parduoda savo produktus ar teikia paslaugas saugiai, ženklu.

Nacionalinėje kibernetinio saugumo strategijoje Krašto apsaugos ministerija yra išsikėlusi tikslą didinti mažų ir vidutinių privataus verslo atstovų kibernetinio saugumo brandą. Šis dokumentas buvo inicijuotas Krašto apsaugos ministerijai bendradarbiaujant su programos „Kurk Lietuvai“ komanda kaip priemonė, padėsianti kelti smulkiojo verslo sąmoningumo lygį ir skatinti įmones pradėti labiau rūpintis kibernetiniu saugumu, kad kiekviena įmonė jaustųsi saugiau skaitmeninėje erdvėje. Pirmojo tokio tipo bazinio lygio kibernetinio saugumo vadovo tikslas yra padėti mažų įmonių vadovams geriau suprasti kibernetinio saugumo iššūkius ir rizikas, su kuriomis verslas susiduria kiekvieną dieną, dalinantis bazinio lygio patarimais ir gerąja praktika.

Vadovas parengtas bendradarbiaujant su įvairiomis viešojo sektoriaus institucijomis, akademikais ir privataus sektoriaus įmonėmis, dirbančiomis kibernetinio saugumo ar kitų informacinių technologijų (IT) paslaugų srityse. Siekiama, kad naudotis šiuo informaciniu vadovu būtų paprasta, o pateikti žingsniai būtų suprantami ir lengvai įgyvendinami smulkiai (bet aktualūs ir vidutinio dydžio) verslo įmonei, todėl rekomendacijos yra suskirstytos į dvi dalis: bazinio ir aukštesnio lygio.

Svarbu pažymėti, kad kibernetinis saugumas nėra baigtinis procesas ir jokia įmonė negali užtikrinti visiško atsparumo kibernetinėms grėsmėms. Šiame dokumente pateikiamų rekomendacijų įgyvendinimas negarantuos šimtaprocentinės apsaugos nuo visų galimų kibernetinių įvykių, tačiau čia rasite paaiškinimus ir pavyzdžius, kaip paprastais žingsniais galima žymiai sustiprinti įmonės duomenų bei skaitmeninio turto saugumą ir verslo reputaciją. Vadovaudamiesi šiomis rekomendacijomis, Jūs galėsite išmintingai subalansuoti kibernetinio saugumo ir verslo plėtros poreikius.

Jei nusprendėte, kad norite pradėti labiau rūpintis savo įmonės kibernetiniu saugumu, atnaujinti turimas žinias ar patikrinti jau įgyvendintų priemonių efektyvumą, šis kibernetinio saugumo vadovas būtent tai padės Jums padaryti.

## DOKUMENTĄ PARENGĖ:

Kurk Lietuvai

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

KRAŠTO APSAUGOS MINISTERIJA

## BENDRADARBIAUTA SU:

ATEA

adeo web

BlueBridge

btt cloud

CYBER SECURITY ACADEMY

eset CYBERSECURITY EXPERTS ON YOUR SIDE

e | saugumas

HERMITAGE Solutions

ivpk INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETAS

Vilniaus universitetas Kauno fakultetas

NRD Cyber Security

PROACT

RRT

TERASKY

TGS BALTIC VARUL GRUNTE SUTKIENE

# Turinys

# 01

# Kas yra kibernetinis saugumas?

## Kibernetinis saugumas – tai veiksmai, kurių imamasi norint apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumą, vientisumą bei konfidencialumą.

Tai apima vidinius teisės aktus, organizacinius procesus ir technines priemones, leidžiančias išvengti, aptikti ir reaguoti į kibernetinius incidentus, įvertinti rizikas. Tokiomis priemonėmis siekiama palaikyti įprastinę informacinių sistemų ir verslo procesų veiklą ir apsaugoti turimus duomenis bei IT įrangą, kurie gali būti ypač svarbūs tiek didesnei, tiek smulkesnei įmonei.

Kibernetinis saugumas gali būti suvokiamas kaip asmeninė higiena. Taip, kaip kiekvienas laikomės higienos, norėdami išlaikyti gerą sveikatos būklę ir savijautą, taip pat turėtume žiūrėti ir į kibernetinį saugumą, kuris užtikrins geresnį Jūsų įmonės ir klientų duomenų saugumą bei sumažins neigiamo poveikio verslui riziką. Kibernetinis saugumas reikalauja nuolatinio vadovų dėmesio, pastangų ir lėšų, nes kibernetinės grėsmės gali kilti tiek iš išorės, tiek iš vidaus, todėl svarbu į kibernetinį saugumą žiūrėti visapusiškai.

Bazinių kibernetinio saugumo priemonių naudojimas dažnai nereikalauja didelių investicijų ir efektą galima pasiekti su turimais resursais, tačiau darbuotojams nesilaikant kibernetinės higienos principų tie patys techniniai sprendimai gali prarasti veiksmingumą. Be to, ilgainiui technologiniai sprendimai pasensta, taikomų priemonių efektyvumas mažėja ir juos reikia atnaujinti, kaip ir žinias, kuriomis vadovaujasi IT administratorius. Dėl šių priežasčių **rekomenduojama kibernetinio saugumo klausimus apsvarstyti diegiant ar atnaujinant verslo valdymo procesus bei vykdant kasdienę įmonės veiklą**.

### SVARBU ŽINOTI, KAD KIBERNETINIS SAUGUMAS UŽTIKRINAMAS TRIMIS PAGRINDINIAIS ASPEKTAIS:

**Konfidencialumas** (angl. *Confidentiality*) – užtikrinimas, kad bet kokia įmonės, klientų ar verslo partnerių informacija yra pasiekiama tik įgaliotiems asmenims, kuriems yra būtina žinoti, ir jiems suteikta tokia prieiga.
Konfidencialios informacijos pavyzdžiai: banko sąskaitų išrašai, darbuotojų ir klientų asmeninė informacija ar komercinės / gamybos paslaptys.

**Vientisumas** (angl. *Integrity*) – užtikrinimas, kad informacija ir duomenys yra teisingi, nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklastojami dėl kenkimo programinės įrangos ar neteisėto užvaldymo, techninės ar programinės įrangos gedimo.

Versle tai siejasi su situacijomis, kai programišiai neteisėtai gauną prieigą prie įmonės el. puslapio, į jį įsilaužia ir įdiegia kenkimo kodą, o svetainių lankytojai, patys nežinodami, nusiunčiami į kitus virusais užkrėstus puslapius, arba sukuriama galimybė pavogti lankytojų paskyrų prisijungimo duomenis. Kitas galimas (ir ateityje tikriausiai bus dažniau sutinkamas) atvejis, kai įmonės naudojasi išmaniaisiais įrenginiais, leidžiančiais automatizuoti gamybos ar kitus verslo procesus. Įsilaužėliams tyčia ar IT darbuotojams netyčia pakeitus programinį kodą, procesų sutrikimai gali nutraukti verslo veiklą (pramonės kontrolės sistemos išjungimas) ar net sukelti pavojų žmogaus sveikatai (pastato šildymo sistemos perkonfigūravimas).

**Prieinamumas** (angl. *Availability*) – užtikrinimas, kad visada yra prieiga prie tam tikros informacijos, duomenų bazės ar kitų elektroninių paslaugų.
Įmonėje tai galėtų būti nuolatinės svetainės ar duomenų bazės prieigos užtikrinimas. Sutrikus veiklai ir nesant galimybės pasiekti reikiamą informaciją, net ir trumpą laiką, įmonė gali būti priversta laikinai nutraukti savo veiklą ir prarasti pajamas, sukelti klientų nepasitenkinimą bei pakenkti savo reputacijai.

Kibernetiniai incidentai gali grėsti visur, o bandymų įsilaužti į įmonių tinklus ar darbuotojų paskyras skaičius tik didėja, ir mažai tikėtina, kad ši tendencija[1] artimiausiu metu keisis. Būtina suvokti, kad **kibernetinės atakos auka gali tapti kiekviena įmonė, nepriklausomai nuo dydžio, vykdomos veiklos ar naudojamų kibernetinio saugumo priemonių modernumo**. Dėl to kibernetinis saugumas turi tapti net ir paties smulkiausio verslo prioritetu. Taip, kaip kiekvieną dieną išeidami iš namų užrakiname duris, taip pat kiekvieną darbo dieną turėtume imtis kibernetinės higienos priemonių, kad piktavaliams patekti į Jūsų įmonės vidų būtų neįmanoma.

**Vienas didžiausių šių dienų SVV skaudulių yra kibernetinės atakos, susijusios su išpirkos reikalaujančiomis kenkimo programomis (angl. *ransomware*)**. Šių virusų veikimo principas yra ganėtinai paprastas: per apgaulingus laiškus ar kitą kenkimo kodą virusui patekus į kompiuterį užšifruojami visi ten ar visame vidiniame tinkle esantys duomenys, o už prieigos grąžinimą prašoma piniginio atlygio. Nesumokėjus išpirkos, pavogti duomenys yra ištrinami negrįžtamai arba paviešinami, tačiau dažnai, net ir sumokėjus prašomą sumą, duomenys nebūna grąžinami. Neretai įmonėms prireikia kelių savaičių ar net mėnesių, kad būtų atkurta normali veikla.

Didžiausią žalą iki šios dienos padaręs *ransomware* virusas yra 2017 m. pasklidęs „WannaCry“ kenkimo kodas. Šis virusas palietė daugiau nei 150 tūkst. įmonių visame pasaulyje ir daugiau nei 100 adresatų Lietuvoje. Nepaisant to, kad išpirkos suma buvo santykinai maža, **bendra padaryta žala globaliam verslui yra daugiau nei 1 mlrd. dolerių**. „WannaCry“ atmainos dar iki šios dienos sutinkamos kibernetinėje erdvėje.

Išpirkos dydis skirtingais atvejais gali siekti nuo kelių šimtų iki keliolikos tūkstančių eurų ar netgi daugiau.

## NORINT TO IŠVENGTI IR SUMAŽINTI GALIMĄ RIZIKĄ, PRIVALU LAIKYTIS PAGRINDINIŲ KIBERNETINIO SAUGUMO TAISYKLIŲ

### Pagrindiniai patarimai:

- Nuolatos darykite atsarginės dokumentų kopijas.
- Nemokėkite išpirkos.
- Nespauskite neaiškių nuorodų ar priedų el. laiškuose.
- Programinę įrangą atnaujinkite pagal gamintojo siūlomas rekomendacijas.
- Naudokite antivirusinę ar kitą pažangesnę nuo kenkimo apsaugančią programą.

Daugiau informacijos apie kibernetinio saugumo tendencijas Lietuvoje rasite Krašto apsaugos ministerijos Nacionalinio kibernetinio saugumo būklės ataskaitoje (2019 m.): **http://kam.lt/download/68298/nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf**.


[1] Cisco, *„Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats"* (2018), **https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf**.

02

# Kibernetinio saugumo svarba

Stambusis Lietuvos ir pasaulio verslas vis daugiau investuoja į informacinio ir kibernetinio saugumo užtikrinimą – žmogiškuosius išteklius, technologinius sprendimus. Dėl šios priežasties kibernetiniams nusikaltėliams stambusis verslas tampa sunkiau įkandamu taikiniu, o tai verčia juos sąmoningai atsisukti į smulkųjį verslą, kuris dėl savo ribotų išteklių ir nepakankamo kibernetinio saugumo lygio tampa lengva programišių auka.

Tačiau būtina pabrėžti, kad ne visada tikslingai taikomasi į vieną ar kitą įmonę – programišiai dažnai naudoja automatizuotus įrankius atakoms vykdyti ir taikosi į įmones, nesirūpinančias savo kibernetine higiena ir bazinėmis apsaugos priemonėmis. **Tad kiekviena įmonė, savo veikloje naudojanti elektroninį tinklalapį, elektroninį paštą ar tiesiog kompiuterį su interneto ryšiu, gali tapti kibernetinio incidento auka**.

Nėra svarbu, ar Jūsų įmonė parduoda prekes elektroninėje parduotuvėje ar teikia grožio salono paslaugas, – Jūsų verslas ar jo reputacija priklauso nuo interneto ryšio ar kitų elektroninių paslaugų. Ar tai būtų prekių užsakymai, atsiskaitymai ir pardavimai, *Excel* failas su klientų duomenimis, gaminių projektavimo procesai, naršymas socialiniuose tinkluose, ar interneto aplikacijų naudojimas rinkodaros tikslais – kiekviena Jūsų verslo operacija dažnai yra susijusi su informacijos apdorojimu. **Bet kokia Jūsų kompiuteryje ar kitame įrenginyje laikoma informacija gali būti vertingesnė, nei patys įsivaizduojate. Dėl to Jūsų įmonės turimas turtas ir informacija bet kada gali sudominti kibernetinius nusikaltėlius**.

Svarbu suprasti, kad Jūsų įmonė nėra izoliuota nuo kitų įmonių ar organizacijų. Tiek verslo įmonės, tiek patys įrenginiai tampa vis labiau tarpusavyje susiję ir sujungti skaitmeniniu būdu, siekiant gerinti ar automatizuoti veiklos procesus. Išnaudodami tai, **programišiai vis dažniau taikosi į mažesnių įmonių neapsaugotus tinklus ir įrenginius**, tad nereikėtų pamiršti, jog Jūsų įmonės kompiuteriai ar tinklas bet kada gali būti panaudoti kaip tiltas įsilaužti ir pakenkti kitoms įmonėms Jūsų tiekimo grandyje.

Kuo daugiau įmonių tiekimo grandyje, tuo daugiau durų, per kurias įsilaužėliai gali patekti į Jūsų įmonės ar Jūsų partnerių vidinį kiemą. Taigi **smulkiosios įmonės programišių akimis gali būti matomos kaip lengvas būdas įsibrauti į didžiųjų įmonių tinklus ar perimti jų informaciją**. Taip ne tik kyla kibernetinių incidentų rizika, bet ir patiriama papildomų nuostolių. Įmonės kompiuteriams ar serveriams tapus programišių tolimesnių atakų infrastruktūros dalimi iš karto didėja resursų sutvarkymo kaštai, taip pat staiga padidėja elektros suvartojimo sąskaita.

Taigi **Jūsų kibernetinis pasirengimas nėra tik rūpinimasis Jūsų pačių saugumu, bet kartu ir svarbus atsakingo verslo komponentas**. Tai leidžia manyti, kad ateityje vis daugiau įmonių prašys jų tiekimo grandyje esančių tiekėjų ir tarpininkų atitikti tam tikrus kibernetinio saugumo standartus. „Kurk Lietuvai“ programos projekto Krašto apsaugos ministerijoje vykdyta apklausa parodė, kad 3 iš 4 SVV įmonių vadovams yra svarbu, kad jų verslo partneriai atitiktų kibernetinio saugumo standartus ar jų laikytųsi.

### KIBERNETINIO SAUGUMO MITAS

**Mes per maži – atakos mus aplenks**

Viena dažniausių verslo vadovų sąmoningumo klaidų – galvojimas, kad maža įmonė niekada netaps atakos auka ar kad ji paprasčiausiai neturi ko saugoti.

„Kurk Lietuvai“ programos dalyvių Krašto apsaugos ministerijoje atlikta apklausa parodė, kad beveik pusė (44 proc.) SVV įmonių nemano, kad galėtų tapti atakų aukomis.

Tačiau „Ponemon“ instituto duomenys rodo, kad **net 66 proc. SVV įmonių 2018 metais patyrė kibernetines atakas**.

Tad jeigu Jūs nebūsite įsidiegę bent jau bazinio lygio kibernetinio saugumo priemonių, didės tikimybė, kad prarasite patikimumą ir konkurencingumą verslo rinkoje. Verta pabrėžti ir tai, kad kibernetiniai incidentai dažnai įvyksta paprasčiausiai dėl žmogaus klaidos. Įvairūs tyrimai rodo, kad ketvirtadalis kibernetinio saugumo pažeidimų įvyksta būtent dėl žmogaus neapdairumo ar žinių trūkumo įmonėse. Dėl šios priežasties itin didelis dėmesys turėtų būti skiriamas darbuotojams paruošti – labai svarbu, kad jie žinotų, kaip rūpintis Jūsų įmonės kibernetiniu saugumu.

## Kibernetinių incidentų sukelti nuostoliai apima:

01 finansinius nuostolius dėl banko ar kitų finansinių duomenų praradimo arba pinigų vagysčių;

02 finansinius nuostolius dėl vykdomos veiklos sutrikdymo, ypač jei pagrindinė įmonės veikla yra prekyba internetu;

03 išlaidas, susijusias su paveiktų IT sistemų sutvarkymu, atkūrimu bei remontu;

04 baudas dėl Bendrojo duomenų apsaugos reglamento nesilaikymo, kai yra asmens duomenų pažeidimų;

05 teisininkų paslaugas;

06 įmonės veiklai reikalingos informacijos praradimą ir jos atkūrimą;

07 poveikį įmonės reputacijai ir klientų pasitikėjimo praradimą;

08 žalą kitoms įmonėms ar kitiems verslo partneriams, kuriems teikiate savo prekes ar paslaugas.

Mažesnių įmonių kibernetinio saugumo priemonės dažnai yra nepakankamos, o įvykus kibernetiniam incidentui mažesnės įmonės neturi pakankamai žmogiškųjų ir techninių išteklių incidentui suvaldyti ir padėčiai atkurti. **Net ir vienas tyčinis ar netyčinis kibernetinis incidentas gali būti pražūtingas Jūsų verslui**. IT sistemų ir kompiuterių bei informacijos atkūrimas gali užsitęsti neapibrėžtą laiką, o tai gali sukelti rimtų pasekmių smulkesniam verslui[3].

Svarbu nepamiršti, kad mažų įmonių veiklos poreikiai nėra tokie sudėtingi, todėl **didelė dalis kibernetinio saugumo sprendimų gali būti įgyvendinti mažais ir nesudėtingais žingsniais**. Dažnai įsivaizduojama, kad kibernetinis saugumas yra labai kompleksiškas ir daug resursų reikalaujantis procesas, bet žvelgiant į jį kaip į nuolatinį verslo procesą ir veiklos sudėtinę dalį geresnės savo verslo apsaugos galima siekti gana paprastais žingsniais ir praktikomis.

**Nuolatinė kibernetinio ir informacinio saugumo praktika** ne tik apsaugos Jūsų verslą, **bet gali padėti įmonei didinti konkurencingumą, išlaikyti ir pritraukti naujų klientų, darbuotojų ir verslo partnerių**. Jūsų klientai, darbuotojai ir partneriai tikisi, kad jų asmeninė ir konfidenciali verslo informacija bus apsaugota nuo vagysčių, neteisėto atskleidimo ir netinkamo panaudojimo. Klientų informacijos apsauga yra kokybiško klientų aptarnavimo ir socialiai atsakingo verslo pavyzdys, kuris parodys visuomenei, kad Jums rūpi daugiau nei vien finansinių išteklių didinimas[4].

Kelias link saugesnio verslo prasideda nuo teisingo požiūrio. Kiti verslo atstovai ar investuotojai įvertins Jūsų pastangas laikytis kibernetinį saugumą reglamentuojančių teisės aktų, taikyti gerąją praktiką ir rūpintis turimos informacijos saugumu, o tai atneš naujų galimybių Jūsų verslui, ir, priešingai, jei Jūs nesirūpinsite savo saugumu, partneriai ir klientai Jums nepatikės savo informacijos.

Vienas garsiausiai nuskambėjusių kibernetinių įsilaužimų įvyko 2013 metais, kai buvo įsilaužta į JAV didmeninės prekybos korporacijos „Target“ tinklą ir pavogti net **110 milijonų klientų mokėjimo kortelių duomenys**.

### Kaip tai įvyko?

Programišiai nesunkiai įsilaužė į mažos įmonės, tiekiančios „Target“ parduotuvėms šaldytuvus, nesaugią elektroninio pašto sistemą. Nusikaltėliai, žinodami, kad ši įmonė yra „Target“ tiekimo partnerė, pasinaudojo mažos įmonės pažeidžiamumu, kad galėtų lengvai įsiskverbti į stambaus verslo tinklą ir pavogti klientų duomenis. Ekspertai teigia, kad net kas trečias amerikietis buvo paveiktas šio incidento.

