Kurk Lietuvai

NATIONAL CYBER SECURITY CENTRE

Kibernetinis saugumas: kaip valstybė galėtų padėti užtikrinti Trečiųjų šalių valdymą.

Teisinio reguliavimo ir teorijos analizė

Autoriai: Aurelija Požytė Grinė ir Paulius Bagdonas

2023 11 10

Turinys

Sąvokos

Kibernetinio saugumo subjektas – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.

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

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

Ypatingos svarbos informacinė infrastruktūra – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

Ypatingos svarbos paslauga – paslauga, kurios neteikimas ar teikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams.

Ypatingos svarbos informacinės infrastruktūros valdytojas – asmuo, valdantis ypatingos svarbos informacinę infrastruktūrą.

Valstybės informaciniai ištekliai – informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma.

Ryšių ir informacinė sistema – elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.

Viešasis pirkimas (toliau – pirkimas) – vienos ar daugiau perkančiųjų organizacijų atliekamas prekių, paslaugų ar darbų įsigijimas su pasirinktu (pasirinktais) tiekėju (tiekėjais) sudarant viešojo pirkimo–pardavimo sutartį (sutartis), neatsižvelgiant į tai, ar prekės, paslaugos ar darbai yra skirti viešajam tikslu.

Tiekimo grandinė – organizacijų, žmonių, technologijų, veiklos, informacijos ir išteklių sistema, susijusi su tiekėjo prekės ar paslaugos (gamintojo) suteikimu pirkėjui.

IRT sistemos – taikomųjų programų, paslaugų, informacinių technologijų išteklių, IRT išteklių ar kitų informacijos tvarkymo komponentų rinkinys, apimantis ir veiklos aplinką.

IRT paslaugos – per IRT sistemas ir paslaugų teikėjus vienam ar keliems vidaus arba išorės naudotojams teikiamos paslaugos.

Informaciniai ištekliai – materialūs ar nematerialūs informacijos rinkiniai, kuriuos verta apsaugoti.

Pažeidžiamumas – išteklių ar kontrolės silpnoji vieta, jautrumas ar trūkumas, kuriuo gali būti pasinaudota vienai ar kelioms grėsmėms sukelti.

Trumpiniai

NKSC – Nacionalinis kibernetinio saugumo centras

ISO – Organizacijos kokybės sistema

YSII – Ypatingos svarbos informacinės infrastruktūros

VII – valstybės informaciniai ištekliai

OTR – organizaciniai ir techniniai reikalavimai

VPN – (angl. Virtual Private Network) virtualus privatus tinklas

DDoS – paskirstyto atsisakymo aptarnauti kibernetinė ataka

IoT – (angl. Internet of Things) daiktų interneto įrenginiai, pavyzdžiui, išmanieji televizoriai, išmanieji telefonai ir pan.

PĮ – programinė įranga

RIS – ryšių ir informacinė sistema

IRT – Informacinių išteklių tvarkymas

Santrauka

Dokumento tikslas: apžvelgti "trečioji šalis" terminą, susipažinti su šiuo metu taikomais teisės aktais, susijusiais su šia sąvoka, išnagrinėti esamas kibernetines grėsmes ir apžvelgti kibernetinio saugumo valdymo metodus, kurie yra taikomi įtraukiant trečiąsias šalis.

Apžvelgtos 4 temos:

1. Trečiosios šalies sąvokos samprata.
2. Lietuvos teisinė bazė (LR kibernetinio saugumo įstatymo įgyvendinimo nutarimas, LR nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas, LR nutarimas „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, LR viešųjų pirkimų įstatymas), kurioje galima rasti kibernetinio saugumo pagrindinius reikalavimus ir Europos teisinį reguliavimą (BDAR, TIS2 direktyva).
3. Kibernetinės 2022 metų ir 2030 metų grėsmės esančios Europoje.
4. Populiariausi tarptautiniai SANS, NIST, ISC² ir ISO 27002 valdymo modelių principai.

Metodika: atlikta šaltinių analizė (teisės aktai, publikacijos ir pan.)

Išvados:

- Trečioji šalis samprata remiantis įvairiais šaltiniais gali kisti atsižvelgiant į pramonės šaką ir taikymo kontekstą.
- Terminas "trečioji šalis" (angl. Third – party) nėra greitai ir lengvai surandamas, kuris tiesiogiai susietas su kibernetiniu saugumu, tačiau Lietuvos banko valdybos priimto nutarimo „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų “ trečioji šalis įvardinama kaip „subjektas, su kuriuo įstaiga užmezgusi verslo santykius ar sudariusi sutartis dėl produkto ar paslaugos teikimo, įskaitant rangovus ir tiekėjus”. Remiantis ir vadovaujantis Europos draudimo ir profesinių pensijų institucijos (EIOPA) „Informacinių ir ryšių technologijų saugumo ir valdymo gairėmis“ sutapatinama paslaugų teikėjas su „trečioji šalis, kuri pagal užsakomųjų paslaugų susitarimą vykdo procesą (arba jo dalį), teikia paslaugas (arba jų dalį) arba vykdo veiklą (arba jos dalį)“.
- Šiame dokumente sąvoka „trečioji šalis“ suprantama kaip bet koks subjektas, su kuriuo įmonė užmezga verslo santykius, įskaitant tiekėjus, partnerius, filialus, brokerius, gamintojus ir agentus. Trečiosios šalys gali apimti grandinės dalyvius tiek iš viršaus (t.y. tiekėjus), tiek iš apačios (t.y. perpardavinėtojus), taip pat ir nesutartinio pobūdžio šalis.
- Teisinis reguliavimas apibrėžia kibernetinio saugumo techninius ir organizacinius reikalavimus, kurių privalo laikytis tiek organizacijos, tiek jų tiekėjai.
- Kibernetinio saugumo valdymo modeliai (SANS, NIST, ISC², ISO 27002) remiasi veiksmų planavimo ir realizacijos ciklu (Plan-Do-Check-Act). Visi šie modeliai yra sukoncentruoti į tris pagrindines valdymo sritis: fizinė sauga užtikrina prieigos kontrolės sistemas, administracinė sauga grindžiama vidinėmis nuostatomis ir procedūromis, o technologinė sauga pabrėžia informacinių technologijų sprendimų reikšmę.
- Kibernetinio saugumo modeliai padeda organizacijoms integruoti trečiųjų šalių (angl. Third – party) valdymą į savo saugumo strategijas, užtikrinant, kad išoriniai partneriai ir tiekėjai taip pat laikytųsi tų pačių fizinių, administracinių ir technologinių saugumo standartų.
- Kibernetinio saugumo valdymo modelių įgyvendinimas dažnai yra neprivalomas ir priklauso nuo pačios organizacijos požiūrio į kibernetinės saugos prioritetą, ypač tokių, kurios dirba pasaulinėje rinkoje arba turi didelį darbuotojų skaičių.
  Kibernetinio saugumo valdymo modeliai bei teisinio reguliavimo reikalavimai skirti užtikrinti saugumą skirtingose organizacijose.

Įvadas

Tyrimo metodai – apžvelgta Lietuvos Respublikos teisinė bazė (LR kibernetinio saugumo įstatymas įgyvendinimo nutarimas, LR nutarimas „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, LR viešųjų pirkimų įstatymas, LR nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas), Europos teisinė bazė (TIS2 direktyva, BDAR), publikacijos, elektroninė duomenų bazė, internete esantys šaltiniai.

Tyrimo laikotarpis – 2023 09 18 - 2023 10 31

Analizės tikslas:

- Apžvelgti trečiosios šalies sąvokos apibrėžimą bei sampratą;
- Apžvelgti esamus **Lietuvos ir Europos** teisinius reguliavimus;
- Apžvelgti Europoje esančias kibernetines 2022 metų ir 2030 metų **grėsmes**;
- Apžvelgti tarptautinių SANS, NIST, ISC² ir ISO 27002 **valdymo modelių principus**.

Problema. Kibernetiniai incidentai, atsirandantys dėl trečiųjų šalių, kurie gali kelti grėsmę informacijos saugumui ir infrastruktūrai bei gali turėti neigiamų pasekmių. Kaip valstybės teisinė sistema reguliuoja trečiųjų šalių, arba tiekėjų, įtraukimą, remiantis vadybos ir informacinių technologijų metodikomis?

Aktualumas. Dabartinėje kibernetinės saugos sferoje susiduriama su grėsmėmis, kurios yra nuolatinių pokyčių ir augančio sudėtingumo objektas, dėl to reikalaujantis išankstinės analizės ir prevencijos strategijų. Kibernetiniai incidentai paliečia ne tik pagrindinius saugumo dalyvius, bet ir trečiąsias šalis (kurios yra suprantamos kaip bet koks subjektas, su kuriuo įmonė užmezga verslo santykius, įskaitant tiekėjus, partnerius, filialus, brokerius, gamintojus ir agentus. Trečiosios šalys gali apimti grandinės dalyvius tiek iš viršaus (t.y., tiekėjus), tiek iš apačios (t.y., perpardavinėtojus), taip pat ir nesutartinio pobūdžio šalis))[1]. Pastebima, kad spartėjanti skaitmenizacija ir naujų technologijų populiarėjimas yra esminiai veiksniai skatinantys pokyčius. Dėl šių tendencijų auga operacijų sudėtingumas, reikalaujantis proaktyvių sprendimų bei aukštesnio visuotinio supratimo apie kibernetinės saugos kultūrą, atsižvelgiant į tai, kad grėsmės tampa sudėtingesnės.

