MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

RYTIS GASPARAVIČIUS
KIBERNETINIO SAUGUMO VALDYMAS

KIBERNETINIO SAUGUMO VERSLO SPRENDIMŲ MODELIAVIMAS IR PLĖTRA

Magistro baigiamasis darbas

Vadovas: **Prof. dr. T. Limba**

Vilnius, 2024

MYKOLAS ROMERIS UNIVERSITY

FACULTY OF PUBLIC ADMINISTRATION AND BUSINESS

INSTITUTE OF BUSINESS AND ECONOMY

RYTIS GASPARAVIČIUS

CYBER SECURITY MANAGEMENT

MODELING AND DEVELOPMENT OF CYBER SECURITY BUSINESS SOLUTIONS

Master Thesis

Supervisor: **Prof. dr. T. Limba**

Vilnius, 2024

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

SANTRUMPOS IR SĄVOKOS

1. **EU** - Europos Sąjunga (angl. k. European Union).
2. **JAV** - Jungtinės Amerikos Valstijos (angl. k. United States of America).
3. **CIA** - Konfidencialumas, vientisumas, prieinamumas (angl. k. Confidentiality, Integrity, and Availability).
4. **GRC** - Valdymas, Rizikos Valdymas ir Atitiktis (angl. k. Governance, Risk Management, and Compliance)
5. **BMC** - Verslo Modelio Drobė (angl. k. Business Model Canvas)
6. **CIS** – Kritinės Saugumo Kontrolės (angl. k. Center for Internet Security Controls)
7. **NIST** - Nacionalinis Standartų ir Technologijų Institutas (angl. k. National Institute of Standards and Technology)
8. **PCI DSS** - Mokėjimo Kortelių Pramonės Duomenų Saugumo Standartas (angl. k. Payment Card Industry Data Security Standard)
9. **ISO/IEC 27001** - Informacijos Saugumo Valdymo Sistemos Standartai (angl. k. International Organization for Standardization/International Electrotechnical Commission 27001)
10. **GDPR** - BDAR Bendrasis Duomenų Apsaugos Reglamentas (angl. k. General Data Protection Regulation)
11. **APT** - Pažangiosios Nuolatinės Grėsmės (angl. k. Advanced Persistent Threats)
12. **ENISA** - Europos Sąjungos Tinklo ir Informacijos Saugumo Agentūra (angl. k. European Union Agency for Cybersecurity)
13. **OCEG** - Atviroji Atitikties ir Etikos Grupė (angl. k. Open Compliance and Ethics Group)
14. **IDS** - Įsibrovimo aptikimo sistema (angl. k. Intrusion Detection System).
15. **IPS** - Įsibrovimo prevencijos sistema (angl. k. Intrusion Prevention System).
16. **IT** - Informacinės technologijos (angl. k. Information Technology).
17. **IoT** - Daiktų internetas (angl. k. Internet of Things).
18. **DLP** - Duomenų nuotėkio prevencija (angl. k. Data Loss Prevention).
19. **SOC** - Saugumo operacijų centras (angl. k. Security Operations Center).
20. **VPN** - Virtualus privatusis tinklas (angl. k. Virtual Private Network).
21. **Kill Chain** - Kibernetinės atakos vektorius (angl. k. Cyber Kill Chain)
22. **C&C (Command and Control)** - Valdymo ir kontrolės serveris (angl. k. Command and Control)

Magistro baigiamojo darbo tema – „Kibernetinio saugumo verslo sprendimų modeliavimas ir plėtra“
Magistro baigiamojo darbo vadovas – prof. Dr. Tadas Limba
Magistrinio darbo išplėstinis planas:

ĮVADAS

Temos aktualumas. Šiais laikais spartus skaitmeninis ir technologinis proveržis pakeitė įmonių veiklas ir sukūrė naujus vertės kūrimo ir mainų būdus, tačiau stiprėjant organizacijų tarpusavio ryšiams kyla kibernetinių grėsmių pavojus gyvybiškai svarbiems veiklos aspektams. Daugeliui yra svarbu suprasti ryšį tarp verslo modeliavimo ir kibernetinio saugumo, ir kaip jų susiliejimas gali lemti tvirtesnius kibernetinio saugumo verslo sprendimus.

Žvelgiant kitaip, kiekvienas iš mūsų esame tam tikros informacijos nešiotojai ir taip pat, vienaip ar kitaip esame susiję su verslais ir įvairiomis organizacijomis, ja dalindamiesi, ar patikėdami ją saugoti. Mokslininkai tyrinėjantys kibernetinį saugumą pripažįsta, kad žmogiškasis faktorius laikomas didžiausia kibernetinio saugumo spraga. Todėl šiame moksliniame projekte vyraus platus požiūris į verslo modeliavimą ir kibernetinį saugumą. Šių elementų sąveikų išaiškinimas sukurs aiškesnį paveikslą ne tik šių sričių specialistams ar mokslinei bendruomenei, bet ir paprastam žmogui.

Šiame mokslo darbe bandysime išsiaiškinti svarbiausias verslo modelių sudedamąsias dalis ir jų pokyčių tendencijas. Vėliau bandysime susipažinti su kibernetinio saugumo sritimi, įvertinti naujausias kibernetinio saugumo praktikas ir geriausius pavyzdžius.

Tyrimo metu bus siekiama išnagrinėti ir atpažinti pagrindinius verslo modelių komponentus bei jų evoliucijos tendencijas. Taip pat bus gilinamasi į kibernetinio saugumo sritį, analizuojamos naujausios šios srities praktikos ir pavyzdžiai. Bus mėginama suprasti, kaip kibernetinį saugumą galima integruoti į verslo modelį, bus ieškoma atsakymų, kaip organizacijos galėtų efektyviau apsaugoti savo veiklą nuo kibernetinių grėsmių ir tuo pačiu sukurti pridėtinę vertę.

Šis tyrimas bus atliktas taikant mišrią metodiką, apimančią literatūros analizę, atvejų studijas bei ekspertų interviu. Siekiama išgryninti praktines gaires ir strategijas, kurios padėtų organizacijoms užtikrinti ilgalaikį sėkmingą veikimą, atsižvelgiant į dinamiškai kintančią kibernetinės saugos aplinką.

Temos naujumas/ teorinis reikšmingumas. Šios temos mokslinės naujovės ir teorinis aktualumas grindžiamas verslo modeliavimo ir kibernetinio saugumo sankirtos nagrinėjimu bei kibernetinio saugumo verslo sprendimų kūrimu. Tai svarbi tema, nes mokslinės literatūros Lietuvoje tiriančios šių dviejų dalykų sankirta mažai, todėl išnagrinėjus dabartinę kibernetinio saugumo padėtį

įmonėse ir efektyviausius duomenų bei išteklių apsaugos metodus, šiuo tyrimu praturtinsime mokslinę literatūrą.

Šis mokslinis darbas suteiks vertingą įnašą į mokslinę literatūrą, atskleisdamas naujausias tendencijas ir efektyviausias praktikas šioje srityje. Tai neabejotinai prisidės prie verslo ir technologijų srities pažinimo, teikdamas pagrindą būsimiems tyrimams ir suteikdamas naudingas žinias šiose srityse dirbantiems specialistams bei padidins supratimą apie šių dviejų sričių sąveikos svarbą.

Mokslinė problema – Kaip galima ištirti verslo modeliavimo ir kibernetinio saugumo sankirtos svarbą?

Tyrimo objektas – Kibernetinio saugumo verslo sprendimų modeliavimas

Tyrimo dalykas – Kibernetinio saugumo įmonių paslaugų aktualumas Lietuvos verslui

Projekto tikslas – Ištirti verslo sprendimų modeliavimo ypatumus ir sukurti teorinį kibernetinės saugos verslo modelį.

Projekto uždaviniai:

1. Ištirti ryšį tarp verslo modeliavimo ir kibernetinio saugumo.
2. Išnagrinėti efektyvių kibernetinio saugumo sprendimų verslui kūrimą.
3. Identifikuoti pagrindinius sėkmingo verslo modelio komponentus ir šios srities iššūkius bei tendencijas.
4. Ištirti dabartinę kibernetinio saugumo būklę versle ir geriausią informacijos ir turto apsaugos praktiką.
5. Pateikti praktines gaires organizacijoms, norinčioms užsitikrinti savo ateitį skaitmeniniame amžiuje.

Duomenų rinkimo metodai:

1. Mokslinės literatūros sisteminimas, analizė, palyginimas.
2. Atvejų analizė.
3. Ekspertinis pusiau struktūrizuotas struktūruotas interviu (kokybinio tyrimo strategija).

Duomenų analizės metodai:

1. Kokybinė turinio analizė.
2. Pusiau struktūrizuoto interviu kokybinė turinio analizė ir interpretavimas.
3. Lyginamoji gautų duomenų analizė.

1. VERSLO MODELIAVIMO TEORINIAI ASPEKTAI.

Šiuolaikiniame versle, intensyviai veikiamame technologinių naujovių ir nuolat besikeičiančių komunikacijos būdų, tradicinių verslo modelių modernizavimas tampa neišvengiamas. Šie pokyčiai neabejotinai įtakoja įmonių strateginius sprendimus, operacijas ir siekiamus tikslus, iškelia reikalavimą būti lanksčiais ir gebėti prisiderinti prie rinkos kaitos.

Verslo modelis, kaip teorinis konstruktas nagrinėtas daugelio Lietuvos ir užsienio autorių. Todėl šiame skyriuje bus išnagrinėta detaliai sampratos raida, pritaikomumas ir reikšmė formuojant verslo strategijas. Taip pat bus pristatyti įvairūs praktiniai verslo modelių kūrimo ir taikymo pavyzdžiai, apibendrinant, kaip jie galėtų veikti organizacijų finansinius rezultatus ir jų pozicijas konkurencinėje rinkoje.

1.1.Verslo modelio apibrėžimas.

Verslas apibūdinamas kaip organizuota veikla, kurios pagrindinis tikslas – sukurti ir parduoti prekes ar paslaugas, siekiant pelno. Ši veikla apima visus etapus: nuo idėjos gimimo iki galutinio produkto ar paslaugos pateikimo rinkai. Tačiau verslo veiklą lydi ne tik pelno generavimas, svarbios yra ir kitos sudedamosios dalys tokios kaip: organizacijos struktūra, strateginė kryptys, rinkodaros iniciatyvos, klientų poreikių suvokimas ir jų tenkinimas V. Bagdžiūnienė (2011). Ši veikla yra esminė ekonomikos dalis, prisidedanti prie visuomenės gerovės ir ekonominio augimo. Kaip matyti iš šio aprašymo verslą sudaro tam tikri elementai, moduliai.

Vertinant verslo modelio sąvoką, reikėtų įsigilinti ir ką reiškia sąvoka „modelis“. Modelis[1], pasak Vytauto Bujausko, Leono Simanausko ir Rimvydo Skyriaus (2009) (lot. modulus-matas) – tai originalaus objekto pakaitalas. Modelis yra vertingas įrankis, leidžiantis išgryninti ir išryškinti esmines originalo ypatybes, sutelkiant dėmesį į tyrėjui svarbiausius aspektus. Jis padeda mums suvokti verslo modelį ne tik kaip abstraktų terminą, bet kaip praktiškai taikomą struktūrinį įrankį. Modelio pagalba galima sistemingai analizuoti ir suprasti verslo komponentus bei procesus, kas yra būtini norint efektyviai valdyti verslo veiklą.

Prieš pereinant prie verslo modelio apibrėžimo, verta paminėti, kad susidomėjimas verslo modelių tyrimais auga ir tai rodo šių temų tyrimų gausą akademiniuose leidiniuose. Verslo modelio samprata ir apibrėžtis yra analizuojama tiek Lietuvos (Kinderis (2012); Kinderis, Jucevičius (2013); Burinskienė, Daškevič (2013), tiek užsienio ((Chesbrough, Rosenbloom (2002); Magretta (2002); Osterwalder

[1] Originalai ir modeliai. Modeliuojant visada yra dviejų rūšių objektai: originalai, kuriuos reikia tirti, ir modeliai kuriuos tiriame vietoje originalų. Originalus keičiame modeliais norėdami supaprastinti, pagreitinti, atpiginti originalo ar jame vykstančių procesų nustatymą ar tyrimą. V. Bujausko, L. Simanauskas, R.Skyrius „Kompiuterinis sprendimų modeliavimas“ p.13, (2009)

(2004); Chesbrough (2007); D.Teece (2010); Osterwalder ir Pigneur (2010); Baden-Fuller, Morgan 10 2010); George, Bock (2011); R.Cassadesus-Masanell, J.Ricart (2015); Raphael Amit, Christoph Zott (2020); B.W. Wirtz (2020)) autorių.

Verslo modeliai yra tiriami įvairiais aspektais, įskaitant elektroninį verslą, inovacijas ir naujus verslo metodus, tačiau trūksta autorių vieningo sutarimo, kas išties tai yra. Terminai, tokie kaip „*verslo modelis*“, „*strategija*“ dažnai painiojami tarpusavyje, netinkamai vartojami kaip sinonimai (Magretta 2002). Nors kai kurie autoriai laiko verslo modelio apibrėžimus pernelyg abstrakčiais, nes jie apima daugybę verslo vadybos aspektų, šie apibrėžimai išlieka svarbūs, suteikiantys aiškumą ir struktūrą, būtiną verslo procesams ir strategijai suprasti (Osterwilder ir Pigneur 2010).

Būtina suprasti, kad verslo modelio sąvoka yra nevienareikšmiškai traktuojama ir nuolatos keičiasi. Įvairūs autoriai siūlo skirtingas šios sąvokos apibrėžimus, kurie atspindi jų individualius požiūrius į verslą, jo vykdomuosius principus ir strategiją. Todėl, norint išsiaiškinti verslo modelio sampratos įvairovę, būtina atlikti mokslinės literatūros analizę, išryškinant pagrindinius sąvokos raktažodžius ir konceptus. Ši analizė padės suprasti, kaip įvairūs autoriai supranta ir apibrėžia verslo modelį bei išskiria svarbiausias šios sąvokos dedamąsias dalis (žr. 1 lentelę.).

1 Lentelė. Lentelė „Verslo Modelio Apibrėžimai“

Autoriai	**Metai**	**Verslo Modelio Apibrėžimas**	**Raktažodžiai**
Magretta	2002	Būdas, kaip organizacija sukuria ir realizuoja vertę.	Organizacija, vertė.
Chesbrough, Rosenbloom	2002	Konstruktas tarpininkaujant vertės kūrimo procese.	Tarpininkavimas, vertė.
R. G. McGrath	2009	Verslo modelio konstrukcija siūlo keletą intriguojančių galimybių geriau užfiksuoti, kaip tam tikras išteklių rinkinys virsta tuo, už ką klientas nori mokėti.	Verslo konstrukcija, išteklių rinkiniai, vertė.
D. Teece	2010	Verslo modelis, apibūdinantis jame naudojamų vertės kūrimo, pristatymo ir fiksavimo mechanizmų dizainą arba architektūrą.	Vertės kūrimo koncepcija, architektūra, vertės pristatymo ir fiksavimo dizainas.
Osterwalder, Pigneur	2010	Verslo modelis yra įrankis, kuris sudaro esminius verslo elementus ir jų tarpusavio ryšius, atspindėdamas specifinę įmonės logiką. Jis apibūdina, kaip įmonė sukuria	Kainos nustatymas, tikslinis klientas, paskirstymo kanalai, ryšiai, kainos

		ir pateikia vertę savo klientams, apimančią verslo struktūrą, partnerių tinklą, siekiant užtikrinti pelningumą ir nuoseklius pajamų srautus.	konfigūracija, pagrindinės kompetencijos, partnerių tinklas, sąnaudų struktūra, pajamų modelis.
Amit, Zott	2010	Verslo veiklos sistemos charakteristikos: turinys, struktūra ir valdymas.	Veiklos turinys, struktūra, valdymas.
Burinskienė, Daškevič	2013	Verslo modelis, susijęs su įmonės struktūra, prekybos praktikomis ir veiklos procesais.	Įmonės struktūra, prekybos praktikos, veiklos procesai.
Kinderis, Jucevičius	2013	Verslo modelis yra pagrindine įmonės veiklos logika, aiškinančia vertės kūrimo procesą ir pajamų generavimą.	Inovacija, vadybos disciplina, veiklos logika, vertė, pajamų generavimas.
R.Cassadesus-Masanell, J.Ricart	2015	Verslo modelis – tai vadovybės priimtų sprendimų visuma, kuri nulemia verslo procesų eigą, teikiamas prekes ar paslaugas. Šie sprendimai apima politikos, turto ir valdymo aspektus: nuo darbo jėgos pasirinkimo, įmonės vietos nustatymo iki įrangos bei technologijų panaudojimo.	Sprendimų sistema, technologijų naudojimas, organizaciniai sprendimai, veiklos procesai.
B.W. Wirtz	2020	Verslo modelis susideda iš penkių pagrindinių etapų: projektavimo, įgyvendinimo, veikimo, pritaikymo ir modifikavimo bei valdymo	Projektas, įgyvendinimas, veikimas, pritaikymas ir modifikavimas, valdymas.

Šaltinis: sudarytas autoriaus, remiantis Joan Magretta (2002), Chesbrough, Rosenbloom (2002), D. Teece (2009), R. G. McGrath (2009), Osterwalder, Pigneur (2010), Amit, Zott (2010), Burinskienė, Daškevič (2013), Kinderis, Jucevičius (2013), R.Cassadesus-Masanell, J.Ricart (2015), B.W. Wirtz (2020).

Analizuojant įvairių autorių darbus apie verslo modelius, pastebima, kad nors kiekvienas mokslininkas pateikia savitą verslo modelio sampratą, keli pagrindiniai bruožai išlieka bendri ir būdingi visoms interpretacijoms:

1. **Vertės kūrimas ir pateikimas:** Beveik visi autoriai pabrėžia, kad verslo modelis yra glaudžiai susijęs su vertės kūrimu ir jo pristatymu vartotojui. Tai rodo, kad verslo modelis veikia kaip dinaminė priemonė, padedanti organizacijai nustatyti, kaip sukurti ir pristatyti vertę, atitinkančią klientų lūkesčius ir poreikius.
2. **Strateginiai sprendimai ir veiklos procesai:** Dauguma apibrėžimų akcentuoja verslo modelio vaidmenį organizuojant įmonės veiklą ir priimant strateginius sprendimus. Sprendimus susijusius su įmonės struktūra, rinkodara, partnerių santykiais, resursų paskirstymu ir veiklos efektyvumu.
3. **Sąveika su rinka ir klientais:** Verslo modelis glaudžiai susijęs su įmonės sąveika su rinka ir klientais. Svarbu, kad įmonės ne tik suprastų klientų lūkesčius, bet ir gebėtų greitai bei veiksmingai atsiliepti į jų poreikius.
4. **Pelningumo ir tvarumo užtikrinimas.** Galiausiai, verslo modelis yra būtinas norint užtikrinti ilgalaikį įmonės pelningumą ir tvarumą. Tai apima ne tik pelno generavimą, bet ir suteikia įmonei gebėjimą lanksčiai prisitaikyti prie besikeičiančių rinkos aplinkybių ir naudotis atsirandančiomis naujomis galimybėmis.