[2] Ponemon Institute, IBM Security, „*Cost of a Data Breach Study 2019*“ (2019), https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.

[3] Cisco, „*Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats*“ (2018).

[4] KPMG, „*Cyber security guide for SMEs*“ (2017), https://assets.kpmg/content/dam/kpmg/nz/pdf/May/cyber-security-guide-for-smes-kpmg-nz.pdf.

03

# Kibernetinio saugumo kultūros kūrimas Jūsų įmonėje

Dažnai galvojama, kad sprendžiant kibernetinio saugumo problemas užtenka pasitelkti įvairius technologinius sprendimus. Manoma, kad kokybiškos antivirusinės programos įdiegimas apsaugo nuo visų išorinių grėsmių. Tačiau šiandien matyti, kad to nebepakanka. Antivirusinės programos įsigijimas yra tik vienas iš pirmųjų žingsnių kibernetinio saugumo link. Jūs negalėsite užtikrinti savo įmonės saugumo, jei Jūsų darbuotojai nesupras, kodėl reikia būti atsargiems internete, arba jeigu neįgyvendinsite organizacinių kontrolės mechanizmų, kurie žymiai apsunkins sąlygas kibernetiniams nusikaltėliams patekti į Jūsų įmonės tinklą.

Tinkamai pasirinktos techninės priemonės gali sumažinti kibernetinių incidentų riziką, tačiau be darbuotojų žinių šioje srityje apsisaugoti nepavyks. Didesnį kibernetinį saugumą galėsite pasiekti, jei Jūsų įmonėje bus ugdomas darbuotojų kibernetinio saugumo sąmoningumas, įdiegtos techninės apsaugos priemonės ir nustatytos taisyklės, kaip reikia tinkamai jomis naudotis. **Jei kibernetinis saugumas taps Jūsų verslo procesų dalimi, bus paprasčiau neatsilikti nuo nuolat kintančių kibernetinių grėsmių, o darbuotojams lengviau įsitraukti į kibernetinio saugumo įgyvendinimą**.

Aktyviai aiškinkite savo įmonės kibernetinio saugumo principus ne tik darbuotojams. Pasikalbėkite ir su savo verslo partneriais iš kitų įmonių. Jie taip pat gali pasidalyti gerąja kibernetinio saugumo sąmoningumo ugdymo patirtimi, o galbūt kaip tik Jūs būsite tas žmogus, kuris įtikins ir kitą įmonę imtis tinkamų veiksmų. **Padidindami aplinkos, kurioje dirbate, saugumą, skatinsite ir kitus atidžiau elgtis skaitmeninėje erdvėje**.

Šiame dokumente pateikti patarimai leis Jums mažinti kibernetinio saugumo rizikas stiprinant prevencines saugos priemones, diegiant spragų ar žmogaus klaidų aptikimo įrankius bei padės sąmoningai elgtis kibernetinėje erdvėje. Tačiau nepamirškite, kad kibernetinio saugumo stiprinimas nesibaigia perskaičius šį vadovą ir įgyvendinus rekomenduojamas priemones. Kibernetinės grėsmės ateityje tik tobulės ir bus vis įvairesnės, o verslo poreikiai gali keistis, tad likite budrūs: domėkitės, mokykitės ir konsultuokitės, nes tik taip būsite pasiruošę ateities pavojams. Pastebėję kenkėjišką veiklą kibernetinėje erdvėje, savanoriškai pateikite faktus vertinti Nacionaliniam kibernetinio saugumo centrui (NKSC).

## Kodėl tvarkos ir atsakomybių apsibrėžimas bei jų laikymasis yra svarbu?

Kibernetiniai nusikaltėliai nėra visažiniai programišiai ir nors jų veiksmai gali sukelti realią finansinę žalą ir sutrikdyti veiklą, kiekviena įmonė gali pati įgyvendinti priemones, leidžiančias apsisaugoti nuo daugelio bandymų įsilaužti. Įtraukus kibernetinio saugumo klausimus į įprastinę įmonės veiklą, suradus tinkamą balansą tarp įsilaužimo rizikos, galimų padarinių bei reikiamų investicijų į saugumo priemones, Jūsų verslas taps atsparesnis kibernetinėms grėsmėms.

Vienas iš pirmųjų etapų, leidžiančių įmonėms žengti pirmuosius žingsnius link aukštesnio kibernetinio saugumo sąmoningumo ir atsparumo, yra **verslo kibernetinio saugumo politikos suformavimas**. Tai yra dokumentas, kuris apibrėžia įmonės veiklos, susijusios su informacijos apdorojimu, elektroninių prietaisų naudojimu ir pan., tvarką bei atsakomybes. Jame turėtų būti išvardyti visi principai, kuriais Jūsų verslas ir darbuotojai vadovausis užtikrindami įmonės kibernetinį saugumą.

## Tai leis:

01 Jūsų darbuotojams suprasti, kaip kibernetinės higienos principai įsilieja į kasdienio darbo procesus;

02 parodyti verslo klientams bei partneriams, kad Jūsų įmonė rūpinasi jų duomenų apsauga;

03 užtikrinti, kad Jūsų įmonės atliekamos asmens duomenų tvarkymo procedūros atitinka Bendrojo duomenų apsaugos reglamento reikalavimus.

Kibernetinio saugumo politikos dokumentas neturi būti ilgas ir kompleksiškas. Svarbiausia, kad, net **jeigu įmonėje dirba vos keli žmonės, kiekvienas žinotų, kaip darbuotojas užtikrina įmonės atsparumą kibernetinėms grėsmėms**. Tokiame dokumente turėtų būti išdėstyta bendra įmonės skaitmeninio turto, rizikų ir incidentų valdymo, informacijos apdorojimo bei saugojimo tvarka, darbuotojų teisės, atsakomybė ir pan.

Labai reikšminga yra tai, kad visi Jūsų įmonės darbuotojai, tiek seniai dirbantys, tiek nauji, susipažintų su šiuo dokumentu, suprastų su kibernetiniu saugumu susijusias teises ir atsakomybes, įsigilintų ir pasirašytų pasižadėjimą jų laikytis. Reguliarūs pokalbiai apie kibernetinį saugumą bei jo svarbą padidins darbuotojų dėmesį ir sąmoningumą šioje srityje.

Politika bus tiesiog popieriaus lapas, jeigu ji nebus įgyvendinama ir nebus laikomasi jos principų. Tai yra Jūsų, kaip įmonės vadovo, atsakomybė. **Itin reikšminga yra Jūsų lyderystė ir rodomas pavyzdys, kad kibernetinė higiena taptų įmonės prioritetu ir darbuotojai suprastų, kodėl reikia rūpintis įmonės kibernetiniu saugumu**. Jei tai bus tik formalus dokumentas, kurio įgyvendinimui nebus skiriamas dėmesys, tikėtina, kad Jūsų verslas anksčiau ar vėliau nukentės dėl darbuotojų neapdairumo.

**Kibernetinio saugumo politika turėtų būti reguliariai peržiūrima ir atnaujinama bent kartą per metus**. Organizaciniai procesai, technologijos bei grėsmės nestovi vietoje, todėl svarbu, kad Jūsų įmonė neatsiliktų nuo besikeičiančių kibernetinio saugumo tendencijų.

# Įmonės kibernetinis saugumas – kiekvieno darbuotojo rankose

Jokia kibernetinio saugumo kultūra įmonėje negali būti kuriama be vieno elemento – žmonių. Deja, bet tyrimai rodo, jog **viena iš svarbiausių priežasčių, kodėl verslas yra itin pažeidžiamas kibernetinių grėsmių, yra būtent žmogiškasis faktorius**. „IBM“ kompanijos ir „Ponemon“ instituto tyrimas parodė, kad netyčinės žmogaus klaidos ir sistemų pažeidimai yra beveik pusės (49 proc.) duomenų pažeidimų priežastis. Be to, net 70 proc. „Ponemon“ instituto apklaustų informacijos saugos vadovų išskiria kompetentingų darbuotojų trūkumą kaip didžiausią iššūkį siekiant užtikrinti įmonės kibernetinį saugumą[6].

Įmonių vadovai, suvokdami kibernetinio saugumo svarbą, investuoja į IT apsaugos priemones, bet neretai pamiršta tai, kad didelę grėsmę verslui gali sukelti žmogus. Darbuotojų patiklumas, noras padėti, skubotas nurodymų vykdymas ar žinių trūkumas susidūrus su apgaulingomis užklausomis gali nulemti jų veiksmus, dėl kurių jie asmeniškai ar įmonė gali prarasti duomenis, gali sutrikti programų ir sistemų veikimas, nutekėti konfidenciali informacija ar būti patiriami tiesioginiai finansiniai nuostoliai.

Pasak „IBM“ ir „Ponemon“ tyrimo, dėl duomenų pažeidimo smulkusis verslas patiria neproporcingai didelius nuostolius, palyginti su didelėmis įmonėmis. Todėl **smulkiajam verslui ypač svarbu ugdyti savo darbuotojus, kad jie galėtų atpažinti elektroninius sukčiavimo laiškus, suvoktų saugaus įrenginių naudojimo, dalinimosi informacija ir kitus saugumo principus**.

Kaip darbuotojus apsaugoti nuo patekimo į socialinės inžinerijos pinkles ir kokius jų įgūdžius ugdyti, aptariama šioje dalyje.

## Didžiausias iššūkis – socialinė inžinerija

Bandymai apgauti yra pagrįsti socialinės inžinerijos metodais. Imituojant įvairias gyvenimo / darbo aplinkybes ir situacijas, siekiama apgavystės taikinį suklaidinti, paveikti psichologiškai ir taip išvilioti pinigus, jautrius duomenis arba išprovokuoti daryti veiksmus, kurie gali pažeisti IT infrastruktūrą. **Socialinės inžinerijos tikslas – išgauti konfidencialią informaciją, asmeninius, banko ar kitus finansinius duomenis arba kitą asmeninę informaciją, kurią galima panaudoti šantažuojant, užverbuojant ir pan**.

## Kaip veikia socialinė inžinerija?

Tokiais metodais veikia telefoniniai sukčiai, bandantys įtikinti, kad Jūsų artimas žmogus pateko į nelaimę arba kad Jūs netikėtai laimėjote loterijoje. **Telefonu ar el. paštu dažnai atakuojamos ir verslo įmonės**, jų darbuotojams pranešama, kad įmonės vadovui reikalinga skubi pinigų perlaida, arba atsiunčiama apgaulinga sąskaita, kurią darbuotojas skatinamas tuoj pat apmokėti. Taikantieji tokius apgavystės metodus naudojasi žmonių jausmais ir emocijomis, bandydami darbuotojus įtikinti imtis skubių veiksmų prieš tai jų gerai neapgalvojus. Vis dažniau kibernetiniai nusikaltėliai siunčia individualizuotas užklausas, kurios būna pritaikytos pagal įmonės veiklą, darbuotojo pareigas, amžių ir pan. Dažnai tokiais metodais manipuliuojama žmogaus neapdairumu, patiklumu ar žinių trūkumu.

### LIETUVOJE 2019 M. ŽINIASKLAIDA SKELBĖ APIE TOKIUS SUKČIAVIMO ATVEJUS:

Įmonės Alytuje buhalterė, gavusi apgaulingą elektroninį laišką nuo direktoriumi apsimetusio asmens, jam pervedė beveik **20 tūkstančių eurų**.

Kita įmonė Tauragėje prarado **daugiau nei 5 tūkstančius eurų** vos keliais mygtuko paspaudimais, kai į įmonei priklausantį mobilųjį telefoną buvo atsiųsta apgaulinga užklausa, prašanti atnaujinti banko programėlę. Paspaudusi nuorodą moteris buvo nukreipta į netikrą elektroninės bankininkystės puslapį.

[6] Ponemon Institute, IBM Security, *„Cost of a Data Breach Study 2019“* (2019).

**Labiausiai paplitęs socialinės inžinerijos metodas – sukčiavimas** (angl. *phishing*), kai potencialioms aukoms siunčiami suklastoti laiškai ar žinutės, panašūs į siunčiamus bankų, programinės įrangos gamintojų, verslo partnerių, siuntų pristatymo paslaugų teikėjų ir t. t. Tokių sukčiavimo laiškų per pastaruosius 12 mėn. gavo net pusė „Kurk Lietuvai" atliktoje apklausoje dalyvavusių SVV įmonių. Žinutės ir laiškai, pranešantys apie problemas kompiuteryje, virusus, neapmokėtas sąskaitas ar neatsiimtus siuntinius, gali atkeliauti su priedais ir (ar) nuorodomis, kuriuose slepiasi kenksmingi programiniai kodai.

> Geriausia apsaugos nuo elektroninių sukčių priemonė – kritiškas informacijos vertinimas.

Egzistuoja ir daugiau socialinės inžinerijos atmainų. Pavyzdžiui, **klastojant kito asmens tapatybę siekiama išprovokuoti darbuotoją atskleisti prisijungimo duomenis prie IT sistemų ar informaciją apie kitus darbuotojus** (angl. *pretexting*). Darbuotojais gali manipuliuoti ir sukčiai, bandantys apgauti siųsdami iš pažiūros įprastą nuorodą, kviečiančią reguliariai atnaujinti prisijungimo duomenis, tikintis, kad sukurtas naujas slaptažodis bus panaudotas ir kitose prieigose. Svarbu paminėti, kad piktavaliai užsiima vadinamąja **banginių medžiokle** (angl. *whaling*). Tai sukčiavimo rūšis, kai naudojamos tos pačios apgavystės technikos, bet yra taikomasi į tam tikrą auditoriją – įmonės vadovus, kurie turi prieigą prie svarbiausios informacijos ir sistemų, tačiau ne visada turi laiko įsigilinti į laiško turinį, o juos apgavus įmonės nuostoliai gali siekti net milijonus.

**Nesvarbu, kokio tipo Jūsų verslas, kokio dydžio Jūsų įmonė, tikimybė gauti apgaulingų elektroninių laiškų ir žinučių – didelė**. Vis daugėjant socialinės inžinerijos atvejų (vidutiniškai 25 proc. per metus[7]) ir jiems vis kintant ir tobulėjant, itin svarbu užtikrinti, kad Jūsų įmonės darbuotojai būtų tinkamai pasiruošę.

[7] Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, 2018 m. *Nacionalinio kibernetinio saugumo būklės ataskaita* (2019), https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf.


**BEVEIK KAS ANTRAS DUOMENŲ PAŽEIDIMAS ĮVYKSTA DĖL NETYČINĖS ŽMOGAUS KLAIDOS AR SISTEMŲ PAŽEIDIMŲ**


**70 PROC. INFORMACIJOS SAUGOS VADOVŲ IŠSKIRIA KOMPETETINGŲ DARBUOTOJŲ TRŪKUMĄ KAIP DIDŽIAUSIĄ IŠŠŪKĮ SIEKIANT UŽTIKRINTI ĮMONĖS KIBERNETINĮ SAUGUMĄ**



Ponemon Institute, IBM Security, „*Cost of a Data Breach Study 2019*“ (2019).

# IoT

# Kaip įvertinti kibernetinių grėsmių pavojų Jūsų įmonei?

Šiuolaikiniame versle kibernetinio saugumo aspektas yra neatsiejama įmonės veiklos dalis ir turėtų būti įtraukta į bet kokį įmonės rizikų vertinimą ar verslo tęstinumo planą. „Kurk Lietuvai“ projekto Krašto apsaugos ministerijoje atlikta apklausa parodė, kad įmonės, turinčios kibernetinio saugumo politiką ir reguliariai atliekančios rizikų vertinimą, geriau suvokia, kodėl svarbu rūpintis kibernetiniu saugumu, ir jaučiasi labiau pasiruošusios atremti kibernetines atakas. **Suvokę, kokia atsakomybė gali tekti įmonei už prarastus duomenis, ir tinkamai įvertinę potencialius verslo nuostolius incidento atveju, galėsite lengviau nuspręsti, kokių organizacinių ir techninių kibernetinio saugumo priemonių reikia Jūsų verslui. Visos informacijos saugumas kainuoja daug, todėl būtina įvertinti, kokią informaciją reikia apsaugoti pirmiausia ir labiausiai.**

Galbūt turite savo įmonės svetainę, galbūt Jūsų darbuotojai naudoja asmeninius telefonus, kompiuterius darbui įmonės biure, o galbūt Jums, kaip vadovui, tenka dažnai pasinaudoti viešuoju belaidžiu tinklu – visa tai kelia riziką, kad tyčia ar netyčia kenkimo kodas pateks į įmonės tinklą. Taip Jūs galite prarasti savo asmeninius ar klientų duomenis. Dėl šių priežasčių į visas rizikas būtina žiūrėti atsakingai ir parengti valdymo planą, kaip jas mažinti.

Rizikų valdymo procesas nėra lengvas ir paprastas, dėl to, esant sunkumams, rekomenduojama kreiptis ir konsultuotis su ekspertais bei įmonėmis, teikiančiomis kibernetinių rizikų audito ir vertinimo paslaugas.

## Rizikų valdymas

### 01 Žinokite, kokias sistemas naudojate ir su kokia informacija dirbate

Pirmiausia, prieš įvertinant rizikas, reikia suprasti visus verslo veiklos procesus ir įvertinti, kokios IT sistemos ar platformos naudojamos šiems procesams vykdyti. Išsiaiškinkite, kaip šios sistemos tvarko, saugo ir perduoda įmonės ir klientų informaciją. **IT sistemos gali būti naudojamos iš išorės arba iš vidaus**, pavyzdžiui:

- išorinė sistema: Jūs naudojatės „Microsoft Office 365“ ar „GSuite“ biuro paslaugų paketu, kuriame laikote klientų asmens duomenis ir svarbius apskaitos dokumentus, arba prieglobos (angl. *hosting*) paslaugų teikėjo infrastruktūroje laikote savo duomenis;
- vidinė sistema: Jūs naudojate vidiniame įmonės tinkle esantį serverį ar kompiuterį, kuriame įdiegėte Jums reikalingą programinę įrangą ir kuris Jums teikia vidinę paslaugą.

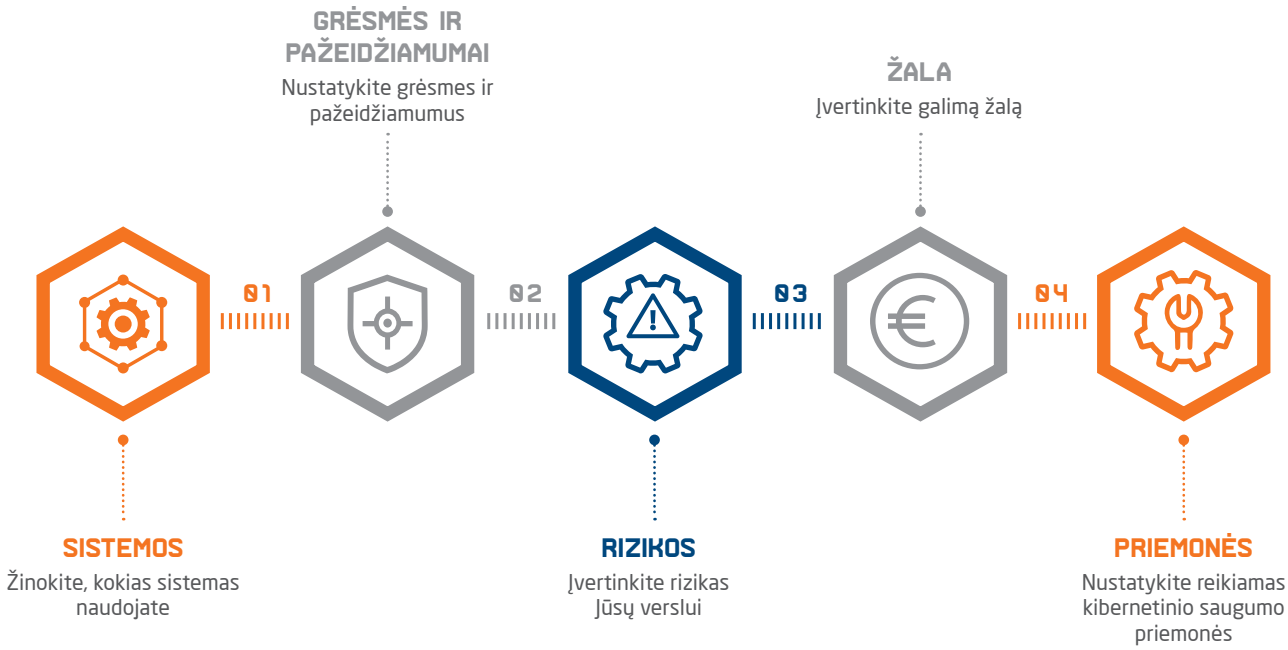
Nuspręskite, kurių sistemų ar kokių duomenų apsauga Jūsų verslui yra svarbiausia. Pradėkite nuo svarstymo, kurių sistemų veikimas yra būtinas verslo tęstinumui ir kuriose sistemose yra laikoma verslo procesams reikalinga informacija. Tai gali būti bet kokia sistema, kurioje yra laikomi klientų asmens duomenys ar verslo partnerių informacija. Galbūt tai sistema, apdorojanti įvairius mokėjimus (pvz., interneto prieigą turintys kasos aparatai), ar vidinės sistemos duomenys, reikalingi verslo procesui vykti.