NKSC skelbti duomenys rodo, kad 2021 m. kibernetinių incidentų skaičius Lietuvoje išliko panašus kaip ir 2020 m., tačiau pastebėtas didesnių ir sudėtingesnių incidentų augimas, kurie daro didesnį neigiamą poveikį. Ši kibernetinių incidentų tendencijos padariniai gali turėti ilgalaikį poveikį tiek valstybės, tiek privataus sektoriaus subjektams. Pagal pateiktus duomenis, su trečiosiomis šalimis susiję kibernetiniai incidentai yra problema pasaulio mastu, ir jie gali turėti ne tik finansinį poveikį įmonėms. 2021 m., 39% pagrindinių organizacijų visame pasaulyje pranešė, kad per pastaruosius du metus patyrė trečiųjų šalių kibernetinio incidento įtaką[2]. „Kaspersky“ tyrimai parodė, kad trečiųjų šalių incidentai buvo brangiausi įmonių duomenų pažeidimai 2021 m., o vidutinis tokių įvykių finansinis poveikis įmonei siekė 1,4 mln. USD, tad tai tapo brangiausiu incidento tipu iki šiol[3]. Be to, „CRA Business Intelligence“ ataskaita rodo, kad 66% organizacijų pastebėjo trečiųjų šalių saugumo incidentų padidėjimą per pastaruosius 12 mėnesių[4].

---

1 Cybersecurity and Third – party risk. Gregory C. Rasner

2 Statista. Vieša prieiga: https://www.statista.com/statistics/1315334/cyber-incidents-in-organizations-worldwide/#:~:text=Published%20by%20Ani%20Petrosyan%20%2C,However

3 Kaspersky. Vieša prieiga: https://www.kaspersky.com/about/press-releases/2021_partnership-costs-third-party-incidents-became-most-costly-enterprise-data-breaches-in-2021

4 SCMEDIA a cyberRisk Allance Resource. Vieša prieiga: https://www.scmagazine.com/research-article/over-90-of-organizations-had-a-security-incident-linked-to-a-third-party-partner-in-last-year

Trečiosios šalies sąvokos apibrėžimas kibernetinio saugumo kontekste

„Trečioji šalis“ apibrėžimas skirtas kibernetiniam saugumui nėra nurodytas „Lietuvos kalbos žodyne“ (LKŽ) arba „Dabartinės lietuvių kalbos žodyne“ (DLKŽ) bei sunkiai randamas terminas. Tačiau sąvokos sutinkamos skirtinguose šaltiniuose, kurios aprašomos bendrame kontekste arba skirta tik nurodytiems sektoriams, pavyzdžiui:

- Europos Sąjungai nepriklausanti šalis. Reikšmė aiškiausia tada, kai dviejų ES valstybių narių tarpusavio santykiai atskiriami nuo santykių su kita – trečiąja šalimi, nepriklausančia Europos Sąjungai[5].
- Asmuo arba įstaiga, pripažinta nepriklausoma nuo šalių, dalyvaujančių nagrinėjant tam tikrus klausimus[6].
- Dalyvaujančios šalys paprastai atstovauja tiekėjo (pirmoji šalis) ir pirkėjo (antroji šalis) interesams[7].
- Fizinis ar juridinis asmuo, kuris nėra tiesioginis sandorio, sutarties, susitarimo ar ginčo dalyvis. Trečioji šalis gali reikšti šalį, kuri nėra tiesioginis atitinkamo proceso dalyvis, tačiau kuri vis tiek patiria to proceso poveikį[8].

Tik Lietuvos banko nutarime „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinime” įvardinama:

- **Trečioji šalis** – subjektas, su kuriuo Įstaiga užmezgusi verslo santykius ar sudariusi sutartis dėl produkto ar paslaugos teikimo, įskaitant rangovus ir tiekėjus[9].

Remiantis ir vadovaujantis Europos draudimo ir profesinių pensijų institucijos (EIOPA) „Informacinių ir ryšių technologijų saugumo ir valdymo gairėmis“ įvardinama:

- **Paslaugų teikėjas** – **trečioji šalis**, kuri pagal užsakomųjų paslaugų susitarimą vykdo procesą (arba jo dalį), teikia paslaugas (arba jų dalį) arba vykdo veiklą (arba jos dalį)[10].

Tačiau iš šios sąvokos apibūdinimo bei konteksto, teisės aktuose (žr. skyrius) sutinkami keletas pavadinimų kaip:

- **Trečiasis asmuo** – fizinis ar juridinis asmuo, kuriam pagal sandorius, nurodytus šio įstatymo 13 straipsnio 4 dalies 1 punkto a papunktyje, suteikiama teisė gauti prieigą ar kitaip susipažinti su įmonės saugumo planuose ar kituose įmonės vidaus dokumentuose nustatytomis ryšių ir informacinėmis sistemomis (ar jų dalimis), kurios yra reikšmingos įmonės veiklai, šių ryšių ir informacinių sistemų (ar jų dalių) technologijomis, duomenų bazėmis ar jose esamais duomenimis arba šiems asmenims būtų suteikta teisė aptarnauti ar kitaip susipažinti su tokiomis ryšių ir informacinėmis sistemomis (jų dalimis)[11].
- **Tiekėjas – ūkio subjektas** – fizinis asmuo, privatusis ar viešasis juridinis asmuo, kita organizacija ir jų padalinys arba tokių asmenų grupė, įskaitant laikinas ūkio subjektų asociacijas, kurie rinkoje siūlo atlikti darbus, tiekti prekes ar teikti paslaugas[12].

5 European Commission. Vieša prieiga: European Commission, official website (europa.eu)

6 LST EN ISO 14050:2010 Aplinkos apsaugos vadyba. Aiškinamasis žodynas (ISO 14050:2009)

7 VLKK terminai. Vieša prieiga: https://terminai.vlkk.lt/paieska?search=tre%C4%8Dioji+%C5%A1alis&limit=15

8 Finero Žodynas. Vieša prieiga: https://www.finero.lt/zodynas/finansai/trecioji-salis/

9 Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f63d6331302a11eb8c97e01ffe050e1c

10 Europos draudimo ir profesinių pensijų institucijos (EIOPA) „Informacinių ir ryšių technologijų saugumo ir valdymo gairėmis“. Vieša prieiga: https://www.eiopa.europa.eu

11 Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498/asr

12 Lietuvos Respublikos viešųjų pirkimų įstatymas Dok. Nr. I-1491 Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.30614/asr

- **Pagalbinės viešųjų pirkimų veiklos paslaugų teikėjas** – tiekėjas, rinkoje siūlantis pagalbinės viešųjų pirkimų veiklos paslaugas.
- **Viešojo pirkimo dalyvis (toliau – dalyvis**) – pirkimui pasiūlymą pateikęs tiekėjas.

Terminas „trečioji šalis“ įvairiose aplinkybėse yra interpretuojamas nevienodai. Kibernetinio saugumo kontekste šis terminas dažniausiai apibrėžia išorės organizacijas ar asmenis, kurie nėra tiesiogiai susiję su informacijos sistemos naudojimu arba valdymu, ir nėra integrali įmonės dalis, tačiau jiems gali būti suteikta prieiga prie įmonės informacinių sistemų ar duomenų. Tokios šalys apima, bet neapsiriboja: tiekėjais, verslo partneriais, subrangovais, konsultantais, audito kompanijomis ir pan., kurie įmonėms teikia įvairias paslaugas arba produktus. Šiuo atveju, autorius Gregory C. Rasner trečiąsias šalis apibūdina, kaip bet koks subjektas, su kuriuo įmonė užmezga verslo santykius, įskaitant tiekėjus, partnerius, filialus, brokerius, gamintojus ir agentus. Trečiosios šalys gali apimti grandinės dalyvius tiek iš viršaus (t.y., tiekėjus), tiek iš apačios (t.y., perpardavinėtojus), taip pat ir nesutartinio pobūdžio šalis)[13]. Ši sąvoka yra glaudžiai susijusi su tiekimo grandinės saugumo ir išorinių šalių keliamos rizikos valdymo klausimais.

Skirtingi autoriai dažnai trečiąsias šalis apibūdina kaip potencialius **rizikos** šaltinius, kurie gali neigiamai paveikti organizacijos kibernetinį saugumą per tiekimo grandinę, išorines paslaugas ar net per darbuotojus, kurie veikia kaip nepriklausomi rangovai ar konsultantai[14]. Trečiosios šalys dažnai yra identifikuojamos kaip **grėsmės** vektorius, per kurį gali būti pradėti kibernetiniai išpuoliai, pavyzdžiui, per "phishing" atakas arba pažeidžiamas sistemas[15].

Autorių išvada. Apžvelgus sąvokų analizę, daroma išvada, kad nėra vieningo supratimo, kas yra trečioji šalis kibernetinio saugumo kontekste, be to, terminas "trečioji šalis" naudojama plačiai ir itin skirtingose srityse. Todėl rekomenduojama:

1. Termino „trečioji šalis“ dalys temos kontekste turėtų būti suprastos kaip – pirmoji šalis NKSC, antroji šalis YSII subjektai, trečioji šalis visi subjektai su kuriais užmegzti verslo santykiai.
2. Oficialiai patvirtinti sąvoką arba suvienodinti per įstatymus – samprata.

Toliau dokumente sąvoka “trečioji šalis” bus naudojama apibūdinti bet kokį subjektą, su kuriuo įmonė užmezga verslo santykius, įskaitant tiekėjus, partnerius, filialus, brokerius, gamintojus ir agentus.

13 Cybersecurity and Third – party risk. Gregory C. Rasner

14 Managing Third-Party Risk in a Changing Regulatory Environment" - Deloitte

15 "Third Party Risk Management: Driving Enterprise Value" - RMA

Kibernetinių grėsmių tipai

Šiame skyriuje pristatomi skirtingi kibernetinio saugumo grėsmių tipai remiantis Europos Sąjungos kibernetinio saugumo agentūros ENISA informacija, apžvelgtos Europoje esančios dabartinės ir numatytos būsimos 2030 metams kibernetinės grėsmės, kurios liečia kibernetinius subjektus t. y. ir trečiųjų šalių tiekėjus.