Literatūros analizė atskleidė skirtingus autorių požiūrius į verslo modelio sampratą, iš kurios matyti, kad nepaisant skirtingų interpretacijų, verslo modelis išlieka kompleksinė ir daugiasluoksnė struktūra.

1 Pav. Bendra verslo modelių bruožų sąveika

Šaltinis: Sukurta Autoriaus

Visgi daugelis autorių sutinka, kad formalioje kalboje dauguma žmonių painioja [2]„Verslo Modelio“ ir „Verslo Strategijos“ sąvokas, kartais išsireikšdami, kad tai yra vienas ir tas pats (Magretta 2002,

[2] Tačiau verslo modelis nėra tas pats, kas strategija, nors daugelis žmonių šiandien vartoja terminus pakaitomis. Magretta 2002 „Why do business models matter“. “Tačiau daugumoje tyrimų nepavyksta aiškiai atskirti verslo modelio nuo gautų

Gerard George, Adam Jay Block 2009, R. Kinderis, G. Jucevičius 2012,),todėl būtų naudinga atskleisti skirtumus tarp šių dviejų sąvokų.

Išanalizavus įvairių autorių požiūrius į verslo modelio sampratą ir palyginus juos su verslo strategijos koncepcija, išryškėja esminiai skirtumai tarp šių dviejų sąvokų. **Verslo modelis**, kaip jau minėta, yra daugiasluoksnis ir kompleksinis konceptas, apibūdinantis įmonės veiklos struktūrą, jos elementų sąveiką ir vertės kūrimo mechanizmus. Kitaip tariant***, verslo modelis atskleidžia, kaip įmonė sujungia savo išteklius, procesus ir veiklas siekdama sukurti ir pristatyti vertę savo klientams***.

Tuo tarpu **verslo strategija** yra glaudžiai susijusi su konkurencine aplinka ir atsako į klausimą, kaip įmonė ketina išsiskirti ir būti pranašesnė už konkurentus (M.E. Porter 1998, Magrett 2002). Strategija apibrėžia unikalų požiūrį ir metodiką, kaip įmonė siekia aukštesnių rezultatų ir efektyviau konkuruoja rinkoje (Casadesus-Masanell, Ricart 2010). Tai reiškia, kad ***verslo strategija įtraukia konkurencijos analizę ir sprendimus, kurie padeda įmonei pasiekti pranašumą prieš konkurentus***, pvz., pasirenkant specifines rinkas, klientų segmentus arba unikalius produktus ir paslaugas. Svarbu suprasti, kad verslo modelis ir strategija nors ir yra tarpusavyje susiję, tačiau atlieka skirtingas funkcijas įmonės veikloje. Pasak Remigijaus Kinderio (2012) „verslo modelis[3] yra tai, kas sujungia strategiją ir jos įgyvendinimą bei yra verslo koncepcijos esmė, kuri vėliau perkeliama ir į praktiką“. Kitaip tariant, strategija yra planas, pagal kurį verslo modelis yra adaptuojamas.“

1.2.Verslo modeliavimo tendencijos ir iššūkiai

Šiuolaikinėje rinkoje veikiančios įmonės, tiek senosios, tiek naujai atsiradusios, susiduria su iššūkiais, kaip išsiskirti ir pristatyti vertę savo klientams naujais būdais. Technologinių pokyčių aplinkoje verslai skatinami ne tik prisitaikyti, bet ir pirmauti inovacijų srityje. Jie kuria unikalius verslo modelius ir sprendimus, kurie atsako į šiuolaikinio vartotojo lūkesčius ir prisitaiko prie greitai kintančios rinkos.

Tačiau kaip sistemingai ištirti naujas idėjas norint efektyviai sukurti ir įgyvendinti verslo modelius? Kaip kritiškai įsivertinti esamas praktikas, jei jos gali būti nebeaktualios dabartinėje rinkoje?

Norint efektyviai spręsti verslo iššūkius, buvo sukurti įvairūs verslo modeliavimo ir strategijos analizės įrankiai. Šie metodai leidžia organizacijoms geriau suprasti vidinius ir išorinius veiksnius, kurie yra itin svarbūs kuriant ir tobulinant veiksmingus verslo modelius:

organizacinių konstrukcijų, tokių kaip strategija“ G. George, A.J.Block 2009. Verslo modelis nėra strategija, tačiau jis apima daugelį strategijai būdingų elementų R.Kinderis, G.Jucevičius 2012

[3] „Verslo modeliai – jų semantinė raiška ir struktūrą“. Ekonomika ir vadyba: aktualijos ir perspektyvos. 2012. 1 (25). 17–27 R. Kinderis

1. **SWOT Analizė** (S.S.G.G liet. Stiprybės, Silpnybės, Galimybės, Grėsmės) Albert Huphrey (1960-1970): Šis analizės būdas padeda įvertinti įmonės stipriąsias ir silpnąsias puses, galimybes bei grėsmes.
2. **Porterio Penkių Jėgų Modelis**: Michael Porterio (1979) sukurtas modelis, padedantis suprasti pramonės konkurencinę aplinką per penkias jėgas: konkurentų tarpusavio sąveiką, potencialių naujų konkurentų grėsmę, pakaitalų grėsmę, derybų galią tiekėjų atžvilgiu ir derybų galią klientų atžvilgiu.
3. **PEST Francis Aguilar** (1960) Analizė (Political, Economic, Social, Technological): Ši analizė įvertina makroaplinkos veiksnius ir jų poveikį verslui – politinius, ekonominius, socialinius ir technologinius.
4. **Ansoffo Matrica** Igor Ansoff (1965): Fokusuojasi į rinką ir produktų derinius augimui skatinti, apibrėždama keturias strategijas: įskverbimą į rinką, rinkos plėtrą, produktų plėtrą ir diversifikaciją.

Nors šie įrankiai suteikia svarbų pagrindą verslo analizei, pastaruoju metu verslo atstovų ir mokslo bendruomenės dėmesys krypsta į labiau dinamiškesnes metodikas.

Viena tokių – Alexander Osterwalder ir Yves Pigneur (2006) sukurtas „**Business Model Canvas**“. Ši metodika, pasak Osterwalderio (2010) „suteikia galimybę vadovams aiškiai užfiksuoti, suprasti ir keisti įmonės verslo logiką. Ji leidžia integruoti tiek vidinius, tiek išorinius veiksnius, atskleidžiant naujas galimybes įmonės tobulinimui ir inovacijoms."

'Business Model Canvas' (B.M.C.) yra vienas iš labiausiai pripažintų įrankių verslo modeliavime. Platus naudojimas ir teigiami atsiliepimai iš įvairių sričių ekspertų patvirtina metodikos efektyvumą ir pritaikomumą įvairiose verslo aplinkose ir situacijose.

2 Pav. Verslo Modelio Drobė

Šaltinis: Osterwalder, Pigneur (2010) iš Anglų kalbos vertė autorius

Prieš išsamiai nagrinėjant "Business Model Canvas" (BMC[4]) segmentus, svarbu pabrėžti, kad šis įrankis yra tarsi paveikslo drobė, padedanti plėtoti ir struktūruoti verslo modelį. Ji leidžia organizacijoms vizualiai suderinti pagrindines veiklas ir strategijas, būtinas sėkmingai veiklai rinkoje. "Business Model Canvas" yra esminė įmonės strateginio planavimo dalis, padedanti identifikuoti sritis, kuriose galima sukurti didžiausią vertę ir efektyviausiai išnaudoti verslo potencialą. Kaip pavaizduota 2 Paveikslėlyje „Verslo Modelio Drobę“ sudaro devyni svarbiausi segmentai:

1. Klientų segmentai;
2. Siūloma vertė;
3. Pristatymo kanalai;
4. Santykiai su klientais;
5. Pajamų struktūra;
6. Pagrindiniai ištekliai;
7. Pagrindinės veiklos;
8. Pagrindiniai partneriai;
9. Sąnaudų struktūra;

Klientų segmentavimas suteikia organizacijoms galimybę klasifikuoti ir giliau suprasti savo klientų grupes. Segmentuojant klientus, atsižvelgiama į įvairias charakteristikas, tokias kaip geografinė padėtis, demografiniai duomenys, elgsena, poreikiai, pajamų dydis ir pirkimo įpročiai. Pavyzdžiui, jauniems vartotojams gali būti siūlomi inovatyvūs produktai, o vyresniems klientams – patikimi ir ilgaamžiai sprendimai. Sėkmingas klientų segmentavimas leidžia įmonėms nustatyti efektyviausius rinkodaros kanalus, tinkamiausius bendravimo būdus ir optimaliausias kainodaros strategijas užtikrinant efektyvesnį resursų panaudojimą ir didesnį klientų pasitenkinimą (Osterwalder, Pigneur 2010). Taip pat segmentavimas padeda atpažinti pelningiausias klientų grupes ir nukreipti pastangas į jų poreikių patenkinimą, taip maksimizuojant verslo žinomumą, sėkmę ir augimą.

Siūloma vertė Siūloma vertė yra vienas svarbiausių „BMC“ elementų, suteikiantis įmonei išskirtinumą ir patrauklumą. Jis apibrėžia unikalią vertę, kurią įmonė siūlo savo klientams ir kuri tampa pagrindine jų pasirinkimo priežastimi. Siūloma vertė gali varijuoti – nuo inovatyvių produktų iki aukščiausios kokybės paslaugų, unikalios klientų aptarnavimo patirties ar konkurencingos kainos.. Efektyviai suformuluota siūloma vertė padeda išsiskirti rinkoje, pritraukti ir išlaikyti klientus, taip pat įtvirtinti įmonės pozicijas konkurencingoje aplinkoje. Pasak Steve Jobs [5](2007) „*Įmonės, kurios geba aiškiai komunikuoti savo siūlomą vertę, dažnai turi didesnį klientų lojalumą ir didesnes pajamas*.“

[4] Verslo modelio drobė (trumpinys BMC), (Angl k. vertimas „Business Modeling Canvas“)
[5] S.Jobs interviu apie marketinga ir vertės pasiūlymą : https://www.youtube.com/watch?v=4mvHgLy_YV8

Pristatymo kanalai skirti nustatyti, kaip įmonė pateikia ir pristato savo produktus, ir paslaugas klientams. Tai apima visas priemones ir būdus, per kuriuos įmonė komunikuodama su klientais pateikia savo vertės pasiūlymą. Kanalai gali būti įvairūs: nuo tradicinės parduotuvės iki internetinės prekybos, socialinių tinklų ar tiesioginio pardavimo. Efektyvūs pristatymo kanalai didina klientų pasiekiamumą, gerina vartotojų patirtį bei skatina pardavimus. Svarbu, kad šie kanalai būtų suderinti su įmonės bendru verslo modeliu ir kliento poreikiais. Pristatymo kanalai atlieka kelias funkcijas:

- Padeda klientams įvertinti įmonės vertės pasiūlymą t.y. jos produktus ir paslaugas;
- Leidžia klientams įsigyti atpažįstamų produktų ir paslaugų;
- Budas kuriuo įmonėms pristato savo vertės pasiūlymą;

Santykiai su klientais yra vienas svarbiausių verslo modelio segmentų, kuris tiesiogiai susijęs su įmonės sąveika skirtingais klientais. Šis ryšys atspindi įmonės siekį užtikrinti ilgalaikį klientų lojalumą ir jų pasitikėjimą. Įmonės formuoja ir palaiko ryšius su klientais įvairiais būdais, nuo asmeninio dėmesio iki automatizuotų paslaugų, įskaitant lojalumo programas, klientų aptarnavimo paslaugų ir individualizuotų bendravimo strategijų. Efektyvūs santykiai ne tik skatina pakartotinius pardavimus, bet ir stiprina prekės ženklo teigiamą įvaizdį rinkoje. Pavyzdžiui, įmonė „Apple“ išsiskiria ypatingu klientų aptarnavimu ir asmeniniu dėmesiu klientų poreikiams, kas suteikia jai konkurencinį pranašumą. Stiprūs klientų santykiai leidžia įmonėms išlaikyti esamus klientus ir pritraukti naujus, formuojant patikimą ir lojalią klientų bazę.

Pajamų srautai yra vienas esminių verslo modelio segmentų, nurodantis kaip įmonė uždirba pajamas. *„Jeigu vartotojai yra verslo modelio „širdis“, tai pajamų srautai yra jos „arterijos“*, įvardina Osterwalder (2010). Kiekvienas pajamų kanalas gali turėti skirtingas strategijas nuo pardavimų ir prenumeratų iki reklamos, ir licencijavimo. Pavyzdžiui, įmonė gali generuoti pajamas tiesiogiai pardavinėdama produktus, arba per abonementus, suteikiančius nuolatinį pajamų srautą. Tinkamai valdomi pajamų srautai yra būtini siekiant užtikrinti verslo tvarumą ir augimą. Svarbu, kad šie pajamų modeliai būtų suderinti su įmonės vertės pasiūlymu ir klientų segmentais, siekiant maksimalaus efektyvumo ir pelningumo. Pavyzdžiui, įmonės kaip "Netflix[6]" (S.Hansen 2021) ar "Spotify[7]" (P.J.Parson 2018) pasinaudojo prenumeratos modeliu, siekdamos pastovaus pajamų srauto, o "Amazon" kombinuoja pardavimus su prenumerata ir reklama, sukurdama įvairiapusišką pajamų modelį.

Pagrindiniai ištekliai yra tie esminiai komponentai, kurie reikalingi įmonei sėkmingai veikti. Tai apima fizinę infrastruktūrą, tokią kaip gamybos įrenginiai, biuro patalpos, žmogiškuosius išteklius, įskaitant darbuotojus ir jų kompetencijas, taip pat intelektinę nuosavybę, pavyzdžiui, patentus, technologijas ir autorių teises.

[6] „Netflix“ yra amerikietiška prenumeruojama vaizdo įrašų srautinio perdavimo paslauga pagal pareikalavimą.
[7] „Spotify“ vienas didžiausių muzikos srautinio perdavimo paslaugų teikėjų, turintis daugiau nei 590 milijonų aktyvių naudotojų per mėnesį 2023.

Pagrindinės veiklos apima esminius procesus, kurie lemia, kaip įmonė savo veiklą paverčia realiais rezultatais. Jos apima ne tik produktų kūrimą ar rinkodarą, bet ir kasdienes operacijas, kaip klientų aptarnavimas ar tiekimo grandinės priežiūrą. Svarbu yra tai, kad šios veiklos turi būti glaudžiai susijusios su įmonės siekiais ir vertybėmis, kad galėtų teikti nuoseklią ir vertingą patirtį klientams. Tinkamas šių veiklų valdymas ir tobulinimas yra raktas į ilgalaikį įmonės augimą ir konkurencinį pranašumą.

Svarbiausi partneriai verslo modelyje apima tiek tiekėjus, tiek kitas organizacijas, su kuriomis įmonė bendradarbiauja siekdama sėkmės. Šie partneriai gali padėti sumažinti riziką ir išlaidas, pasidalinti žiniomis ir resursais arba padėti pasiekti naujas rinkas. Efektyvus ir abiems šalims naudingas bendradarbiavimas su partneriais gali būti lemiamas veiksnys, siekiant verslo tikslų ir užtikrinant ilgalaikį verslo modelio tvarumą. Vienas iš pavyzdžių, kaip mažai žinoma įmonė išaugo dėl svarbių partnerystės ryšių, gali būti "Dropbox". Pradžioje nedidelė startuolio kompanija, kuri vystė duomenų saugojimo „debesų kompiuterijoje“ sprendimus pasiekė didelį augimą ir populiarumą, bendradarbiaudama su didelėmis technologijų kompanijomis, tokiomis kaip "Samsung" ir "HP", integruodama savo paslaugas į jų prietaisus. Šis bendradarbiavimas ne tik padidino "Dropbox" matomumą, bet ir suteikė prieigą prie didelės klientų bazės, kas buvo lemiamas veiksnys jų augimo istorijoje J.C. Perez „Cumputerworld“ (2014).

Sąnaudų struktūra. Šiame segmente analizuojama, kokios sąnaudos yra susijusios su įmonės veikla ir kaip jos turi įtakos bendram verslo efektyvumui. Sąnaudos gali būti suskirstytos į tiesiogines, pvz., žaliavų pirkimas, darbuotojų atlyginimai ir netiesiogines pvz., marketingas, nuoma, administracinės išlaidos. Efektyvus sąnaudų valdymas yra būtinas norint išlaikyti verslo pelningumą ir konkurencingumą rinkoje Osterwalder, Pigneur (2010).

Atlikus išsamų Osterwalder, Pigneur "BMC" dimensijų analizę, įmonė galėtų aiškiai suprasti savo verslo modelio stipriąsias, silpnąsias puses ir atrasti naujų galimybių. Kaip teigė Trimble (2015) „*Dėl vaizdinio ir kartotinio BMC drobės pobūdžio net studentai, turintys ribotą kontaktą su verslu, gali suvokti konkretaus verslo pranašumus ir iššūkius.“*

Šiame skyriuje, atlikus mokslinės literatūros analizę apie verslo modeliavimo tendencijas ir iššūkius, išryškėja metodų, tokių kaip SWOT, Porterio Penkių Jėgų modelio, PEST analizės ir „BMC“ svarba. Kiekvienas metodas atskleidžia skirtingas verslo aspektų puses ir leidžia įmonėms lanksčiai prisitaikyti prie besikeičiančių rinkos sąlygų. Tačiau būtent „Verslo Modelio Drobė“, kaip vienas iš šiuolaikinių metodų, ypatingai vertinimas už savo paprastumą, lankstumą ir aiškumą.

2. KIBERNETINIO SAUGUMO IŠŠŪKIAI IR SPRENDIMAI VERSLE

2.1.Kibernetinio saugumo apibrėžimas

Per pastaruosius du dešimtmečius kibernetinis saugumas tapo neatsiejama verslo, teisės ir technologijų dalimi. Šiuolaikinių organizacijų vidiniai valdymo procesai yra neįmanomi ir neįsivaizduojami be informacinių technologijų ir informacinių sistemų bei interneto prieigos. „*Kibernetinis saugumas tampa vienu iš pagrindinių tikslų, turint omenyje, kad grėsmės elektroninėje erdvėje kyla ne tik atskiriems vartotojams, bet net valstybėms*“ D.Štitilis (2013). Todėl kibernetinio saugumo samprata apima nebe tik informacijos saugą, bet ir daug platesnį saugumo iššūkių spektrą.