### 02 Nustatykite grėsmes, jų šaltinius ir pažeidžiamumus

Įvertinę naudojamų sistemų ir duomenų svarbą, galėsite pereiti prie galimų grėsmių įmonės veiklai nustatymo. **Bet kuri įmonė, naudojanti skaitmenines paslaugas, gali tapti netikslinių atakų auka**. Pavyzdžiui, programišiai gali pasitelkti kenkimo programinę įrangą, kuri automatiškai ieško žinomų saugumo spragų, panaudoti paviešintus nulaužtus slaptažodžius ir taip įsilaužti į Jūsų serverį ar darbuotojų el. pašto dėžutes. Įvertinkite ir nustatykite, kokiais būdais įsilaužėliai gali gauti prieigą prie įmonės tinklo ar duomenų.

## RIZIKŲ VERTINIMAS

Kaip įvertinti ir valdyti rizikas?




Grėsmės nebūtinai būna piktybinės. **Kibernetinis ar informacijos saugumo pažeidimas gali įvykti darbuotojui atidarius užkrėstą dokumentą arba ištrynus ar redagavus svarbius įmonės duomenis**. Dėl to šioje stadijoje labai svarbu dirbti drauge su savo darbuotojais. Taip galėsite kartu nustatyti, kokios verslo procesų vietos yra pažeidžiamiausios ir gali kelti grėsmę duomenų saugumui. Tam gali praversti ir kibernetinio saugumo specialistų pagalba. Atkreipkite dėmesį, kad poveikį, grėsmes turėtų vertinti ne IT administratorius, o procesų šeimininkai, verslo atstovai, kurie geriausiai išmano konkrečias sritis. IT administratorius dalyvauja šiame procese kaip palaikanti pusė, suteikianti reikiamą informaciją iš IT srities.

## 03 Įvertinkite grėsmių riziką Jūsų verslui

Rizika gali būti apibrėžiama kaip bet kokia aplinkybė ar įvykis, galintis turėti neigiamą poveikį ryšių ir informacinių sistemų saugumui. Kibernetinio saugumo rizikos gali būti skirstomos pagal minėtas kategorijas: grėsmė informacijos konfidencialumui, vientisumui arba prieinamumui.

### Pavyzdžiui:

- jeigu naudojate „Wordpress“ turinio valdymo sistemą, laiku neatnaujinus įdiegtų įskiepių, programišiai gali pasinaudoti atsiradusiomis spragomis ir įdiegti kenkimo kodą į įmonės svetainę ar pridėti nuorodą į kitus kenksmingus puslapius, ar užvaldyti Jūsų klientų duomenis;
- programišiams patekus į tinkamai neapsaugotą el. pašto dėžutę, atsiranda rizika, kad bus pasisavinta konfidenciali įmonės informacija ar išsiųsti apkrėsti sukčiavimo el. laiškai (angl. *phishing*).

Rizikos turėtų būti suskirstytos pagal saugos pažeidimo tikimybę ir įtakos kriterijus. Nepamirškite, kad **rizikų visiškai pašalinti neįmanoma, jos gali būti tik sumažinamos iki priimtino lygio, todėl** su kai kuriomis rizikomis tiesiog reikės susitaikyti ir jas nuolatos stebėti, o kitos turės būti valdomos ir mažinamos įvairiomis techninėmis ir organizacinėmis priemonėmis.

**Svarbiausia yra pasiekti balansą tarp rizikų ir taikomų kontrolės mechanizmų**, nes taip galėsite sėkmingai siekti savo komercinių tikslų ir suderinti juos su įmonės kibernetinio atsparumo užtikrinimu. Nepamirškite, kad šis balansas laikui bėgant gali kisti: tobulinant ar keičiant verslo procesus bei atsirandant naujoms kibernetinėms grėsmėms, rizikų tikimybė ir poveikis gali keistis. **O svarbiausia, kad rizikos mažinimo priemonės neturėtų kainuoti daugiau nei galimi saugumo pažeidimo rizikos padariniai**.

## 04 Įvertinkite galimą poveikį

Kaip minėta anksčiau, kibernetinio saugumo incidentai gali sukelti įvairialypę žalą Jūsų verslui. Dėl to **būtina įvertinti, kokią žalą gali sukelti vieno ar kito tipo incidentas**. Pavyzdžiui, kokia tiesioginė (pajamų praradimas) ar netiesioginė (baudos ar partnerių klientų sankcijos) žala bus verslui dėl įrenginio užkrėtimo sutrikus įmonės veiklai ar nutekinus asmens ar mokėjimo kortelių duomenis. Incidentai taip pat turėtų būti suskirstyti pagal patiriamos žalos apimtį: nuo minimalios žalos (nėra sutrikdomi verslo procesai) iki kritinės įtakos (kibernetinis pažeidimas galutinai ir negrįžtamai nutraukia įmonės veiklą).

## 05 Nustatykite reikiamas kibernetinio saugumo priemones

Būti pasiruošusiam tam, kas gali ir neįvykti, yra naudingiau, nei būti nepasiruošus tam, kas įvyks. Nustatę ir įvertinę galimas kibernetinio saugumo rizikas bei galimus nuostolius Jūsų verslui, galėsite sukurti planą, kokių prevencinių priemonių reikėtų imtis rizikoms valdyti. Tai ne tik leis aiškiai nustatyti, kokių organizacinių ir techninių kibernetinio saugumo priemonių ar sprendimų reikia Jūsų verslui, bet ir padės geriau suprasti, kokių papildomų kaštų reikės, kad būtų pasiektas tinkamas balansas tarp investicijų į kibernetinio saugumo technines ir organizacines priemones kainos ir jų grąžos.

Nepamirškite, kad rizikų vertinimas nėra vienkartinis veiksmas, o bene svarbiausias, nuolat kartojamas verslo procesas. **Periodiškai, bet ne rečiau kaip kartą per dvejus metus, rekomenduojama peržiūrėti ir iš naujo atlikti rizikos vertinimą. Jeigu diegiate naujas IT sistemas ar įrenginius arba keičiate verslo valdymo procesus, siūlytina prieš tai atlikti kibernetinių rizikų vertinimą**, kad žinotumėte, kokią įtaką kibernetinio saugumo pokyčiai darys Jūsų įmonėje.

**Norint daugiau sužinoti apie rizikų vertinimo metodologijas ir susipažinti su gerosiomis užsienio kibernetinio ir informacinio saugumo valdymo praktikomis, rekomenduojama susipažinti su toliau nurodytais šaltiniais**. Mažesnėms įmonėms šie standartai gali būti gana kompleksiški, o jų įgyvendinimas reikalauti daug kaštų, tačiau tai yra naudingi šaltiniai, padedantys verslui įvertinti pasiruošimą reaguoti į kibernetinius incidentus:

- JAV NIST savanoriškas kibernetinio saugumo struktūros modelis. Pritaikyta įvairaus dydžio įmonėms bei verslui, kuris dar tik pradeda keisti požiūrį ir kurti savo kibernetinio saugumo politiką;
- tarptautinis ISO 27000 šeimos informacijos apsaugos sistemos standartas;
- tarptautinis ISO 22301 standartas ir verslo tęstinumo valdymo sistema;
- tarptautinis ISO 20000 standartas ir paslaugų valdymo principai;
- tarptautinis ISO 27031 standartas, kuriame rasite saugumo užtikrinimo metodus bei informacinių ir komunikacinių technologijų pasirengimo verslo tęstinumui gaires;
- detalus rizikos analizės vadovas **https://www.nksc.lt/doc/rizikos_analize.pdf**.

# Teisinė atsakomybė

Svarbu ne tik žinoti, su kokiomis kibernetinio saugumo grėsmėmis galima susidurti ir kaip nuo jų apsisaugoti naudojant technines kibernetinio saugumo priemones bei keliant darbuotojų žinių lygį, bet ir susipažinti su **teisės aktų nustatytomis taisyklėmis, susijusiomis su informacijos saugumu**, nes už netinkamą asmens duomenų saugojimą gali būti taikoma teisinė atsakomybė. **Pagrindiniai teisės aktai, reglamentuojantys kibernetinį saugumą ir asmens duomenų apsaugą**, yra Lietuvos Respublikos kibernetinio saugumo įstatymas (**KSĮ**) ir Bendrasis duomenų apsaugos reglamentas (**BDAR**).

## Kibernetinio saugumo įstatymas

KSĮ detalizuoja pagrindinius kibernetinio saugumo principus, kibernetinio saugumo subjektų pareigas. KSĮ taikomas **ne visiems ūkio subjektams**, o tik tiems, kurie užsiima specialia veikla – *valdo ir prižiūri valstybės informacinius išteklius, ypatingos svarbos informacinę infrastruktūrą, teikia viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas, teikia elektroninės informacijos prieglobos (angl. hosting) paslaugas ir skaitmenines paslaugas*. KSĮ smulkaus dydžio įmonėms, atitinkančioms šiuos kriterijus, numato nemažai reikšmingų pareigų:

- pareiga užtikrinti jų valdomų ryšių ir informacinių sistemų ar teikiamų paslaugų kibernetinį saugumą, jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams;
- pareiga atlikti rizikos vertinimą, įdiegti pažangiausias ir nustatytai rizikai proporcingas technines ir organizacines kibernetinio saugumo priemones (rizikos vertinimas turi būti atliekamas ne rečiau kaip kartą per dvejus metus arba po esminių organizacinių ar sisteminių pokyčių);
- pareiga viešai tinklalapyje skelbti informaciją bei rekomendacijas dėl priemonių kibernetiniam saugumui užtikrinti;
- pareiga panešti NKSC apie jų ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus;
- pareiga teikti policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamų veikų požymių, kibernetinėje erdvėje užkardyti ir tirti, vykdyti kitus policijos nurodymus;
- pareiga paskirti asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą, ir pateikti NKSC kontaktinę informaciją;
- pareiga vykdyti NKSC nurodymus (pvz., apriboti savo paslaugų teikimą).

**Svarbu**: šie reikalavimai netaikomi **skaitmenines paslaugas** (pvz., elektroninės prekyvietės, paieškos internete ir (arba) debesijos paslaugas) Lietuvoje ar ES valstybėje narėje **teikiančioms mažoms ir labai mažoms įmonėms (iki 50 darbuotojų)**.

## Bendrasis duomenų apsaugos reglamentas

BDAR nustato asmens duomenų tvarkymo, saugumo užtikrinimo reikalavimus, asmens duomenis tvarkančių (ar valdančių) subjektų teises ir pareigas bei duomenų subjektų – fizinių asmenų, kurių duomenys tvarkomi, teises. Reglamentas taikomas **visiems ūkio subjektams**, tvarkantiems (ar valdantiems) asmens duomenis. Savo veikloje dauguma mažų įmonių tvarko nemažai įvairių asmens duomenų – darbuotojų, verslo partnerių (tiekėjų), klientų, todėl jie laikytini šių duomenų valdytojais (ar tvarkytojais).

Neretai pasitaiko atvejų, kai įmonės laikosi pozicijos, kad BDAR joms netaikomas, nes jos dirba tik su verslo subjektais, o verslo subjekto duomenims (pavadinimo, įmonės

Daugiau informacijos apie tai, kuo skiriasi duomenų valdytojas nuo duomenų tvarkytojo, galite rasti Europos Komisijos pateikiamoje suvestinėje **https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_lt**.

kodo, bendrųjų kontaktų) tvarkyti BDAR netaikomas. Šiuo požiūriu verta atkreipti dėmesį, kad kiekviena įmonė tvarko ne tik verslo subjekto, bet ir jo atstovų (darbuotojų, vadovo, kontaktinio asmens) asmens duomenis, taip pat savo darbuotojų asmens duomenis, todėl duomenų valdytojo statusą įgyja kiekviena įmonė.

### BDAR duomenų valdytojams kelia daug svarbių reikalavimų ir pareigų, susijusių su:

- duomenų apsaugos principų įgyvendinimu ir užtikrinimu;
- tinkamų organizacinių ir techninių saugumo priemonių užtikrinimu;
- duomenų subjektų informavimu ir jų teisių įgyvendinimu;
- pasitelkiamų duomenų tvarkymo patikimumo įvertinimu;
- rizikos duomenų apsaugai vertinimu;
- duomenų saugumo pažeidimų dokumentavimu ir pan.

BDAR nustato įmonėms, kaip duomenų valdytojoms ar duomenų tvarkytojoms, pareigą įgyvendinti tinkamas techninės ir organizacines priemones, kad būtų užtikrinamas pakankamas asmens duomenų saugumas. Nors BDAR nenustato jokių konkrečių duomenų saugumo priemonių, tačiau įtvirtina jų pasirinkimo kriterijus, t. y. saugumo priemonės pasirenkamos atsižvelgiant į techninių galimybių lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat pavojus fizinių asmenų teisėms ir laisvėms. Įmonė turėtų įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, jei reikia:

- asmens duomenų konfidencialumą ir jų šifravimą;
- gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą;
- gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis kibernetinio incidento atveju;
- reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą.

Daugiau informacijos apie tai, kaip Jūsų įmonė galėtų tvarkyti asmens duomenis, rasite Valstybinės duomenų apsaugos inspekcijos (VDAI) parengtose tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėse, skirtose SVV įmonėms. Dokumente pateiktais patarimais bus galima pasinaudoti tiek rengiant asmens duomenų apsaugos dokumentaciją, tiek atliekant konkrečius asmens duomenų tvarkymo veiksmus. Gaires galite rasti čia: **https://vdai.lrv.lt/uploads/vdai/documents/files/VDAI_saugumo_priemoniu_gaires-2019-12-18.pdf**.

Daugiau informacijos apie tai, kaip elgtis įvykus duomenų saugumo pažeidimui, rasite VDAI puslapyje **https://vdai.lrv.lt/lt/asmens-duomenu-apsaugos-reforma/pranesimas-apie-duomenu-saugumo-pazeidima**.

Įmonėms **rekomenduojama užtikrinti sistemingą techninių, organizacinių ir teisinių priemonių taikymą visuose procesuose** ir atnaujinimą laiku: parengti duomenų apsaugą reguliuojančius dokumentus, taip pat dokumentus, užtikrinančius asmens duomenų konfidencialumo užtikrinimą, numatyti organizacinius ir techninius resursus ir priemones, kad nustatyta tvarka būtų įgyvendinama praktikoje, peržiūrėti esamas ir įdiegti būtinas naujas technines priemones ir pan.

Įvykus kibernetiniam incidentui ar asmens duomenų saugumo pažeidimui svarbu ne tik formaliai įvykdyti reikalavimus, tačiau ir nustatyti incidento priežastis, sudaryti veiksmų planą, kad tokios priežastys būtų pašalintos, o saugumo pažeidimų rizika ateityje – suvaldyta.

Tais atvejais, kai kibernetinis incidentas yra taip pat ir asmens duomenų saugumo pažeidimas, duomenų valdytojas privalo per **72 valandas** nuo sužinojimo apie įvykusį ar galintį įvykti pažeidimą, VDAI, išskyrus atvejus, kai toks pažeidimas nekelia pavojaus asmenų teisėms ir laisvėms (pvz., nutekėję asmens duomenys buvo šifruoti). Tuo atveju, kai asmens duomenų saugumo pažeidimas įvyksta duomenų tvarkytojo veikloje, duomenų tvarkytojas per 24 valandas turi informuoti duomenų valdytoją, o šis, laikydamasis minėto 72 valandų termino (įskaitant terminą, per kurį gautas pranešimas iš duomenų tvarkytojo), jei reikia, informuoja VDAI.

Kai gali kilti **didelis pavojus** fizinių asmenų duomenų teisėms ir laisvėms (pvz., banko kortelių duomenų nutekėjimas), apie įvykusius duomenų saugumo pažeidimus duomenis valdanti įmonė privalo informuoti ir duomenų subjektus, kurių asmens duomenims kilo (galėjo kilti) grėsmė. Jeigu nesate tikri, ar incidentas yra laikomas duomenų saugumo pažeidimu, ar jis gali kelti grėsmę duomenų subjektų teisėms ir (ar) laisvėms, rekomenduojama susisiekti su VDAI ir pranešti apie galimą pažeidimą. Tai padėtų ne tik užtikrinti tinkamą BDAR reikalavimų vykdymą, bet ir įvertinti, kokių priemonių būtų tikslinga imtis situacijai suvaldyti ir tinkamam saugumui atkurti.

**Atsakomybė įmonei gali kilti ne tik pažeidus asmens duomenų saugumą**. VDAI turi teisę atlikti įmonių patikrinimus ir savo iniciatyva ar gavusi duomenų subjekto skundą. Atlikusi tyrimą, VDAI gali skirti atitinkamas poveikio priemones – nurodymą (pavyzdžiui, sustabdyti asmens duomenų tvarkymą), papeikimą, baudą ir pan. BDAR yra numatyta dvejopa duomenų valdytojo atsakomybė. Baudą gali skirti VDAI. Jos dydis gali siekti iki 20 mln. eurų arba iki 4 proc. metinės apyvartos, atsižvelgiant į tai, kuri suma didesnė. Dėl duomenų nutekėjimo nukentėję asmenys taip pat turi teisę kreiptis ir dėl žalos atlyginimo – šį klausimą vertina tik teismai.

Būtent šiame vadove toliau pateikiami gerosios praktikos pavyzdžiai ir rekomendacijos leis Jums sustiprinti įmonės pasiruošimą apsisaugoti nuo kibernetinių incidentų bei asmens duomenų pažeidimų, ir imtis reikiamų prevencinių priemonių, kurios sumažins situacijų, dėl kurių Jums grėstų teisinė atsakomybė, riziką.

## Kibernetinių incidentų valdymo planas ir veiklos tęstinumas

Kaip ir gyvenime, taip ir versle – įvykus neplanuotam ar netikėtam įvykiui, visada yra svarbu nepanikuoti ir gebėti valdyti krizines situacijas. Žinant, kad neįmanoma turėti visiško atsparumo kibernetinėms grėsmėms ir kad užtenka vienos mažos spragos sistemoje ar darbuotojų veiksmuose, kad programišius įsilaužtų į IT sistemą ar vidinį tinklą, **Jūsų įmonė turėtų pasiruošti incidentų valdymo ir veiklos tęstinumo planą**. Pirmieji veiksmai, kurių imamasi įvykus kibernetiniam incidentui ar duomenų pažeidimui, yra labai svarbūs, nes dažnai nulemia, koks bus poveikis įmonei, gebėjimą atstatyti verslo veiklą ir ateities įsilaužimų tikimybę.