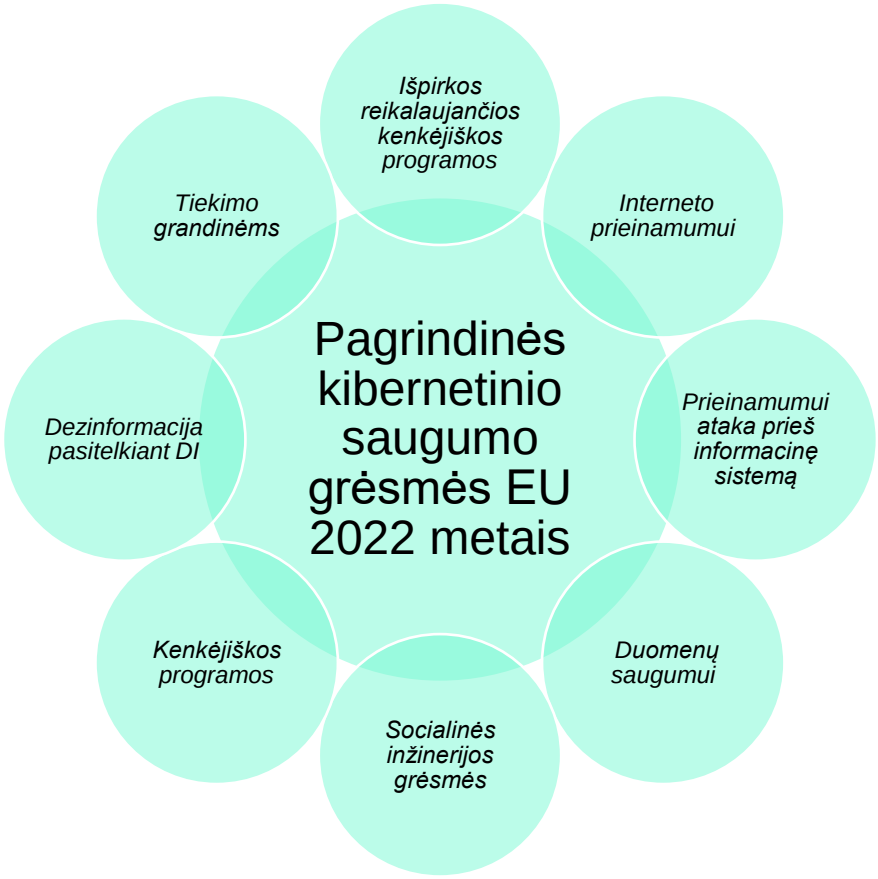
Pagrindinės kibernetinės grėsmės 2022 metais pagal ENISA

8 pagrindinės ir populiariausios kibernetinio saugumo **grėsmės** užfiksuotos Europos Sąjungos kibernetinio saugumo agentūros ENISA 2022 m. *(žr. originalas priedas 1)*[16]:

1. **Išpirkos reikalaujančios kenkėjiškos programos** – kibernetiniai nusikaltėliai taikosi į sudėtingesnius turto grobimo būdus.
2. **Kenkėjiškos programos** – įvairių tipų virusai, šnipinėjimo programos.
3. **Socialinės inžinerijos grėsmės** – pasinaudojimas žmogaus klaidomis informaciją išgauti, populiarus sukčiavimas el. paštu ar tekstinėmis žinutėmis.
4. **Grėsmės duomenų saugumui** – 82% pažeidimų. Manipuliavimas žmonėmis ir žmogiškosios klaidos – vienas iš pagrindinių modelių.
5. **Grėsmės prieinamumui, ataka prieš informacinę sistemą** (angl. distributed denial of service) – tampančios didesnėmis ir sudėtingesnėmis, apimančios ir mobiliuosius įrenginius ir daiktų interneto.
6. **Grėsmės interneto prieinamumui** – apima fizinį interneto infrastruktūros perėmimą ir sunaikinimą. Pavyzdys, kad karo metu Ukrainoje 2022 metų birželio mėnesį buvo sunaikinta apie 15% šalies interneto infrastruktūros.
7. **Dezinformacija** – dirbtinis intelektas tampa pagrindinis dezinformacijos kūrimo ir skleidimo šaltiniu. Pavyzdžiui, soc. tinkluose apsimetant kažkokiu žmogumi naudojantis robotų funkcija.
8. **Grėsmės tiekimo grandinėms** – ataka prieš, pavyzdžiui, paslaugų tiekėją, siekiant gauti prieigą prie klientų duomenų. Tiekimo grandinės atakos gyvavimo ciklas susideda iš dviejų pagrindinių dalių: atakos prieš tiekėją ir ataką prieš klientą.

16 Europos parlamentas. Vieša prieiga: https://www.europarl.europa.eu/news/lt/headlines/society/20220120STO21428/kibernetinis-saugumas-pagrindines-gresmes#ssh

Paveikslas 1: 8 pagrindinės kibernetinio saugumo grėsmės 2022 metais Europoje



Šaltinis: sudarytas autorių remiantis Europos Sąjungos kibernetinio saugumo agentūros ENISA informacija

Europos Sąjungos identifikuojamos kibernetinės pasaulinės 2030 metų grėsmės

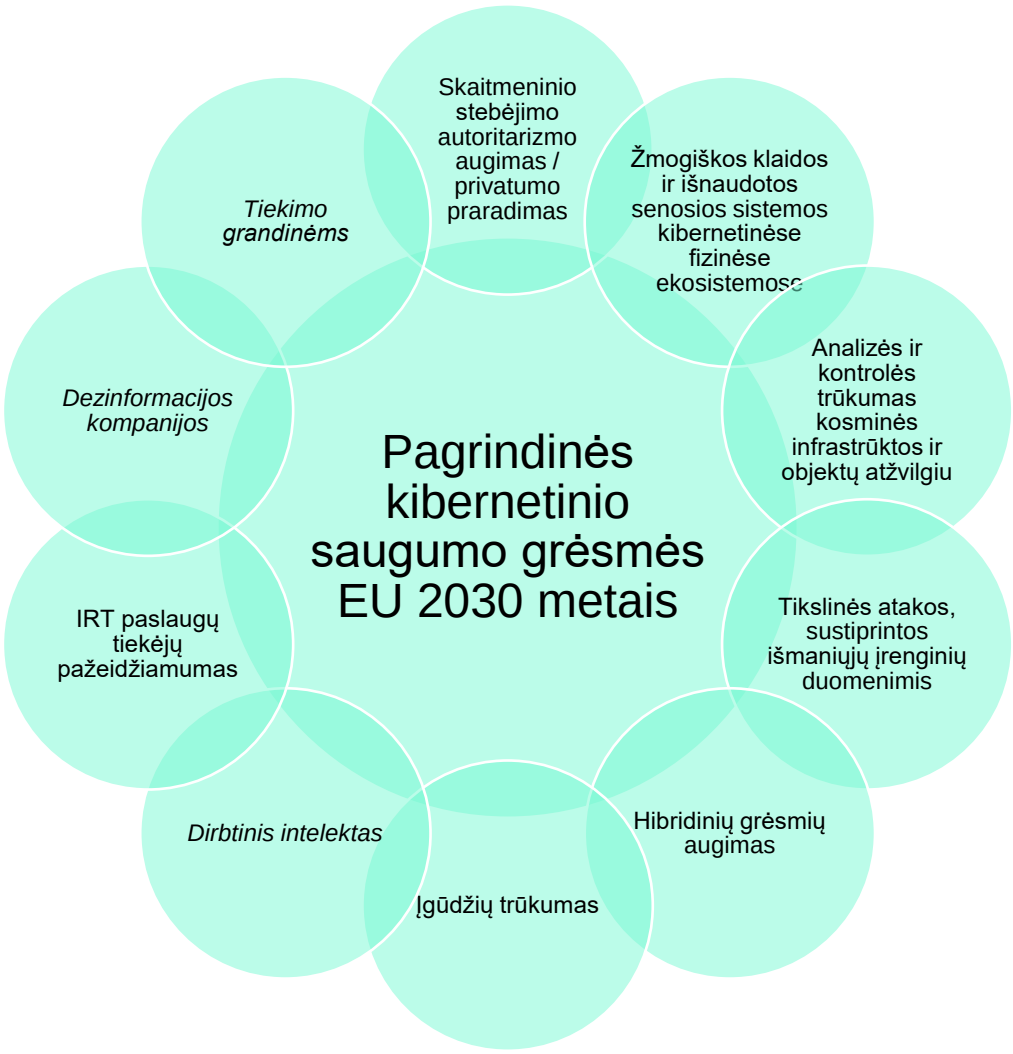
Europos Sąjungos kibernetinio saugumo agentūra – ENISA, CSIRT tinklo ir EU CyCLONE ekspertai tyrimo metu išskyrė ir numatė **TOP 10 kibernetinio saugumo grėsmių tendencijas 2030** metams, atsižvelgta bei į tinklo ir informacijos apsaugos sistemų (TIS) 2 direktyvos pokyčius[17] *(žr. originalas priedas 2)*:

1. PĮ priklausomybių kompromitavimas tiekimo grandinėje. Rinka reikalauja greitų gaminių išleidimo ciklų, daugiau komponentų ir paslaugų integravimo į naujus produktus. Dėl šios priežasties atsiras naujų ir nenumatytų pažeidžiamumų ir atsiras daugiau galimybių pasireikšti piktybiškiems veikėjams, kurie pažeis tiekimo grandinę iš tiekėjo ir kliento pusės siekdami politinių trikdžių, finansinės naudos ar šnipinėjimo. Tiekimo grandinėje yra keturi pagrindiniai elementai:
    - Tiekėjas – subjektas, kuris tiekia produktą ar paslaugą kitam subjektui.
    - Tiekėjo turtas – vertingi elementai, kuriuos tiekėjas naudoja gamindamas produktą ar paslaugą.
    - Klientas – subjektas, kuris vartoja tiekėjo pagamintą produktą ar paslaugą.
    - Kliento turtas – vertingi elementai, priklausantys taikiniui.
2. Pažangios dezinformacijos kampanijos;
3. Skaitmeninio stebėjimo autoritarizmo augimas arba privatumo praradimas;

17 Europos Sąjungos kibernetinio saugumo agentūra (Enisa). Vieša prieiga: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

4. Žmogiškos klaidos ir išnaudotos senosios sistemos kibernetinėse fizinėse ekosistemose;
5. Tikslinės atakos, sustiprintos išmaniųjų įrenginių duomenimis;
6. Analizės ir kontrolės trūkumas kosminės infrastruktūros ir objektų atžvilgiu;
7. Pažangių hibridinių grėsmių augimas;
8. Įgūdžių trūkumas;
9. Tarpvalstybiniai IRT paslaugų teikėjai, kaip pavienis pažeidos taškas. Valstybės infrastruktūros sektoriai tokie kaip transportas, sveikatos priežiūra, elektros tinklai ir pramonė, vis labiau priklausys nuo IRT paslaugų teikėjų ir jų infrastruktūros, kad galėtų prisijungti prie interneto ir prie jo valdyti visus tarp įrenginių ryšius. Taigi šie paslaugų teikėjai taps dažnu vyriausybių, teroristų ir nusikalstamų grupių taikiniais.
10. Piktnaudžiavimas dirbtiniu intelektu.