Toliau nagrinėsime kaip kibernetinis saugumas veikia šiuolaikinės verslo aplinkos struktūras ir kaip jis įgyvendinamas. Aptarsime kibernetinio saugumo strategijų pritaikymą verslo procesuose ir kaip įmonės gali efektyviai jas išnaudoti. Ištirsime skirtingus kibernetinio saugumo lygius, jų svarbą ir taikymą praktikoje.

Kibernetinio saugumo samprata ir jos raida yra įdomi bei sudėtinga istorija, atspindinti technologijų evoliuciją ir visuomenės suvokimo pokyčius. Tai dinaminis procesas, kuriame technologijų vystymasis ir kibernetiniai nusikaltėliai varžosi, nuolat formuodami ir transformuodami apsaugos metodus ir strategijas.

Pažvelkime giliau į technologinių proveržių chronologiją, kad suprastume, kaip šie pokyčiai paveikė šiandieninę kibernetinio saugumo realybę:

- 1960-aisiais: Kompiuterių laiko dalijimosi principas (kai keli vartotojai dalijasi vienu įrenginiu) lėmė poreikį juos apsaugoti nuo neautorizuotos prieigos. Šiuo laikotarpiu buvo pradėta naudoti slaptažodžių sistema, kuri išliko svarbi iki šių dienų.
- 1970-aisiais: ARPANET, ankstyvoji interneto forma, pažymėjo naują etapą kibernetinio saugumo srityje. Tuo metu buvo sukurti pirmieji kompiuteriniai virusai (pvz., Creeper) ir antivirusinė programinė įranga (Reaper), reaguojant į naujas grėsmes E. Coutry (2023).
- 1980-aisiais: Prasidėjo komercinių antivirusinių programų era. Tuo laikotarpiu buvo sukurtos naujos antivirusinės programos, reaguojant į besiplečiantį internetą ir augantį kibernetinių atakų skaičių.
- 1990-aisiais: Interneto plėtra ir vartotojų polinkis dalintis asmenine informacija skatino kibernetinius nusikaltėlius vogti duomenis. Atsirado poreikis masinei apsaugos programinės įrangos gamybai.
- 2000-aisiais: Informacijos skaitmeninimas ir interneto augimas sustiprino kibernetinių grėsmių įvairovę. Vyriausybės ėmėsi griežtesnių priemonių kovai su kibernetiniais nusikaltimais.

- 2010-aisiais: Kibernetinių atakų mastas ir sudėtingumas toliau didėjo, o jų taikiniai tapo vis svarbesni strateginiai objektai ir infrastruktūra. Kibernetinio saugumo srityje svarbus tapo ne tik techninis, bet ir žmogiškasis aspektas, akcentuojantis žmonių klaidas ir emocinį manipuliavimą, kaip reikšmingą kibernetinių nusikaltėlių įrankį.

Tęsiant kibernetinio saugumo raidos chronologiją iki šių dienų, pastaruoju dešimtmečiu matome, kaip kibernetinis saugumas tampa vis labiau susijęs su geopolitika ir nacionalinio saugumo klausimais. Ypač tai pasakytina apie karinius konfliktus, tokius kaip situacija Ukrainoje. 2010-ųjų pabaigoje ir 2020-ųjų pradžioje kibernetinis saugumas tapo svarbiu konflikto ir karinės strategijos elementu. Ypač žinomas yra 2015 m. incidentas Ukrainoje, kai buvo užfiksuoti kibernetiniai išpuoliai prieš šalies elektros tinklą K. Zetter (2016). Šie išpuoliai, kuriuos dažnai sieja su Rusijos kibernetinėmis pajėgomis, buvo vieni pirmųjų kartų, kai kibernetinis išpuolis turėjo tiesioginių ir rimtų pasekmių valstybės infrastruktūrai. Šie išpuoliai atkreipė pasaulio dėmesį į kibernetinio saugumo svarbą ne tik kaip įmonių, bet ir valstybių lygmeniu KAM (2018). Nuo to laiko kibernetinis saugumas tapo neatsiejama dalimi nacionalinio saugumo strategijų, o valstybės ir tarptautinės organizacijos skiria vis daugiau dėmesio bei išteklių kibernetinėms grėsmėms atpažinti ir neutralizuoti. Šiuolaikinė kibernetinio saugumo aplinka apima tiek tradicines grėsmes, tokias kaip virusai ir kenkėjiškos programos, tiek naujus iššūkius, susijusius su aukšto lygio šnipinėjimu, infrastruktūros pažeidimais ir nacionaliniu saugumu.

Suprantant kibernetinio saugumo svarbą ir jo poveikį tarptautiniame kontekste, ypač akivaizdžių įvykių fone, kaip Ukrainos krizė, būtina atkreipti dėmesį į kibernetinio saugumo sampratos evoliuciją ir teisinį reguliavimą. Kibernetinis saugumas ne tik atspindi technologines pažangas ir grėsmes, bet taip pat yra formuojamas ir teisės aktų, kurie nustato gaires, kaip ši sritis yra suvokiama ir reguliuojama tiek nacionaliniu, tiek tarptautiniu lygmeniu. Todėl, artėjant prie kibernetinio saugumo apibrėžimo, svarbu pabrėžti šių teisės aktų vaidmenį ir jų poveikį kibernetinio saugumo sampratai bei praktikai.

Lietuvos Respublikos kibernetinio saugumo įstatyme Nr. XII-1428 LR Vyriausybė (2014) pateikiami svarbūs apibrėžimai ir principai, formuojantys kibernetinio saugumo pagrindus. Įstatymo pirmasis straipsnis nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia institucijų, veikiančių šioje srityje, vaidmenis ir atsakomybę. Antrasis straipsnis apima pagrindines kibernetinio saugumo sąvokas, tokias kaip "kibernetinė erdvė", "kibernetinis incidentas" ir "kibernetinis saugumas" konkrečiau atskleidžiama kibernetinio saugumo samprata: „**Kibernetinis saugumas** – *visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti*“. Trečiasis straipsnis išdėsto kibernetinio saugumo principus, pabrėžiant nediskriminavimą, proporcingumą ir viešojo intereso viršenybę. Šie straipsniai apibrėžia kibernetinio saugumo sąvoką, jos

taikymo sritį, atsakomybę ir koordinavimą, taip pat numato kibernetinio saugumo politikos įgyvendinimo būdus. Ši informacija pagrindinė suprasti kaip įstatymuose Lietuva įvardina kibernetinį saugumą ir tai taip pat yra svarbu, bet kokiam išsamiam kibernetinio saugumo analizės darbui.

2018 m. rugpjūčio 13 d. priimtas nutarimas Nr. 818 dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo yra svarbus dokumentas, nustatantis konkrečias kibernetinio saugumo priemones ir atsakomybes (LR Vyriausybė 2018). Jame patvirtinama nacionalinė kibernetinio saugumo strategija, ypatingos svarbos informacinės infrastruktūros identifikavimo metodika, reikalavimai kibernetinio saugumo subjektams ir nacionalinis kibernetinių incidentų valdymo planas. Nutarimas taip pat pabrėžia nevyriausybinių organizacijų ir viešojo bei privataus sektoriaus atstovų dalyvavimą įgyvendinant kibernetinio saugumo strategiją.

Lietuvos nacionalinė kibernetinio saugumo strategija nustato pagrindines šalies kibernetinio saugumo politikos kryptis (LR Vyriausybė 2018). Strategijoje pabrėžiami penki pagrindiniai tikslai:

- stiprinti valstybės kibernetinį saugumą ir gynybos pajėgumus;
- užtikrinti nusikalstamų veiklų kibernetinėje erdvėje prevenciją;
- skatinti kibernetinio saugumo kultūrą ir inovacijas;
- stiprinti viešojo ir privataus sektorių bendradarbiavimą;
- stiprinti tarptautinį bendradarbiavimą;

Strategija atspindi Lietuvos siekį efektyviai reaguoti į kibernetinius incidentus, užkirsti kelią jų atsiradimui ir valdyti sukeltas pasekmes, užtikrinant saugų informacinių ir ryšių technologijų naudojimą visuomenei. Strategijos įžangoje tuometinis krašto apsaugos ministras R. Karoblis (2018) įvardina kibernetinio saugumo sampratą kaip: „**kibernetinis saugumas** *suprantamas ne kaip savarankiškas valstybės tikslas ar tik kaip atsakas į šiuolaikinės skaitmeninės Lietuvos valstybės keliamus iššūkius, bet į kibernetinį saugumą žvelgiama kaip į vieną iš integruotos skaitmeninės ekosistemos dalių“.*

2021 m. lapkričio 11 d. Nr. XIV-638 ir NR. XIV-413 2021 m. birželio 17 priimti įstatymai atnaujina Lietuvos kibernetinio saugumo įstatymo nuostatas, įvedant svarbius pakeitimus, susijusius su ryšių ir informacinių sistemų spragų paieška ir pranešimu apie jas, kibernetinių incidentų valdymo procedūromis, taip pat asmens duomenų apsaugos politikos įgyvendinimu kibernetinio saugumo srityje (LR Vyriausybė 2018).

Atsižvelgiant į tai, kad kibernetinis saugumas yra svarbus tarptautiniu mastu, ir atsižvelgiant į Lietuvos narystę Europos Sąjungoje, svarbu išnagrinėti ir ES lygmens teisės aktus bei strategijas. ES teisės aktai ir strategijos nustato bendrus standartus ir reikalavimus, kurie lemia nacionalinės kibernetinio saugumo politikos formavimą ir įgyvendinimą. Todėl toliau būtina atkreipti dėmesį į pagrindinius ES teisės aktus ir strategijas, siekiant suprasti, kaip jie veikia ir formuoja Lietuvos kibernetinio saugumo politiką.

Europos Sąjungoje (ES) taip pat paskelbti svarbūs teisės aktai ir direktyvos, susijusios su kibernetiniu saugumu. Vienas iš esminių dokumentų yra 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148, žinoma kaip NIS 1.0 Direktyva, kuria siekiama užtikrinti aukštą bendrą tinklų ir informacinių sistemų saugumo lygį visoje Europos Sąjungoje. Ji nustato minimalius saugumo reikalavimus ir pranešimų apie kibernetinius incidentus procedūras. Taip pat šiame įstatymo projekte įvardijamas kibernetinio saugumo apibrėžimas: „**kibernetinis saugumas** – *visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių*“.

Dar aktualesnis yra 2022 m. reglamentas (ES) 2022/2555, žinomas kaip NIS 2.0, susijęs su ENISA (Europos Sąjungos kibernetinio saugumo agentūra) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimu. Šį reglamentą taip pat 2024-ųjų rudenį turėtų patvirtinti Lietuvos Vyriausybė. Šiame įstatymo projekte taip pat įvardijamas kibernetinio saugumo apibrėžimas: „**kibernetinis saugumas** *yra daugelio ypatingos svarbos sektorių pagrindinė priemonė įgalinanti sėkmingai vykdyti skaitmeninę transformaciją ir visapusiškai pasinaudoti skaitmeninimo teikiama ekonomine, socialine ir tvarumo nauda*“. Šie teisės aktai kartu su ES kibernetinio saugumo strategija formuoja pagrindą ES kibernetinio saugumo politikai ir jos įgyvendinimui valstybėse narėse.

Vertinant pateiktus teisės aktus ir įvairių ekspertų požiūrius, akivaizdu, kad kibernetinis saugumas yra ne tik sudėtingas, bet ir nuolat besivystantis reiškinys įtakojantis tiek nacionalines, tiek tarptautines struktūras. Kiekvienas šaltinis atskleidžia savitą kibernetinio saugumo aspektų matymą – nuo gynybinių metodų iki teisinių ir vadybinių sprendimų praktikos. Lentelėje pateikiama ši įvairovė, padedanti giliau suvokti kibernetinio saugumo sampratos raidą ir jos taikymą įvairiose srityse.

2 Lentelė. Lentelė „Kibernetinio Saugumo Apibrėžimai“

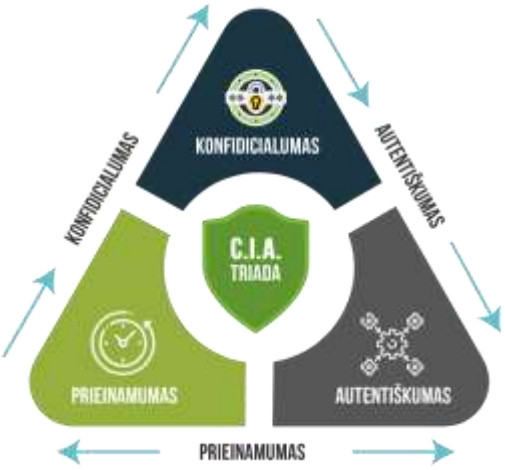
Autoriai	**Metai**	**Kibernetinio saugumo apibrėžimas**	**Raktažodžiai**
R.A. Kemmer	2003	Kibernetinį saugumą daugiausia sudaro gynybiniai metodai, naudojami galimiems įsibrovėliams aptikti ir sutrukdyti.	Gynybiniai metodai, įsibrovėlių aptikimas, prevencija.
LR Vyriausybė Kibernetinio saugumo įstatymas Nr. XII-1428 LR	2014	Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo	Teisinės priemonės, informacijos sklaida, organizacinės priemonės, techniniai sprendimai.

		sistemų veiklai, įvykus šiems incidentams, atkurti.	
dr. Darius Štitilis, dr. Paulius Pakutinskas, dr. Marius Laurinaitis, Inga Malinauskaitė-van de Castel	2014	Kibernetinis saugumas tai tinklų ir informacinių sistemų pajėgumas, tam tikru patikimumo lygiu išlikti atsparus bet kuriems veiksmams, keliantiems pavojų saugomų, perduodamų ar tvarkomų duomenų, arba atitinkamų teikiamų, ar per tas tinklų ir informacines sistemas gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui.	Praktiniai gebėjimai, valdymo kompetencijos, teisinės ir technologinės žinios, autentiškumas, vientisumas, konfidencialumas.
ES NIS 1.0 Direktyva 2016/1148	2016	Kibernetinis saugumas – visa veikla, būtina tinklų ir informacinėms sistemoms, tokių sistemų naudotojams ir kitiems susijusiems asmenims apsaugoti nuo kibernetinių grėsmių.	Tinklų ir sistemų apsauga, bendra veikla, grėsmių prevencija.
R. Karoblis Lietuvos nacionalinė kibernetinio saugumo strategija	2018	Kibernetinis saugumas suprantamas ne kaip savarankiškas valstybės tikslas ar tik kaip atsakas į šiuolaikinės skaitmeninės Lietuvos valstybės keliamus iššūkius, bet į kibernetinį saugumą žvelgiama kaip į vieną iš integruotos skaitmeninės ekosistemos dalių.	Integruota skaitmeninė ekosistema, strateginis požiūris, valstybės tikslas.
ES NIS 2.0 Direktyva 2022/2555	2022	Kibernetinis saugumas yra daugelio ypatingos svarbos sektorių pagrindinė įgalinanti priemonė siekiant sėkmingai vykdyti skaitmeninę transformaciją ir visapusiškai pasinaudoti skaitmeninimo teikiama ekonomine, socialine ir tvarumo nauda.	Skaitmeninė transformacija, ekonominė ir socialinė nauda, tvarumas.

Šaltinis: sudarytas autoriaus, remiantis R.A. Kemmer (2003), LR Vyriausybė (Kibernetinio saugumo įstatymas Nr. XII-1428 LR, 2014), D. Štitilis (2018), R. Karoblis (2018), ES (Direktyvos 2016/1148, 2019 ir 2022/2555, 2022)

Ankstesnėje dalyje išnagrinėjome ir apibendrinome įvairių teisės aktų bei ekspertų nuomones apie kibernetinio saugumo sampratą, kurios buvo pateiktos lentelės formatu (žr. 2 lentelę). Tačiau, be šių teorinių įžvalgų, svarbu paminėti ir praktinę kibernetinio saugumo pusę. Remiantis minėtais teisės aktais ir atliktu tyrimu, galima išskirti pagrindines kibernetinio saugumo sudedamąsias dalis arba esmines savybes, kurios lemia šios srities efektyvumą: Autentiškumas, konfidencialumas ir prieinamumas. Šios dalys yra neatsiejamos kibernetinio saugumo sistemoje ir žymi jos esmines charakteristikas. Siekdami pateikti aiškesnį vaizdą apie tai, kaip šie elementai saveikauja ir kaip jie yra svarbūs užtikrinant informacijos ir skaitmeninių išteklių saugumą pateikiama sutrumpinta informacija (žr. 3pav „C.I.A. Triada“):

3 Pav. „C.I.A Triada“



Šaltinis: Sudarytas Autoriaus

- **Autentiškumas**: Autentiškumo principu užtikrinama, kad informacija, duomenys ar funkcionalumas yra teikiami ir naudojami tik leistinų ir patikimų šaltinių. Tai reiškia, kad tik patvirtinti naudotojai ar procesai gali prieiti prie sistemų ar duomenų. Autentiškumas apima įvairias technologijas ir procedūras, tokias kaip stiprūs slaptažodžiai, dviejų veiksnių autentifikavimas, skaitmeniniai sertifikatai ir biometriniai duomenys.
- **Konfidencialumas**: Konfidencialumo principas reiškia, kad informacija ar duomenys yra prieinami tik tiems asmenims, kuriems yra suteikta teisė juos peržiūrėti ar naudoti. Tai apima duomenų šifravimą atliekant perdavimą tarp skirtingų tinklo taškų arba saugant duomenis serveryje. Konfidencialumo priemonės apsaugo organizacijos duomenis nuo neteisėtos prieigos ir nutekinimo.
- **Prieinamumas**: Prieinamumo principas užtikrina, kad informacijos ir duomenų sistemos yra pasiekiamos ir veikia, kai jos yra reikalingos. Tai apima tinkamo tinklo veikimo užtikrinimą,

duomenų atsarginių kopijų kūrimą ir atkūrimo planus, kad būtų galima greitai atstatyti sistemas po nesklandumų ar kibernetinių išpuolių.

Šių trijų principų derinys – autentiškumas, konfidencialumas ir prieinamumas, žinomi kaip kibernetinio saugumo 'CIA' triada, užtikrina, kad organizacijos skaitmeniniai duomenys būtų apsaugoti nuo neleistinos prieigos, nutekinimo ar praradimo. Tai yra savotiškas kibernetinio saugumo fundamentas, tačiau nors šie trys aspektai yra svarbūs, jie yra tik dalis kompleksinio proceso, reikalaujančio visapusiško požiūrio į kibernetinio saugumo strategijas ir praktikas.