### Reagavimo į incidentus taisykles turėtų sudaryti tokios dalys:

- **IT bei kitų įmonės darbuotojų vaidmuo ir atsakomybės įvykus kibernetiniam incidentui**. Kokie žmonės bus atsakingi už incidento valdymo, pažeidimų pašalinimo ir sistemų atkūrimo žingsnius? Kas turėtų kreiptis dėl incidento į atitinkamas institucijas / tarnybas ir pan.?
- **Veiksmai su laikomais duomenimis ir IT sistemomis**. Kokių veiksmų būtų imamasi įvykus tam tikriems kibernetiniams incidentams, paveikus tam tikras IT sistemas ar vidinį tinklą ir pan.? Pavyzdžiui, įvykus rimtam incidentui, rekomenduojama atjungti kompiuterius ar kitus prietaisus nuo tinklo, tačiau neišjungti jų maitinimo ar neperkrauti įrenginių iš naujo, kad neprarastumėte informacijos, naudingos incidento

analizei ir skaitmeniniam tyrimui atlikti (angl. *digital forensics*).

- **Suinteresuotų institucijų sąrašas ir kontaktai**. Ką ir kaip informuosite?
- **Komunikacijos planas**. Kaip informuosite savo darbuotojus įmonėje, kada ir kokiais atvejais informuosite klientus ir verslo partnerius apie įvykusį kibernetinį incidentą, ypač tuo atveju, kai yra žinoma arba numanoma, kad pavogti klientų asmens duomenys? Jeigu saugumo pažeidimas nėra pašalinamas greitai ir tinkamai arba jeigu klientai yra klaidinami dėl pažeidimo masto, Jums gresia didelė ilgalaikio klientų bazės praradimo ir žalos Jūsų verslo reputacijai rizika.
- **Veiklos tęstinumo planas**. Kokių žingsnių imsitės, kad neveikiant įmonės IT sistemoms galėtumėte tęsti veiklą ir užtikrinti vidinę įmonės komunikaciją? Kokius resursus pasitelksite, norėdami greičiau atkurti veiklos tęstinumą? Incidentai rodo, kad tokiais atvejais įmonės darbuotojai susisiekia tarpusavyje telefonu arba naudodami susirašinėjimo programėles „Messenger“ ar „WhatsApp“ (bet tai svarbu daryti jokiu būdu nenaudojant įmonės belaidžio tinklo).
- **Veiklos avarinio atkūrimo planas**. Kokių veiksmų imsitės, kad būtų atkurta operatyvi IT veikla bei įmonės duomenys? Be šio punkto veiklos tęstinumo planas prarastų savo prasmę. Dar būtina pabrėžti, kad šie planai turi būtų periodiškai testuojamai (kaip yra daroma ir su priešgaisrinėmis pratybomis).

Detalesnį sąrašą su rekomendacijomis, kas turėtų būti įtraukta į incidentų valdymo planą, rasite Europos tinklų ir informacijos apsaugos agentūros (ENISA) puslapyje **https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/incident-management-plan/**.

06

# 10 PIRMŲJŲ ŽINGSNIŲ KIBERNETINIO SAUGUMO LINK

Susipažinus su kibernetinio saugumo svarba verslui bei grėsmėmis, kitas žingsnis – atlikti pirmuosius veiksmus, padidinsiančius Jūsų įmonės kibernetinį atsparumą. Veikdami pagal šiame skyriuje pateiktus patarimus, suprasite, kas Jums, kaip smulkiai įmonei, yra svarbiausia kibernetinio saugumo srityje ir kaip paprastais žingsniais galite apsaugoti savo įmonės informaciją ir IT nuo labiausiai paplitusių kibernetinių grėsmių.

Gerosios kibernetinio saugumo praktikos pavyzdžių rinkinys parengtas atsižvelgiant į konsultacijas su kibernetinio saugumo ekspertais bei analizuojant užsienio šalių kibernetinio saugumo vadovus, kurių tikslas yra padėti smulkiajam verslui stiprinti savo kibernetinį atsparumą.

## 01 SLAPTAŽODŽIŲ POLITIKA

Įsitikinkite, kad Jūsų įmonėje yra laikomasi saugaus slaptažodžio kūrimo ir naudojimo principų.

## 02 KELIŲ ŽINGSNIŲ AUTENTIFIKAVIMAS

Jei yra galimybė, naudokite aukštesnio lygio apsaugos priemones, kad galėtumėte saugiai naudotis savo svarbiausiomis paskyromis.

## 03 ANTIVIRUSINĖS PROGRAMOS

Apsaugokite įmonės kompiuterius ir kitus įrenginius nuo kenkimo programų ir užkrėstų dokumentų.

## 04 AUTOMATINIAI ATNAUJINIMAI

Įsitikinkite, kad įmonės kompiuteriai bei įrenginiai turi įdiegtą naujausią programinę įrangą.

## 05 ATSARGINĖS DUOMENŲ KOPIJOS

Apsaugokite savo įmonės dokumentus nuo informacijos nutekėjimo, vagysčių ar kitų nelaimių.

## 06 PRIEIGOS KONTROLĖ

Žinokite, kokie žmonės gali pasiekti svarbią įmonės informaciją.

## 07 IŠMOKYTI DARBUOTOJAI

Sumažinkite žmogaus klaidų riziką savo įmonėje.

## 08 DARBO IR ASMENINIŲ PRIETAISŲ ATSKYRIMAS

Įsitikinkite, kad darbuotojai saugiai naudojasi savo įrenginiais.

## 09 UGNIASIENĖS

Sukurkite saugią neutralią zoną tarp interneto ir Jūsų įmonės.

## 10 SAUGUS BEVIELIS TINKLAS

Neleiskite, kad Jūsų maršrutizatorius taptų atviromis durimis programišiams patekti į Jūsų įmonės tinklą.

# 01 Slaptažodžių politika

Slaptažodis – lyg raktas nuo namų. Jis ne tik patvirtina konkretaus žmogaus tapatybę, bet ir leidžia apsaugoti prieigą prie asmeninės, komercinės informacijos ar kitų svarbių duomenų. Nors dauguma didžiausių informacinių sistemų turi papildomas apsaugas nesankcionuotoms prieigoms išvengti, vis vien **svarbu laikytis tam tikrų taisyklių formuojant ir tvarkant slaptažodžius**.

Saugus slaptažodis – svarbiausia apsisaugojimo priemonė. Ši tema yra itin jautri verslui – jų slaptažodžiai saugo ne tik asmeninius duomenis, bet ir komercines paslaptis, finansinę informaciją, klientų įrašus. Šios informacijos praradimas ar patekimas į piktavalių rankas gali reikšti ne tik milžiniškus nuostolius verslui, bet gali nulemti ir jo pabaigą. Nepamirškite, kad šie patarimai taip pat galioja ir visiems įmonėje naudojamiems išmaniesiems telefonams ar bet kokiems kitiems interneto prieigą turintiems įrenginiams.

**2017 m. „Verizon“ asmens duomenų pažeidimų tyrimas** parodė, jog viena dažniausių duomenų saugumo pažeidimo priežasčių (81 proc., 2017 m. duomenimis) – silpni, nesaugūs slaptažodžiai ir jų pakartotinis naudojimas keliose platformose.

## SAUGUS SLAPTAŽODIS

### NENAUDOKITE POPULIARIŲ SLAPTAŽODŽIŲ

Programišiai, bandydami prisijungti prie paskyrų, pirmiausia išbandys populiariausius slaptažodžius, pavyzdžiui: *qwerty, 123456, password* ar kitus dažnai naudojamus variantus. Įsitikinkite, kad Jūsų slaptažodis nėra populiariausiųjų sąraše[8]. Šiuos ir panašius slaptažodžius programišiai gali nulaužti per kelias sekundes.

### NENAUDOKITE VIENODŲ SLAPTAŽODŽIŲ SKIRTINGOMS PASKYROMS

Viena dažniausiai pasitaikančių ir lengvai išsprendžiamų saugumo spragų įmonėse – slaptažodžių pakartotinis naudojimas. Piktavaliai neretai naudojasi slaptažodžių duomenų bazėmis iš prieš tai atliktų atakų, todėl jei naudojate tą patį slaptažodį prisijungdami prie kitų paskyrų, visose šiose paskyrose padidėja pažeidžiamumo rizika[9].

### SLAPTAŽODŽIO ILGIS

Kurdami slaptažodį, atminkite, kad slaptažodžio ilgis yra vienas svarbiausių saugumo faktorių. Pavyzdžiui, piktavalis užtruks mažiau nei vieną sekundę spėdamas sugalvotą slaptažodį, jei jį sudarys keturi simboliai. Tuo tarpu jam teks paplušėti porą metų, jei slaptažodis bus sudarytas iš ne mažiau kaip 10 simbolių. Specialūs simboliai (`!@$%^&*()–_=+[];:'",<.>/?) suteikia slaptažodžiui papildomą apsaugą.

### SLAPTAŽODŽIO SUDĖTINGUMAS

Norint sukurti saugų slaptažodį, būtina įtraukti didžiąsias raides, skaičius ir simbolius (pvz., *SauGikl!s466*). Reikėtų vengti įprastų ir mūsų aplinkoje pasitaikančių objektų: produktų pavadinimų (pvz., *volkswagen*), vardų (pvz., *saulius*), pavardžių (pvz., *petraitis*), naminių gyvūnėlių vardų (pvz., *brisius*), gimtadienių (pvz., *0921*) ar vestuvių metinių datų. Siekiant sukurti lengvai atsimenamą slaptažodį, dažniausiai sukuriamas slaptažodis, kurį lengva ir nulaužti.

Tikrai saugius slaptažodžius dažniausiai bus sudėtinga atsiminti. Išimtis – slaptafrazės (angl. *passphrases*). Tai yra slaptažodžiai, susidedantys iš kelių žodžių ir sudarantys frazę, – jie gali būti ir saugesni, ir lengviau įsimenami (pvz., *saugiklissaugoskydine*).

## Slaptažodžių valdymo įrankiai

Slaptažodžių valdymo įrankiai (angl. *password managers*) padeda saugiai laikyti jautrius duomenis tiek asmeniniame gyvenime, tiek ir darbo aplinkoje. Jie sugeneruoja saugius slaptažodžius ir juos saugo, leidžia jais disponuoti komandos nariams ar įmonės darbuotojams. Taip padedama valdyti prieigų kontrolę įmonėse ir be didelių investicijų sustiprinamas bendras informacijos saugumas. Naudojant šifravimo algoritmus, duomenys yra užšifruojami ir tampa neperskaitomi net ir programišiams sugebėjus įsilaužti į serverius ar duomenų bazes.

Šie įrankiai gali būti integruoti į Jūsų kompiuteriuose esančias interneto naršykles ar įdiegti kaip atskiras naršyklės įrankis, atskira programinė įranga. Prieigai prie slaptažodžių valdymo įrankių reikėtų naudoti kelių žingsnių autentifikavimą, kad Jūsų slaptažodžiai būtų laikomi saugiai.

2016 m. spalį iš tarptautinės pavežėjimo paslaugas teikiančios įmonės „Uber“ buvo **nutekinti daugiau nei 56 mln. vairuotojų asmens duomenys**. Šis kibernetinis incidentas įvyko, nes IT specialistas laikė slaptažodžius viešai prieinamoje „Github“ saugykloje.

Įrankiai, skirti komandoms (įmonės darbuotojams), leidžia ne tik saugiai laikyti ir, kai reikia, su bendradarbiais dalytis slaptažodžiais, bet ir valdyti prieigas priskiriant vartotojams vaidmenis (komandos paskyros savininkas, administratorius, įprastas vartotojas) bei teises matyti / naudoti / atnaujinti slaptažodžius masiškai ar po vieną.

[8] Populiariausių slaptažodžių sąrašą galite rasti čia: https://github.com/lexcor/LT-SecList.

[9] Pasitikrinkite, ar buvo pavogti Jūsų prisijungimo duomenys svetainėje „Have I Been Pwned?“ („Ar aš buvau sutriuškintas?“): https://haveibeenpwned.com/.

# 02 Kelių žingsnių autentifikavimas


Dažnai slaptažodis yra vienintelis dalykas, apsaugantis Jūsų duomenis nuo įsilaužėlio. Piktavaliai, naudodamiesi socialinės inžinerijos metodais, slaptažodžius gali išvilioti, o nesaugius slaptažodžius gali atspėti naudodami automatines priemones. Dėl šios priežasties jautriausią informaciją svarbu apsaugoti keliais būdais. Rekomenduojama, kai tai įmanoma, naudojamose paskyrose ar programinėje įrangoje įjungti dviejų ar daugiau žingsnių autentifikavimo funkciją.

Nors šio funkcionalumo pritaikymo būdai įvairūs, tačiau veikimo principas gana paprastas: jungiantis su įprastais prisijungimo duomenimis (pvz., prisijungimo vardas ir slaptažodis), vartotojo prašoma įvesti papildomą vienkartinį kodą, sugeneruotą ar nusiųstą į antrinį įrenginį, pavyzdžiui, į el. paštą, atsiunčiant kodą trumpąja SMS žinute, sugeneruojant jį specialioje aplikacijoje ar prijungiant fizinį įrenginį, išduotą asmeniškai (USB, ID kortelės skaitytuvas).

Didelė dalis platformų, aplikacijų ir įrankių internete šiandien turi dviejų (ar daugiau) žingsnių autentifikavimo funkcionalumą. **Jis leidžia užtikrinti aukštesnį vartotojo ir jo duomenų saugumo lygį naudojant įrankius ar platformas internete**. Nesvarbu, ar tai būtų el. bankininkystės paskyra, prieiga prie socialinių tinklų paskyrų ar biuro programų platformos (pvz.: „Office 365“, „GSuite“), ši funkcija užtikrina papildomą Jūsų duomenų apsaugą.

Esminis aspektas, užtikrinantis aukštesnį saugumo lygį, net ir vartotojui praradus (ar programišiams pavogus) pagrindinį įrenginį (pvz., kompiuterį), yra tai, kad jo duomenys išliks saugūs, nes piktavaliai negalės prisijungti prie vartotojo paskyros neturėdami antrinio įrenginio, o Jūs būsite tuoj pat informuoti apie mėginimus pasinaudoti paskyra.



## 03 Antivirusinės programos

Antivirusinės programos yra vienas elementariausių techninių kibernetinio saugumo būdų, apsaugančių įmonę nuo įsilaužimo į Jūsų kompiuterį. Šiais laikais antivirusinės programos dažnai yra įdiegiamos kartu su populiariosiomis operacinėmis sistemomis (pvz., „Windows Defender“ ar „Gatekeeper“ „Apple“ kompiuteriuose), tad dauguma iš Jūsų tikriausiai jau susidūrėte su jomis.

Antivirusinės programos saugo vartotojus nuo daugumos į juos orientuotų piktavališkų programišių veiksmų ir kitų kibernetinių grėsmių, tokių kaip neautorizuotų USB atmintinių ar kitų išorinių laikmenų naudojimas, el. laiškų priedų skenavimas ir pan.

Gali atrodyti, kad norint apsisaugoti nuo kibernetinių grėsmių tiesiog pakanka naudoti antivirusinę programą, tačiau su tuo nesutinka kibernetinio saugumo ekspertai [10]. Asmeniniam naudojimui dažnai pakanka ir nemokamų sprendimų (pvz., įdiegti nemokamą antivirusinę programą), tačiau įmonės turi kompleksiškesnę informacinių išteklių infrastruktūrą. Dėl šios priežasties neturėtumėte šio sprendimo palikti tik IT specialistui. Rekomenduojama labiau įsigilinti į kibernetinio saugumo klausimą ir atsižvelgti į tai, jog poreikiai, rizikos ir nuostoliai versle yra visai kitokie. Neišsigąskite, rinkoje egzistuoja ir smulkiam verslui skirti kibernetinio saugumo sprendimai.

Iš pradžių būtina identifikuoti svarbiausias sritis (pvz., el. paštas, mobilieji įrenginiai). Jas identifikavus, galima įvertinti ir komercinius sprendimus. Galbūt pakaktų įsigyti komercinę antivirusinę programą su el. pašto paslauga? Galbūt tiekėjai už prieinamą kainą gali pasiūlyti centralizuotus mobiliųjų įrenginių valdymo sprendimus? O kaip dėl informacijos šifravimo? Rinkoje galite rasti kibernetinio saugumo sprendimus, padedančius spręsti šiuos klausimus. Naudodami tokius įrankius, vienu metu galite saugoti visus įmonės įrenginius (kompiuterius, išmaniuosius telefonus ir pan.) ir turėti daugiasluoksnę apsaugą (ko negali pasiūlyti nemokamos antivirusinės programos), galinčią sustabdyti iki keliasdešimt skirtingų tipų atakų.

Taip pat svarbu, kad būtų **įjungta automatinio atnaujinimo funkcija** (pageidautina bent kartą per dieną), tada galėsite mažiau jaudintis dėl naujų grėsmių.

Jeigu Jūsų įmonės darbuotojai turi galimybę dirbti nuotoliniu būdu ir tam naudoja savo asmeninius kompiuterius, apsvarstykite galimybę įsigyti verslo naudojamos antivirusinės programos kopiją arba reikalaukite, kad darbuotojai įdiegtų saugią antivirusinę programą į asmeninius prietaisus.

Daugiau informacijos apie tai, kokių veiksmų galite imtis esant apkrėstam kompiuteriui, rasite puslapyje **https://esaugumas.lt/lt/kompiuteriu-virusai/greitoji-pagalba-apkrestam-kompiuteriui/110**.

[10] David Ford, „Why Free Anti-Virus is Not Enough For Your Business“, Live Consulting, paskelbta 2017 m. gruodžio 19 d., **https://www.liveconsulting.com/news/why-free-anti-virus-is-not-enough-for-your-business/**.

**Nepamirškite, kad, siekiant apsisaugoti nuo dažniausiai pasitaikančių kibernetinių grėsmių, neužtenka turėti tik antivirusinę programą**.

Įvertinus saugumo informacijos svarbą, verta apsvarstyti ir didesnį apsaugos priemonių paketą, kuris įtrauktų tokius įrankius kaip išpirkos reikalaujančių virusų šalinimo programa (angl. *anti–ransomware*), smėlio dėžė (angl. *sandbox*), kuri izoliuotoje aplinkoje patikrina, ar failai nėra kenksmingi, ar pažeidžiamumų patikra (angl. *vulnerability assessment*). Tačiau nepamirškite, kad šių priemonių ir įrankių naudojimas turėtų remtis atliktu rizikų vertinimu, nes ne visoms įmonėms reikalingi tokie pažangūs sprendimai.

## 04 Automatiniai atnaujinimai

Programinės įrangos atnaujinimai yra labai svarbus kibernetinio saugumo ir skaitmeninių sistemų saugaus funkcionavimo elementas. Kaip ir alyvos keitimas Jūsų automobilyje, taip ir įrangos, sistemų atnaujinimai yra tiesiog būtini. Atnaujindami programinę įrangą, Jūs galite panaikinti didžiąją dalį paliktų spragų Jūsų įmonės naudojamose programose ir platformose.

Įsilaužėliai mėgsta pasinaudoti programinės įrangos silpnybėmis – saugumo skylėmis arba klaidomis, padarytomis kuriant programinę įrangą ar operacinę sistemą, nes tai yra paprasčiau, nei pačiam ieškoti naujų spragų. Pasinaudoję rasta žinoma spraga, programišiai gali apkrėsti Jūsų įrenginius[11] . Kenkimo kodas gali būti įterptas į Jūsų kompiuterį tiesiog apsilankius užkrėstoje svetainėje ar atidarius užkrėstą elektroninio laiško priedą.

Kas nutinka po to? Kenkimo programos gali pasisavinti Jūsų kompiuteryje saugomus duomenis, leisti įsilaužėliams užvaldyti Jūsų kompiuterį ar užkoduoti įmonės svarbius duomenis.