Paveikslas 2: TOP 10 kibernetinio saugumo grėsmių tendencijos 2030 metams Europoje



Šaltinis: sudarytas autorių remiantis Europos Sąjungos kibernetinio saugumo agentūros ENISA informacija

Kibernetinių grėsmių palyginimas

Nors abu sąrašai aprėpia plačius kibernetinio saugumo iššūkius, jie turi skirtingus akcentus. **Pirmasis sąrašas (2022 m.)** yra specifiškesnis kai kurių sričių atveju, kaip antai, išpirkos reikalaujančios programos ir Ukrainos konflikto įtaka internetui, tuo tarpu **antrasis sąrašas (2030 m.)** apima platesnį spektrą besivystančių ir sudėtingų grėsmių, įskaitant kosminę infrastruktūrą ir kibernetinės saugos geopolitiką.

Žemiau pateikta kibernetinių grėsmių tipų Europoje lyginamoji lentelė.

Kenkėjiškos programos ir išpirkos.	Abu sąrašai kalba apie kenkėjiškas programas. Antrasis sąrašas numato platesnę kenkėjiškų programų kategoriją.
Tiekimo grandinės saugumas.	Tiekimo grandinės grėsmės minimos abiejuose sąrašuose, bet pirmasis sąrašas akcentuoja kompleksiškumą ir tiesioginius išpuolius prieš tiekėjus, tuo tarpu antrasis – programinės įrangos priklausomybių kompromitavimą tiekimo grandinėje.
Socialinė inžinerija ir žmogiškos klaidos.	Socialinė inžinerija yra aiškiai minima pirmajame sąraše, tuo tarpu antrasis įtraukia žmogaus klaidas kaip platesnę kategoriją, kuri apima socialinės inžinerijos taktikų riziką.
Dezinformacija.	Abu sąrašai iškelia dirbtinio intelekto naudojimo dezinformacijai problemą, pirmasis sąrašas konkrečiai kalba apie dezinformacijos platinimą naudojant AI, o antrasis sąrašas pabrėžia platesnį AI piktnaudžiavimo potencialą.
Sistemos ir interneto prieinamumas.	Pirmasis sąrašas kalba apie DDoS atakas ir infrastruktūros fizinio sunaikinimo atvejus, ypatingai minėdamas konfliktą Ukrainoje. Antrasis sąrašas šių temų tiesiogiai nemini.
Skaitmeninis stebėjimas ir privatumas.	Skaitmeninio stebėjimo ir privatumo praradimo augimas yra aiškiai nurodytas antrajame sąraše, pirmasis sąrašas tiesiogiai šios problemos neakcentuoja.
Išmaniųjų įrenginių duomenys ir hibridinės grėsmės.	Antrasis sąrašas kalba apie išplėstines dezinformacijos kampanijas, hibridines grėsmes ir tikslines atakas, kurias sustiprina išmaniųjų įrenginių duomenys, parodant dėmesį į besivystančią kibernetinių grėsmių sudėtingumą. Pirmasis sąrašas įvardina pažangias DDoS atakas, bet nesiliečia hibridinių grėsmių temos.
Įgūdžių trūkumas ir tarptautiniai tiekėjai.	Antrasis sąrašas identifikuoja įgūdžių trūkumą kibernetinio saugumo srityje ir rizikas, susijusias su tarpvalstybiniais IT paslaugų teikėjais, kurie neminimi pirmajame sąraše.
Kosminė infrastruktūra.	Tik antrasis sąrašas iškelia susirūpinimą dėl kosminės infrastruktūros, kuri siejasi su nauja TIS2 direktyvos įsigaliojimu, siūlydamas platesnį kibernetinių iššūkių apmąstymą.

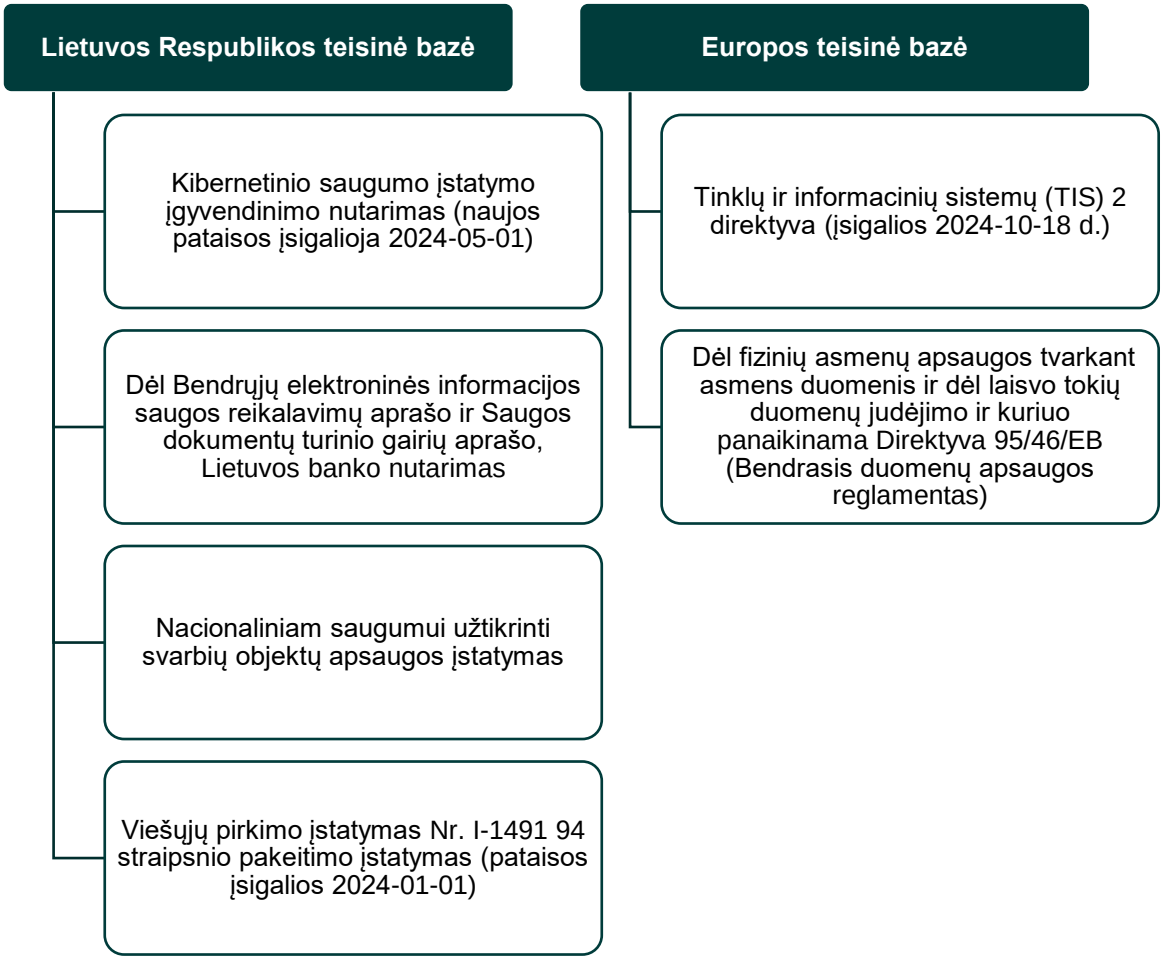
Lietuvos Respublikos ir Europos pagrindiniai kibernetinio saugumo įstatymai ir nutarimai

Lietuvos Respublikos ir Europos teisinis reglamentas susijęs su trečiosiomis šalimis.

Skyrelio tikslas – apžvelgti bei išrašyti esminius reikalavimus skirtus paslaugų tiekėjams iš Lietuvos Respublikos ir Europos teisinės bazės.

Išskirti pagrindiniai teisės aktai pagal kuriuos vadovaujamasi kibernetinis saugumo subjektai:

Paveikslas 3: Kibernetinio saugumo pagrindiniai teisės aktų sąrašas



Šaltinis: autoriai

Lietuvos Respublikos ir Europos teisinės bazės tikslų ir reikalavimų apžvalga

Apsaugant kibernetinį saugumą, trečiosioms šalims būtina atitikti gausybę teisinių reglamentų ir standartų, ypač tada, kai šios šalys suteikia paslaugas arba gauna prieigą prie organizacijos duomenų. Keletas tarptautinių ir nacionalinių standartų bei teisės aktų, kurie taikomi kaip bendrieji reikalavimai kibernetiniams subjektams, apima:

Teisės akto pavadinimas	Teisės akto tikslas	Pagrindiniai reikalavimai susiję su trečiosiomis šalimis
Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo nutarimas[18] **Nutarimo Dok. Nr.: 818** **Lietuvos Respublikos kibernetinio saugumo įstatymas:** **Įstatymo Dok. Nr. XII – 1428 (šiuo metu galioja)[19]** **Pakeis įstatymas Nr.: XII -1428 13 (įsigalios 2024 05 01) [20]** **Dok. Nr.:XIV - 1864**	Tikslas - nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos ir pranešimo apie jas ir kibernetinius incidentus pagrindus, taip pat nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir įgaliojimu.	III skyrius. Organizacinių ir techninių kibernetinio saugumo reikalavimai, taikomi kibernetinio saugumo subjektams. 13. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, pirkdami paslaugas, darbus ar įrangą, susijusius su valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, turi: 13.1. pirkimo dokumentuose iš anksto nustatyti, kad tiekėjas privalo užtikrinti atitiktį Reikalavimams tokia apimtimi, kiek tai susiję su pirkimo objektu, ir laikytis konkrečių perkančiosios organizacijos nustatytų informacijos saugumo, kibernetinio saugumo reikalavimų; 13.2. į sutartis su tiekėju įtraukti reikalavimus, susijusius su informacijos saugumo, kibernetinio saugumo užtikrinimu, tokia apimtimi, kiek tai susiję su pirkimo objektu ir prieiga prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros. IV skyrius. Techniniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams. V skyrius. Reikalavimai viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų tiekėjams.