2.2. Kibernetinės grėsmės: dinamika ir evoliucija

Ankstyvaisiais kompiuterių populiarėjimo laikais, tradicinės sukčiavimo praktikos pradėjo persikelti į skaitmeninę erdvę, sukeldamos iki tol neįvertintas saugumo grėsmes.

Pavyzdžiui, 2011 m. Havajų Kaneohe regione, moteris buvo apkaltinta vaiduoklių[8] darbuotojų schemos sukūrimu, kurioje ji įtraukė fiktyvius darbuotojus į atlyginimų sąrašą, neteisėtai pasisavindama apie 200 tūkst. JAV dolerių iš saugumo įmonės, kurioje dirbo (Star-Adviser 2011).

Vadinamasis „Saliamio pjaustymo“ metodas [9] (angl. "Salami slicing") yra dar vienas sukčiavimo būdas, pagrįstas menkų sumų sistemingomis transakcijomis į gavėjo sąskaitą, pasinaudojant pinigų apvalinimo ypatumais. Ši technika leidžia sukčiams nepastebimai pervedinėti mažas pinigų sumas, kurios ilgainiui užauga iki reikšmingos (P.Guupta 2023). Kita „Fantominių prekių“ sukčiavimo schema [10] pasireiškia, kuomet pardavėjai priima užsakymus ir mokėjimus už prekes, kurių iš tikrųjų neturi, ir jų niekada neplanuoja siųsti pirkėjui (M. Stephens, C. Hymas, The Telegraph, 2023). Ši praktika su laiku greitai išplito internetinėje prekyboje ir sutelktinio finansavimo platformose. Dar viena sukčiavimo forma yra aukcionų manipuliavimas (Los Angeles Times 2000), žinomas kaip varžytinių sukčiavimas [11](angl. "shill bidding"), kur fiktyvūs pasiūlymai naudojami siekiant dirbtinai išpūsti prekių kainas aukcionuose. Šis metodas sukuria klaidingą konkurencijos įspūdį, priverčiantis tikruosius pirkėjus mokėti daugiau už prekę nei reali jos vertė. Skaitmeninių technologijų naudojimo augimas sukūrė palankią terpę įvairioms sukčiavimo formoms atsirasti, skatindamas tiek naujus sukčiavimo būdus, tiek adaptuojant senąsias praktikas naujoje skaitmeninėje aplinkoje.

[8] Angl.k „Ghost Payroll“ – Darbuotojas vaiduoklis yra darbuotojas, įtrauktas į jūsų darbo užmokesčio sąrašus, kad gautų atlyginimą, net jei jis nėra įdarbintas jūsų įmonėje

[9] Saliamio pjaustymo taktika yra praktika, kai naudojama daugybė mažų teisėtų veiksmų, siekiant sukurti daug didesnį veiksmą ar rezultatą kuris bus nelegalus.

[10] „fantominių prekių“ sukčiai, reklamuoja prekes itin pigiomis kainomis populiariose ir patikimose svetainėse. Sąrašuose dažnai pateikiami netikri teigiami atsiliepimai, rodantys, kad pardavėju galima pasitikėti.

[11] „Shill bidding“ yra vienas iš aukcionų sukčiavimo būdų, kuomet pardavėjas anonimiškai siūlo savo prekę pirkti taip dirbtinai keldamas savo prekės kainą.

Informacinės technologijos ne tik atvėrė naujas galimybes sukčiavimui, bet ir sudarė sąlygas jauniems žmonėms išbandyti savo įgūdžius įsibrauti į skaitmenines sistemas. Taip prasidėjo nauja karta, paauglių įsilaužėlių amžius. Jaunuoliai laike savotišku individualiu iššūkių, prisijungti prie kokio nors kompiuterio, ar sistemos ar ją sukompromituoti. Šios praktikos ir tapo ištakomis pirmųjų kibernetinių nusikaltimų ir šnipinėjimų.

Vienas labiausiai žinomų kibernetinių nusikaltėlių Kevinas Mitnikas (Kevin Mitnick), kitaip žinomas slapyvardžių „Condor“, daugiau nei dešimtmetį brovėsi ir kompromitavo įvairiausias sistemas tik norėdamas įrodyti, kad jis tai sugeba. Vėliau jis visgi buvo sugautas ir nuteistas (Kevin Mitnick 2021)

Augant žiniatinklio naudojimui, interneto tinklapiai ir verslo portalai vis dažniau sulaukdavo nuobodžiaujančių paauglių atakų, paliekančiu paprastą žinutę „prigavau jus“ („i-got-you“). Dar vėliau kibernetiniai išpuoliai jau tapdavo labiau politiškai motyvuoti ir nukreipiami į politines organizacijas. Tokio pobūdžio veikla pradėta vadinti „hacktyvizmu[12]“ (Angl.k „Hacktivism“).

Devintojo dešimtmečio pabaigoje elektroninė prekyba tapo svarbia ekonomikos dalimi, tai paskatino organizuoto kibernetinio nusikalstamumo augimą. Nusikaltėlių grupuotės tapusios labiau organizuotos pradėjo kitaip vertinti mažos rizikos ir didelio pelningumo atakų potencialą internete. Kibernetiniai nusikaltimai pradėjo sparčiai augti, o vienas pagrindinių tapo kreditinių ir debetinių kortelių duomenų vagystės. Tai tapo didele riziką įmonėms, nes kredito kortelių pramonė įvedė baudas už kibernetinio saugumo standartų nesilaikymą.

Didėjant visuomenės priklausomybei nuo IT sistemų, dar viena iškilusi grėsmė saugumui tapo paslaugų atsisakymo [13]ataka (Angl.k. DDoS - distributed denial-of-service)., kurios metu užpuolikas užkrėstų kompiuterių tinklais užtvindo svetainę ar paslaugą užklausomis ir srautu. Tuo pačiu metu sistema nesugebėdama atsakyti į visas ateinančias užklausas būna sutrikdyta arba sugadinama. Vienas įspūdingesnių DDos atakos pavyzdys įvyko 2014m. vasario mėnesį (P. Nicholson 2022), kuomet nežinomas nusikaltėlis pradėjo ataka prieš įvairius taikinius. Ataka naudojo specialią tinklo laiko protokolo (Angl.k. Network Time Protocol (NTP) reflection) savybę duomenims padidinti. Iki to laiko, kol duomenų paketas pasiekdavo tikslą, jis būdavo padidintas 50 kartų, o tai prilygo maždaug 250 000 atskirų užklausų sistemai per sekundę. Vienas iš verslų kuriai buvo skirta ši ataka, buvo užpultas duomenų srautais iš 4278 IP adresų esančiu daugiau nei 80 šalių, kurie siuntė daugiau 400 gigabitų duomenų paketų per sekundę ir tai truko visą valandą (S. Gallagher 2014).

Kai kompiuteriai tebuvo technologijos naujovė, virusai dažnai buvo platinami per disketes, kurios buvo patogus transportavimo būdas. Interneto atsiradimas viską pakeitė, kenkėjiškas programas platinti

[12] Hacktivizmas – (Angl.k sujungus žodžius „Hack“ ir „Actyvism“) yra įsilaužimas į kompiuterinę sistemą siekiant politinių ar socialinių tikslų.

[13] Pasak Microsoft : „DDoS“ atakos metu robotų serija arba robotų tinklas užtvindo svetainę ar paslaugą užklausomis ir srautu. o tai išstumia teisėtus vartotojus. Todėl paslaugos gali būti tam tikrą laikotarpį uždelstos arba kitaip sutrikdytos.

elektroniniu būdu tapo kur kas greičiau ir patogiau nei anksčiau. Fizinis virusų platinimas neišnyko, bet jo populiarumas sumažėjo, o disketes pakeitė patogesnės USB atmintinės. Pačių kenkėjiškų programų rašymas reikalo savotiškos automatizacijos, juk perkelti virusai turėjo atlikti kokią nors funkciją; platintis ir sabotuoti sistemą, net ir neturint priėjimo prie jos. Taip su laiku, kibernetinio nusikalstamumo erdvėje pradėjo veikti ypatingai įgudę programuotojai kurie suvokė, kad efektyvioms ir masinėms atakoms būtina gera automatizacija. Kad pasiektų savo tikslus su didesniu efektyvumu ir mažesne aptikimo rizika, kibernetiniai nusikaltėliai ėmė kurti sudėtingesnes kenkėjiškas programas, galinčias ne tik platintis, bet ir suteikti pilną kontrolę užkrėstose sistemose. Viena tokių "Rootkit[14]" yra gudri kenkėjiškos programinės įrangos forma, kuri ne tik slepiasi operacinėje sistemoje, bet ir gali vykdyti įvairias užduotis be vartotojo žinios.

"***Rootkit***" įterpimas į taikinio sistemą reikalauja, kad kibernetinis nusikaltėlis pirmiausia prasiskverbtų į sistemą, o tada naudotų vadinamąjį instaliavimo mechanizmą vadinama "dropper[15]", kuris įdiegia "rootkit". Kuomet "rootkit" kodas yra įdiegtas pirmiausia jis pažeidžia sistemą taip, kad kiekvieną kartą ją perkrovus jis pasileistu iš naujo ir suteiktų nusikaltėliui nuolatinę prieigą prie užkrėstos sistemos. Skirtingai nei paprasti virusai, "rootkit" automatiškai neplinta, tačiau jis gali būti derinamas su viruso tipo kodu, kad užkrėstų kitas sistemas. "Rootkit" taip pat yra sukurtas apeiti įsilaužimo aptikimo sistemas, pavyzdžiui, išjungiant tam tikras antivirusines programas. Jų užslėpimo gebėjimai yra tokie pažengę, kad "rootkit" gali likti nepastebėtas ilgą laiką, net ir pažangiausiu kibernetinio saugumo sistemų.

Vienas iš pavyzdžių, kaip "rootkit" gali būti naudojami praktikoje, yra TDL3 "rootkit", sukurtas Dogma Millions kibernetinio nusikalstamumo grupės (H.Martin 2010). Šis "rootkit" įsirašo kaip spausdintuvo tvarkyklė, suteikdamas jam pagrindinės sistemos tvarkyklių privilegijas ir leidžiantis jam naudoti užšifruotą failų sistemą savo tikslams. "TDL3" naudojamas atsisiųsti, įdiegti ir paslėpti kenkėjiškus modulius, kurie gali vykdyti klaviatūros paspaudimų stebėjimą (Angl.k.“KeyLogger“), organizuoti atsisakymo teikti paslaugas atakas [16](Angl.k „DDoS“) ir daugelį kitų veiksmų, tuo pačiu metu išliekant nematomas vartotojui ir saugumo sistemoms.

Su laiku tobulėjant kibernetinio saugumo priemonėms, kenkėjiškas įsiskverbimas tapo sudėtingesnis. Todėl kibernetiniai nusikaltėliai ėmė ieškoti naujų būdų, kaip apeiti naujas saugumo sistemas. Tuo metu jau buvo žinoma, kad silpniausia kibernetinio saugumo dalis yra – žmogus.

[14] “Rootkits” yra priemonės, naudojamos hakerių vykdomų kenksmingų veiksmų maskavimui: diegiant „spyware”, vagiant duomenis ir pan.

[15] „Droppers“ yra programos, skirtos išgauti kitus failus iš savo kodo. Paprastai šios programos įrašo kelis failus į kompiuterį, kad įdiegtų kenkėjiškų programų paketą.

[16] „DDoS“ ataka būna nutaikyta į svetaines ir serverius, ji pertraukia tinklo paslaugas bandant išnaudoti programos išteklius. Šias atakas rengiantys užpuolikai užtvindo svetainę srautu, todėl svetainės funkcijos veikia prastai arba ji visiškai atjungiama.

Todėl vienas iš būdų kurį kibernetiniai nusikaltėliai ėmė naudoti „***Pfishing*** [17]“. Tai metodas kuomet sukuriamas įtikinamas laiškas su kenkėjišku kodu arba nuorodą į kenkėjišką tinklapį ir siunčiamas didelei grupei vartotoju. Tikslas – kad bent vienas gavėjas atidarytų laišką, o kenkėjiškas kodas būtų automatiškai įdiegtas. „Spear Pfishing“, labai panašus metodas, pasižymi dar didesniu personalizavimu: elektroninis laiškas yra labai įtikinamas, dažnai siunčiamas apsimetant pažįstamu asmeniu ar autoritetinga organizacija. Ši taktika reikalauja išankstinės aukos žvalgybos, kad būtų galima kuo tiksliau pritaikyti pranešimą pagal konkretaus asmens ar organizacijos ypatybes.

Tam tikri įvykiai, pavyzdžiui, 2022 m. FIFA „World Cup Qatar „pasaulio čempionatas (A.Bizga 2022, J. Kelley 2022) , parodė, kaip jie gali paskatinti "Pfishing" atakų bangą. Pasaulio čempionato laikotarpiu "Pfishing" atakų skaičius, ypač nukreiptų į Artimųjų Rytų regioną, padvigubėjo. Daugelis suklastotų el. laiškų buvo pateikiami esą išsiųsti iš FIFA pagalbos tarnybos, taip klaidinant gavėjus. Šių atakų tikslai buvo įvairūs: nuo finansinio sukčiavimo iki prisijungimo duomenų vagystės ir net vartotojų stebėjimo. Kai kurie el. laiškai skatino lažintis dėl pasaulio čempionato rezultatų, taip suteikdami nusikaltėliams galimybę gauti prisijungimo duomenis, kurie vėliau galėjo būti panaudojami kitoms nusikalstamoms veikoms. Šių atakų pavyzdžiai parodo, kaip renginiai, tokie kaip FIFA pasaulio čempionatas, gali tapti plataus masto kibernetinių atakų katalizatoriumi.

Be "Phishing" atakų, kurios ne tik atveria duris asmeninių ar organizacinių duomenų vagystei, bet ir sudaro sąlygas "Rootkit" įrašymui į sistemas tolesniam nuotoliniam valdymui, kibernetiniai nusikaltėliai taip pat naudoja itin žalingą "Ransomware". Šios išpirkos reikalaujančios programinės įrangos įdiegimas dažnai yra galimas tik per "Rootkit", kuris suteikia nusikaltėliams galimybę slapta įdiegti ir valdyti "Ransomware" be vartotojo žinios. Taigi, "Ransomware" tampa dar viena grėsme, kurią "Rootkit" gali įdiegti užkrėstose sistemose, kartu dar labiau padidindamas kibernetinio saugumo iššūkius ir turi potencialą visiškai sutrikdyti organizacijų veiklą.

"***Ransomware***[18]" arba išpirkos reikalaujanti programinė įranga – tai viena iš labiausiai paplitusių ir žalingiausių kibernetinio saugumo grėsmių. Ši kenkėjiška programinė įranga užšifruoja aukos failus arba užblokuoja prieigą prie sistemos ir reikalauja išpirkos už duomenų atšifravimą ar prieigos atkūrimą. Nusikaltėliai dažnai reikalauja mokėjimo kriptovaliuta, kad būtų sunkiau atsekti mokėjimą ir identifikuoti užpuolikus. "Ransomware" atakos gali paveikti tiek individualius vartotojus, tiek didelius verslus ir net vyriausybines institucijas, sukeldamos ne tik finansinius nuostolius, bet ir sutrikdydamos kritines operacijas.

[17] Europos terminų bazėje IATE teikiamas terminas duomenų viliojimas (angl. Pfishing) apibrėžiamas kaip socialinės inžinerijos metodas skaitmeninėje terpėje, kai apgaulės būdu, apsimetant patikimu fiziniu ar juridiniu asmeniu, siekiama išgauti tokią neskelbtiną informaciją kaip vartotojo vardai ir slaptažodžiai, banko sąskaitos numeriai, mokėjimo ir kredito kortelių numeriai ir pan.

[18] Ransomware yra išpirkos reikalaujančio kenkėjiško programinio kodo šeimai priskiriami virusai. Šie virusai nuo kitų skiriasi savo agresyvumu - užvaldytoje sistemoje jie nesistengia užmaskuoti savo veiklos pėdsakų, svarbiausias jų tikslas yra užšifruoti sistemos savininkui svarbias bylas ar net visą failų sistemą, tikintis, kad savininkas bus pasiryžęs sumokėti išpirką jų atgavimui. (https://www.nksc.lt/rekomendacijos/ransomware.html)

Pavyzdžiui, sveikatos priežiūros įstaigos, patyrusios "ransomware" ataką, gali netekti prieigos prie gyvybiškai svarbių pacientų duomenų, o tai gali turėti rimtų pasekmių pacientų sveikatai. "Ransomware" atakos paprastai prasideda nuo "pfishing" el. laiškų, kurie skatina vartotojus atidaryti kenkėjiškus priedus arba spustelėti ant kenkėjiškų nuorodų. Kai kenkėjiška programinė įranga „***rootkit***“ įsirašo į sistemą, ji atsiunčia „***ransomware***“ kodą ir pradeda užšifravimo procesą, o aukai parodomas pranešimas su išpirkos suma ir mokėjimo instrukcijomis. Viena iš garsiausių "ransomware" atakų yra "WannaCry", kuri 2017 metais paveikė šimtus tūkstančių kompiuterių daugiau nei 150 šalių, įskaitant ligonines, bankus ir kitas institucijas. Ataka parodė, kokiais mastais gali plisti "ransomware" ir kokią žalą ji gali padaryti (CNN, BBC 2017).

Nors "***Ransomware***" ir "***Rootkit***" atakos jau seniai yra kibernetinio nusikaltėlių arsenalo dalis, pastaruoju metu vis dažniau į viešumą patenka žinios apie dar sudėtingesnes ir labiau koordinuotas kibernetines grėsmes. Šios grėsmės, žinomos kaip pažangiosios nuolatinės grėsmės [19](APT), dažnai yra susijusios su valstybinėmis žvalgybos organizacijomis aktoriais arba labai gerai organizuotomis nusikalstamomis grupuotėmis, kurios naudoja išplėstą technologijų arsenalą. Skirtingai nuo paprastų "Ransomware" atakų, kurios dažniausiai siekia greito pelno, APT kampanijos yra itin tikslinės ir skirtos ilgalaikiam įsiskverbimui į aukšto profilio taikinius, pavyzdžiui, vyriausybines institucijas, kritinės infrastruktūros įmones arba tarptautines korporacijas.