Daugelis programinės įrangos tiekėjų stengiasi greitai ir laiku reaguoti į atsirandančias spragas. Gamintojai periodiškai teikia įrangos atnaujinimus (angl. *software patches*), kurie panaikina saugumo spragas ir neleidžia įsilaužėliams jomis pasinaudoti. Todėl **įsitikinkite, kad esate įjungę automatinio programinės įrangos ir operacinės sistemos atnaujinimo funkciją**. Ją galima įjungti per „Windows“, „MacOS“ ar kitos programinės įrangos nustatymus. Nepamirškite, kad šie patarimai taip pat galioja visiems įmonėje naudojamiems išmaniems telefonams ir bet kokiems kitiems prie interneto prieigą turintiems įrenginiams.

**Niekada neatidėliokite siūlomų atnaujinimų**. Kartais luktelėjus tik vieną dieną galima smarkiai padidinti kibernetinio pažeidžiamumo riziką. Atnaujinant programinę įrangą, Jūsų įrenginys gali veikti lėčiau arba net kuriam laikui prarasti funkcionalumą, todėl nustatykite, kad atnaujinimai būtų diegiami per pietų pertrauką ar po darbo, arba sudarykite atnaujinimų diegimo planą, kai įrenginiais naudojamasi mažiau. Taip pat įvertinkite, ar atnaujinimas nepakenks

[11] Patikrinkite, ar Jūsų įmonės naudojamoje programinėje įrangoje yra aptikti ir užfiksuoti pažeidžiamumai ir kiek jų galėjo atsirasti senose programinės įrangos versijose: https://cve.mitre.org/.

2017 m. liepą kredito biuras „Equifox“ pranešė, kad buvo nutekinti 146 mln. klientų asmens duomenys. Pavogtuose ir paviešintuose dokumentuose buvo galima rasti mokėjimų kortelių, pasų ir vairuotojų pažymėjimų informaciją, mokesčių mokėtojų numerius ir kitą jautrią informaciją. Skaičiuojama, jog **ši ataka įmonei kainavo daugiau nei 1.5 mlrd. dolerių**. Silpnąją vietą programišiai rado įmonei laiku neatnaujinus interneto aplikacijų kūrimo programos „Apache Struts“.

esamam sistemos funkcionalumui dėl naujų pokyčių. Nepatartina diegti visų atnaujinimų iškart į visus įrenginius. Iš pradžių atnaujinimą atlikite viename įrenginyje, įvertinkite sistemos veikimą ir tik tada atnaujinkite kitur.

**Nepamirškite**: dažniausiai operacinė sistema atnaujinama tik perkrovus kompiuterį.

**Įsigiję naujus darbinius kompiuterius ar naują programinę įrangą, neužmirškite patikrinti, ar yra įdiegti naujausi atnaujinimai**. Taip pat nevertėtų pamiršti, kad programinės įrangos gamintojai neprivalo teikti saugumo spragų atnaujinimų senesnei įrangai, kurios techninis palaikymas jau yra nutrauktas. Tokiu atveju rekomenduojama įsigyti naujesnę įrangos versiją ar pasirinkti kitą programinės įrangos tiekėją.

### NEPAMIRŠKITE ATNAUJINTI „WINDOWS“ OPERACINĖS SISTEMOS

2020 m. sausio 14 d. „Microsoft“ nutraukė „Windows 7“ ir „Windows Server 2008“ operacinių sistemų (OS) techninį palaikymą. Tai reiškia, kad naujai atrastos saugumo spragos jau nebebus taisomos OS gamintojo. Vadinasi, „Windows 7“ turintys kompiuteriai ir serveriai su „Windows 2008“ tampa lengvais programišių taikiniais. Programišiams atsiranda daugiau galimybių pasinaudoti OS pažeidžiamumu.

Kai kuriais atvejais naujos OS įdiegimas gali trukdyti funkcionalumui derinant darbą su kita įmonės naudojama programine įranga, tačiau atnaujinimo atidėliojimas smarkiai didina įsilaužimo riziką. Todėl rekomenduojama tuoj pat į įmonės ir asmeninius kompiuterius įdiegti „Windows 10“ OS.

## 05 Atsarginės duomenų kopijos

Duomenys skaitmeniniame pasaulyje yra svarbiausias ir vertingiausias dalykas, todėl norint juos apsaugoti būtina imtis papildomų priemonių. Įsivaizduokite, jei vieną dieną skaitmeniniame įrenginyje staiga dingtų visi dokumentai, ataskaitos, sutartys, finansiniai duomenys, klientų ir kita informacija. Neturint atsarginės duomenų kopijos, galima bandyti juos atkurti iš kitų skaitmeninių įrenginių, el. pašto ir pan. Tačiau ar pavyktų atkurti visus duomenis ir kiek tai užtruktų laiko?

Duomenis, saugomus skaitmeniniame įrenginyje, galima prarasti dėl įvairių priežasčių: įrangos gedimo, programinės įrangos sutrikimo, virusų ar kenkimo programos, elektros maitinimo tinklo gedimo ar žmogaus klaidos. **Praradus duomenis, veiklos atkūrimas gali būti labai lėtas, brangus arba neįmanomas**. Siekiant apsaugoti savo duomenis nuo praradimo, rekomenduojama nuolat kurti atsargines duomenų kopijas.

**Tai padės išvengti:**

- atsitiktinių ar piktybinių duomenų sugadinimų bei modifikavimų (ypač įvykus *ransomware* atakai);
- ilgos prastovos ar veiklos sustojimo, kai įmonė negali tęsti savo veiklos be jai reikalingos informacijos;
- konfidencialumo sutarčių pažeidimų ir BDAR reikalavimų nesilaikymo;
- intelektinės nuosavybės praradimo.

# SIEKIANT APSISAUGOTI NUO DUOMENŲ PRARADIMO, REIKIA:

A

## NUSTATYTI, KOKIŲ DUOMENŲ KOPIJOS TURI BŪTI DAROMOS

Būtina nustatyti, kurie duomenys yra svarbūs ir kurių duomenų atsarginės kopijos turi būti saugomos. Pavyzdžiui, turėtų būti kuriamos dokumentų, grafinių, garso ir kitų duomenų kopijos. Taip pat galima pasirinkti, kad būtų sukuriama operacinės sistemos kopija. Tai leidžia atkurti operacinės sistemos darbą (atkuriant ir buvusias įdiegtas programas), kai sistema pradeda veikti nestabiliai ar ji kitaip pažeidžiama.

B

## PASIRINKTI ATSARGINIŲ DUOMENŲ KOPIJŲ KŪRIMO DAŽNUMĄ

Nuspręsti, kaip dažnai turi būti kuriamos atsarginės duomenų kopijos: kasdien, kas kelias dienas, kartą per savaitę ir pan. Vertingesni duomenys turėtų būti kopijuojami dažniau. Taip pat rekomenduojama daryti atsargines kopijas, kai užbaigiami nauji ir pabaigiami redaguoti turimi duomenys bei atliekami pakeitimai IT sistemose (diegiama nauja įranga, atnaujinamos programinės įrangos versijos ir pan.).

C

## PASIRINKTI ATSARGINIŲ DUOMENŲ KOPIJŲ KŪRIMO PRIEMONES

Nors duomenis galima nukopijuoti rankiniu būdu ir juos saugoti kitoje vietoje, vis dėlto rekomenduojama naudoti standartines operacinės sistemos ar trečiųjų šalių siūlomas atsarginių kopijų kūrimo priemones, kurios tai atliks automatiškai.

D

## NUSTATYTI PRIEIGĄ PRIE ATSARGINIŲ DUOMENŲ KOPIJŲ

Nustatyti ir aprašyti, kas turės prieigą prie atsarginių duomenų kopijų.

E

## APRIBOTI ATSARGINIŲ DUOMENŲ KOPIJŲ PRIEINAMUMĄ

Užtikrinti, kad įrenginiai, kuriuose saugomos atsarginės duomenų kopijos, nebūtų nuolat prijungti prie kompiuterio, kuriame jos buvo kuriamos. Tai labai svarbu siekiant sumažinti riziką, kad atsarginės kopijos gali būti prarastos įsilaužus į kompiuterį ar kitais nenumatytais atvejais.

F

## PASIRINKTI ATSARGINIŲ DUOMENŲ KOPIJŲ SAUGOJIMO VIETĄ

Jas galima saugoti išoriniuose įrenginiuose: šifruojamuose išoriniuose diskuose ar debesijos saugyklose. Fizinės rezervinės kopijos neturėtų būti laikomos tose pačiose patalpose, kur yra Jūsų darbovietė.

G

## NUSPRĘSTI DĖL ATSARGINIŲ DUOMENŲ KOPIJŲ SAUGOJIMO KELIOSE VIETOSE

Jei tam tikri duomenys yra labai svarbūs, galima saugoti kelias atsargines jų kopijas skirtingose šifruojamose laikmenose ir vietose. Siekiant apsaugoti atsargines kopijas nuo kenkėjiškų veiksmų ar stichinių nelaimių, rekomenduojama bent vieną atsarginę kopiją laikyti fiziškai izoliuotoje vietoje ar patikimoje debesijos saugykloje.

H

## NUSTATYTI ATSARGINIŲ DUOMENŲ KOPIJŲ SAUGOJIMO TERMINUS

Pavyzdžiui, suėjus tam tikram terminui, senos kopijos būtų sunaikinamos.

I

## PARENGTI DUOMENŲ ATKŪRIMO TVARKĄ

Aprašyti duomenų atkūrimo taisykles įvykus incidentui (kas gali tai atlikti, kokia atkūrimo procedūra ir pan.). Reguliariai tikrinkite, ar įmanoma atkurti duomenis iš atsarginių kopijų.

## 06 Prieigos kontrolė

Prieigos kontrolė yra tarsi fizinė durų apsauga: norint patekti į tam tikrą vietą, tenka prie įėjimo nuskenuoti savo leidimą, kad atsidarytų durys. Svarbu, kad tos durys atsidarytų tik tiems, kam yra suteikta teisė ten patekti, išvengiant pašalinių ir jų galimai padaromų nuostolių.

Taip ir kibernetinėje erdvėje – norint sumažinti galimą incidento žalą, kuri gali būti padaryta neteisėtai naudojantis vartotojų paskyromis, **Jūsų įmonėje turėtų būti apibrėžta darbuotojų, duomenų valdytojų ir kitų asmenų prieigos teisių kontrolė**. Tai sprendimas, sumažinantis tikimybę, kad dėl tyčinių ar netyčinių veiksmų bus sukuriami ir išnaudojami įmonės pažeidžiamumai.

**Niekam iš darbuotojų nesuteikite prieigos prie visų informacinių sistemų ar programinės įrangos** – vadovaukitės „būtina žinoti“ principu. Darbuotojams turėtų būti suteikta prieiga tik prie konkrečių sistemų ar programų, kurių jiems reikia dirbant. Prieiga prie jautrių duomenų turėtų būti suteikta tik tiems darbuotojams, kuriems leidžiama dirbti su svarbia informacija. Aukštesnės privilegijos teisės turėtų būtų išjungtos arba pašalintos, kai tai tampa nebereikalinga.

**Patikrinkite administratoriaus paskyros teises**. Jos turėtų būti naudojamos tik administracinėms užduotims atlikti (pvz., programų diegimas ir atnaujinimas, sistemos ar kompiuterių nustatymų keitimas). Paskyros, turinčios administratoriaus privilegijas, yra dažnas programišių taikinys, nes jos suteikia neribotą prieigą prie jautrios informacijos ir galimybę valdyti įmonės tinklą. Neatsargiai besielgiantis darbuotojas, paspaudęs užkrėstą priedą ar atidaręs nesaugią svetainę, net nežinodamas gali įdiegti pasislėpusią kenkimo programą į įmonės kompiuterį. Todėl jiems neturėtų būti suteiktos administratoriaus teisių pareigos prie darbo kompiuterio, nebent tai priklauso pagal funkcijas.

Darbuotojui palikus Jūsų įmonę, pasirūpinkite, kad jam būtų panaikinta prieiga prie įmonės duomenų ar sistemų. Tam gali prireikti ištrinti darbuotojų paskyras iš visų susietų sistemų, pakeisti slaptažodžius, kuriais yra dalijamasi (pvz., įmonės socialinių tinklų paskyros), ir paimti raktus, taip užtikrinant įmonės fizinį saugumą.

Verta prisiminti ir garsųjį „Grožio chirurgijos“ klinikos atvejį, kai programišiai į įmonės sistemą įsilaužė panaudoję buvusio klinikos darbuotojo prisijungimo duomenis ir taip **pavogė 22 tūkst. klientų asmeninius duomenis**, nuotraukas prieš ir po operacijų. Iš klinikos **buvo reikalaujama 500 tūkstančių eurų vertės išpirkos**, o iš klinikos klientų – **nuo 50 iki 800 eurų**. Ir tai nebuvo vienintelei finansiniai nuostoliai – nukentėjusiųjų ieškinių **suma dėl padarytos neturtinės žalos siekė 230 tūkstančių eurų**.

## 07 Išmokyti darbuotojai – verslo apsauga

**Svarbu suprasti, kad tinkamai išmokyti darbuotojai prisideda prie Jūsų verslo apsaugos nuo kibernetinių grėsmių**. Socialinės inžinerijos apgavysčių atpažinimo ir kitus darbuotojų saugumo įgūdžius ugdyti galima organizuojant tam tikrus mokymus. Tokių mokymų programa gali padėti ugdyti kibernetinę higieną tarp darbuotojų ir taip skatinti bendros atsakomybės jausmą dėl saugaus Jūsų verslo.

Mokymų reguliarumas ir forma gali priklausyti nuo Jūsų veiklos praktikų. Paprastesni mokymai gali būti rengiami ir reguliarių susitikimų metu, kai apžvelgiami pagrindiniai saugumo principai. Galbūt Jums tinkamiausi intensyvesni mokymai kas 12 mėnesių? Tai gali būti mokymai Jūsų darbovietėje, bet gali būti ir kibernetinės saugos pamokos internete. Svarbu, kad tokie mokymai vyktų reguliariai, nes kibernetinis saugumas vis kinta. Darbuotojams būtina pateikti naujausią informaciją apie grėsmes ir saugumo priemones.

## Kaip neužkibti ant kabliuko?

- **Pagalvokite, ar Jūsų darbuotojai žino, kaip elgtis su neįprastomis užklausomis?** Apsvarstykite, kokie papildomi saugumo patikrinimai Jums praverstų tokiais atvejais, kai gaunama užklausa iš žmogaus, apsimetančio įmonės vadovu ar kitu asmeniu.
- **Išmokykite darbuotojus** atpažinti įtartinas užklausas, apgaulingus laiškus, taip pat išmokykite, kaip elgtis su jautria informacija. Gilinkite jų žinias, kad jie galėtų įvertinti laiško siuntėją, turinį, gramatiką, siuntėjo parašą, logotipą ir kitus ženklus, galinčius kelti įtarimą. Informuokite juos, kam reikia pranešti gavus apgaulingų laiškų ir kokių veiksmų imtis, jei jie tapo apgavystės aukomis.
- **Domėkitės kintančiais apgavysčių metodais**. Socialinės inžinerijos technikos keičiasi ir atsiranda vis naujesnių apgavystės metodų. Siekiant nuo jų apsisaugoti, gali prireikti atnaujinti saugos priemones ir žinias.
- **Rekomenduojama riboti darbuotojų prieigą prie socialinių tinklų ir asmeninių el. pašto dėžučių**, jei to nereikia darbo funkcijoms atlikti. Taip mažinama rizika, kad Jūsų įmonės darbuotojas susidurs su sukčiavimu ir galimai apkrės įmonės kompiuterį ir tinklą.
- **Atskleiskite tik reikiamą informaciją apie savo įmonę**. Bet kokia perteklinė informacija apie Jūsų įmonę ar darbuotojus gali būti panaudota socialinės inžinerijos atakoms.

## UGDYKITE SAVO DARBUOTOJŲ ĮPROTĮ ATLIKTI ŠIUOS ŽINGSNIUS VERTINANT GAUNAMAS UŽKLAUSAS:


**STOP** – neskubėkite atidaryti laiško, spausti jame esančių nuorodų, atidaryti priedų ar vykdyti kitų reikalaujamų veiksmų. Žiūrėkite į juos kritiškai ir išlikite budrūs.

**PATIKRINK** – darbuotojas turi apsvarstyti, ar laiškas gautas netikėtai, kokia jo gavimo priežastis, ir atsakyti į šiuos klausimus:

- Ar siuntėjo vardas ir el. pašto adresas sutampa? Ar jie nekelia įtarimų? Ar laiškas skirtas Jums?
- Ar laiško gramatika, naudojami logotipai, siuntėjo parašas nekelia įtarimo?
- Ar esate skatinamas skubiai atlikti tam tikrus veiksmus?
- Jei Jūsų prašoma informacijos, apsvarstykite, kokia tai informacija. Ar tai jautri informacija (pvz., prisijungimo, asmens duomenys)?
- Ar nuoroda, kurią matote, yra logiška, suprantama ir nekelia įtarimo? Užvedę pelės rodyklę ant nuorodos, patikrinkite, kokia nuoroda siunčiama[12].
- Ar priedų pavadinimai, ikonos, plėtiniai nekelia įtarimo?

**PRANEŠK** – kai darbuotojams kyla įtarimas, jog jie gavo apgaulingą laišką, skatinkite juos apie tai pranešti. Venkite kaltinimų, jei darbuotojai tapo apgaulės aukomis, nes taip galite paskatinti juos nutylėti apie kitą incidentą. Svarbu kurti aplinką, kurioje darbuotojai nebijotų pranešti padarę klaidą.

[12] Nuorodų trumpinius galite patikrinti šioje svetainėje: http://www.checkshorturl.com/.

## DARBUOTOJO ATMINTINĖ KIBERNETINEI HIGIENAI PALAIKYTI

- Neprijunkite nežinomų USB atmintinių prie įmonės kompiuterių.
- Nepalikite neužrakinto kompiuterio net trumpam palikę savo darbo vietą. Galima nustatyti automatinio užsirakinimo funkciją.
- Saugokite ir teisingai tvarkykite prisijungimo duomenis.
- Neklijuokite ant ekranų ir nepalikite prisijungimo duomenų kitiems matomose vietose.
- Niekam neatskleiskite savo prisijungimo duomenų.
- Nespauskite ant nuorodų el. laiškuose, ypač gautuose iš nežinomų siuntėjų.
- Neatskleiskite pašaliniams jautrios asmeninės ar įmonės informacijos.
- Baigę darbą, uždarykite programų langus, išjunkite kompiuterį. Nepalikite ant stalo dokumentų ir duomenų laikmenų.
- Įtarę, kad kažką padaryti ar atskleisti prašantis bendradarbis (IT sistemų administratorius ar vadovas) nebūtinai yra tas, kuo dedasi, perskambinkite jam, pasitarkite su kitais bendradarbiais ar vadovu.

Daugiau informacijos apie kenksmingus el. laiškus rasite NKSC puslapyje **https://www.nksc.lt/doc/biuleteniai/2019-06-26%20Malware%20platinimas%20LT%20imoniu%20vardu.pdf**.

Rekomenduojamus interneto naršyklių nustatymus rasite čia: **https://esaugumas.lt/lt/duomenu-vagystes-phishing/rekomenduojami-narsykliu-nustatymai/251**.

Nemokamą mokomąją medžiagą apie saugų elgesį internete taip pat galima rasti „Prisijungusi Lietuva“ portale **https://www.prisijungusi.lt/medziaga/prad/8/#/**.

# 08 Darbo ir asmeninių prietaisų atskyrimas

Su darbo ir asmeninių prietaisų atskyrimu susijusios rizikos gali prasidėti ir nuo aukščiausio lygmens, t. y. įmonės vadovybės veiksmų. Dažnai smulkiojo verslo vadovai pasirenka naudoti vieną įrenginį (pvz., telefoną ar kompiuterį) tiek darbui, tiek asmeniniam naudojimui. Taip patogiau atlikti darbus, tačiau didėja tikimybė atsirasti papildomoms grėsmėms. Kibernetinio saugumo srityje tokia asmeninių prietaisų naudojimo darbui praktika vadinama BYOD (angl. *bring your own device*) – asmeninių įrenginių naudojimo politika.