18 Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo nutarimas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595

19 Lietuvos Respublikos kibernetinio saugumo įstatymas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee?jfwid=-bun155g19

20 Lietuvos Respublikos kibernetinio saugumo įstatymas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e4912752cef911ed9b3c9397e1236c2a?jfwid=-bun155g19

		VI skyrius. Reikalavimai elektroninės informacijos prieglobos paslaugų tiekėjams ir skaitmeninių paslaugų tiekėjams. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, sudaro sąlygas Nacionaliniam kibernetinio saugumo centrui diegti ir valdyti technines kibernetinio saugumo priemones valstybės informaciniuose ištekliuose ir taikyti technines priemones, siekiant įvertinti valstybės informacinių išteklių atsparumą kibernetiniams incidentams. **Apibendrinant reikalavimus:** saugumo politikos laikymasis: paslaugų tiekėjai turi laikytis įmonės ar institucijos kibernetinio saugumo politikos, kuri yra suderinama su nacionaliniais teisės aktais. Rizikos valdymas: reikalinga atlikti rizikos vertinimą ir ją mažinti tiek tiekėjo viduje, tiek bendradarbiavimo metu. Incidentų valdymas: turi būti įgyvendintos procedūros kibernetinių incidentų identifikavimui, pranešimui apie juos ir reagavimui į juos. Saugumo auditai: periodiškai turi būti atliekami saugumo auditai, norint įsitikinti, kad tiekėjų saugumo priemonės yra tinkamos ir veiksmingos. Saugumo sertifikavimas: turėti atitinkamus kibernetinio saugumo sertifikatus. Duomenų apsauga: turi laikytis duomenų apsaugos įstatymų, įskaitant Bendrąjį duomenų apsaugos reglamentą (BDAR), jei tvarko asmens duomenis. Kibernetinio saugumo mokymai: darbuotojai būtų reguliariai mokomi kibernetinio saugumo klausimais. Atsakomybės apibrėžimas: sutartyse turi būti aiškiai nurodyta tiekėjų atsakomybė kibernetinio saugumo incidentų atveju. Saugumo incidentų pranešimo procedūros: privalo turėti aiškias procedūras, kaip ir kam pranešti apie kibernetinio saugumo incidentus.
Lietuvos Banko priimto nutarimo Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio	Tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti valstybės registrų (kadastrų) (toliau – valstybės registras) ir žinybinių registrų duomenis, dokumentus ir informaciją,	6. Užtikrinant elektroninės informacijos saugą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009. 16. Už elektroninės informacijos saugą pagal kompetenciją atsako informacinės sistemos valdytojas ir informacinės sistemos tvarkytojas (-ai). 21. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Aprašo, kitų

gairių aprašo patvirtinimo.[21] **Dok nr.: 716**	valstybės informacinių sistemų ir kitų informacinių sistemų informaciją.	Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis. 4.4. „Reikalavimai, keliami informacinėms sistemoms funkcionuoti reikalingoms paslaugoms ir jų teikėjams“, kuriame turi būti nurodyta: 4.4.1. paslaugų teikėjų prieigos prie informacinės sistemos lygiai ir sąlygos; 6.1.1. subjektai, kuriems bus taikomos šios taisyklės; 6.1.2. prieigos prie elektroninės informacijos principai. 6.3. „Saugaus elektroninės informacijos teikimo informacinės sistemos naudotojams kontrolės tvarka“, kuriame turi būti nurodyta: 6.3.1. tvarka, kuria bus registruojami ir išregistruojami informacinės sistemos naudotojai, ir už šių veiksmų atlikimą atsakingas asmuo; 6.3.2. priemonės informacinės sistemos naudotojų tapatybei nustatyti; 6.3.3. informacinės sistemos naudotojų slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai; 6.3.4. sąlygos ir atvejai, kai panaikinama informacinės sistemos naudotojų teisė dirbti su konkrečia elektronine informacija; 6.3.5. leistini nuotolinio informacinės sistemos naudotojų prisijungimo prie informacinės sistemos būdai.
Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas[22] **Dok.nr: IX-1132**	Tikslas – užtikrinti, kad valstybės nacionaliniam saugumui užtikrinti svarbūs objektai (įmonės, įrenginiai ir turtas bei ūkio sektoriai) ir nacionaliniam saugumui užtikrinti svarbių įmonių, įrenginių ir turto apsaugos zonose (toliau – apsaugos zonos) esantis turtas ir teritorija bei ypatingos svarbos	10. Trečiasis asmuo – fizinis ar juridinis asmuo, kuriam pagal sandorius, nurodytus šio įstatymo 13 straipsnio 4 dalies 1 punkto a papunktyje, suteikiama teisė gauti prieigą ar kitaip susipažinti su įmonės saugumo planuose ar kituose įmonės vidaus dokumentuose nustatytomis ryšių ir informacinėmis sistemomis (ar jų dalimis), kurios yra reikšmingos įmonės veiklai, šių ryšių ir informacinių sistemų (ar jų dalių) technologijomis, duomenų bazėmis ar jose esamais duomenimis arba šiems asmenims būtų suteikta teisė aptarnauti ar kitaip susipažinti su tokiomis ryšių ir informacinėmis sistemomis (jų dalimis). Šiame dokumentu išskirti YSSI ir VII reikalavimai. 6 straipsnis. Nacionaliniam saugumui užtikrinti strategiškai svarbūs ūkio sektoriai. 7 straipsnis. Pirmos kategorijos nacionaliniam saugumui užtikrinti svarbios įmonės.

21 Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399?jfwid
https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399/asr

22 Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.189498/asr

	informacinės infrastruktūros valdytojų sandoriai būtų apsaugoti nuo visų galinčių kelti grėsmę nacionalinio saugumo interesams rizikos veiksnių, ir šalinti tokių veiksnių atsiradimo priežastis ir sąlygas.	
Europos Parlamento ir tarybos direktyva[23] (ES) 2022/2555 **Dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kurią iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)**	Tikslas – tobulinant nacionalinių taisyklių suderinimo priemones sukurti vidaus rinką ir užtikrinti jos veikimą. Subjektams, teikiantiems ekonomiškai svarbias paslaugas arba vykdantiems ekonomiškai svarbią veiklą, nustatyti kibernetinio saugumo reikalavimai valstybėse narės gerokai skiriasi atsižvelgiant į reikalavimų rūšį, jų išsamumo lygį ir priežiūros metodą. Apsaugoti kritines informacinės infrastruktūros sistemas ir užtikrinti, kad telekomunikacijų tinklai ir paslaugos būtų atsparūs	21 straipsnis. Kibernetinio saugumo rizikos valdymo priemonės: d) tiekimo grandinės saugumas; i) žmogiškųjų išteklių saugumą, prieigos kontrolę. 24 straipsnis. Europos kibernetinio saugumo sertifikavimo schemų naudojimas: esminiai ir svarbūs subjektai naudotų konkrečius esminių ar svarbių subjektų sukurtus arba iš trečiųjų šalių nupirktus sertifikuotus IRT produktus, IRT paslaugas ir IRT procesus. 32 straipsnis. Esminių subjektų priežiūros ir vykdymo užtikrinimo priemonės, viena iš priemonių: f) prašyti leisti susipažinti su duomenimis, dokumentais ir informacija, reikalinga jų priežiūros užduotims atlikti. Kibernetinio saugumo stiprinimą: pagrindinių informacinių ir ryšių technologijų tiekimo grandinių; turėtų būti įvertinta ir atsižvelgta į bendrą tiekėjų ir paslaugų teikėjų produktų kokybę; kibernetinio saugumo praktiką, įskaitant saugias produktų ir paslaugų kūrimo procedūras. **Apibendrinant** nurodymas tikslinių priemonių sąrašas: reagavimą į įvykius ir krizių valdymą; pažeidžiamumą valdymą ir atskleidimą; pažeidžiamumo testavimą ir efektyvų šifravimo naudojimą. Subjektai klasifikuojami į kategorijas: ypatingas ir svarbias.

23 Europos paslamento ir tarybos direktyva. Dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti. Vieša prieiga: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32022L2555

	kibernetinėms grėsmėms.	Tiekimo grandinės saugumas: reikia užtikrinti, kad visi tiekimo grandinės dalyviai taip pat atitinka nustatytus kibernetinio saugumo reikalavimus.
Europos Parlamento ir tarybos reglamentas (ES)2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)[24]	Tikslas – užtikrinti asmens duomenų apsaugą ir privatumą bei reguliuoti jų tvarkymą pagal teisine dokumentaciją, procesus ir technologijas visoje Europoje.	**Apibendrinant reikalavimus:** Duomenų perdavimas į trečiąsias šalis ir tarptautines organizacijas: apibrėžiama tvarka, pagal kurią asmens duomenys gali būti perduoti trečiosioms valstybėms ar tarptautinėms organizacijoms, kartu su sąlygomis, kai tai gali būti atliekama. Duomenų subjektų teisės: pateikiamos duomenų subjektų teisės, įskaitant teisę į informaciją, taisymą, ištrynimą, duomenų apribojimą, duomenų perkeliamumą ir kt. Darbuotojų asmens duomenų tvarkymas: apibrėžiami pagrindai, kurių pagrindu tvarkomi darbuotojų asmens duomenys ir išvardijamos teisinės priemonės, kuriomis siekiama užtikrinti jų apsaugą. Sutikimas dėl asmens duomenų tvarkymo: pateikiamos taisyklės ir forma, pagal kurias gali būti reikalaujama duomenų subjekto sutikimo duomenų tvarkymui. Apsaugos priemonės: nurodomos apsaugos priemonės, pvz., apsauga nuo kompiuterinės įrangos gedimų, kurios naudojamos asmens duomenų saugumui užtikrinti. Sutikimo atšaukimas: aiškinama, kad duomenų subjektas gali bet kuriuo metu atšaukti savo sutikimą ir kad tai neturėtų turėti neigiamos įtakos jo teisėms ir laisvėms.
Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491[25] ir pasikeičiantis[26] 94 straipsnio Dok. Nr. XIV – 2002 įsigalioja 2024 01 01	Tikslas – užtikrinti efektyvių ir skaidrių viešųjų pirkimų ir projekto konkursų atlikimą.	Čia užfiksuojama trečioji šalis, kaip ne EU šalis, kitaip tariant nedraugiška ir visur kitur minimi paslaugų tiekėjai, dalyvis. Preliminarioji viešojo pirkimo–pardavimo sutartis (toliau – preliminarioji sutartis) – vienos ar kelių perkančiųjų organizacijų ir vieno ar kelių tiekėjų sudaryta sutartis, kurios tikslas – nustatyti sąlygas, įskaitant kainą ir, kur to reikia, numatomą kiekį, taikomas viešojo pirkimo–pardavimo sutartims, kurios bus sudarytos per tam tikrą nurodytą laikotarpį.