Stuxnet, kuris buvo aptiktas 2010 m., yra ryškus pavyzdys, kaip valstybinės žvalgybos agentūros pritaiko kibernetines atakas prieš pramonines sistemas, siekdamos strateginių tikslų. Šis "Rootkit" buvo sukurtas ne tik techniškai pažangiai, bet ir su aiškiu politiniu bei kariniu motyvu - sutrikdyti Irano branduolinės programos veiklą. Kenkėjiška programa netik užkrėtė daugiau nei 200 000 kompiuterių, bet ir fiziškai sugadino apie 1 000 urano sodrinimo centrifugų (BBC 2010).

Ši ataka atskleidė naują kibernetinės grėsmės dimensiją, galinčią sukelti realaus pasaulio žalą. Stuxnet buvo pritaikytas specifiškai Siemens pramoninei įrangai sutrikdyti, o tai, kad JAV ir Izraelis 2012 m. pripažino sukūrę Stuxnet, tik dar labiau pabrėžė, kad šiuolaikinės kibernetinės atakos gali būti vykdomos valstybių lygmeniu ir tapti sudėtingos geopolitinės strategijos dalimi.

[19] APT – labai platus terminas, vartojamas apibūdinti atakos kampaniją, sudarytą iš daugelio elementų, kurios metu įsibrovėlis arba įsibrovėlių komanda nustato neteisėtą ilgalaikį buvimą tinkle, siekdamas išgauti labai jautrius duomenis arba įvykdyti sabotažą.

2.3. Kibernetinės atakos vektorius

Šiais laikais kibernetinės atakos tapo kur kas sudėtingesnės. Jos dažnai yra vykdomos organizuotų nusikaltėlių ar valstybių remiamų grupuočių, kurios naudoja išsamiai apibrėžtus procesus. 2009 metais „Lockheed Martin“ ekstremalių kibernetinių situacijų reagavimo skyrius (E.M. Hutchins, J.M. Cloppert, R.M. Amin, 2009) paskelbė straipsnį „Žvalgyba grindžiamas kompiuterių tinklų gynybos koordinavimas, remiantis priešo veiksmų analize ir įsilaužimo įvykių grandine[20]“ . Šiame straipsnyje buvo pristatyta plačiai išpopuliarėjusi koncepcija – Kibernetinės Atakos Vektorius (Angl.k. „Cyber Kill Chain®“).

Jų pateiktoje koncepcijoje kibernetinės Atakos Vektorius apibrėžia septynis etapus (žr. 7 paveikslėlį): žvalgyba, ginklavimas, pristatymas, išnaudojimas, įdiegimas, valdymas ir kontrolė, veiksmai ir tikslai.

4 Pav. Kibernetinės atakos vektorius (Angl.k „Kill Chain“)

Šaltinis: Sudaryta S.Sampati „Stages of Cyber Chain, Countermeasures of Security Reconnaissance“

Šie etapai nėra griežtai išdėstyti vienas po kito. Jie gali persidengti ir sąveikauti, kiekvienas iš jų atskleidžia svarbią atakos įgyvendinimo proceso dalį.

Žvalgybą - būdas rasti ir perprasti tinkamą taikinį, silpnąją apsaugos dalį. Tai gali būti tiek techninė sistemos grandis tiek ją besinaudojantis asmuo. Įprastai asmenys prieigai prie interneto naudoja vieną IP adresą[21], suteiktą interneto paslaugų teikėjo, o įmonės – keletą adresų savo interneto domene.

[20] Tikslus pavadinimas Anglų kalba: „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains“, E.M. Hutchins, J.M. Cloppert, R.M. Amin, Lockheed Martin, 2009.
[21] IP adresas –kompiuterio identifikatorius interneto tinkluose

Kai atakos vykdytojas pasirenka verslo ar asmens IP adresą, jis pradeda skenuoti aplinkinius interneto adresus tokiu būdu siekdamas rasti kitas aktyvias sistemas. Tai vadinama ***IP adresų skenavimu.*** Aptikus aktyvius IP adresus, toliau skanuojami jų prievadai (Angl.k. PORT). Tai vadinama ***portų skenavimu,*** ir tai atliekama norint identifikuoti potencialias įėjimo į sistemą vietas. Pvz. netinkamai sukonfigūruotų tinklų įrenginius. Šiandieninės atakos dažniausia nebėra atliekamos rankiniu būdu, dauguma jų vykdomos automatizuotai, naudojant jau prieš tai užvaldytus kompiuterinius tinklus. Šie tinklai, vadinami ***Botnetais***[22], gali turėti tūkstančius ar net milijonus kompromituotų sistemų, leidžiančių vykdyti kibernetines atakas dideliu mastu.

Ginklavimosi etape kibernetinės atakos vykdytojai pasitelkia įvairias taktikas ir technologijas, skirtas žvalgybos metu nustatytiems trūkumams išnaudoti. Dažniausiai tai apima kompiuterinių virusų, šnipinėjimo programų [23](Angl.k „KeyLogger“), trojanų [24](Angl.k „Trojan“) ir kitų kenkėjiškų programų kūrimą arba adaptaciją.

Pristatymas – tai etapas, kuomet kenkėjiška programa yra pristatoma į atrastą silpniausią tinklo ar vartotojų segmentą. Dažniausiai tai įvyksta prisegant užkrėstą dokumentą, pavyzdžiui, PDF failą ar kitą elektroninį objektą prie laiško, kurį atidarius automatiškai įsiskverbia kenkėjiška programa. Šis failas gali būti nusiųstas taikiniui elektroniniu paštu, o toks metodas žinomas kaip "phishing[25]". Kitas būdas – pažeidžiama svetainė užkrečiama kenkėjiška programa, o taikinys kviečiamas ją aplankyti, kas inicijuoja kenkėjiško kodo atsisiuntimą ir infekciją. Taip pat galima naudoti nustatytus prisijungimus ar pavogtus duomenis tiesiogiai įsiskverbti į sistemą. Praktikoje ataka pirmiausiai nukreipiama infekuoti tinklo prieinamiausiąs sistemas, o vėliau jas išnaudoti kaip kenkėjiško kodo platinimo mazgą, skverbiantis gilyn į sistemą iki realaus taikinio. Užkrėsta USB atmintinė, taip pat gali būti efektyvus pristatymo būdas, ypač jei taikinio sistema nėra prijungta prie interneto**.**

Išnaudojimas - etapas yra kritinis momentas kibernetinėje atakoje, kuomet užpuolikas pasinaudoja sistemos pažeidžiamumais, kad prasiskverbtų į ją. Šiuo metu kenkėjiška programinė įranga dar nėra įsitvirtinusi sistemoje, bet naudoja rastas spragas, kad galėtų tai padaryti. Išnaudojimas vyksta naudojant specialius duomenų paketus, kurie atakuoja tam tikrų interneto paslaugų protokolų trūkumus, arba tiesiogiai įsiskverbus į sistemą su pavogtais ar atspėtais prisijungimo duomenimis. Sėkmingai išnaudojus šiuos pažeidžiamumus, užpuolikas gauna galimybę vykdyti savo kitus planus, tokius kaip kenkėjiškos programinės įrangos diegimas ar netiesioginė kontrolė per kompromituotą sistemą.

Diegimo etape dėmesys sutelkiamas į kenkėjiškos programinės įrangos įtvirtinimą sistemoje, siekiant užtikrinti jos ilgalaikį veikimą ir atsparumą pašalinimui. Šiame etape svarbu ne tik įrašyti

[22] Botnetas (angl. Botnet) – internetu sujungtas kompiuterių tinklas, užterštas kenkėjiška programine įranga.
[23] Šnipinėjimo programa (angl. Keylogger) – tai klaviatūros paspaudimų registravimo programa
[24] Trojanas (angl. Trojan) – programinė įranga atliekanti žalingą užduoti be vartotojo žinios ar sutikimo.
[25] Fišingas (angl. Phishing) – Tai sukčiavimo forma, skirta konfidencialiems duomenims išvilioti, naudojant internetinius adresus, panašius į realiai egzistuojančios institucijos adresą.

kenkėjišką kodą į atitinkamas sistemos vietas, bet ir sukurti sąlygas, kad programinė įranga galėtų atkurti savo veiklą net ir po sistemos perkrovimo. Tai sudaryta iš įvairių techninių sprendimų, pavyzdžiui, failų ir procesų maskavimo, automatinio paleidimo funkcijos, kurie neleistų vartotojui ar antivirusinei programai lengvai aptikti ir pašalinti kenkėjišką programinę įrangą.

"Diegimo" etapas yra ***esminis*** tam ,kad užpuolikas galėtų įgyti ir išlaikyti nuolatinę kontrolę su prieiga prie užkrėstos sistemos.

Valdymas ir kontrolė. Po sėkmingo diegimo etapo, kenkėjiška programinė įranga užmezga ryšį su valdymo ir kontrolės serveriu (Angl.k Command&Control). Tai pagrindinis žingsnis, leidžiantis užpuolikui perimti užkrėstos sistemos kontrolę. Šis veiksmas leidžia atakos vykdytojui centralizuotai valdyti ir koordinuoti sistemos veiksmus, suteikiant galimybę atlikti įvairias operacijas atstumu.

- Ryšio Užmezgimas: Pirmiausia kenkėjiška programinė įranga bando užmegzti saugų ir slaptą ryšį su C&C serveriu, naudodama įvairias šifravimo ir anonimiškumo technologijas, siekiant išvengti aptikimo ir blokavimo.
- Registracija ir Ataskaita: Įdiegta kenkėjiška programinė įranga praneša C&C serveriui apie sėkmingą įsiskverbimą ir pateikia informaciją apie kompromituotą sistemą, pvz., operacinę sistemą, turimus teises, įdiegtą programinę įrangą.
- Komandų Gavimas: C&C serveris gali siųsti specifines komandas arba skriptus, nurodančius kenkėjiškai programinei įrangai atlikti tam tikrus veiksmus, pvz., atsisiųsti papildomą kenkėjišką programinę įrangą, rinkti duomenis, vykdyti DDoS atakas, kitų sistemų atžvilgiu arba vykdyti kitas kenkėjiškas operacijas.
- Atlikto Darbo Ataskaitos: Kenkėjiška programinė įranga gali siųsti duomenis atgal į C&C serverį, įskaitant pavogtus failus, slaptažodžius, duomenų bazės įrašus arba informaciją apie kitas kompromituotas sistemas.

Veiksmų ir tikslų etapas reiškia kibernetinės atakos kulminaciją, kuomet vykdytojas, jau turėdamas pilną kontrolę įgyvendina savo galutinius tikslus. Šiame etape vykdomos operacijos yra labai įvairios ir priklauso nuo atakos vykdytojo ketinimų, tačiau vienos populiariausių yra:

- **Duomenų vagystė ar duomenų užšifravimas:** Užpuolikai gali pavogti brangią intelektinę nuosavybę, klientų duomenis, finansinę informaciją ir kitus vertingus išteklius. Taip pat užkoduoti svarbius duomenis su tikslu vėliau prašyti išpirkos duomenų [26]atkodavimui (Angl.k Ransomware).
- **Sistemos sabotažas:** kai kuriais atvejais atakos tikslas gali būti tiesioginis kenkimas ir sistemos kompromitavimas. Pvz. Kritinės infrastruktūros sutrikdymas, svarbių duomenų sunaikinimas ar netgi fizinė žala, jei tai susiję su pramoninės kontrolės sistemomis.

[26] Ransomware yra kenkėjiškų programų rūšis, kuri blokuoja (užšifruoja) prieigą prie aukos duomenų, nebent būtų sumokėta išpirka

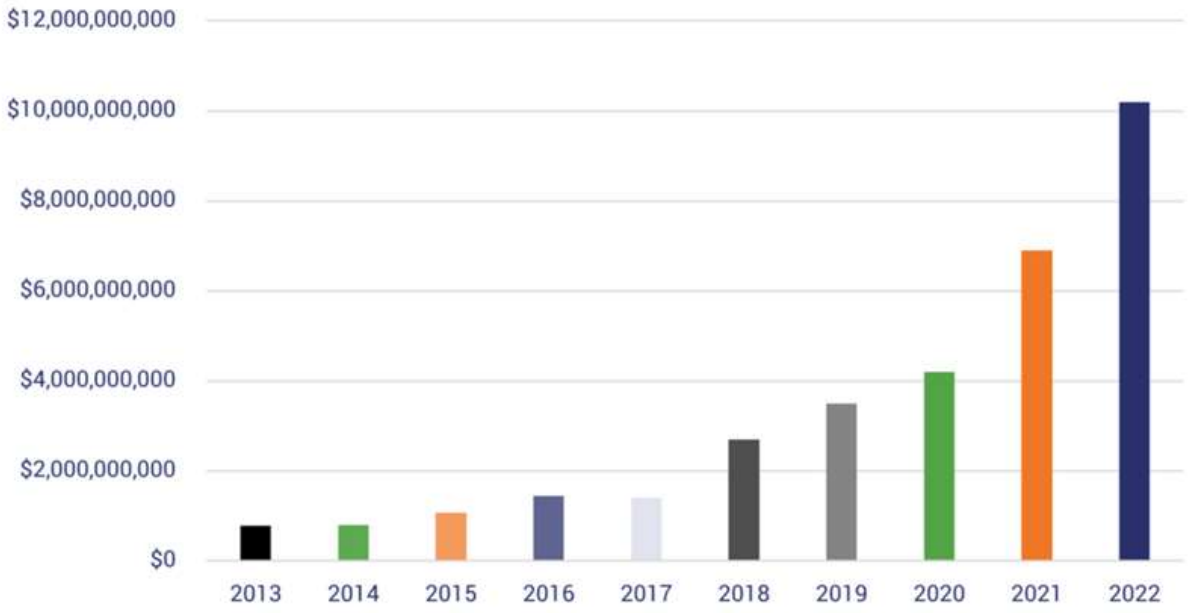
- **Platinimo arba atspirties taškas:** Užkrėsta sistema gali būti naudojama kaip platforma platinti kenkėjišką programinę įranga toliau, pavyzdžiui siunčiant „phishing“ laiškus. Arba ilgalaikėje perspektyvoje prie užkrėstos sistemos vykdytojas gali grįžti vėliau ir panaudoti ją kaip atspirties tašką kitoms atakoms.

"Veiksmų" etape kibernetinės atakos poveikis tampa akivaizdus, tuo pačiu atskleisdamas, ar auka buvo pasiruošusi gynybai. Kiekvienas įvykdytas atakos žingsnis, kibernetinės atakos vektoriuje, vis labiau apsunkina galimybę efektyviai apsiginti ir susigrąžinti sistemų kontrolę. Todėl, būtent dėl šios priežasties, labai svarbu turėti iš anksto parengtus veiksmų planus reagavimui į incidentus, nes tai leistų sušvelninti atakos padarinius ir sumažinti būsimą žalą.

2.4.Kibernetinio saugumo principai ir apsaugos metodai

Per pastaruosius du dešimtmečius kibernetinė erdvė bei vartotojų skaičius augo geometrine progresija, o kartu su jais išaugo ir kibernetinių incidentų skaičius (žr. 4 paveikslėlį). Kibernetinis saugumas tapo nuolatine pokalbių tema kiekvienoje organizacijoje. Tačiau, kaip rasti bendrą kalbą ar formatą, kuomet kiekvienas verslas toks skirtingas, o kibernetinio saugumo metodų tiek daug?

5 Pav. Pranešimai apie kibernetinių nusikaltimų nuostolius per pastarąjį dešimtmetį



Šaltinis: Casey Crane 2023 straipsnį „A Look at 30 Key Cyber Crime Statistics“

Tokie iššūkiai ir paskatino kibernetinio saugumo standartų ir metodikų, tokių kaip PCI DSS, CIS Kontrolė, ISO ir NIST atsiradimą ir tobulėjimą. Šiame skyriuje bus detaliai atskleisime, kaip šios metodikos ir standartai padeda organizacijoms stiprinti apsaugą prieš kibernetines grėsmes. Įvertinsime

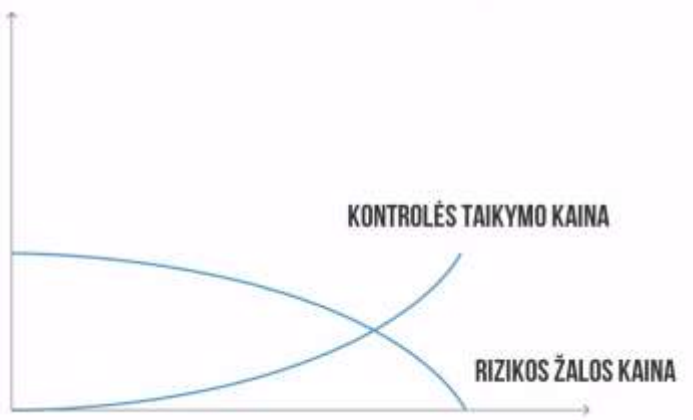
kaip standartai daro įtaka rizikų valdymui, incidentų prevencijai ir duomenų apsaugos strategijų kūrimui, užtikrinant visapusišką informacijos ir tinklų apsaugą.

2.4.1. Kibernetinio saugumo valdymo kontrolės priemonės

Kibernetinis saugumas – tai strategija, skirta apsaugoti objektus kibernetinėje erdvėje nuo įvairių atakų (M. Shore 2023). Tam pasitelkiamos saugumo kontrolės priemonės, kurios turi būti tinkamai suprojektuotos, atsižvelgiant į jų paskirtį ir efektyvumą.

Pirmasis žingsnis projektuojant kontrolės mechanizmus yra įvertinti jų sąnaudų ir naudos santykį. Tai daroma pasveriant, ar kontrolės įgyvendinimo išlaidos yra mažesnės nei galimi nuostoliai, atsiradę dėl incidento poveikio (žr. 5 paveikslėlį). Šiam vertinimui dažnai naudojamas kreivės grafikas, kuriame vaizduojamas vis stiprėjančios kontrolės sąnaudų ir teikiamos naudos santykis. Jeigu papildoma rizikos mažinimo nauda viršija įgyvendinimo sąnaudas, tolesnė kontrolės priemonės nėra vykdomos. (B. Lyon 2021).

6 Pav. Kontrolės sąnaudos ir rizikos žalos santykis



Šaltinis: Sudaryta autoriaus pagal B.Lyoan „Risk Assessment Standarts and Definitions“

Toliau svarbu įvertinti, kaip efektyviai kontrolė apsaugo organizaciją nuo potencialių grėsmių. Toks įvertinimas atliekamas remiantis išsamaus rizikos analizės procesu, kurio metu analizuojamas grėsmių poveikis ir tikimybė. Tokio vertinimo rezultatas vadinamas galima rizika. Įdiegus kontrolės priemones, paprastai sumažėja rizikos lygis, tačiau visada išlieka tam tikras likęs, priimtinas rizikos lygis, žinomas kaip likutinė rizika.