Labai dažnai negalvojama apie tai, kokius asmeninius įrenginius įmonės vadovas, nuolatiniai ar laisvai samdomi darbuotojai naudoja darbo reikalams (ypač nuotolinio darbo atveju), neįvertinamos rizikos, kai prie jautrių sistemų ar duomenų jungiamasi iš namų, viešbučio ar tiesiog naudojantis viešuoju internetu.

Jūs negalite žinoti, ar darbuotojų asmeniniai kompiuteriai, išmanieji telefonai ir kiti elektroniniai prietaisai yra saugūs, dėl to itin padidėja informacijos saugumo rizika. Asmeniniai prietaisai gali būti naudojami lankantis nepatikimuose puslapiuose, prisijungiant prie nesaugaus belaidžio tinklo ar naudojant nesaugią arba nelegalią programinę įrangą, o tai didina riziką užkrėsti naudojamą prietaisą dėl atsirandančių kibernetinių saugumo spragų, kurias lengvai gali išnaudoti programišiai. **Jeigu asmeniniame įrenginyje yra saugomi, kaupiami įmonės jautrūs duomenys, atsiranda didesnė tikimybė juos sunaikinti ar nutekinti**.

Jeigu Jūsų įmonėje leidžiama įrenginius naudoti asmeniniams poreikiams arba leidžiama naudoti ne įmonei priklausančius įrenginius, **rekomenduojama nustatyti prisijungimo taisykles darbuotojams, naudojantiems savo prietaisus**. Jūs taip pat galite naudotis mobiliųjų įrenginių valdymo (angl. *mobile device management*) paslaugomis, kurios užtikrins verslo duomenų apsaugą asmeniniuose įrenginiuose nuo piktavališko ar netyčinio duomenų nutekinimo ar sunaikinimo.

### SIEKIANT APSAUGOTI ĮMONĖS JAUTRIUS DUOMENIS, REKOMENDUOJAMA:

- nenaudoti asmeninio el. pašto paskyros darbo tikslams, ypač tada, kai yra siunčiama ar naudojama jautri įmonės informacija ar asmens duomenys;
- riboti asmeninių įrenginių naudojimą vykdant su verslu susijusią veiklą (pvz., verslo el. bankininkystė);
- neleisti laikyti jautrią, su verslu susijusią informaciją asmeniniuose įrenginiuose (pvz., išmaniajame telefone ar USB atmintinėje) ar asmeninėse duomenų laikmenose internete (pvz., „Google Drive“, „Dropbox“ ar „OneDrive“);
- uždrausti prie įmonės kompiuterių prijungti nežinomas USB laikmenas ar kitus išorinius įrenginius. Prijungus USB įrenginius, kartais prireikia tik 30 sekundžių, kad programiškai nustatytų kompiuterio prisijungimo duomenis, net jei šis yra užrakintas. Kompiuteris gali būti užkrėstas kenkimo programine įranga, pvz., tokia, kuri šnipinės informaciją ir teiks ją konkurentams ar kitiems asmenims;
- įpareigoti darbuotoją užtikrinti įmonės kibernetinio saugumo politikos reikalavimų laikymąsi (pvz., programinės įrangos atnaujinimas laiku, antivirusinės programos įdiegimas, atminties šifravimas, slaptažodžių naudojimas ir pan.).

## Darbas nuotoliniu būdu

Šiandien mūsų darbo vieta nebūtinai yra pastovi – dirbame viešbučiuose, kavinėse, oro uostose ir kitur. Tad dažnai gali tekti jungtis prie ten esančio belaidžio tinklo. Deja, bet negalime matyti kam iš tiesų jis priklauso. Jei kyla abejonių dėl nepažįstamo tinklo saugumo, nesijunkite prie jo. Prisijungus prie nesaugaus tinklo, piktavaliai gali matyti Jūsų atliekamus darbus, prisijungimo informaciją ir pan. Geriausia išeitis – naudoti savo įrenginio mobilųjį internetą, kuriuo galite dalytis ir su kitu savo įrenginiu, pvz., kompiuteriu.

Be to, užsiėmę žmonės dažnai palieka savo įrenginius ant stalo, pameta ar nepastebi, kaip juos pavagia. Dėl to rekomenduojama, kad darbuotojų naudojamuose įrenginiuose būtų įjungtos funkcijos, leidžiančios nustatyti įrenginio buvimo vietą, nuotoliniu būdu jį užrakinti, ištrinti duomenis ar atkurti jame turėtą informaciją.

Jeigu Jums arba Jūsų darbuotojams tenka dirbti nuotoliniu būdu arba kartais naudotis nežinomu ir neapsaugotu belaidžiu tinklu, Jūs turėtumėte apsvarstyti galimybę pasinaudoti **virtualaus privataus tinklo (VPN) technologija**, kuri užtikrins saugesnio ryšio prieigą. Nenaudojant VPN, įvairiais būdais siunčiami duomenys (el. paštu, socialinių tinklų pranešimų būdu ir kt.) gali būti perimti kibernetinių nusikaltėlių, o prieiga prie įmonės tinklo sutrikdyta. Taip pažeidžiamas ne tik naudojamas įrenginys, bet ir kyla pavojus įmonės tinklui.

VPN leidžia sujungti visus nuotoliniu būdu dirbančius darbuotojus ar skirtingus įmonių padalinius į vieną saugų vidinį įmonės tinklą, kuriame jie galės saugiai dalytis vidine informacija ir naudotis bendromis verslo valdymo programomis, telefonijos paslaugomis. Tai Jums ne tik leis užtikrinti saugesnį darbą, bet ir padės Jūsų verslui veikti ir valdyti kritinę informaciją patogiau ir efektyviau.

Daugiau informacijos apie VPN ir kitus privataus naršymo būdus rasite puslapyje **https://www.esaugumas.lt/lt/e.-privatumas/privatusis-ir-anoniminis-narsymas-internete/280**.

Detalesnes saugaus nuotolinio darbo rekomendacijas rasite NKSC puslapyje **https://www.nksc.lt/doc/biuleteniai/2020-03-16_Nuotolinis_darbas.pdf**.

## 09 Ugniasienės

Siekiant stiprinti įmonės kibernetinį saugumą, labai svarbu gebėti kontroliuoti tai, kas patenka į Jūsų įmonės tinklą, ir tai, kas iš jo išeina. Ugniasienių (angl. *firewall*) paskirtis – analizuoti ir valdyti per jas keliaujantį duomenų srautą bei saugoti įmonės tinklo perimetrą nuo išorinių atakų internete. Taip jos tampa savotiška neutralia zona tarp įmonės tinklo ir interneto.

Neretai ugniasienės reikšmė kibernetinei saugai yra nuvertinama, ypač darbo vietose. Patikima ir tinkamai sukonfigūruota ugniasienė būtina visiems įrenginiams, naudojamiems už įmonės ribų, nes jungiantis prie viešo interneto tinklo užkertamas kelias pakliūti į Jūsų įrenginį. **Verslui, naudojančiam prie tinklo prijungtus kasos aparatus, tai yra būtina priemonė**.

Ugniasienės būna įvairių tipų ir formų. Dažniausiai jų tikslas yra blokuoti nepageidaujamą duomenų srautą ar prieigą prie nesaugių ar žalingo turinio puslapių. Kitos ugniasienės, skenuodamos įeinančius duomenis, atpažįsta atakas ir įsilaužimus pagal duomenų bazėje esančius aprašus. Jos taip pat yra naudojamos siekiant apsisaugoti nuo paslaugos trikdymo (*DDoS*) atakų.

Pažengę vartotojai gali nustatyti griežtas ugniasienės taisykles ir taikyti principą „draudžiama viskas, kas nėra leidžiama“ (angl. *whitelist*). Vadinamojo baltojo sąrašo sudarymas reiškia, kad Jūs tiesiogiai kontroliuojate, koks turinys, kokie duomenys ar kokių žmonių laiškai gali pasiekti Jūsų įmonės tinklą, – visas kitas interneto srautas blokuojamas. Tokia politika gali būti taikoma tiek konfigūruojant ugniasienes, tiek apibrėžiant naudojamos programinės įrangos sąrašus ar keičiant kitų apsaugos priemonių nustatymus (pvz., elektroninio pašto filtras).

Tokia priemonė suteiktų daugiau saugumo Jūsų įmonei, tačiau gali padidinti administracinę naštą ar apsunkinti paslaugų teikimą. Tad geresnis sprendimas Jūsų verslui gali būti vadinamojo juodojo sąrašo (angl. *blacklist*) sudarymas („leidžiama viskas, išskyrus, kas yra draudžiama“), kuris leidžia ugniasienei automatiškai blokuoti interneto srautą pagal sudarytą nepageidaujamų gavėjų ar domenų sąrašą. Tai ne taip saugu kaip baltojo sąrašo sudarymas, bet patogesnė ir lankstesnė priemonė kasdieniniam naudojimui.

Geroji praktika parodė, kad specializuota ugniasienė gali padėti ne tik apsisaugoti nuo išorinių grėsmių, bet ir lokalizuoti atakos židinį bei suvaldyti viruso plitimą užkertant nepageidaujamo duomenų srauto plitimą iš užkrėsto kompiuterio vidiniame įmonės tinkle. Šiuo atveju turi būti naudojamos ir vidinės ugniasienės. Taip pat turėtų būti segmentuotas vidinis tinklas ribojant prieigas iš vieno potinklio į kitą. Todėl **rekomenduojama visuose įmonės įrenginiuose įdiegti antivirusinę apsaugos programą su integruota ugniasiene**.

Ugniasienės taip pat gali būti įjungiamos konfigūruojant Jūsų įmonės naudojamus maršrutizatoriaus nustatymus arba įsigijus atskirą techninę įrangą. Siekiant rasti Jūsų įmonei tinkamiausią sprendimą, siūloma konsultuotis su įmonės interneto tiekėjais ir kitais IT techninės įrangos ekspertais.

# 10 Saugus belaidis tinklas

Vienas iš svarbiausių Jūsų įmonės tinklo saugumo elementų yra **užtikrinimas, kad belaidis tinklas yra saugus**. Šis procesas prasideda nuo maršrutizatoriaus (angl. *router*), nes šis prietaisas veikia kaip tiltas tarp Jūsų įmonės tinklo ir plačiojo interneto. Itin svarbu, kad įrenginys, suteikiantis belaidžio tinklo paslaugas, būtų apsaugotas.

- **Pakeiskite numatytąjį belaidžio tinklo maršrutizatoriaus slaptažodį**. Programišiai dažnai pasinaudoja vartotojų užmaršumu, nes jie žino dažniausiai naudojamus pradinius gamintojo nustatytus slaptažodžius. Kai kuriais atvejais maršrutizatoriaus nustatymai gali būti pasiekiami ir be slaptažodžio, jeigu vartotojas jo pats nenustato prieš pradėdamas naudoti belaidį tinklą.
- **Pakeiskite pradinį belaidžio tinklo pavadinimą (SSID)**. Gamyklinis tinklo pavadinimas įsilaužėliams gali sufleruoti, kad vartotojas nėra saugiai sukonfigūravęs savo belaidžio tinklo. Tokiu atveju Jūs galite tapti lengvu programišių taikiniu. Tinklo pavadinimas turėtų būti abstraktus ir neatspindėti jokių asmens ar įmonės duomenų, prieigos taško buvimo vietos ir negali turėti jokių užuominų į tai, koks galėtų būtų prisijungimo slaptažodis.
- Naudokite WPA2 belaidžio tinko protokolą arba, jeigu įrenginys palaiko, – WPA3.
- Rekomenduojama prieigai prie belaidžio tinklo naudoti EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolą, pagal kurį kiekvienas turės skirtingus prisijungimo duomenis prie belaidžio tinklo. Esant vienam slaptažodžiui, kuris skirtas visiems, jį gali tekti dažnai keisti, nes buvęs darbuotojas gali jį panaudoti ir neleistinai patekti į vidinį tinklą.
- Nuolat diekite maršrutizatoriaus programinės ir aparatinės įrangos atnaujinimus.
- Apribokite prieigą prie administravimo sąsajos (maršrutizatoriaus nustatymų puslapio) iš interneto ar belaidžio tinklo.

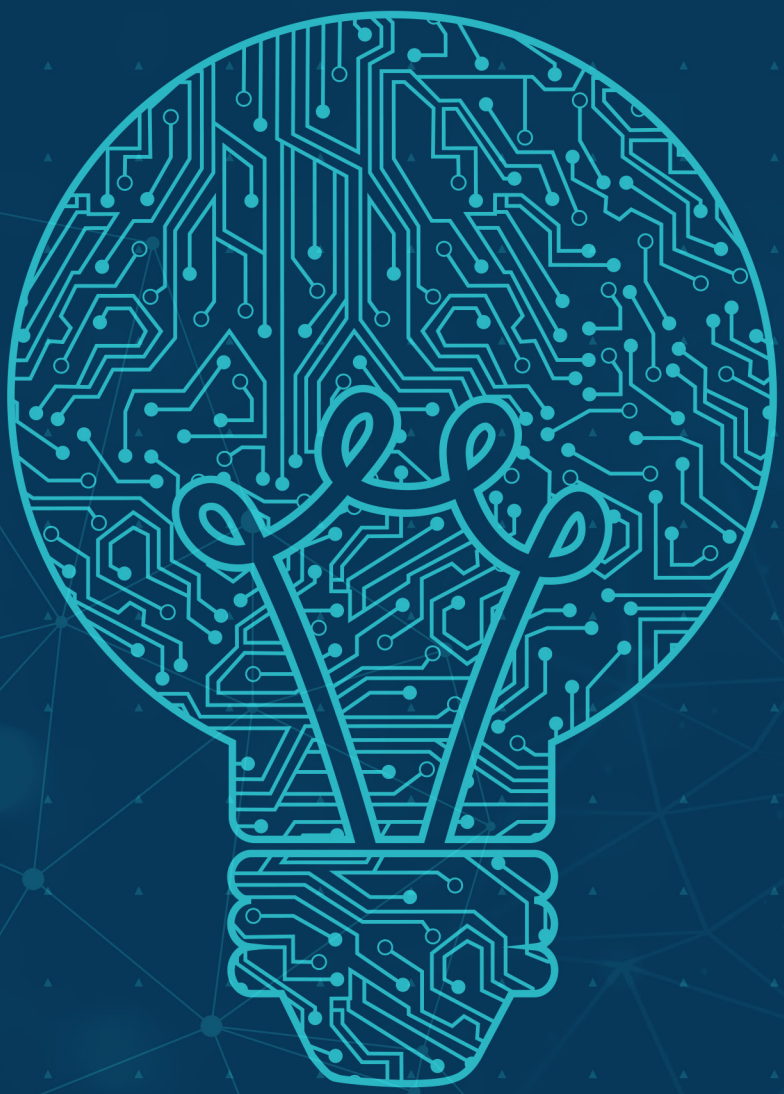
Jeigu savo darbovietėje norite suteikti interneto prieigą klientams ar svečiams, būtinai pasirūpinkite, kad prie šios tinklo prieigos nebūtų prijungti Jūsų įmonės įrenginiai. Viename tinkle realizuota belaidė prieiga leidžia piktavaliams vykdyti komunikacijų srauto šnipinėjimą, įsiterpti į komunikacijas ir taip perimti jautrią informaciją arba įgauti prieigą prie infrastruktūros ir vykdyti tolimesnę kenkėjišką veiklą. Savo svečiams sukūrę atskirą tinklą, kuris visiškai atskirtas nuo to, kuriuo naudojasi įmonės darbuotojai, Jūs išvengsite tokių incidentų rizikos. **Svečių tinklas** turėtų būti sukonfigūruotas taip, kad prisijungęs asmuo galėtų tik naršyti internete ir neturėtų galimybės prisijungti prie kitų įrenginių, susietų su įmonės tinklu.

Ypatingai **svarbu laikytis fizinio saugumo principų** – kaip ir kiti svarbiausi tinklo infrastruktūros įrenginiai, maršrutizatoriai turi būtų laikomi saugioje ir lengvai neprieinamoje vietoje. Tai turėtų būti tik atsakingiems asmenims prieinama vieta, kuri galėtų būtų rakinama. Tai gali būti tiek atskira patalpa, tiek tiesiog užrakinama spintelė, kurioje būtų galima laikyti šį įrenginį. Jeigu paliksite įrenginius lengvai prieinamoje vietoje, didėja rizika, kad tyčia arba netyčia bus pažeistas Jūsų įmonės tinklas.

- Prijungęs vietinio tinklo (angl. *ethernet*) laidą prie vieno iš maršrutizatoriaus prievadų, pašalinis asmuo gali pasiekti privačiai saugomą informaciją, duomenis ar net pakeisti maršrutizatoriaus nustatymus.
- Paspaudus atkūrimo (angl. *reset*) mygtuką ir atkūrus gamyklinius nustatymus, įmonės maršrutizatorius gali tapti prieinamas piktavaliams programišiams.

Daugiau informacijos apie saugų belaidį tinklą galite rasti puslapyje **https://www.esaugumas.lt/lt/belaidzio-tinklo-saugumas/kaip-apsaugoti-savo-belaidi-tinkla/318**.

07



# Kas toliau? Būdai didesniam įmonės saugumui užtikrinti

Jeigu įsisavinote pateiktas bazines kibernetinio saugumo praktikas, pats metas dar labiau sustiprinti savo įmonės atsparumą. Šie patarimai, kaip ir kitos vadove pateiktos rekomendacijos, negarantuoja visapusiškos Jūsų įmonės apsaugos, tačiau jie gali padėti gerokai padidinti Jūsų bendrą kibernetinio saugumo lygį ir sumažinti kibernetinių incidentų riziką. Dėl išsamesnės informacijos rekomenduojama konsultuotis su kibernetinio saugumo ekspertais, o dėl įvykusių kibernetinių incidentų – kreiptis į NKSC.

2019 m. Nacionalinės kibernetinio saugumo būklės ataskaitos duomenimis, net **37 proc. Lietuvoje (su .lt domenu) veikiančių interneto svetainių yra pažeidžiamos**. Daugiausia tokių pažeidžiamumų nustatyta „Wordpress“ ir „Joomla“ turinio valdymo sistemose (TVS).

## Interneto svetainių saugumas

Verslo naudojamos interneto svetainės dažnai nuvertinamos ir suvokiamos tik kaip prekybinis ar komunikacinis įmonės įrankis. Neretai įmonės puslapis gali turėti daug vertingo skaitmeninio turto, reikalingo įmonės veiklai, arba jame gali būti klientų ar darbuotojų duomenų, kurių apsauga reikia pasirūpinti.

Vienas pirmųjų žingsnių, stiprinančių svetainės saugumą ir reputaciją, **yra HTTPS protokolo įdiegimas**. Tai paslauga, leidžianti šifruoti puslapyje esančią informaciją ir užtikrinanti klientų asmens duomenų konfidencialumą. Tai reiškia, kad tik svetaine besinaudojantis klientas gali matyti dalijamą informaciją. **Įdiegus HTTPS protokolą, programišiams užkertamas kelias perimti klientų prisijungimo duomenis ar mokėjimų kortelės informaciją duomenų perdavimo metu**.

Siekiant užtikrinti visišką duomenų perdavimo saugumą, būtinas saugus ir patikimo tiekėjo išduotas SSL (angl. *Secure Sockets Layer*) kriptografinis protokolas. Šis įrankis leis užšifruoti informaciją, siunčiamą tarp svetainės lankytojo ir serverio, ir užtikrins, kad Jūsų įmonės svetainė bus pasiekiama HTTPS protokolu. Sertifikatas taip patvirtina svetainės tapatybę, nes, norėdamas įgyti sertifikatą, savininkas turi įrodyti teisę naudotis domenu, o kai kuriais atvejais patvirtinti įmonės rekvizitus.

**Pereiti prie HTTPS protokolo ypatingai svarbu įmonėms, teikiančioms internetinės prekybos paslaugas ir naudojančioms elektroninės bankininkystės sistemas**. Jeigu Jūsų svetainėje dar nėra įjungta ši funkcija, susisiekite su svetainės prieglobos (angl. *hosting*) paslaugą teikiančia įmone arba įjunkite šią funkciją per naudojamą turinio valdymo sistemą.