24 Europos Parlamento ir tarybos reglamentas (ES)2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) Vieša prieiga: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679
XIII-1426 Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas (lrs.lt)
edpb_recommendations_202001_supplementarymeasurestransferstools_lt.pdf (europa.eu)

25 Lietuvos Respublikos viešųjų pirkimų įstatymas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.30614/asr

26 Lietuvos Respublikos viešųjų pirkimų įstatymo Nr. I-1491 94 straipsnio pakeitimo įstatymas. Vieša prieiga: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/bc426642010011eebc0bd16e3a4d3b97

		46. Viešojo pirkimo subtiekimo sutartis (toliau – subtiekimo sutartis) – laimėjusio dalyvio ir vieno arba kelių ūkio subjektų (toliau – subtiekėjai) arba subtiekėjo ir vieno arba kelių ūkio subjektų (toliau kartu – subtiekėjai) raštu ar žodžiu sudaroma sutartis dėl ekonominės naudos tiekti prekes, teikti paslaugas ar atlikti darbus, nurodytus perkančiosios organizacijos su laimėjusiu dalyviu sudarytoje pirkimo sutartyje. 34. Techninė specifikacija saugumo reikalavimai arba duomenys, apimantys produkto reikalavimus. 5. Perkančioji organizacija, veikianti gynybos srityje, valdanti ypatingos svarbos informacinę infrastruktūrą, veikianti srityse, kurios laikomos nacionaliniam saugumui užtikrinti strategiškai svarbių ūkio sektorių dalimi, ar įrašyta į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą (toliau – Saugiojo tinklo naudotojų sąrašas), atlikdama su nacionaliniu saugumu susijusių prekių, paslaugų ar darbų pirkimus, įvertina visus galinčius kelti grėsmę nacionalinio saugumo interesams rizikos veiksnius ir sprendžia, ar šiuose pirkimuose gali dalyvauti tiekėjai, jų subtiekėjai ir ūkio subjektai, kurių pajėgumais remiamasi, kurie nėra registruoti (jeigu tiekėjas, jų subtiekėjas ar ūkio subjektas, kurio pajėgumais remiamasi, yra fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Europos Sąjungos valstybėje narėje, Šiaurės Atlanto sutarties organizacijos valstybėje narėje ar trečiojoje šalyje, pasirašiusioje šio straipsnio 4 dalyje nurodytus tarptautinius susitarimus. Papildyta straipsnio dalimi: Nr. XIII-2158, 2019-05-30, paskelbta TAR 2019-06-10, i. k. 2019-09411 Straipsnio dalies **Apibendrinant reikalavimus:** šie reikalavimai yra susiję su tiekėjų kvalifikacija, sąžiningumu, profesionalumu, ir galimybe remtis kitų ūkio subjektų pajėgumais: Tiekėjo pasiūlymo atitikimas: tiekėjai turi pateikti pasiūlymus, kurie atitinka visas viešojo pirkimo procedūrose nustatytas reikalavimus, sąlygas ir kriterijus. Tai apima techninius, kokybės vadybos ir aplinkos apsaugos standartus, kurie nustatomi perkančiosios organizacijos. Kvalifikacijos reikalavimai: jei perkančioji organizacija nustato kvalifikacijos reikalavimus tiekėjams, tiekėjai turi juos atitikti. Tai gali apimti tiekėjo įgaliojimą asmeniui pasirašyti paraišką ar pasiūlymą, taip pat kitus reikalavimus, nustatytus perkančiosios organizacijos pirkimo dokumentuose. Sąžiningumo principo laikymasis: tiekėjai turi išvengti bet kokių veiksmų, kurie gali kelti abejonių dėl jų sąžiningumo, pvz., nusikalstamą veiklą ar kitus veiksmus, kurie gali sukelti abejonių dėl jų sąžiningumo.

		Kainos atitiktis: tiekėjų pasiūlytos kainos neturi viršyti perkančiosios organizacijos numatytų lėšų pirkimui. Jei tiekėjo pasiūlyta kaina laikoma nepriimtina arba per didelė, jis gali būti pašalintas iš pirkimo procedūros. Nusikalstamos veiklos ar kitų rimtų pažeidimų nebuvimas: tiekėjai gali būti pašalinti iš pirkimo procedūros, jei jie yra nuteisti už tam tikras nusikalstamas veikas, pvz., dalyvavimą nusikalstamame susivienijime, sukčiavimą, teroristinius nusikaltimus ir kt. Profesinio elgesio laikymasis: tiekėjai turi laikytis profesinių etikos normų, nepažeisti konkurencijos taisyklių ar neįvykdyti rimtų profesinių pažeidimų. Solidari atsakomybė: perkančioji organizacija gali reikalauti, kad tiekėjai ir jų remiami ūkio subjektai prisiimtų solidarią atsakomybę už pirkimo sutarties įvykdymą, tai reiškia, kad visi šie subjektai bus atsakingi už sutarties vykdymą.

Teisės aktų analizė leidžia identifikuoti pagrindines subjektų kategorijas, kurios apima elektroninės informacijos prieglobos paslaugų tiekėjus, skaitmeninių paslaugų tiekėjus, viešųjų ryšių tinklų ir/arba viešųjų elektroninių ryšių paslaugų tiekėjus, taip pat subjektus, atsakingus už valstybės informacinių išteklių valdymą ir/arba tvarkymą, įskaitant ypatingos svarbos informacinės infrastruktūros (YSSI) valdytojus. Organizaciniai ir techniniai kibernetinio saugumo reikalavimai, taikomi prieš tai išvardintiems kibernetinio saugumo subjektams, kurie apima rizikos valdymo strategijas, incidentų tvarkymo ir pranešimo procedūras, kokybės gerinimo standartus. Jie taip pat rekomenduoja vadovautis Lietuvos standartais LST ISO/IEC 27001 arba 27002 ir pabrėžia bendradarbiavimo svarbą. Be to, atsižvelgiama į reikalavimus, keliamus informacinių sistemų funkcionavimui, būtinoms paslaugoms ir jų teikėjams, turintiems prieigą prie kritinės infrastruktūros išteklių.

Trečiosios šalys, numatytos kibernetinio saugumo kontekste pagal įstatymus, gali būti suprantamos, žemiau pateikiama keletas pavyzdžių:

Dalyvis: skirstomi į patikimus ir nepatikimus dalyvius, atliekančius prekių, paslaugų, ar darbų pirkimus. Jie įtraukia techninius, kokybės vadybos ir aplinkos apsaugos standartus, nustatomus perkančios organizacijos. Dažniausiai minima, kaip pirminis etapas prieš ir per viešuosius pirkimus sudarant sutartis ir numatant sutartyse reikalavimus bei įsipareigojimus teikiant paslaugą.

Sutarčių subjektai: apima visus išorinius partnerius, su kuriais organizacija turi sudariusi verslo sutartis. Šios sutartys dažnai įtraukia konfidencialumo ir duomenų apsaugos sąlygas ir reikalauja, kad trečiosios šalys laikytųsi nustatytų saugumo protokolų.

Kibernetinio saugumo reikalavimų turi laikytis ne tik organizacijos, bet ir trečiosios šalys. Bendrame kontekste suprantama, kad pagrindinę atsakomybės dalį už kibernetinį saugumą prisiima organizacijos, naudojančios trečiųjų šalių paslaugas.

Kibernetinio saugumo valdymo modeliai

Kibernetinio saugumo valdymo modeliai, skirti užtikrinti saugumą įvairiose organizacijose, yra ypač svarbūs bendradarbiaujant su trečiosiomis šalimis. Šie modeliai padeda organizacijoms sukurti struktūrizuotą požiūrį į trečiųjų šalių valdymą, nustatyti būtinus saugumo reikalavimus ir procedūras, taip pat užtikrinti nuolatinę trečiųjų šalių veiklos stebėseną ir vertinimą. Taip pat, jie padeda nustatyti atsakomybes ir procedūras, susijusias su duomenų apsauga, prieigos kontrolėmis ir incidentų valdymu, kurie yra būtini, siekiant užtikrinti, kad išoriniai tiekėjai nepažeistų organizacijos saugumo politikos ir standartų.

Visi modeliai dėmesį skiria **fizinei, technologinei ir administracinei saugai**. Svarbu paminėti, kad modelių taikymas daugeliu atveju yra savanoriškas, priklauso nuo organizacijos suvokimo apie kibernetinio saugumo svarbą, ypač tų, kurios veikia globalioje aplinkoje arba turi daug narių.

Fizinė sauga aprūpina prieigos kontrolę, technologinė sauga akcentuoja IT sprendimus, o administracinė sauga remiasi vidaus taisyklėmis ir tvarkomis. Dauguma modelių yra labiau orientuoti į technologinę dimensiją, nors modeliai iš esmės yra technologiškai neutralūs. Modeliuose akcentuojamos kibernetinio saugumo priemonės, kurios tapo esminėmis šiuolaikiniame IT pasaulyje.