Kibernetinėms rizikoms mažinti taikoma daugiasluoksnė arba gynybos gilumoje strategija (angl. Defence in Depth). Yra keturi pagrindiniai kontrolės priemonių tipai, kurių derinimas yra rekomenduojamas siekiant efektyvios apsaugos:

- **Atgrasymo kontrolės:** Šios kontrolės sumažina grėsmės tikimybę, skatindamos potencialius pažeidėjus susimąstyti apie galimas atakos pasekmes. Pavyzdys: Saugumo politikų ir procedūrų viešinimas.
- **Prevencinės kontrolės:** Kontrolės, skirtos užkirsti kelią atakoms prieš jas pasiekiant savo tikslą. Jos apsaugo turtą, neleisdamos atakai pasinaudoti pažeidžiamomis vietomis. Pavyzdys: Slaptažodžių politikos ir kriptografijos naudojimas.
- **Aptikimo kontrolės:** Šios kontrolės atpažįsta ir įspėja apie vykstančias ar įvykusias atakas, leisdamos greitai reaguoti. Pavyzdys: Įsilaužimo aptikimo sistemos (IDS), kurios stebi tinklo srautą ar sistemos veiklą.
- **Korekcinės kontrolės:** Kontrolės, skirtos sumažinti incidento poveikį ir atkurti normalią veiklą. Pavyzdys: Atsarginių duomenų kopijų kūrimas ir atkūrimo planai.

Derinant šias priemones, gynybos gilumoje galima sukurti sistemą, kuri būtų atsparesnė įvairiems kibernetiniams iššūkiams. Kibernetinio saugumo valdymo priemonių lyginamoji analizė parodo, kad efektyviausia strategija yra ta, kuri apima skirtingų tipų kontrolės priemones, taikomas vienu metu.

Pavyzdžiui, siekdami apsaugoti duomenis nuo neautorizuoto sunaikinimo, pradžioje taikome prevencines prieigos kontrolės priemones. Jei ši kontrolė nepasiteisina, įjungiama aptikimo kontrolė, kuri padeda nustatyti paveiktus duomenis. Aptikus duomenų sunaikinimą, taikome korekcines priemones, pvz., duomenų atstatymą iš rezervinių kopijų, siekiant atkurti prarastą informaciją.

Toks integruotas požiūris į kibernetinio saugumo valdymą suteikia brandesnį saugumo lygmenį ir padeda organizacijoms efektyviai atremti įvairius kibernetinius iššūkius.

2.4.2. PCI DSS Tarptautinė kibernetinio saugumo sistema

PCI DSS (*Payment Card Industry Data Security Standard* angl.k.) – tai tarptautinis kibernetinio saugumo standartas, kuris buvo sukurtas siekiant užtikrinti jautrios finansinės informacijos, ypač susijusios su mokėjimo kortelių operacijomis, apsaugą. Šis standartas, inicijuotas 2004 m. pagrindinių kredito kortelių bendrovių, tokių kaip Visa ir MasterCard, ir šiuo metu yra prižiūrimas PCI Saugumo Standartų Tarybos. Nors PCI DSS nėra įstatymiškai įpareigojantis teisės aktas, jis faktiškai tapo beveik privalomu reikalavimu visoms organizacijoms, vykdančioms operacijas su kredito ir debeto kortelėmis, atsižvelgiant į teismų sprendimus ir verslo praktiką.

PCI DSS buvo sukurtas siekiant sumažinti kredito kortelių sukčiavimo atvejus ir užtikrinti nuoseklų saugumo lygį visose prekybos ir finansų sektorių įmonėse. Prieš šio standarto įvedimą kredito kortelių bendrovės naudojosi skirtingais saugumo metodais. PCI DSS suvienodino šiuos reikalavimus,

siekiant užtikrinti, kad prekybininkai ir finansų įstaigos laikytųsi aukštų saugumo standartų, tvarkant, saugant ir perduodant kortelės savininko duomenis.

Standartas susideda iš 12 atitikties reikalavimų, kurie yra suskirstyti į šešias logines grupes, žinomas kaip kontrolės tikslai:

1. **Sukurti saugų tinklą ir sistemas:** užtikrinti tinklo infrastruktūros ir sistemų apsaugą nuo išorinių bei vidinių grėsmių.
2. **Apsaugoti kortelės savininko duomenis:** garantuoti visų kortelės duomenų saugų tvarkymą ir saugojimą.
3. **Turėti pažeidžiamumų valdymo programą:** įdiegti ir vykdyti pažeidžiamumo valdymo strategijas, skirtas apsisaugoti nuo potencialių saugumo spragų.
4. **Užtikrinti kontroliuojamą ir autorizuotą prieigą prie sistemų:** apriboti prieigą prie jautrios informacijos tik įgaliotiems asmenims.
5. **Nuolatinis tinklo stebėjimas ir testavimas:** reguliariai atlikti tinklo saugumo patikras ir testus, siekiant nustatyti ir šalinti galimus pažeidžiamumus.
6. **Visiems įmonės darbuotojams suprantama ir įgyvendinta saugumo politika:** užtikrinti, kad visi įmonės nariai žinotų ir laikytųsi nustatytų saugumo politikų.

Organizacijos, siekiančios patvirtinti savo atitikimą PCI DSS reikalavimams, kasmet privalo atlikti savo sistemų sertifikavimą, kurį gali atlikti tiek išorinis, tiek vidinis vertintojas. Mažesnėms ir mažiau rizikingesnėms organizacijoms leidžiama atlikti savarankišką atestaciją, tačiau tai nemažina jų atsakomybės už saugumo užtikrinimą.

2.4.3. CIS Security Controls saugumo kontrolės kaip efektyvumo standartas

CIS Security Controls „Saugumo Kontrolės“ saugumo standartas sukurtas JAV 2008 m., kuomet Gynybos departamento saugumo skyrius paprašė Nacionalinės saugumo agentūros (NSA) padėti įvardinti veiksmingas kibernetinio saugumo kontrolės priemones. CIS ir SANS Institutų atstovai kartu su kitais viešojo ir privataus sektorių ekspertais sudarė konsorciumą, kuriame vertino grėsmes ir prioretizavo esminius kibernetinio saugumo būdus.

Nuo pat sukūrimo, **CIS** (Center for Internet Security) kontrolės yra nuolat atnaujinamos, atsižvelgiant į dinamiškai besikeičiančią kibernetinio saugumo aplinką, viena arba du kart per metus. Pradžioje CIS metodika siūlė 20 kibernetinio saugumo kontrolės punktų, apimančių įvairius apsaugos aspektus. Tačiau, siekiant efektyvumo ir lankstumo, šis skaičius vėliau buvo optimizuotas iki 18-os. Kontrolės taškų optimizavimas leido ne tik sujungti tam tikras kontrolės funkcijas, bet ir užtikrinti, kad šios kontrolės būtų pritaikomos įvairių dydžių ir tipų organizacijoms.

CIS kontrolės yra struktūrizuotos į tris įgyvendinimo grupes, kurios yra pritaikytos atsižvelgiant į skirtingų organizacijų kibernetinio saugumo brandos lygius ir specifinius saugumo poreikius:

1. **Įgyvendinimo Grupė 1 (IG1)** (viso 56 apsaugos priemonių) skirta organizacijoms, formuojančioms savo kibernetinio saugumo strategijas. Ši grupė apima pagrindinius saugumo elementus, būtinus bet kuriai organizacijai ir sudaro esminį saugumo užtikrinimo lygį.
2. **Įgyvendinimo Grupė 2 (IG2)** (viso 130 apsaugos priemonių) orientuota į organizacijas, kurios jau įdiegė pagrindines saugumo praktikas ir siekia toliau didinti savo saugumo atsparumą. IG2 praplečia IG1 taikomas saugumo priemones, įtraukdama papildomas strategijas, skirtas saugumo infrastruktūros stiprinimui.
3. **Įgyvendinimo Grupė 3 (IG3)(**viso 153 apsaugos priemonių) reprezentuoja aukščiausią saugumo užtikrinimo lygį, skirtą saugumo atžvilgiu, atsparioms organizacijoms, norinčioms pasiekti maksimalų saugumo efektyvumą. Ši grupė apima sudėtingas ir išsamesnes saugumo strategijas, siekiant užtikrinti aukščiausią įmanomą apsaugos lygį.

Kiekviena iš šių įgyvendinimo grupių grupės leidžia organizacijoms palaipsniui tobulėti saugumo srityje, laipsniškai pereinant iš IG1 į IG3 kibernetinės saugos brandos lygį.

CIS Kontrolės apima esmines apsaugos sritis, reikalingas organizacijai savo ekosistemai apsaugoti (žr. 3 Lentelę).

3 Lentelė. Lentelė „CIS Control 18 kibernetinio saugumo kontrolės punktų“

Inventorizacija ir Turto Kontrolė	Konfigūracijos Valdymas	Duomenų Apsauga	Saugumo Įvykių Stebėjimas	Kredencialų Valdymas	Saugumo Konfigūracijos
E-pašto ir Interneto Apsauga	Programinės Įrangos Apsauga	Tinklo Perimetro Apsauga	Fizinio Saugumo Kontrolė	Saugus Duomenų Atsarginių Kopijų Kūrimas	Incidentų Valdymas ir Atstatymas
Tinklo Stebėjimas ir Gynyba	Saugumo Mokymai ir Sąmoningumas	Aplikacijų Saugumo Valdymas	Incidentų Tyrimas ir Analizė	Mobilusis Saugumas	Įrangos ir Sistemų Pažeidžiamumų Valdymas

Šaltinis: Sudaryta autoriaus pagal www.cisecurity.org „Critical Security Controls“

Įgyvendinant šias kontrolės priemones, organizacija gali būti užtikrinta, kad ji taiko efektyvias saugumo priemones. Svarbu pabrėžti, kad CIS ištekliai yra nemokami ir bet kokios organizacijos gali naudotis jais be jokių apribojimų.

2.4.4. NIST kibernetinio saugumo modelis

2018 metais Nacionalinis Standartų ir Technologijų Institutas (NIST), priklausantis JAV Komercijos departamentui, pristatė atnaujintą kritinės infrastruktūros kibernetinio saugumo valdymo modelio versija. Atnaujinimu buvo siekiama sustiprinti kritinės infrastruktūros atsparumą kibernetinėms grėsmėms. Be to, NIST išleido Specialųjį Leidinį 800-53, kuris teikia saugumo priemonių katalogą skirtą JAV federalinėms informacinėms sistemoms. Šis leidinys reguliariai atnaujinamas, kad atitiktų naujausias technologijas ir rizikos scenarijus, ir apima rizikos valdymo metodus, orientuotus į blogiausio atvejo poveikio analizę. Šio standarto gairės taip pat padeda federalinėms agentūroms įgyvendinti 2002 m. Federalinį Informacijos Saugumo Valdymo Aktą (FISMA), nustatantį standartus federalinių agentūrų informacijos saugumui.

NIST 800-53 standartas yra būtinas ne tik federalinėms agentūroms, bet ir privačioms organizacijoms, siekiančioms užmegzti ar palaikyti verslo ryšius su JAV valstybinėmis įmonėmis, garantuojant, kad jos atitinka nustatytus kibernetinio saugumo standartus. Organizacijos, net kurios nesiekia tiesioginių verslo santykių su federalinėmis agentūromis, gali savanoriškai integruoti šio standarto rekomenduojamus saugumo elementus, pritaikydamos juos pagal savo specifinius saugumo poreikius, taip užtikrindamos universalumą ir lankstumą saugumo praktikose. NIST kibernetinio saugumo valdymo modelis susideda iš trijų sričių, kurios siekia apibrėžti ir užtikrinti organizacijos vykdomų funkcijų ir vidaus procesų integraciją į kibernetinio saugumo valdymą:

1. **Kibernetinio saugumo modelio branduolys** – kibernetinio saugumo modelio esmę sudaro veiklos, kurios grindžiamos pasauliniais standartais, metodikomis ir praktikomis. Ši pagrindinė dalis leidžia organizacijoje perduoti aiškią informaciją apie kibernetinio saugumo veiklas ir rezultatus visiems organizacijos nariams, nuo strateginio iki vykdomojo lygio. Modelio šerdis apima penkis pagrindinius elementus, kurie, sujungti į vieną bendrą procesą, formuoja visapusišką kibernetinio saugumo valdymo sistemą organizacijoje. Šie penki būtini elementai yra:
    - **1.1. Identifikavimas** (angl. Identify): Ši funkcija padeda organizacijoms nustatyti, kokius išteklius, duomenis ir sistemas būtina saugoti. Tai apima verslo aplinkos įvertinimą, kritinių funkcijų palaikymo išteklius ir susijusias kibernetines rizikas. Identifikavimas leidžia organizacijai sutelkti ir prioretizuoti savo pastangas, atsižvelgiant į jos rizikos valdymo strategiją ir verslo poreikius.
    - **1.2. Apsauga** (angl. Protect): Funkcija reikalinga kritinių infrastruktūros paslaugų teikimui užtikrinti ir potencialaus kibernetinio įvykio poveikio ribojimui. Tai apima tapatybės

valdymą ir prieigos kontrolę, darbuotojų mokymus, duomenų saugumą, informacijos apsaugos procesus ir procedūras, technologinių išteklių priežiūrą ir apsaugą.

1.3. **Aptikimas** (angl. Detect): Aptikimo funkcija apibrėžia veiklas, skirtas nustatyti kibernetinio saugumo įvykį. Tai apima kibernetinių įvykių prevenciją, nuolatinį saugumo stebėjimą ir procesų priežiūrą. Tai leidžia organizacijai laiku aptikti kibernetinius incidentus.

1.4. **Reagavimas** (angl. Respond): Ši funkcija skirta reaguoti į aptiktą kibernetinį incidentą. Tai apima atsakymo planavimą, komunikacijos valdymą per ir po įvykio, taip pat analizės planus, užtikrinančius veiksmingą atsakymą ir palaikančius atkūrimo pastangas.

1.5. **Atkūrimas** (angl. Recover): Atkūrimo funkcija skirta veiklos atnaujinimui įvykus kibernetiniam incidentui ir kaip būdas sumažinti jo poveikį organizacijai. Tai sudaryta iš atkūrimo planavimo procesų, nuolatinių strategijų peržiūrėjimo ir komunikacijos su suinteresuotaisiais per, ir po incidento.

2. **Kibernetinio saugumo pakopos** – Šios pakopos atspindi, kaip organizacija suvokia ir valdo kibernetinio saugumo riziką, apibūdindamos kibernetinio saugumo valdymo lygį organizacijoje, svyruojantį nuo pradinio (1 pakopa) iki adaptacinio lygio (4 pakopa). Pakopos įvertina kibernetinio saugumo procesų charakteristikas ir atsparumą grėsmėms bei apima rizikos valdymo praktiką, grėsmių aplinką, teisinio reguliavimo reikalavimus, organizacijos tikslus ir apribojimus. NIST apibrėžia kibernetinio saugumo lygius remdamasi trimis pagrindiniais elementais: rizikos valdymo procesu, rizikos valdymo programa ir organizacijos integracija į plačiąją kibernetinio saugumo ekosistemą. Šie elementai sudaro aiškią struktūrą, kuri padeda organizacijoms efektyviai valdyti ir reaguoti į kibernetinio saugumo iššūkius. Toks universalius saugumo pagrindas suteikia galimybę kiekvienai organizacijai pritaikyti jį atsižvelgiant į savo specifinius poreikius ir su jais susijusį rizikos lygį:

2.1. **Pradinė (1 pakopa):** Šiame saugumo valdymo lygyje organizacija nesilaiko išsamios kibernetinio saugumo rizikos valdymo strategijos; jos veiksmai dažniausiai yra spontaniški ir netvarkingi. Prioritetų nustatymas retai atitinka organizacijos rizikas ar esamus reikalavimus. Be to, pastebima ryški bendradarbiavimo su kitomis organizacijomis stoka.

2.2. **Informacinė (2 pakopa):** Rizikos valdymo procesas patvirtintas, bet ne visiškai įgyvendintas. Organizacija žino apie kibernetinio saugumo riziką, tačiau informacija apie grėsmes skleidžiama neoficialiais kanalais. Bendradarbiavimas su kitomis organizacijomis yra ribotas, o kibernetinio tiekimo grandinės rizikos suvokiamos, bet nenuosekliai sprendžiamos.

2.3. **Integruota (3 pakopa):** Rizikos valdymo procesai šiame lygyje yra aiškiai dokumentuoti, taikomi kasdienėje veikloje ir nuolat atnaujinami atsižvelgiant į verslo reikalavimus bei grėsmių aplinkos pokyčius. Organizacija aiškiai supranta savo vaidmenį kibernetinio saugumo ekosistemoje, veiksmingai bendradarbiauja su kitomis organizacijomis, keičiasi informacija, ir formaliai bei aktyviai tvarko rizikas, susijusias su kibernetinio saugumo apsauga.

2.4. **Adaptyvi (4 pakopa):** Šiame lygyje organizacija dinamiškai prisitaiko prie kibernetinių grėsmių, remdamasi ankstesne patirtimi ir esamais veiksmų planais. Kibernetinio saugumo valdymo programa yra pilnai integruota į verslo procesus, o saugumo stebėjimas ir planavimas yra traktuojami lygiagrečiai su finansinių grėsmių vertinimu. Organizacija aktyviai įsitraukia į kibernetinio saugumo ekosistemą, dalijasi įžvalgomis ir prisideda prie bendros rizikos suvokimo ir valdymo.

3. **Kibernetinio saugumo valdymo profilis.** Šis profilis yra pritaikytas derinant organizacijos verslo reikalavimus, rizikos toleranciją bei turimus išteklius su specifinėmis saugumo funkcijomis, kategorijomis ir subkategorijomis. Profilis yra svarbus įrankis kuriant realistišką kibernetinio saugumo rizikos mažinimo planą, kuris atsižvelgia į organizacijos tikslus, teisinius reikalavimus ir praktikas. Jis suteikia aiškią struktūrą, padedančią identifikuoti ir šalinti saugumo spragas, taip nuolat gerinant organizacijos kibernetinio saugumo būklę. Organizacijos gali sukurti keletą skirtingų profilių, kad optimaliai atitiktų įvairias veiklos sritis ir atskiras specifines kibernetinio saugumo reikmes.

NIST kibernetinio saugumo valdymo modelis apima daugiau nei 1000 kontrolės ir saugumo priemonių, kurios yra skirstomos į žemos, vidutinės ar aukštos kategorijas pagal jų poveikio stiprumą. Nors šio modelio įgyvendinimas nėra privalomas organizacijoms, išskyrus tam tikrus Specialiojo leidinio NIST 800-53 punktus, skirtus JAV federalinėms įstaigoms, kritinės infrastruktūros valdytojai ir kitos organizacijos gali jį savanoriškai taikyti.