Jeigu įmonės puslapis yra sukurtas interneto svetainių kūrimo paslaugas teikiančios įmonės, nepamirškite pasikonsultuoti ir dėl svetainių nuolatinės priežiūros paslaugos.

### Taip pat nepamirškite:

- **atnaujinti** (ir įjungti automatinę atnaujinimo funkciją) **visus naudojamus įskiepius** (angl. *plugin*), turinio valdymo sistemą. Jų neatnaujinę, sukuriate galimybę programišiams pasinaudoti Jūsų svetainėje atsiradusiomis spragomis. Taip pat ištrinkite nebenaudojamus įskiepius;
- **paprašyti** domeno tiekėjo, **kad būtų užtikrinama automatinė domeno pratęsimo paslauga**. Nesusimokėjus domenas tampa laisvas ir taip atsiranda galimybė sukčiams jį nusipirkti ir perparduoti. Įsigiję domeną, jie gali klaidinti Jūsų klientus, nes sukuriama suklastota interneto svetainė, kurioje už netikrų prekių ar paslaugų slepiasi kenkimo kodas;

- **kurti atsargines svetainės kopijas**. Tai ypač naudinga prieš atnaujinant svetainę ar diegiant naujus įskiepius, nes įsivėlus klaidai galėsite nesunkiai atkurti ankstesnę svetainės versiją;
- **apriboti interneto svetainės administravimą** nuo išorinio tinklo arba Jums nežinomų IP adresų.

NKSC taip pat teikia nemokamą interneto svetainių tikrinimo paslaugą. Šis įrankis leidžia įvertinti, ar Jūsų įmonės turima interneto svetainė neturi pažeidimų ar / ir spragų. Atlikus patikrinimą, Jūsų įmonė gaus detalią ataskaitą su užfiksuotais pažeidimais ir patarimais, kaip būtų galima sustiprinti įmonės svetainės saugumą. Nemokamą įrankį rasite paspaudę šią nuorodą: **https://site-check.cert.lt/**.

Daugiau informacijos apie interneto svetainių apsaugą rasite NKSC puslapyje **https://www.nksc.lt/rekomendacijos/interneto_svetainiu_apsauga.html**.

## Turinio filtravimas

El. pašto filtrai yra dar viena puiki priemonė, leidžianti valdyti turinį ir informaciją, pasiekiančią Jūsų įmonės kompiuterius. Šis įrankis apsaugo el. pašto dėžutę nuo pavojingų laiškų, kuriuose yra nuorodų į kenkimo puslapius, ar priedų, kuriuos atidarius galite užkrėsti įmonės kompiuterį ir tinklą. El. pašto filtras taip pat neleis nepageidaujamiems laiškams ir kitoms „šiukšlėms“ (angl. *spam*) patekti į Jūsų el. pašto dėžutes.

Dauguma el. pašto arba svetainių prieglobos (angl. *hosting*) paslaugų tiekėjų siūlo šią paslaugą. Patikrinkite, ar Jūs jau aktyvavote šią funkciją. Jeigu ši paslauga dar neįjungta, būtinai susisiekite su tiekėju dėl šios paslaugos pasirinkimo. Jeigu Jūsų įmonė turi atskirą el. pašto serverį, nepamirškite pasitikrinti, ar įjungta ši funkcija.

Panašiu principu veikia ir interneto turinio filtravimo (angl. *web filter*) įrankiai. Ši priemonė blokuoja darbuotojų prieigą prie nelegalių, žalingo turinio ar apkrėstų svetainių. Tai leidžia užkirsti kelią neteisėtai veiklai, pvz., piratavimui ir netyčiniams pažeidimams, kai atsidarius puslapį į įmonės kompiuterį atsiunčiami užkrėsti failai.

Daugelis interneto naršyklių turi interneto filtravimo funkciją arba siūlo specialius papildinius (angl. *extensions*), kurie vartotojui praneša, kad interneto puslapis galimai yra užkrėstas. Patikrinkite, ar Jūs įjungėte šią funkciją. Dauguma ugniasienių ir maršrutizatorių taip pat gali blokuoti interneto puslapius, kuriuose aptinkamos saugumo spragos. Tai vadinama juoduoju sąrašu, kurį galima surasti internete arba gauti kartu su tiekiamomis interneto arba modernių antivirusinių paslaugomis.

Daugiau informacijos apie apsaugos priemones kovai su brukalu rasite NKSC puslapyje **https://www.nksc.lt/doc/biuleteniai/2019-06-26%20Malware%20platinimas%20LT%20imoniu%20vardu.pdf**.

„E. saugumas“ puslapyje taip pat patariama, kaip galima apsisaugoti nuo žalingos informacijos internete, ir pateikiamas rekomenduojamų turinio filtravimo priemonių sąrašas. Jį rasite čia: **https://esaugumas.lt/lt/turinio-filtravimo-programos/316**.

# Debesija: privalumai ir saugumo sumetimai

Įmonės ne tik visame pasaulyje, bet ir Lietuvoje vis daugiau savo informacijos patiki debesijos paslaugų teikėjams – perkelia savo informacines sistemas į debesų kompiuterijos infrastruktūrą (angl. *Infrastructure as a Service*, IaaS), talpina ir apdoroja verslo informaciją su debesijos paslaugomis gaunama programine įranga (angl. *Software as a Service, SaaS*) ar kuria savo sprendimus ir verslo aplikacijas debesijos paslaugų platformose (angl. *Platform as a Service, PaaS*). Šitaip įmonės išnaudoja debesų kompiuterijos teikiamas galimybes: taupo lėšas, užsitikrina patikimumą, didesnį IT resursų pajėgumą ir greitesnį prisitaikymą prie besikeičiančių verslo poreikių.

Tačiau įmonėms tampa vis sunkiau suprasti, kur laikoma jų verslo ir klientų informacija, kaip (ar) užtikrinamas jos saugumas, ar verslas tokiu atveju atitinka BDAR reikalavimus.

Todėl įmonėms būtina žinoti, kokias debesijos paslaugas jos naudoja, koks yra atsakomybės už saugą pasiskirstymas tarp įmonės ir debesijos paslaugų teikėjo, kokias IT saugos kompetencijas įmonė turi užtikrinti viduje iš arba savo partnerio, teikiančio debesijos paslaugų priežiūros paslaugas.

## Skirtingos debesijos paslaugų rūšys ir atsakomybių pasiskirstymas

Debesijos paslaugos yra įvairių rūšių, o įmonės, dažnai net nežinodamos, naudojasi bent keliomis įvairių rūšių debesijos paslaugomis. Svarbu suprasti, kokios yra debesijos paslaugų rūšys ir kokio saugumo atsakomybės pasiskirstymo tarp įmonės ir debesijos paslaugų teikėjo turėtų tikėtis įmonė.

Toliau lentelėje pagal kiekvieną iš debesijos paslaugų rūšių pateikiamas tipinis atsakomybių už saugumo užtikrinimą ir saugų įmonės informacijos tvarkymą pasiskirstymas tarp debesijos paslaugų teikėjo ir įmonės.

| ATSAKOMYBĖ | Kai teikiama IaaS rūšies paslauga | Kai teikiama PaaS rūšies paslauga | Kai teikiama SaaS rūšies paslauga |
|---|---|---|---|
| Įmonės darbuotojų **prieigos** prie debesijos paslaugų ir jų saugomos, apdorojamos bei perduodamos informacijos **valdymas** | Įmonė | Įmonė | Įmonė |
| Saugus įmonės darbuotojų atliekamas **informacijos tvarkymas**, naudojant su paslauga gautą taikomąją ir / arba sisteminę programinę įrangą | Įmonė | Įmonė | Įmonė |
| Įmonės **informacijos**, apdorojamos naudojant su paslauga gautą taikomąją ir/ arba sisteminę programinę įrangą, **prieinamumo** ir **vientisumo** užtikrinimas, įskaitant rezervinį kopijavimą ir atkūrimą įvykus incidentui | Įmonė | Įmonė | Paslaugų teikėjas |
| Įmonei naudotis patikimos **taikomosios programinės įrangos** ir joje įgyvendintų procesų, skirtų kliento duomenims apdoroti, saugumas, prieinamumas, rezervinis kopijavimas ir veiklos atkūrimas įvykus incidentui | Įmonė | Įmonė | Paslaugų teikėjas |
| Įmonės aplikacijoms veikti, duomenims saugoti ir perduoti naudojamos **platforminės ir sisteminės programinės įrangos saugumas**, prieinamumas, rezervinis kopijavimas ir veiklos atkūrimas įvykus incidentui | Įmonė | Paslaugų teikėjas | Paslaugų teikėjas |
| Duomenų centro ir **visos kitos fizinės IT infrastruktūros** saugumas, prieinamumas, rezervinis kopijavimas ir veiklos atkūrimas įvykus incidentui | Paslaugų teikėjas | Paslaugų teikėjas | Paslaugų teikėjas |

## Saugumas debesyje prieš debesies saugumą

Patikimi debesijos paslaugų teikėjai privalo pasirūpinti paslaugų teikimo priemonių saugumu ir patikimumu. Dažniausiai įmonės patikimo debesijos paslaugų teikėjo sutartyse ras jo įsipareigojimus užtikrinti kliento informacijos saugumą, konfidencialumą ir patikimumą. Taip pat sutartyse dažniausiai nurodomos debesijos paslaugų teikėjo garantijos ir veiklos draudimo įsipareigojimai. Dėl visų šių išvardytų priežasčių galima teigti, jog patikimo tiekėjo valdomas debesis yra saugus. Tačiau ar debesyje yra saugi pati įmonė?

Populiarųjį ledkalnio viršūnės palyginimą galima pritaikyti ir šiuo atveju, t. y. paties debesies saugumas, kuris dažniausiai akcentuojamas, yra tik labiausiai ir aiškiausiai matoma ledkalnio dalis. Pačių debesijos paslaugų naudotojų saugumas debesyje ir rūpinimasis juo niekur nedingsta ir, net pasirinkus patį patikimiausią tarptautinį debesijos paslaugų teikėją, išlieka pačios įmonės atsakomybė.

Norėdamos užtikrinti savo informacijos saugumą, vientisumą ir konfidencialumą, įmonės turi investuoti į kompetentingus, kvalifikuotus ir debesijos paslaugų saugumo valdymą išmanančius darbuotojus arba pasitelkti patikimus debesijos paslaugų valdymo partnerius. Be to, įmonės turi nepamiršti, kad debesų kompiuterijos technologija šiuo metu yra labiausiai kintanti IT sritis, todėl reikėtų turėti kompetentingų darbuotojų. Būtina užtikrinti jų nuolatinį tobulėjimą, kvalifikacijos kėlimą ir nuolatinį domėjimąsi debesijos paslaugų pokyčiais.

# Jautrių duomenų šifravimas

Viena iš techninių priemonių, užtikrinančių, kad piktavaliai nepasiektų Jūsų įmonės jautrios informacijos, yra šifravimas. Tai informacijos kodavimas, kuris leidžia apsaugoti Jūsų dokumentus, kad pašaliniai asmenys negalėtų jų perskaityti, pasisavinti ar sugadinti. **Šifravimas – ne tik svarbus duomenų apsaugos elementas, bet ir privaloma techninė priemonė pagal BDAR**.

### Šifravimo priemonės gali būti įgyvendinamos keliais lygiais:

- **Kompiuterio kietojo disko (arba nešiojamos laikmenos) šifravimas**. Tai leidžia apsaugoti įmonės duomenis nuo nutekėjimo tais atvejais, kai kompiuteris ar kietasis diskas yra fiziškai prarandamas, pasisavinamas arba sugadinimas. Šį įrankį nemokamai siūlo dauguma operacinių sistemų[13].
- **Duomenų srautų šifravimas**. Jeigu Jūsų verslas dažnai dalijasi jautria įmonės ar klientų informacija, Jums turėtų būti svarbu, kad ši informacija pasiektų tik tam skirtą gavėją. Duomenų srauto šifravimas veikia taip: Jūsų siunčiama informacija, pridėti failai yra užrakinami ir užšifruojami, juos gali pasiekti tik konkretūs asmenys, kurie turi jų tapatybę patvirtinantį ir prieigą prie užšifruotos informacijos suteikiantį privatų raktą (angl. *private key*).
- **Pavienių dokumentų šifravimas**. Tai priemonė, užtikrinanti, kad svarbūs Jūsų įmonės dokumentai nebus pasiekiami ar modifikuojami pašalinių asmenų.

***Primename: nepamirškite šifravimo slaptažodžio ar rakto! Pametę ar pamiršę raktą, galite galutinai prarasti svarbią Jūsų įmonės ar klientų informaciją. Išsaugokite šifravimo slaptažodžio arba rakto kopiją saugioje vietoje arba ten, kur laikote svarbiausių dokumentų atsargines kopijas.***

Užpuolikai paprastai nesistengia atgaminti užšifravimo algoritmo veikimo. Vietoj to jie ieško šifravimo programinės įrangos pažeidžiamumų arba bando užkrėsti sistemą kenkimo programomis, kad galėtų užfiksuoti slaptažodžius arba šifravimo raktus, kai jie yra apdorojami. Siekiant sumažinti šią riziką, versle svarbu naudoti nepriklausomai patvirtintą šifravimo produktą ir įdiegti pažangią, naujausią kenkimo programų aptikimo priemonę.

[13] Instrukcijas „Windows“ kompiuterių naudotojams rasite čia: **https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption**.

Instrukcijas „Mac“ kompiuterių naudotojams rasite čia: **https://support.apple.com/en-us/HT204837**.

Jeigu didžiąją dalį įmonės duomenų saugote išorinio IT paslaugų tiekėjo duomenų centre, įsitikinkite, kad jie taip pat taiko aukščiausius šifravimo standartus. Užtikrinkite, kad įmonės ir Jūsų klientų asmens duomenys yra pasiekiami tik šios informacijos savininkams, t. y. Jūsų įmonės atitinkamiems darbuotojams arba tiems, kam esate patikėję priėjimą prie šios informacijos.

Daugiau informacijos apie šifravimo principus ir priemones siunčiant el. laiškus rasite puslapyje **https://www.esaugumas.lt/lt/e.-privatumas/sifravimas/277**.

## Duomenų nutekėjimo prevencija

Kiekvienam verslui yra svarbu apsisaugoti nuo duomenų nutekėjimo. Jį sukelti gali ir įmonės darbuotojai tyčiniu ar neatsargiu elgesiu – atsisiųsdami kenksmingas programas ar prijungdami neautorizuotus įrenginius. Tik tinkama programinė įranga padeda saugoti visus duomenų nutekėjimo kanalus (įskaitant ir prarastus įrenginius, nes duomenys juose yra užšifruojami).

Duomenų nutekėjimo prevencijos (angl. *data loss prevention*, DLP) programos identifikuoja įtartiną veiklą, atliekamą su įmonės dokumentais, ar informaciją įmonės naudojamuose įrenginiuose, apsaugo svarbius failus nuo patekimo į netinkamas rankas, perspėdama vadovybę apie potencialią grėsmę dar prieš patiriant rimtus nuostolius arba užkardydama draudžiamus veiksmus. Tokia įranga neleidžia darbuotojams pasiimti svarbios informacijos net naudojant savo asmeninius įrenginius, skirtus darbo funkcijoms atlikti.

Pažangesnė programinė įranga gali kontroliuoti spausdintuvų, programų naudojimą ir apriboti daug laiko atimančias veiklas (lankomų svetainių, veiklos darbo ekrane, mygtukų paspaudimų fiksavimas ar el. laiškų tikrinimas). Taip sukuriama galimybė gauti informaciją apie darbuotojus, kurie dirba su jautriais duomenimis. Programa įvertina saugumo incidentų riziką ir įspėja apie įtartiną darbuotojų veiklą. Duomenų nutekėjimo programos dar pačioje pradžioje gali aptikti socialine inžinerija pagrįstas atakas, nustatyti bandymą šantažuoti ir taip apsaugoti nuo pakenkimo įmonei.

## Saugus senų įrenginių nurašymas

Labai svarbi kibernetinės saugos dalis, apie kurią dažniausiai nėra pagalvojama, – nebenaudojamos įrangos tinkamas sutvarkymas. Mažiau patyręs kompiuterių ar išmaniųjų įrenginių naudotojas mano, kad paspaudus mygtuką „panaikinti“ (angl. *delete*) duomenų failai yra ištrinami. Pirmiausia jie patenka į vadinamąją šiukšliadėžę (angl. *recycle bin*), iš kurios gana nesudėtingai galima atkurti ištrintus failus. Net ir ištrynus juos iš šiukšliadėžės, failai vis tiek yra saugomi įrenginio kietajame diske ar atminties laikmenoje.

**Kiekvienas nenaudojamas įrenginys**: išorinis kietasis diskas, išmanusis telefonas, nešiojamas ar stacionarus kompiuteris, **turi būti tinkamai išvalytas prieš jį sunaikinant, atiduodant perdirbti ar parduodant antrinėje rinkoje**. Todėl įmonėje turi būti nustatyta, kokie veiksmai atliekami su neeksploatuojama įranga ir kas yra atsakingas už jos tinkamą parengimą atidavimui ar pakartotiniam naudojimui.

Būtina atkreipti dėmesį ne tik į tinkamą įrangos apskaitą, bet ir į tai, kad visuose įrenginiuose yra saugoma įmonės informacija. Todėl, nurašant nenaudojamą įrangą, turi būti įvertintas informacijos iš įrenginio pašalinimo aspektas – kokiomis priemonėmis bus sunaikinta informacija, esanti įrenginiuose, kad ja nebūtų galima pasinaudoti.

**Saugiausias būdas – fizinis įrenginio sunaikinimas** kartu su jame esančia informacija. Specializuotos perdirbimo įmonės teikia specialias kietųjų diskų smulkinimo paslaugas. Toks sprendimo būdas ypač aktualus įmonėms, naudojančioms daug jautrių duomenų ir atsakingai vertinančioms savo

skaitmeninio turto saugumą. Kitas būdas – išimti kietąjį diską iš jau nebenaudojamo kompiuterio ir jį archyvuoti.

Tačiau diskų archyvavimas ar daužymas ne visada yra geriausias pasirinkimas. Daug **racionaliau sunaikinti kietojo disko duomenis programiškai, o įrenginį sėkmingai naudoti toliau** asmeniniais tikslais ar atiduoti perdirbti, parduoti antrinėje rinkoje, nes tai ekonomiškai ir ekologiškai naudingiau ir atsakingiau. Sunaikinti kietojo disko duomenis galite naudodamiesi disko valymo (angl. *disk wiping*) ar gamyklinių nustatymų atkūrimo (angl. *factory reset*) funkcijomis arba įsigiję atskirą programinę įrangą, kuri negrįžtamai sunaikina visus duomenis skaitmeniniuose įrenginiuose.

## Daiktų internetas

Daiktų internetas (angl. *Internet of Things*) apima visus įrenginius, kurie yra prijungti prie interneto ir tarpusavyje dalijasi informacija. Vis daugiau tokių išmaniųjų prietaisų (pvz.: mokėjimo kortelių skaitytuvai, išmaniosios spynos, temperatūros kontrolės sistema ir kt.) tampa naudingi ir versle. Tokius prietaisus dažniausiai galime valdyti ir stebėti nuotoliniu būdu. Jie buvo sukurti mums padėti susitvarkyti su kasdienėmis užduotimis, tačiau jiems atsiradus kyla ir papildomos rizikos.

Jūsų darbovietėje naudojamas išmanusis įrenginys yra dar vienas galimas tiltas į Jūsų įmonės tinklą. Pastaraisiais metais fiksuojamas sparčiai didėjantis kibernetinių atakų skaičius prieš išmaniuosius įrenginius. Programišiai stengiasi išnaudoti esančius pažeidžiamumus ir spragas siekdami išgauti naudos arba panaudoja įrenginius kitoms atakoms.