Modeliuose nedaug dėmesio skiriama personalo valdymui, išskyrus kai kurias sritis, pvz., personalo mokymą ir atranką. NIST modelis yra labiausiai išsivystęs personalo saugumo srityje, nes jame skiriamas dėmesys tiek vidiniams darbuotojams, tiek išoriniams partneriams.

Visi modeliai remiasi **veiksmų planavimo ir realizacijos ciklu** (Plan-Do-Check-Act). Tarp jų, NIST modelis yra labiausiai pritaikytas kintančiai kibernetinio saugumo aplinkai, nes jis numato organizacijos adaptaciją. Atsižvelgiant į skirtingus modelius, svarbu suprasti, kad visa sistema reikalauja platesnio požiūrio į kibernetinį saugumą nei tradiciniai modeliai, siekiant užtikrinti visapusišką apsaugą.

Toliau pristatomi:

SANS kontrolės valdymo modelis, kuris susideda iš 5 gynybos principų (t.y. kaip reiktų organizuoti gynybą) ir 3 domenų (domenai parodo brandos stadiją). Visi šie domenai yra tarpusavyje susiję, todėl organizacijoms, norinčioms įgyvendinti šį modelį, rekomenduojama pradėti nuo bazinio domeno, kuris taip pat vadinamas kibernetine higiena, ir tada eiti link kitų dviejų sričių.

NIST modelyje yra teikiama prioritetinė svarba privataus sektoriaus kibernetinio saugumo valdymo strategijoms, kurių tikslas – sukurti organizaciją, gebančią efektyviai atsispirti kibernetinėms grėsmėms. Sudarytas iš 5 sričių kurių tikslas įvardinti ir užtikrinti kibernetinio saugumo procesų vykdymą. Svarbi detalė, kad šis modelis yra paremtas veiklos tęstinumu, todėl tai turėtų tapti įprasta įmonės veikla.

ISO27002 priemonių rinkinys apibrėžia būtinąsias valdymo priemones, kurios turi būti pritaikomos, reguliariai stebimos ir tobulinamos norint pasiekti nustatytus saugumo tikslus. Remiantis šiuo modeliu, kibernetinis saugumas yra suprantamas kaip technologinis procesas. Vis dėlto, būtina pažymėti, kad vien šio aspekto nepakanka, todėl organizacijoms reikėtų orientuotis ne tik į technologinius sprendimus, bet ir į valdymo procesus. Modelyje išskiriamos 3 grėsmių atsiradimo sritis ir 14 valdymo sričių, į kurias orientuojamos atitinkamos valdymo priemonės.

ISC² valdymo modelis, kuris yra grindžiamas 8 kibernetinio saugumo domenų funkcinėmis sritimis. Jame ypatingas dėmesys yra skiriamas technologiniam įgyvendinimui ir naudojimui. Svarbu pažymėti, kad šis modelis nepakankamai nagrinėja darbuotojų ir trečiųjų šalių klausimus, o dėmesys sutelkiamas tik į organizacijos vidinę aplinką, neatsižvelgiant į išorinės aplinkos poveikį.

SANS - kontrolės priemonių valdymo modelis

SANS institutas pabrėžia 5 kibernetinės gynybos principus[27]:

Gynybos mechanizmų parinkimas:

- svarbu pasirinkti technologijas, atsižvelgiant į realias kibernetines atakas. Tai padeda organizacijoms stiprinti saugumo strategijas.

Prioritetų nustatymas:

- pagrindinis dėmesys turi būti skiriamas technologijoms, kurios užtikrina didžiausią rizikos mažinimą, atsižvelgiant į esamas grėsmes ir organizacijos aplinką.

Vertinimo sistemos nustatymas:

- universalios vertinimo sistemos įdiegimas leidžia organizacijos nariams vienodai vertinti saugumo priemones, tokiu būdu greičiau nustatant ir įgyvendinant reikiamus pakeitimus.

Nuolatinis stebėjimas:

- įdiegus nuolatinį saugumo stebėjimo procesą, galima efektyviai įvertinti esamas ir naujas saugumo priemones, taip mažinant kibernetines grėsmes.

Apsaugos automatizavimas:

- automatizavimas mažina žmogiškųjų klaidų riziką, suteikdami organizacijai greitesnį ir tikslesnį kibernetinio saugumo vertinimą.

SANS instituto kibernetinio saugumo valdymo modelis yra padalintas į tris domenus:

Bazinis domenas:	apima techninių ir programinių išteklių kontrolę, pažeidžiamumų valdymą, prieigos nustatymus, techninės įrangos konfigūraciją ir proceso stebėjimą.
Pagrindinis domenas:	fokusuojasi į elektroninio pašto ir interneto technologijų apsaugą, kenkėjiškos programinės įrangos prevenciją, fizinę prieigą, duomenų apsaugą, tinklo įrenginių konfigūravimą ir belaidžio tinklo aspektus.
Organizacinis domenas:	apima kibernetinio saugumo mokymus, programinės įrangos stebėjimą, incidentų valdymą ir organizacijos atsparumo grėsmėms tikrinimą.

27 CIS Controls Version. Vieša prieiga: https://www.defensis.it/ecms/file/CIS-Controls-Version-7.pdf

NIST – kibernetinio saugumo sistema

Tiekėjų vertinimas apima finansines, operacines ir kibernetines rizikas. Įmonės vis dažniau vertina ne tik tiekėjų gebėjimus, bet ir jų produktus bei paslaugas kibernetinio saugumo kontekste. Saugumo reikalavimai tiekimo grandinėje tapo esminiai, o įmonės taiko geriausias praktikas, siekdamos užtikrinti tiekėjų atitikimą ir mažinti riziką[28].

Kibernetinės tiekimo grandinės rizikos:

- kaip tiekėjai vertina savo darbuotojus, ypač tuos, kurie turi prieigą prie kliento duomenų.
- Tiekėjų paslaugų vertinimo procedūras. Bet kuris paslaugų teikėjas gali kelti kibernetinę riziką.
- Kaip tiekėjai vertina savo produktus ir programinę įrangą, ypač produktus su integruota IT, kurie bus integruoti į kliento sistemas.

Tiekėjų saugumo reikalavimai:

- fiziniai ir kibernetiniai saugumo procesai vertinami tiekėjų atrankos metu. Daugelis įmonių taip pat įtraukia procesų reikalavimus į tiekėjų sutartis.

Tiekėjų valdymo geriausios praktikos:

- įmonės nustatė įvairias praktikas, padėjusias veiksmingiau valdyti tiekėjus. Šias praktikas apima prekės ženklo vientisumo akcentavimą, daugiašalius įsigijimo sprendimus, standartinius saugumo terminus sutartyse, tiekėjų vertinimus vietoje jų vertinimų ir kitas praktikas.

Tiekėjų rizikos valdymo priemonės:

- vertinant tiekimo grandinės partnerius už pirmojo lygio yra daugelio įmonių iššūkis. Trečiosios šalys siūlo sprendimus, kurie padeda rinkti, valdyti ir centralizuoti tiekėjų rizikos valdymo duomenis, padidindami veiksmingumą ir mažindami naštą tiekėjams.

NIST kibernetinio saugumo valdymo modelis padeda organizacijoms tvarkyti kibernetinį saugumą[29]:

Kibernetinio saugumo valdymo pakopos:	**1 pakopa (pradinė)**: neformalus rizikų valdymas.
	2 pakopa (informacinė): teisiniai dokumentai patvirtina rizikų valdymo procesą, tačiau ne visiškai įdiegtas.
	3 pakopa (integruota): aiškiai dokumentuotas ir įgyvendintas rizikų valdymo procesas.
	4 pakopa (adaptyvi): organizacija sparčiai reaguoja į grėsmes, visiškai integruoja saugumo planavimą su verslo procesais

28 Framework for Improving Critical Infrastructure Cybersecurity. Vieša prieiga: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

29Framework for Improving Critical Infrastructure Cybersecurity. Vieša prieiga: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

ISO27002 – kibernetinio saugumo valdymo priemonės

Pagal šį standartą organizacijos turėtų įvertinti keletą aspektų[30]:

Rizikos vertinimas:

- Nustatomi pavojai, išteklių pažeidžiamumas ir galimas poveikis organizacijai

Teisiniai reikalavimai:

- Organizacijos privalo laikytis teisinių, reguliavimo ir kitų sutartinių reikalavimų.

Informacijos išteklių panaudojimo reikalavimai:

- Svarbu užtikrinti organizacijos veiklos tęstinumą.

Sėkmingam kibernetinio saugumo valdymui yra būtina atsižvelgti į galimą žalą dėl saugumo pažeidžiamumų ir numatyti atitinkamas prevencines priemones.

Standartas nurodo 14 saugumo valdymo sričių. Organizacijos turi pasirinkti, kurios iš jų yra svarbiausios jų veiklai[31]. Pavyzdžiui:

Informacijos saugumo politika:

- Nustatomi saugumo tikslai ir gairės, vadovybė, saugumo priemonės bei jų svarba.

Informacijos saugumo organizavimas:

- Aprašomos saugumo įgyvendinimo, naudojimo ir kontrolės sistemos. Apibrėžiama technologinės ir organizacinės priemonės, narių atsakomybės, grėsmės.

Žmogiškųjų išteklių saugumo sritis:

- Svarbu užtikrinti darbuotojų atsakomybę ir sąmoningumą.

Išteklių valdymo, prieigos prie techninės įrangos ir vartotojų identifikavimo sritys:

- Apima turto, prieigos ir vartotojų valdymo klausimus.

Kriptografinių priemonių naudojimas:

- Užtikrinamas duomenų konfidencialumas ir vientisumas.

Fizinis ir darbo saugumas:

- Apima fizinės apsaugos priemones ir IT įrangos eksploatavimo veiklą.