Įdiegdamos NIST modelį, organizacijos turi galimybę nuspręsti, kokio lygio kibernetinio saugumo pakopos siekia, atsižvelgdamos į turimus išteklius, ir parengti atitinkamą įgyvendinimo planą. Šis planas yra lankstus ir gali būti koreguojamas atsižvelgiant į organizacijos prioritetus bei situacijos pokyčius. NIST modelis apima ne tik technologines, bet ir žmogiškuosius organizacijos išteklius, o taip pat traktuoja organizaciją kaip integralią kibernetinio saugumo ekosistemos dalį. Nors sertifikavimas pagal šį modelį nėra privalomas, jis gali būti taikomas siekiant patvirtinti modelio įgyvendinimą įstaigoje siekiant atitikti tam tikrus standartus ar reikalavimus.

2.4.5. ISO/IEC 27001/2:2022 - Informacijos saugumo valdymo sistemos standartai

ISO/IEC 27001/2 standartai sukurti, o vėliau atnaujinti 2022 m. Tarptautinio Standartizacijos Organizacijos (ISO) ir Tarptautinės Elektrotechnikos Komisijos (IEC). Jie atsirado kaip atsakas į vis didėjantį poreikį tvarkingai valdyti informacijos saugumą. ISO/IEC 27001 standartas, išsivystytas iš anksčiau egzistavusių praktikų ir standartų, teikia organizacijoms aiškią ir sistemingą informacijos saugumo valdymo struktūrą. Šis standartas nustato informacijos saugumo valdymo sistemoms (ISMS[27]) sukurti ir palaikyti reikalavimus, padedančius organizacijoms identifikuoti, valdyti ir mažinti saugumo rizikas bei užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą. ISO/IEC 27001 apima aiškius procesus ir struktūras, kurios yra būtinos veiksmingam informacijos saugumo valdymui.

Svarbu paminėti, kad ISO sertifikavimas yra taikomas standartams, kurių numeracija baigiasi skaitmeniu „1“. Todėl ISO/IEC 27002 priedas aprašo išsamias saugumo priemones ir kontrolės mechanizmus, kurių pagalba organizacija galėtų atitikti ISO/IEC 27001 standartą, tai savotiškas gidas.

Naujausioje ISO 27001 (2022) versijoje yra 93 kontrolės priemonės, kurios yra suskirstytos į keturias pagrindines temas. Šios temos skyriai apima įvairias informacijos saugumo valdymo sritis ir teikia gaires, kaip kiekvieną iš šių sričių įgyvendinti praktikoje:

- **Organizacinės kontrolės (A.5)**: Apima 37 kontrolės elementus, orientuotus į žmonių, programinės ir aparatinės įrangos bei sistemų elgsenos valdymą. Jos padeda suderinti visas organizacijos veiklas su nustatytais saugumo standartais.
- **Personalo kontrolės (A.6):** Ši kategorija apima 8 kontrolės elementus, kurie yra sukurti siekiant užtikrinti, kad darbuotojai laikytųsi saugumo standartų. Tai, būtinos žinios, švietimas ir įgūdžiai, suteikiant personalui priemones tinkamai pasirengti saugumo iššūkiams.
- **Fizinės kontrolės (A.7):** Šiame elemente yra 14 kontrolės priemonių, susijusių su fizinio saugumo aspektais, įskaitant įrangos ir įrenginių, kurie sąveikauja su žmonėmis ir objektais, valdymą. Jos užtikrina, kad būtų išlaikomas tinkamas fizinis saugumas ir apsauga nuo potencialių fizinio pavojaus šaltinių.
- **Technologinės kontrolės (A.8):** Sudaryta iš 34 kontrolės elementų, šios kontrolės yra orientuotos į efektyvų programinės ir aparatinės įrangos naudojimą. Tai ir įvairios technologijos, pvz., antivirusinės programos ir atsarginių duomenų kopijų kūrimo metodai, skirti apsaugoti organizacijos informacines sistemas ir duomenis nuo kibernetinių grėsmių.

[27] Informacijos saugumo valdymo sistemos (angl.k. Information security management systems)

7 Pav. PDCA Ciklas

Šaltinis: Sudaryta autoriaus

ISO 27001 standarto įgyvendinimas remiantis Planuok-Daryk-Tikrink-Veik (PDCA) ciklu yra veiksmingas būdas užtikrinti informacijos saugumo valdymo sistemos (ISMS) kokybę ir tobulinimą. Šis ciklas (žr. 6 paveikslėlį), kilęs iš kokybės užtikrinimo srities, padeda organizacijoms įgyvendinti ir nuolat gerinti informacijos saugumo valdymo procesus. PDCA ciklas ISO 27001 standarte susideda iš keturių pagrindinių žingsnių:

- **Planuok (Plan):** Šiame etape organizacija nustato informacijos saugumo tikslus ir procedūras, remdamasi išsamiu rizikos vertinimu. Tai apima saugumo politikos sukūrimą, saugumo tikslų nustatymą ir ISMS taikymo apimties nustatymą.
- **Daryk (Do):** Čia vykdomos suformuluotos procedūros ir politikos, įgyvendinant nustatytas kontrolės priemones sudarant saugumo priemonių diegimą, darbuotojų mokymą ir saugumo procesų įdiegimą praktikoje.
- **Tikrink (Check):** Šiame žingsnyje organizacija vertina ir peržiūri ISMS veiksmingumą., atliekant reguliarius auditus, saugumo įvykių analizę ir veiksmų efektyvumo vertinimą atsižvelgiant į iškeltus saugumo tikslus.
- **Veik (Act):** Atsižvelgdama į gautą informaciją ir išanalizavusi esamą situaciją, organizacija pradeda vykdyti ISMS (informacijos saugumo valdymo sistemos) tobulinimo veiksmus. Šie veiksmai turėtų sudaryti procesų atnaujinimą, saugumo politikos peržiūrą, naujų kontrolės priemonių diegimą bei esamų metodų optimizavimą, siekiant užtikrinti pastovų saugumo lygio kėlimą.

ISO 27001 standartas integruoja PDCA (Plan-Do-Check-Act) ciklą, kuris yra esminis komponentas užtikrinant, kad informacijos saugumo valdymo sistema (ISMS) būtų dinamiška ir nuolat atnaujinama. PDCA ciklas padeda organizacijoms planuoti saugumo strategijas (Plan), įgyvendinti nustatytas priemones (Do), vertinti jų veiksmingumą (Check) ir atlikti būtinas korekcijas (Act), kad būtų prisitaikyta prie besikeičiančių aplinkos sąlygų ir naujų saugumo grėsmių. Šis metodas suteikia struktūrišką ir ciklišką požiūrį į saugumo valdymą, leidžiantį nuolatos tobulinti ir pritaikyti saugumo procesus.

ISO 27001 standarte taip pat numatytas ISMS sertifikavimas, kuris patvirtina, kad organizacija laikosi tarptautiniu lygmeniu pripažintų informacijos saugumo valdymo standartų. Sertifikavimo procesas apima tris etapus:

1. **Pradinis įvertinimas**: Tai neformalus ISMS [28]įvertinimo etapas, kurio metu auditorius atlieka pirminę sistemų peržiūrą. Šioje stadijoje identifikuojamos pagrindinės savybės ir nustatomos galimos tobulinimo sritys.
2. **Išsamus atitikties auditas**: Antrasis etapas yra oficialus ir detalus. Per šį audito etapą įvertinama, kaip organizacija įgyvendina ISO 27001 standarto reikalavimus, įskaitant saugumo politikas, procesus ir kontrolės priemones.
3. **Nuolatiniai auditai:** Reguliariai atliekami auditai patikrina, ar organizacija atitinka ISO 27001 standarto reikalavimus. Tai nuolatinis ISMS veiksmingumo tikrinimas, jos atnaujinimai.

Verta paminėti, kad nors ISO 27001 sertifikavimas yra mokamas ir reikalauja išorinio akredituotojo paslaugų, organizacijos gali naudotis standarto turiniu ir be sertifikavimo, siekiant pagerinti savo informacijos saugumo praktikas. ISO 27002 standartas, būdamas ne sertifikuojamas, veikia kaip pagalbinė medžiaga ir savotiškas „gidas“, padedantis organizacijoms suprasti ir įgyvendinti ISO 27001 saugumo priemones.

ISO 27001 yra vienas populiariausių egzistuojančių informacijos saugos standartų. Nepriklausomas akredituotas standarto sertifikatas pripažįstamas visame pasaulyje. Per pastaruosius dešimt metų sertifikatų skaičius išaugo daugiau nei 450 proc. (ITGovernance.co.uk 2023). Standarto įgyvendinimas taip pat padeda atitikti įstatymų, tokių kaip JK ir ES GDPR (Bendrasis duomenų apsaugos reglamentas) ir NIS (tinklo ir informacinių sistemų) reglamentas, reikalavimus.

2.4.6. Kibernetinio saugumo valdymo modelių lyginamoji analizė

Kibernetinio saugumo valdymo srityje išsiskiria keturi pagrindiniai standartai, kurių kiekvienas yra unikaliai struktūrizuotas su savo kontrolės mechanizmais ir reikalavimais. Šie standartai apima PCI DSS, CIS kontrolės, NIST ir ISO 27001, ir kiekvienas jų yra sukurtas siekiant užtikrinti organizacijų duomenų saugumą, atitinkant jų specifinius poreikius ir rizikos valdymo strategijas. Nors jie dalijasi tam tikrais panašumais, svarbu išskirti jų skirtingus požiūrius į saugumo valdymą ir taikymo sritį.

Kibernetinio saugumo valdymo modelių įvairovė suteikia organizacijoms galimybę rinktis standartą, atitinkantį jų saugumo reikalavimus ir strategiją. Kiekvienas modelis, įskaitant PCI DSS, CIS kontrolės, NIST ir ISO 27001, atlieka svarbų vaidmenį ne tik technologinių saugumo priemonių diegime, bet ir atsakingame rizikų valdyme. PCI DSS yra skirtas kredito kortelių duomenų apsaugai ir reikalauja kasmetinio sertifikavimo, o CIS siūlo lankstesnes saugumo praktikas be privalomo

[28] Informacijos saugumo valdymo sistemos (angl.k. Information security management systems)

sertifikavimo. NIST dominuoja JAV, o ISO 27001 plačiai taikomas tarptautiniu lygiu, abu pabrėždami saugumo brandos lygius, siekiant efektyvaus duomenų saugumo.

4. Lentelė PCI DSS, CIS kontrolė, NIST, ISO 27001 palyginimas

Kriterijus	**PCI DSS**	**CIS Kontrolė**	**NIST**	**ISO 27001**
Pritaikomumas	Kredito kortelių duomenų sauga	Bendri kibernetinio saugumo principai	Bendroji praktika, JAV valstybinės įstaigos	Bendroji informacijos sauga
Kontrolių skaičius	12 reikalavimų, 5-20 kontrolės kiekvienoje	18 kontrolės, 153 apsaugos priemonės	20 grupių, daugiau nei 1000 kontrolių	4 skyriai, 93 kontrolės
Sertifikavimas	Būtinas kasmet	Neprivalomas	Būtinas tik NIST 800-53 vyriausybinėms įstaigoms	Galimas tik per akredituotą auditą
Brandos lygiai	Nėra	Yra	Yra	Yra
Populiarumas	Globalus	Globalus	Daugiausia JAV	Globalus
Konceptualūs Atnaujinimai	Vidutiniškai kas 2-3 metus	Vidutiniškai kas 1-2 metus	Vidutiniškai kas 2 metus	Kas 5is metus

Šaltinis: Sudaryta autoriaus PCI DSS, CIS, NIST, ISO 27001 palyginimas

Šių saugumo modelių taikymas skatina organizacijas mokytis ir prisitaikyti prie kintančių kibernetinių grėsmių, formuojant tarptautinio saugumo politiką ir įtvirtinant jų patikimumą pasauliniu mastu. Integracija į verslo procesus sukuria "domino efektą": kai viena organizacija pradeda taikyti tam tikrus saugumo standartus, tai dažnai tampa privaloma sąlyga verslo partnerystėms, skatindama vis plačiau naudoti šiuos standartus. Tokiu būdu įmonės siekia užtikrinti saugumo politikos suderinamumą su partneriais, didindamos šių standartų populiarumą.

3. KIBERNETINIO SAUGUMO INTEGRACIJA Į VERSLO MODELIAVIMĄ

Pasauliniai dinamiški skaitmeninimo procesai reikalauja, kad organizacijos greitai prisitaikytų prie naujų sąlygų ir savo verslo modelius pritaikytų prie skaitmeninės paradigmos. Įmonių vidinių ir inovatyvių strategijų sinchronizavimas su išorinių ekonominės sistemos parametrų sąlygomis yra būtina sąlyga veiksmingai įmonių veiklai skaitmeninės ekonomikos realijose.[29]

Integruojant verslo modelius su teisės aktų bei kibernetinės saugos principais, atsiveria naujos efektyvaus verslo planavimo galimybės todėl, itin svarbu ne tik išsamiai suprasti įstatymus bei keliamus reikalavimus, bet ir gebėti juos taikyti praktikoje taip, kad tai netaptų kliūtimi verslo plėtrai. Organizacijoms tenka investuoti reikšmingus išteklius tiek supratimui apie šiuos reikalavimus, tiek jų adekvačiam įgyvendinimui, siekiant išvengti pernelyg didelės administracinės naštos.

3.1. Įstatymai ir Direktyvos: Kibernetinio saugumo Teisinė Bazė

Kibernetinis saugumas, svarbus tiek vietiniu, tiek tarptautiniu lygmeniu, remiasi sudėtinga teisine baze, skirta stiprinti skaitmeninę erdvę prieš naujai atsirandančias grėsmes. Šios sistemos pagrindą Europos Sąjungoje ir Lietuvoje sudaro Bendrasis duomenų apsaugos reglamentas (GDPR) ir Tinklų bei informacinių sistemų saugumo direktyva (Angl.k. NIS), užtikrinantys duomenų apsaugą ir tvirtą tinklų saugumą kritinėse sektoriuose. Lietuva dar labiau sustiprina šią poziciją savo Kibernetinio saugumo įstatymu, suderindama nacionalines pastangas su platesniais ES tikslais.

3.1.1. Bendrasis duomenų apsaugos reglamentas (GDPR)

Bendrasis duomenų apsaugos reglamentas (GDPR), kuris įsigaliojo 2018 m. gegužės 25 d., yra esminis Europos Sąjungos (ES) teisės aktas, sukuriantis išsamų asmens duomenų tvarkymo ir apsaugos reglamentavimą. Šis reglamentas buvo parengtas atsižvelgiant į didėjančią skaitmeninių technologijų integraciją į visuomenės kasdienybę ir augantį poreikį užtikrinti aukštesnį asmens duomenų saugumo lygį.

GDPR [30]taikymo sritis apima visus subjektus, tvarkančius ES piliečių asmens duomenis, neatsižvelgiant į jų geografinę veiklos vietą. Tai reiškia, kad reglamentas gali būti taikomas tiek didelėms tarptautinėms korporacijoms, tiek nedidelėms vietinėms įmonėms ir net individualiems verslininkams,

[29] 71. O. Kibik, O. Taran-Lala, V. Saienko, T Metil, T. Umanets, I.Maksymchuk „Vectors for Enterprise Development in the Context of the Digitalization of the Economy“ (2022), Volume 13, Issue 2, pages: 384-395| https://doi.org/10.18662/po/13.2/460

[30] Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 https://eur-lex.europa.eu/eli/reg/2016/679/oj

jeigu jie renka ar tvarko asmeninius duomenis savo veikloje. Tačiau GDPR netaikomas fiziniams asmenims, vykdantiems duomenų tvarkymą grynai asmeniniais ar šeimos tikslais.

Reglamento esmė – stiprinti asmenų teises ir kontroliuoti savo asmens duomenis. GDPR nustato aiškius reikalavimus, kaip turi būti informuoti duomenų subjektai apie jų duomenų tvarkymą, įskaitant tvarkymo tikslus ir duomenų saugojimo trukmę. Asmenys įgijo teisę reikalauti prieigos prie jiems priklausančių duomenų, jų taisymo ar ištrynimo, vadinamąją „teisę būti pamirštam“, bei teises į duomenų perkeliamumą ir prieštaravimą jų tvarkymui.

Be to, GDPR nustato griežtus duomenų saugumo reikalavimus įmonėms ir organizacijoms, tvarkančioms asmeninius duomenis. Privaloma įgyvendinti efektyvias technines ir organizacines priemones, užkertančias kelią duomenų nutekinimui, neteisėtam jų naudojimui ar kitokiems saugumo pažeidimams. Įstatymas taip pat įpareigoja organizacijas nedelsiant pranešti atitinkamoms priežiūros institucijoms ir patiems duomenų subjektams apie rimtus duomenų saugumo pažeidimus.

Šiandien GDPR laikomas vienu iš pagrindinių standartų, reglamentuojančių asmens duomenų apsaugą pasauliniu mastu, ir yra svarbus žingsnis užtikrinant asmenų privatumą bei saugumą skaitmeninėje erdvėje.

3.1.2. Europos Sąjungos NIS 2 direktyva

NIS2 [31]direktyva, priimta 2022 m. pabaigoje, yra svarbus žingsnis siekiantis sustiprinti kibernetinį saugumą Europos Sąjungoje. Įsigaliojusi 2023 m., ji keičia 2016 m. priimtą pirmąją NIS [32]direktyvą ir įveda griežtesnius reikalavimus bei platesnę taikymo sritį. Direktyva apima ne tik kritinės infrastruktūros operatorius, bet ir kitas organizacijas, teikiančias svarbias paslaugas ar vykdančias veiklas, kurios gali turėti didelį poveikį visuomenės ar ekonomikos stabilumui. Tai reiškia, kad daug daugiau subjektų, nepriklausomai nuo jų dydžio, bus įpareigoti laikytis direktyvos nustatytų kibernetinio saugumo standartų.

Viena iš svarbiausių NIS2 direktyvos naujovių yra išsamiai apibrėžti kibernetinio saugumo reikalavimai organizacijoms.

Tai apima:

- **Rizikos vertinimo procesus:** Organizacijos turi reguliariai atlikti rizikos vertinimus, kad nustatytų ir įvertintų potencialias kibernetines grėsmes bei pažeidžiamumus savo sistemose ir procesuose.