Tai tik įrodo, kad techninių kibernetinio saugumo priemonių nepakanka. **Labai svarbu tinkamai apsibrėžti ir valdyti įmonės organizacinius procesus**. Daiktų interneto naudojimas versle gali padėti Jums pagreitinti tam tikrus procesus, deja, bet tai padidina ir Jūsų pažeidžiamumo riziką, todėl svarbu vadovautis tais pačiais kibernetinio saugumo principais. Naudojant tokius prietaisus versle, reiktų atsižvelgti į šiuos aspektus:

### Prieš pradėdami naudoti:

- pasidomėkite prekės saugumo kokybe. Prieš pirkdami prietaisą, būtinai įvertinkite prekės saugumo kokybę. Jums gali padėti kitų naudotojų atsiliepimai, ekspertų rekomendacijos. Prietaisus pirkite tik iš patikimų tiekėjų;
- žinokite, kur ir kaip, kilus nesklandumams, galėsite kreiptis į prietaiso gamintojus;
- susipažinkite su prietaiso instrukcija;
- įvertinkite prietaisų suderinamumą su Jūsų įmonėje apibrėžtomis kibernetinio saugumo taisyklėmis.

### Naudodami:

- pakeiskite prietaisų automatiškai nustatytus prisijungimo vardus ir slaptažodžius;
- nepamirškite atnaujinti įrangos programinę dalį;
- tinklus su jautria informacija laikykite izoliuotus nuo šių prietaisų. Pagalvokite apie galimybę sukurti atskirą tinklą tokiems prietaisams;
- įsitikinkite, kad įrenginys turi sistemos atkūrimo funkciją;
- kontroliuokite, kas ir kaip gali šiais prietaisais naudotis;
- nepamirškite į rizikos vertinimą (ar įsilaužimo testavimus) įtraukti visų prie įmonės tinklų prijungtų išmaniųjų įrenginių.

**Vienas labiausiai nuskambėjusių atvejų pasaulyje įvyko JAV, kai buvo pavogti kazino klientų duomenys įsilaužus į viduje esančio akvariumo išmanųjį termometrą**. Nepaisant to, kad įmonė turėjo įdiegusi ne vieną techninę kibernetinio saugumo priemonę, dėl vieno nesaugaus įrenginio programišiai sugebėjo gauti prieigą prie įmonės tinklo, surasti svarbių klientų duomenis ir per termometrą atsisiųsti juos į savo debesų laikmenas. Tai rodo, kad rizikų vertinimas buvo atliktas netinkamai – minėto įrenginio saugumas buvo tiesiog pamirštas.

Kitas gerai žinomas atvejis, kai programišiai įsilaužė į **daugiau nei 100 tūkstančių įvairių išmaniųjų įrenginių**, panaudodami jų nepakeistus gamyklinius prisijungimo duomenis. Vėliau jie buvo įtraukti į kompiuterių zombių tinklą (angl. botnet), kuriuo naudojantis buvo įvykdyta paslaugos trikdymo ataka (DDoS). Ši ataka laikinai sutrikdė „Twitter“, „Paypal“ ir „Netflix“ platformų sistemų veiklą.

Daugiau informacijos apie išmaniųjų prietaisų saugumo sumetimus ir atsakingą naudojimą versle rasite šiame Kanados nacionalinio kibernetinio saugumo centro puslapyje: **https://www.cyber.gc.ca/en/guidance/internet-things-security-small-and-medium-organizations-itsap00012**.

## Kibernetinių rizikų draudimas

Kibernetinių rizikų draudimas, kaip ir bet kokia kita draudimo paslauga, leidžia įmonėms sumažinti kibernetinio incidento žalos įtaką įmonei, apdrausti įmonės ir klientų skaitmeninį turtą ir padėti įmonei tęsti veiklą įvykus pažeidimui. Kibernetinių rizikų draudimas nepadės geriau apsaugoti Jūsų įmonės, tačiau šios paslaugos įsigijimas gali būti traktuojamas kaip tam tikras rizikos perkėlimas trečiosioms šalims. Tai gali būti ypač patraukli priemonė toms įmonėms, kurios turi ribotas galimybes investuoti į techninius kibernetinio saugumo sprendimus.

Kai kuriais atvejais draudimo įmonės siūlo ir kibernetinio saugumo ekspertų paslaugą. Jie gali padėti Jums nustatyti pažeidžiamas vietas įmonėje, identifikuoti, kokiais veiksmais galima sustiprinti įmonės IT infrastruktūrą, padėti ištirti kibernetinį incidentą ir pranešti apie tai atitinkamoms institucijoms (jų sąrašą rasite vadovo priede).

Augant kibernetinių įvykių skaičiui, kibernetinių rizikų draudimas tapo vienu sparčiausiai augančių sektorių pasaulinėje draudimo rinkoje. Lietuvoje ši praktika taip pat populiarėja. Tačiau, **kaip ir renkantis bet kokį kitą draudimą, labai svarbu išnagrinėti teikiamo poliso sąlygas ir Jūsų įmonės rizikas**.

Svarbu pabrėžti, kad ne visi kibernetinių rizikų draudimo polisai draudžia atvejus, kai kibernetiniai pažeidimai įvyksta dėl žmogaus klaidos ar neapdairumo. Taip pat, prieš suteikdamos paslaugą, draudimo kompanijos įsitikina, ar tikrai ėmėtės visų būtinų procesinių ir techninių priemonių incidento rizikai sumažinti. Dažnai toks auditas padeda nustatyti įmonės saugumo lygį ir išsiaiškinti tai, kaip jos supranta galimas grėsmes. Sudarydami draudimo sutartį, visada įsigilinkite į sutarties taisykles ir sąlygas, kad atsitikus nelaimei nesijaustumėte apgauti, jei įvykis nebus pripažintas draudiminiu.

## Įsilaužimų testavimas

Vienas efektyvių būdų įvertinti Jūsų įmonės kibernetinio saugumo pasiruošimo lygį yra įsilaužimo testavimas (angl. *penetration testing*). Tai yra įvairių IT saugumą užtikrinančių paslaugų tiekėjų ir kibernetinio saugumo įmonių siūloma paslauga, kai simuliuojama kibernetinė ataka prieš Jūsų įmonę siekiant išsiaiškinti, ar egzistuoja tinklo, IT infrastruktūros ar kitų įrenginių bei aplikacijų spragos, kurios leistų tikriems programišiams įsibrauti į Jūsų tinklą ir informacinę sistemą.

Kibernetiniai nusikaltėliai atakoms vykdyti naudoja naujausias žinias ir technologijas, todėl esamo kibernetinio saugumo pasiruošimo gali nebeužtekti baziniam saugumui užtikrinti. Tokiu atveju rekomenduojama turėti profesionalius konsultantus, kurie galėtų išanalizuoti ir parodyti Jums esamas spragas, kol dar niekas piktybiškai neįsilaužė į Jūsų tinklą.

Atlikusios testavimą, paslaugą teikiančios įmonės pateiks Jums detalią ataskaitą ir konkrečius pasiūlymus, kaip būtų galima spręsti iškilusias problemas. Internete galima rasti ne vieną nemokamą įrankį, leidžiantį atlikti įvairius pažeidžiamumų vertinimus, tačiau jie dažnai nėra tokie visapusiški ir neatskleidžia realios situacijos, o ir rezultatus ne visada lengva suprasti ir interpretuoti. Tačiau tai gali būti vienas iš rizikų vertinimo žingsnių prieš pasinaudojant profesionalia testavimo paslauga.

Dažnai atliekant įsilaužimo testus ieškoma ne tik technologinių spragų, bet ir tikrinamas darbuotojų budrumas. Kontroliuojamos atakos metu naudojami socialinės inžinerijos metodai, kai, pasinaudojus įmonės darbuotojų aplaidumu, bandoma gauti prieigą prie įmonės kompiuterių ir tinklo. Darbuotojų patiklumą galima tikrinti ir atskirais el. sukčiavimo testais, kai įmonės vadovui sutikus darbuotojams yra išsiunčiamos klaidinančių laiškų simuliacijos.

**Reguliariai atliekant testavimus, įmonės saugumo sistemos bus nuolat atnaujinamos, o sistemų administratoriai nepraras budrumo ir galės mokytis, kaip tinkamai reaguoti į tikrus išpuolius.**

## Saugumo įvykių valdymas

Vienas būdų stebėti, rinkti informaciją apie tai, kas vyksta Jūsų įmonės informaciniuose ištekliuose, ir informuoti apie galimus arba įvykusius pažeidimus yra aktyvus saugumo įvykių valdymas (angl. *SIEM*). Jeigu pastebėjote, kad dažnai bandoma prisijungti prie Jūsų svarbiausių paskyrų arba bandoma prisijungti iš neįprastų vietų (ar neįprasto IP adreso), didelė tikimybė, kad programišiai bando įsilaužti į Jūsų tinklą.

Dauguma internetinių platformų (pvz., „Facebook“ ar „Wordpress“), antivirusinių programų ir ugniasienių gali fiksuoti ir saugoti informaciją apie tokius įvykius. Ši funkcija yra vadinama **žurnalinių įvykių (angl. *logs*) kaupimu**. Įsitikinkite, kad ši funkcija yra įjungta ir, jei yra galimybė, įjunkite pranešimų apie bandymus prisijungti prie el. pašto funkciją. IT saugos užtikrinimo paslaugas ir sprendimus tiekiančios įmonės taip pat siūlo galimybę įsidiegti centralizuotas informacijos kaupimo sistemas, leidžiančias fiksuoti ne tik prisijungimus, bet ir duomenis apie atakas, užkratus, prieigą prie kritinių sistemų ir pan.

### Galimybė rinkti, kaupti ir archyvuoti žurnalinius įvykius turėtų būti bent tada, kai:

- naudojamos biuro programų platformos (pvz., „Office 365“, „GSuite“);
- prisijungiama prie Jūsų turinio valdymo sistemų ir daromi ten esančių failų pakeitimai;
- keičiami žurnaliniai įvykiai;
- keičiami slaptažodžiai;
- atmetami dviejų žingsnių autentifikavimo (2FA) prašymai;
- įjungti antivirusinių programų pranešimai;

- naudojamos informacinės sistemos, kuriose atliekami asmens duomenų tvarkymo veiksmai;
- keičiamos naudotojų teisės;
- atliekami bet kokie IT administratorių administravimo veiksmai;
- naudojamos tinklo jungtys, įeinančios ir išeinančios iš Jūsų tinklo.

**Šiuos duomenis rekomenduojama saugoti bent šešis mėnesius ir laikyti saugioje vietoje**. Pastebėjus neįprastas tendencijas ar užfiksavus įtartinas veiklas, patartina kreiptis į savo IT įrangos tiekėjus ar kibernetinio saugumo ekspertus. Žurnaluose esanti informacija leidžia geriau suprasti tikrąją įsilaužimo kryptį ar pasekmes. Tai taip pat parodys užslėptas rimtesnes problemas arba informuos apie tai, kad Jūsų įmonei reikia imtis rimtesnių saugumo užtikrinimo priemonių.

# Priedai

## SVV įmonių kibernetinio saugumo sąmoningumo apklausa

**129**

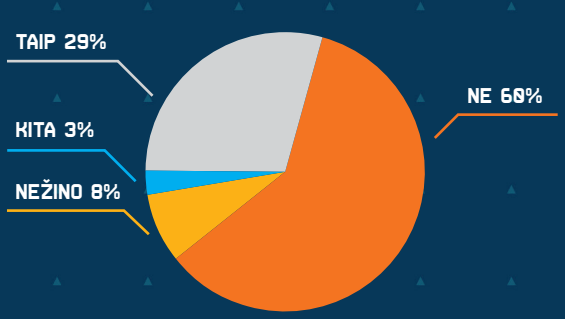
### SVV ĮMONIŲ VADOVAI

dalyvavo apklausoje apie jų įmonės kibernetinio saugumo pažeidžiamumą, sąmoningumą ir jo ugdymą.

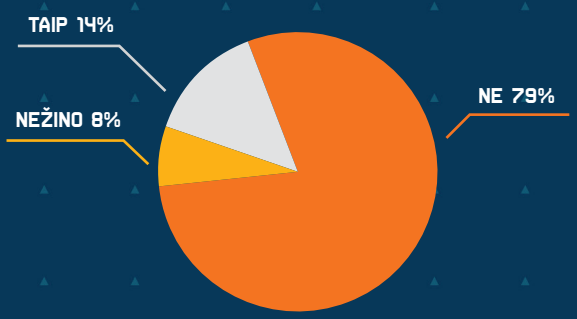
### ĮMONĖS DYDIS

apklausoje dalyvavo 41% labai smulkaus (iki 10 darbuotojų), 40% smulkaus (iki 50 darbuotojų) ir 19 % vidutinio dydžio įmonių (iki 250 darbuotojų).

### AR JŪSŲ ĮMONĖ TURI FORMALIAI APIBRĖŽTĄ IR REGULIARIAI ATNAUJINAMĄ KIBERNETINIO SAUGUMO POLITIKĄ?




### AR PER PASTARUOSIUS 12 MĖN. JŪS VYKDĖTE ĮMONĖS KIBERNETINIO SAUGUMO RIZIKOS VERTINIMĄ?




### 72% ĮMONIŲ TEIGĖ, KAD NEŽINO ARBA NĖRA TIKROS AR ŽINO KAIP ĮSIVERTINTI KIBERNETINIO SAUGUMO RIZIKAS IR SPRAGAS

**74%**

YRA NEPASIRUOŠUSIOS ARBA NEŽINO AR YRA PASIRUOŠUSIOS ATREMTI KIBERNETINES ATAKAS

**44%**

ĮMONIŲ NEMANO ARBA NEŽINO, KAD GALI BŪTI KIBERNETINIO INCIDENTO AUKOMIS

**58%**

ĮMONIŲ SUTINKA, KAD KIBERNETINIS INCIDENTAS TURĖTŲ DAUG ĮTAKOS JŲ ĮMONEI

### KIBERNETINIO SAUGUMO POLITIKĄ TURINČIOS ĮMONĖS (43%) JAUČIASI LABIAU PASIRUOŠUSIOS ATREMTI KIBERNETINES ATAKAS NEI TOS, KURIOS JOS NETURI (18%)

### DAUGIAU NEI PUSĖ

kibernetinių incidentų patyrusių įmonių vadovų teigė nežinantys, kokios yra šių incidentų pasekmės ir jų padaryta žala

### 74% ĮMONIŲ

teigė, kad neturi arba nežino, ar turi pakankamai žinių, kokias kibernetinio saugumo priemones būtina pasirinkti

### 40% ĮMONIŲ

per praėjusius metus neinvestavo nė vieno euro į įmonės kibernetinį saugumą

### 76% ĮMONIŲ

svarbu, kad verslo partneriai laikytųsi kibernetinio saugumo standartų

Programos „Kurk Lietuvai“ projekto Krašto apsaugos ministerijoje SVV įmonių kibernetinio saugumo sąmoningumo apklausos duomenys:
http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

# Kam pranešti apie įvykusį kibernetinį incidentą?

## Nacionalinis kibernetinio saugumo centras

Pranešti apie patirtas atakas, galimas grėsmes:

- užpildant specialią formą https://www.nksc.lt/pranesti.html
- rašant laišką el. p. cert@nksc.lt
- skambinant tel. 1805

## Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo 5-oji valdyba

Pranešti, jei kibernetinis incidentas gali turėti nusikalstamos veikos požymių:

- https://www.epolicija.lt/
- rašant laišką el. p. cyberpolice@policija.lt
- skambinant tel. 112

## Valstybinė duomenų apsaugos inspekcija

Pranešti, jei kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais:

- https://vdai.lrv.lt/
- rašant laišką el. p. ada@ada.lt
- skambinant tel. +370 5 271 2804

# Informaciniai šaltiniai (anglų kalba)

- Airija – *12 Steps to Cyber Security*, **https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf**
- Australija – *Cyber Security: the Small Business Best Practice Guide*, **https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-research-report.pdf**
- Belgija – *Cyber Security Guide for SMEs*, **https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf**
- Belgija – komunikacinių priemonių rinkinys, skirtas SVV įmonių ir kitų organizacijų vadovams didinti KS sąmoningumą įmonės ar organizacijos viduje, **https://www.cybersecuritycoalition.be/resource/cyber-security-kit/**
- *Center for Internet Security (CIS)* – pagrindinių kibernetinio saugumo kontrolės priemonių įgyvendinimo gairės smulkiam ir vidutiniam verslui, **https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf**
- *Global Cyber Alliance* – nemokamų kibernetinių saugumo priemonių rinkinys smulkiam ir vidutiniam verslui, **https://gcatoolkit.org/smallbusiness/**
- Jungtinė Karalystė – *Cyber Security: Small Business Guide*, **https://www.ncsc.gov.uk/files/cyber_security_small_business_guide_1.3..pdf**
- Jungtinės Amerikos Valstijos – *Small Business Cybersecurity Corner* – interneto svetainė su įvairiomis gerosiomis kibernetinio saugumo praktikomis smulkiajam verslui, **https://www.nist.gov/itl/smallbusinesscyber**
- Jungtinės Amerikos Valstijos – *Small Business Information Security: the Fundamentals*, **https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf**
- Jungtinės Amerikos Valstijos – *Small Biz Cyber Planner* – interaktyvus įrankis, leidžiantis įmonėms susikurti individualų įmonės kibernetinio saugumo politikos dokumentą, **https://www.fcc.gov/cyberplanner**
- Kanada – *Get Cyber Safe Guide for Small and Medium Businesses*, **https://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/smll-bsnss-gd-eng.pdf**
- Vokietija – nemokami klausimynai, kurių tikslas padėti SVV įmonėms įvertinti savo kibernetinio saugumo pasirengimo lygį ir pateikti rekomendacijas tolesniam saugumo stiprinimui, **https://www.vds-quick-check.de/en/**

## Išlyga

Informacija, pateikta šiame dokumente, yra rekomendacinio pobūdžio. Informacijos platintojas neprisiima jokios atsakomybės, susijusios su jos naudojimu. Pateikta informacija nėra laikoma baigtine ir nesuteikia saugumo garantijos. Naudotojai turi savarankiškai nuspręsti, ar pateikta informacija yra tinkama siekiant užtikrinti įmonės kibernetinį saugumą. Naudotojai dėl šių ir papildomų kibernetinio saugumo rekomendacijų įgyvendinimo turėtų konsultuotis su IT ir kibernetinio saugumo ekspertais.

## Apie „Kurk Lietuvai“

Šį dokumentą inicijavo „Kurk Lietuvai“ programos dalyviai Rūta Beinoriūtė, Gabrielė Bilevičiūtė ir Justas Kidykas projekto „Smulkiojo ir vidutinio verslo įmonių kibernetinio saugumo sąmoningumo didinimas“ Krašto apsaugos ministerijoje metu. Programa „Kurk Lietuvai“ – pirmoji ir kol kas vienintelė profesinio tobulinimo ir gerosios užsienio praktikos pritaikymo programa Lietuvos viešajame sektoriuje, kuri nuo 2012 m. suteikia galimybę tarptautinės patirties turintiems profesionalams savo žiniomis ir idėjomis prisidėti prie strateginių Vyriausybės projektų ir modernios Lietuvos ateities kūrimo.

Kurk Lietuvai

# KIBERNETINIS SAUGUMAS IR VERSLAS

## KĄ TURĖTŲ ŽINOTI KIEKVIENAS ĮMONĖS VADOVAS

Redaktoriai: Rūta Beinoriūtė, Gabrielė Bilevičiūtė, Justas Kidykas
Kalbos redaktorės: Rasa Sirvydienė, Reda Šauklė
Dizaineris Andrej Garbar
Grafiniai elementai naudoti iš Freepik.com archyvo
Tiražas 225 vnt. Užsakymas Nr. GL-237
Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
Maketavo Krašto apsaugos ministerijos bendrųjų reikalų departamento
Vaizdinės informacijos skyrius, Totorių g. 25, LT-01121 Vilnius
Spausdino Lietuvos kariuomenės Karo kartografijos centras,
Muitinės g. 4, Domeikava, LT-54359 Kauno r.