Kiekviena organizacija, taikydama šį standartą, turėtų adaptuoti reikalavimus pagal savo specifiką ir verslo poreikius. Tiekėjų pasirinkimas ir valdymas turėtų atsižvelgti į rizikos vertinimą, todėl rekomenduojama dirbti su tiekėjais, kurie jau turi ISO 27001 sertifikavimą arba ekvivalentą. Svarbu palaikyti ryšį su tiekėjais, informuoti juos apie bet kokius pakeitimus ir įtraukti jų paslaugas į metinius peržiūros procesus.

30 International Standart ISO/IEC 27001. Vieša prieiga: http://www.itref.ir/uploads/editor/d3d149.pdf

31 International Standart ISO/IEC 27001. Vieša prieiga: http://www.itref.ir/uploads/editor/d3d149.pdf

ISC² – kibernetinio saugumo valdymo modelis

Programa padeda organizacijoms įdiegti saugumo valdymo modelį pagal (ISC)² standartus, kuris yra suskirstytas į domenus[32]:

Saugumo ir rizikų valdymo domenas.	Susijęs su organizacijos saugumo principais, politika ir standartais, skirtais informacijos išteklių apsaugai ir veiksmingumui vertinti.
Išteklių saugumo domenas.	Nagrinėja, kaip stebėti ir apsaugoti organizacijos valdomus išteklius siekiant užtikrinti jų konfidencialumą, vientisumą ir prieinamumą.
Architektūros domenas.	Aptaria saugumo principus ir standartus, naudojamus informacinių sistemų saugumo užtikrinimui, įskaitant technologinės architektūros ir programinės įrangos saugumo aspektus.
Telekomunikacinių tinklų saugumo domenas.	Nagrinėja duomenų perdavimo technologijas ir saugumo priemones, užtikrinančias duomenų konfidencialumą ir vientisumą.
Prieigos valdymo ir tapatybės nustatymo domenas.	Apima prieigos kontrolės aspektus infrastruktūros, informacinių sistemų ir personalo lygmenyse, užtikrinant duomenų ir išteklių saugumą.
Saugumo vertinimas ir testavimas.	Aprašo kibernetinio saugumo vertinimo ir testavimo metodus, kad būtų atpažinti sistemos trūkumai ir užkirsti kelią būsimiems pažeidžiamumams.
Saugumo užtikrinimo domenas.	Apibrėžia auditavimo ir stebėjimo priemones kritiniams organizacijos ištekliams identifikuoti ir apsaugoti.

Nors dažnai akcentuojama informacinių sistemų prieigos kontrolė kibernetinio saugumo srityje, saugumo ekspertams būtina užtikrinti, kad organizacijos taip pat skiria dėmesį programinės įrangos saugumui. Dauguma kibernetinio saugumo incidentų atsiranda dėl programinės įrangos pažeidžiamumą, kurie neretai tampa potencialiomis įsilaužimo vietomis įmonių sistemose.

32 Official isc2 guide. Vieša prieiga: https://manpreetstorage.files.wordpress.com/2016/07/official-isc2-guide-to-the-cissp-cbk-fourth-edition-2015.pdf

Išvados

"Trečioji šalis" yra sąvoka, kuri interpretuojama įvairiai, atsižvelgiant į sektorių ir kontekstą.

Nors oficialiame Lietuvos kalbos žodyne šios sąvokos nėra, kuri tiktų kibernetinio saugumo kontekste, Lietuvos banko įstatymo „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų “ **trečioji šalis** įvardinama, kaip subjektas, su kuriuo įstaiga užmezgusi verslo santykius ar sudariusi sutartis dėl produkto ar paslaugos teikimo, įskaitant rangovus ir tiekėjus. Taip pat trečioji šalis sutapatinama su paslaugos tiekėju. Lietuvos ir Europos teisinėje bazėje, vadovaujantis šiuo apibrėžimu, pagal kontekstą galima taip pat sutikti kitaip įvardintus, kaip **trečiasis asmuo, tiekėjas – ūkio subjektas,** pagalbinės viešųjų pirkimų veiklos **paslaugų teikėjas,** viešojo pirkimo **dalyvis (toliau – dalyvis**), **ir kt.**

Teisės aktuose, knygose ir žodynuose nurodoma, kad valstybinio kibernetinio saugumo kontekste "trečioji šalis" apibrėžiama kaip bet koks subjektas ar organizacija, kuri neturi tiesioginio ryšio su valstybe, bet gali įgyti prieigą prie svarbios valstybės informacijos, sistemų ar infrastruktūros. Tai apima privačias įmones, tiekėjus, užsienio įstaigas ir kitas įstaigas, teikiančias paslaugas ar atliekančias operacijas valstybės įmonių ar institucijų užsakymu. Šios trečiosios šalys, turėdamos galimybę prieiti prie jautrios informacijos ar sistemų, potencialiai gali daryti įtaką ir kelti grėsmę nacionaliniam kibernetiniam saugumui.

Remiantis pateikta Europos Sąjungos kibernetinio saugumo agentūros ENISA duomenimis, Europoje esančios 8 pagrindinės ir numatytos TOP 10 būsimos, 2030 metams, **kibernetinės grėsmės** - liečia visus. Tos pačios grėsmės išliks ir kai kurių sudėtingumas tik plėtosis ir apjunks daugiau atakos tipų. Tiekimo grandinės grėsmės išliks, kurios turės žymiai skaudžių pasekmių tiek klientams, tiek paslaugų tiekėjams, kurios turi tarpusavio glaudų ryšį (yra priklausomos viena nuo kitos). Viešojo sektoriaus paslaugos veikimo sutrikdymas ypač kritinės infrastruktūros, gali tapti pasauline problema. Viešieji sektoriai, kaip transportas, sveikatos priežiūra, elektros tinklai ir pramonė, vis labiau priklausys nuo IRT paslaugų teikėjų ir jų infrastruktūros. Norint sumažinti rizikas, svarbus ne tik bendradarbiavimas, bet ir aukšta kibernetinio saugumo branda, bandyti iš anksto numatyti pažeidžiamumas ir jiems ruoštis. Norint sumažinti arba išvengti žmogiškųjų klaidų reikia išsiaiškinti kodėl tai įvyksta ir skirti saugumo priemones.

Autoriaus Gregory C. Rasner, įvardinama, kad kibernetinio saugumo kontekste trečiųjų šalių rizika yra susijusi su grėsmėmis ir pažeidžiamumais, privalomu tiekėjų valdymu, kuriuos šios šalys gali sukelti organizacijos informacinių technologijų infrastruktūrai ir duomenų saugumui. Todėl efektyvus trečiųjų šalių rizikos valdymas apima jų saugumo praktikų auditą, saugumo reikalavimų nustatymą sutartyse, nuolatinę trečiųjų šalių priežiūrą ir atitikimo vertinimą, teisinių reguliavimų normų laikymosi, taip pat atsako už incidentų planų rengimą ir dar daug kitų aspektų, atsižvelgiant į trečiųjų šalių sukeltas grėsmes.

Pasitelkiant teisiniu reglamentavimu, kibernetinio saugumo žiniomis, praktikomis bei kibernetinio saugumo valdymo modeliais sukuria kibernetinio saugumo kultūra ir padeda gerinti kibernetinę brandą. Kibernetinės saugumo grėsmės susijusios su trečiųjų šalių valdymu turi būti sprendžiamos ir minimizuojamos.

Išnagrinėjus įvairius kibernetinio saugumo valdymo modelius, aiškėja, kad jie yra esminiai siekiant užtikrinti kibernetinį saugumą įvairiose organizacijose, įskaitant valstybės institucijas, privačias įmones ir gynybos sektoriaus subjektus. Kibernetinio saugumo valdymo modelių integravimas su trečiųjų šalių (third party) valdymu yra svarbus aspektas, užtikrinant išsamią organizacijos apsaugą. Kai organizacijos bendradarbiauja su išoriniais tiekėjais ar partneriais, atsiranda papildomų rizikos veiksnių, susijusių su duomenų saugumu ir tinklo apsauga. Modeliai pabrėžia fizinių, technologinių ir administracinių saugumo priemonių integravimą, atspindint būtinybę turėti išsamius vidaus protokolus, atitinkančius teisinę bazę ir organizacijos strategiją. Šiuolaikinėje informacinėje visuomenėje technologinės saugumo priemonės yra ypač akcentuojamos, nors dauguma modelių yra technologiškai neutralūs. Nepaisant to, kibernetinio saugumo kultūra ir personalo valdymo aspektai dažnai lieka nepakankamai išsamūs, išskyrus NIST modelį, kuris išryškina darbuotojų švietimą ir bendradarbiavimą su išoriniais partneriais. Visi modeliai remiasi veiksmų planavimo ir įgyvendinimo

ciklu (Plan-Do-Check-Act), kuris yra būtinas visoms organizacinėms veikloms, tačiau NIST išsiskiria savo brandumo lygių nustatymu, skatinančiu organizacijas siekti aukštesnio kibernetinio saugumo vystymosi. Palyginus su kitais modeliais NIST modelis atrodo labiausiai tinkamas dėl jo gebėjimo prisitaikyti prie nuolat kintančios kibernetinės aplinkos, skatinant organizacijas tapti lankstesnėmis ir atsparesnėmis prieš naujas grėsmes.

Fiziniai saugumo sprendimai yra esminis apsaugos sluoksnis, skirtas užkirsti kelią neautorizuotam patekimui į įmonės kompiuterines sistemas iš išorės, tad tai turėtų būti nepamirštas saugumo domenas kalbant apie informacines technologijas. Šios fizinės apsaugos priemonės paprastai derinamos su informacijos saugumo sprendimais, tokiomis kaip tapatybės valdymas, prieigos kontrolė ir įsilaužimo aptikimo sistemos, formuodamos pirmąją gynybos liniją nuo potencialių grėsmių ir apsaugodamos organizacijos konfidencialią informaciją bei išteklius.

Priedas 1

TOP 8 svarbiausios kibernetinio saugumo grėsmės 2022 metais

Figure 1: ENISA Threat Landscape 2022 - Prime threats

Šaltinis: Europos Sąjungos kibernetinio saugumo agentūra ENISA

Priedas 2

TOP 10 svarbiausios kibernetinio saugumo grėsmės 2030 metais

Šaltinis: Europos Sąjungos kibernetinio saugumo agentūra ENISA