[31] Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[32] Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 https://eur-lex.europa.eu/eli/dir/2016/1148/oj

- **Informacinių sistemų saugumo priemones:** Privaloma įdiegti atitinkamas technines ir organizacines saugumo priemones, siekiant apsaugoti informacines sistemas ir juose saugomus duomenis nuo kibernetinių grėsmių.
- **Incidentų valdymo procesus:** Aiškiai apibrėžti veiksmai ir procedūros, kaip elgtis atsiradus kibernetinio saugumo incidentams, įskaitant incidentų aptikimą, analizę, atsaką ir paslaugų atkūrimą.
- **Verslo tęstinumo planavimą ir krizių valdymą:** Privalu parengti planus, kaip užtikrinti svarbiausių verslo funkcijų tęstinumą ir atkurti veiklos operacijas po kibernetinių incidentų.
- **Kibernetinio ir informacinio saugumo mokymus:** Svarbu įgyvendinti nuolatines mokymo ir švietimo programas darbuotojams, siekiant juos informuoti apie kibernetinio saugumo grėsmes ir skatinti laikytis geriausių praktikų.
- **Tiekimo grandinės saugumas:** Tiekimo grandinės saugumo užtikrinimas, reikalaujant organizacijoms vertinti ir valdyti savo tiekėjų kibernetinio saugumo rizikas.

Vadovybės atsakomybė už kibernetinio saugumo užtikrinimą yra naujas aspektas, pabrėžiamas NIS2 direktyvoje. Ši direktyva įpareigoja aukščiausio lygio vadovus ne tik užtikrinti efektyvias kibernetinio saugumo priemones, bet ir asmeniškai atsakyti už jų įgyvendinimą bei incidentų prevenciją. Tai reiškia, kad esant saugumo trūkumams, vadovai bus tiesiogiai atsakingi. Be to, NIS2 direktyva reikalauja, kad organizacijos nuolat ir aktyviai vertintų savo atitiktį direktyvos reikalavimams, įgyvendintų būtinas priemones ir stiprintų savo kibernetinio saugumo sistemą

Be to, direktyva nustato aiškias terminų taisykles pranešimams apie incidentus. Organizacijos įpareigotos pranešti apie saugumo incidentus atitinkamoms priežiūros institucijoms per konkretų laiką nuo incidento aptikimo. Pradinis pranešimas turi būti pateiktas per 24 valandas, o atnaujinta informacija – per 72 valandas. Galutinė ataskaita su visomis incidento detalėmis turi būti pateikta per vieną mėnesį. Šios taisyklės turėtų užtikrinti, kad incidentai būtų valdomi efektyviai ir, kad būtų imamasi būtinų veiksmų, siekiant sumažinti galimą žalą, bei užkirsti kelią panašiems incidentams ateityje.

ENISA[33], kaip centrinė Europos Sąjungos kibernetinio saugumo agentūra, yra itin svarbi NIS2 direktyvos įgyvendinimo dalis, teikianti būtiną paramą valstybėms narėms, skatindama bendradarbiavimą ir pasidalijimą žiniomis. Agentūra, dirbdama kartu su nacionaliniais kibernetinio saugumo centrais, užtikrina organizacijų atitiktį direktyvos reikalavimams per reguliarius patikrinimus ir auditus. Ši veikla ne tik padeda apsaugoti organizacijas nuo kibernetinių grėsmių, bet ir yra pagrindas stipriam Europos Sąjungos skaitmeninio saugumo pagrindui.

[33] Europos Sąjungos Kibernetinio Saugumo Agentūra (ENISA) https://www.enisa.europa.eu/topics/cybersecurity-policy/data-protection

3.1.3. Lietuvos kibernetinio saugumo įstatymas

Lietuvos Respublikos kibernetinio saugumo įstatymas[34], priimtas 2018 m., yra svarbus nacionalinis teisės aktas, skirtas stiprinti šalies kibernetinį saugumą. Jis nurodo kibernetinio saugumo valdymo, incidentų valdymo ir atsakomybės principus, taikomus tiek valstybės, tiek privačiose įstaigose. Įstatymas taip pat numato Nacionalinio kibernetinio saugumo centro įsteigimą, kuris atlieka svarbų vaidmenį koordinuojant ir vykdant kibernetinio saugumo politiką Lietuvoje.

Įstatymas nurodo aiškias gaires, kaip įvairios organizacijos turi tvarkyti kibernetinio saugumo klausimus, įskaitant duomenų apsaugą, informacinių sistemų saugumą ir reagavimą į incidentus. Jis taip pat nustato įpareigojimus įmonėms ir institucijoms pranešti apie kibernetinius incidentus bei užtikrinti tinkamas prevencines priemones.

- Įstatyme išdėstyti konkretūs įpareigojimai dėl kibernetinių incidentų pranešimo, įskaitant:
- Kas turėtų pranešti apie incidentus
- Kokius incidentus būtina pranešti
- Per kiek laiko po incidento aptikimo turi būti pateiktas pranešimas,
- Į kurią instituciją ar organą turi būti pateiktas pranešimas.

Atsižvelgiant į NIS2 direktyvos patvirtinimą, kurio reikalavimai buvo išsamiai aptarti ankstesniame skyriuje, šiame skyriuje detaliai neaptarsime Lietuvos kibernetinio saugumo įstatymo, priimto 2018 m., kadangi jis bus atnaujintas atsižvelgiant į NIS2 direktyvą iki 2024 m. rudens.

3.1.4. JAV ir kiti tarptautiniai reglamentai

JAV ir tarptautiniai reglamentai formuoja pagrindą, ant kurio organizacijos privalo statyti savo kibernetinio saugumo politikas. Pavyzdžiui, 2014 m. JAV priimtas Federalinės informacijos saugumo modernizavimo įstatymas (FISMA) nustato griežtus reikalavimus federalinių agentūrų informacijos sistemų saugumui. Įstatymas reikalauja, kad federalinės agentūros ne tik įdiegtų efektyvias informacijos apsaugos priemones, bet ir sukurtų išsamias rizikos valdymo programas. Šis reglamentavimas yra vienas iš daugelio pavyzdžių, kaip nacionaliniai ir tarptautiniai teisės aktai tiesiogiai veikia organizacijų veiklas, skatindami jas ne tik sekti naujausias saugumo praktikas, bet ir reguliariai atnaujinti savo saugumo strategijas atsižvelgiant į kintančią teisinę aplinką.

Nagrinėjant FISMA 2014 įstatymą, svarbu išskirti esminius saugumo reikalavimus, kurie yra būtini federalinėms JAV agentūroms ir įmonėms, siekiant užtikrinti aukštą informacijos sistemų

[34] Lietuvos Respublikos Kibernetinio Saugumo Įstatymas: https://www.e-tar.lt/portal/legalAct.html?documentId=67b9e0b07eb711e8ae2bfd1913d66d57

saugumo lygį. Šie reikalavimai padeda organizacijoms tinkamai valdyti ir apsaugoti jų informacines sistemas bei duomenis:

1. **Sistemų rizikos kategorijos:** Informacinės sistemos turi būti suskirstytos pagal rizikos lygius atsižvelgiant į informacijos tipus ir nustatytomis saugumo kontrolės priemonės.
2. **Bazinių saugumo kontrolės priemonių įgyvendinimas:** Federalinės sistemos privalo atitikti minimalius saugumo reikalavimus, nurodytuose NIST SP 800-53 standartuose.
3. **Kontrolės priemonių dokumentavimas:** Saugumo ir privatumo planas (SSPP) yra pagrindinis dokumentas, kuriame fiksuojamos bazinės saugumo priemonės, skirtos sistemos apsaugai.
4. **Rizikos vertinimas:** Sistemų rizika turėtų būti reguliariai vertinama, siekiant patikrinti esamų saugumo priemonių veiksmingumą ir nustatyti, ar reikia papildomų priemonių.
5. **Kasmetinės saugumo revizijos:** Programų vadovai ir agentūrų vadovai privalo atlikti kasmetines saugumo sistemos revizijas, siekiant gauti FISMA sertifikatą.
6. **Nuolatinė stebėsena:** Agentūros privalo nuolat stebėti FISMA akredituotas sistemas, siekiant nustatyti galimas silpnąsias vietas. Bet kokie atlikti pakeitimai turi būti fiksuojami SSPP.

Įgyvendinant šiuos FISMA reikalavimus, įmonės ne tik užtikrina aukštą saugumo lygį, bet ir demonstruoja atsakomybę bei įsipareigojimą saugoti valstybinius ir asmeninius duomenis, tuo pačiu stiprinant pasitikėjimą jų veikla.

2021 m. įsigaliojęs CIRCIA[35] įstatymas, esantis Nacionalinio gynybos akto dalis, įveda pranešimo apie kibernetinius incidentus reikalavimus JAV kritinės infrastruktūros subjektams. Nors CIRCIA tiesiogiai taikomas tik JAV teritorijoje, jo principai yra aktualūs ir tarptautinėms bendrovėms, bendradarbiaujančioms su JAV. Tai skatina skaidrumą ir glaudesnį bendradarbiavimą kibernetinio saugumo srityje.

FISMA ir CIRCIA, būdami JAV vidiniais reglamentais, vis dėlto daro didelę įtaką tarptautiniams verslams, ypač tiems, kurie siekia bendradarbiavimo su JAV federalinėmis agentūromis ar veikia kritinės infrastruktūros sektoriuje. Lietuvos įmonėms, norinčioms plėsti savo veiklą tarptautinėje arenoje ar stiprinti ryšius su JAV partneriais, būtina ne tik išsamiai išmanyti šiuos reglamentus, bet ir integruoti jų pagrindinius principus į savo kibernetinio saugumo strategijas, kad būtų užtikrintas aukštas duomenų apsaugos lygis ir atitikimas teisės aktams.

Taip pat reikėtų paminėti ir anksčiau aptartus PCI DSS standartus bei NIST 800-53 rekomendacijas, kurie nustato gaires mokėjimo kortelių duomenų saugumui ir informacijos saugumo rizikos valdymui užtikrinti. Šių standartų įgyvendinimas yra esminis, bet kurios organizacijos

[35] Cyber Incident Reporting for Critical Infrastructure Act of 2022 https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

siekiančios apsaugoti savo informacinius išteklius ir užtikrinti sklandų atitikimą kibernetinio saugumo reikalavimams, kibernetinio saugumo strategijos elementas.

3.2. Valdymo, Rizikos Valdymo ir Atitikties (GRC) Modelio Taikymas

Valdymo, rizikos valdymo ir atikties (GRC[36]) metodika, sukūrta Atvirosios Atitikties ir Etikos Grupės (angl. Open Compliance and Ethics Group, OCEG), siūlo struktūrizuotą ir sistemingą būdą, kaip organizacijos galėtų įgyvendinti atitiktį būtiniausiems įstatymais ir standartams, kartu efektyviai valdydamos rizikas. Šis metodas remiasi požiūriu, kad valdymas, rizikos valdymas ir atitikties užtikrinimas yra būtini veiksniai, neatskiriami nuo visapusiškai sėkmingo verslo valdymo. Mokslinėje literatūroje (P.Vincente, M. Silva 2011, A.Gericke, H-G. Fill, D.Karagiannis, R. Winter 2009, N. Racz, E. Weippl, A. Seufert 2010) ir įvairiuose įmonių publikacijose kibernetinio saugumo tema (Amazon Web Services[37], Microsoft [38](2024)) teigiama, kad GRC principų taikymas suteikia galimybes kurti naujus verslo modelius, atitinkančius ne tik reguliavimo reikalavimus, bet ir užtikrinančius tvarumą saugumo srityje.

Pabrėžiant GRC reikšmę, svarbu akcentuoti valdymo praktikos svarbą, siūlant metodus, kaip organizacija gali pasiekti savo tikslus ir adekvačiai reaguoti į iššūkius bei kurti plėtros strategijas. Šis požiūris užtikrina saugų ir atsakingą augimą.

Todėl sieksiu pritaikyti GRC principus verslo modeliavimui ir kibernetinei saugai apjungti, remdamasis GRC pagrindiniais principais: valdymu, rizikos valdymu ir atitikties užtikrinimu.

Prieš gilinantis į GRC modelio – tris pagrindinius elementus, svarbu paminėti Atvirąją Atitikties ir Etikos Grupę (OCEG) ir jos vaidmenį šiame kontekste. OCEG, įkurta 2002 m. kaip atsakas į didžiules korporacijų nesėkmes ir "dot com" burbulą, prasidėjo kaip diskusijų iniciatyva siekianti sužinoti kaip pagerinti verslų atitiktį ir etiką. Šios diskusijos greitai virto platesnėmis ir apimančiomis veiklos valdymą, rizikų valdymą ir atitikties užtikrinimą.

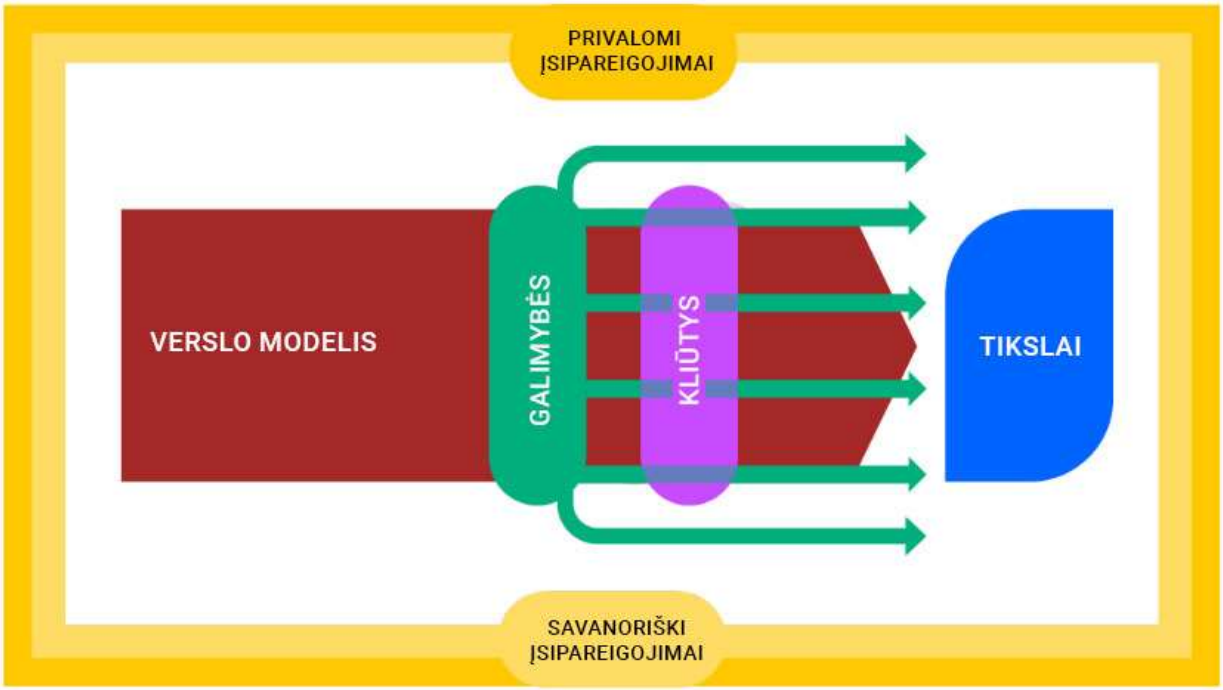
Pažvelgus iš platesnės perspektyvos, svarbu suprasti, kad kiekviena organizacija yra sukūrusi savo veiklos modelį, kurio tikslas – pasiekti nustatytus tikslus, susiduriant su įvairiais iššūkiais ir neapibrėžtumu.

[36] Anglų.k. Governance, Risk and Compliance

[37] Amazon What is GRC (Governance, Risk, and Compliance)? https://aws.amazon.com/what-is/grc/

[38] The Microsoft 365 Maturity Model – Governance, Risk, and Compliance Competency https://learn.microsoft.com/en-us/microsoft-365/community/microsoft365-maturity-model--governance-and-compliance

8 Pav. Verslo aplinka pagal GRC



Šaltinis: „GRC Compability Model 3.5 2024, OCEG Red book

Organizacijos veikla yra susijusi su galimybėmis, kurios dažniausiai siejamos su nauda ir veiklos rezultatais, kliūtimis, kurios atitinka riziką, ir įsipareigojimais, kurių laikymasis užtikrina atitikties valdymą. Tad, veiklos, rizikos ir atitikties valdymas bei užtikrinimas yra būtinas norint išlaikyti subalansuotą ir sveiką organizacijos ekosistemą (žr. 8 paveikslėlį):

Galimybės dažniausiai yra susijusios su teigiamu poveikiu ir nauda organizacijai, kurią galima išmatuoti kaip pasiekimus. Šie pasiekimai fiksuojami ir valdomi naudojant veiklos valdymo sistemas ir pagrindinius veiklos rodiklius (KPI) (angl.k Key Performance Indicator).

Kliūtys, su kuriomis susiduria organizacija, dažnai yra susijusios su rizika – tai neigiamas aspektas, turintis įtakos organizacijos tikslams. Su šiomis kliūtimis kovojama įdiegiant rizikos valdymo sistemas ir nustatant pagrindinius rizikos rodiklius (KRI) (angl.k. Key Risk Indicator).

Įsipareigojimų laikymasis organizacijoje paprastai siejamas su atitikties užtikrinimu, t.y. kaip gerai organizacija atitinka nustatytus reikalavimus ir įsipareigojimus. Ši sritis reguliuojama naudojant atitikties valdymo sistemas ir pagrindinius atitikties rodiklius (KCI) (angl.k. Key Control Indicators).

GRC taip pat laikomas kelrodžiu į principingą veiklą, apimantį platų skirtingų skyrių ir galimybių spektrą. Neretai GRC suprantamas klaidingai – kaip valdybos užduotis, tam tikra programinė įranga, atitikties programa ar netgi IT saugumo sritis. Tačiau iš tikrųjų GRC reiškia gebėjimų integraciją ir vadovavimą, apimantį šešias kritines disciplinas, kurios turi ir panašumų, ir išskirtinumų.

9 Pav. GRC 3.5 kritinės disciplinos

Šaltinis: „GRC Compability Model 3.5 2024, OCEG Red book

3.2.1. Valdymas ir priežiūra kritinė GRC disciplina

Valdymas ir priežiūra GRC modelyje yra esminis pagrindas, nustatantis, kaip organizacija veikia ir užtikrina savo tikslų įgyvendinimą. Valdymas čia interpretuojamas kaip struktūra, kuri nukreipia ir reguliuoja organizaciją. Tai apima visus procesus, politikas ir praktikas, kurios vadovauja organizacijos veiklai ir sprendimų priėmimui. Iš esmės, valdymas tarnauja kaip organizacinis centras, sujungiantis įvairias veiklas, tokias kaip IT operacijos, mokymai, produktų kūrimas ir daugiau, užtikrinant, kad visos šios veiklos būtų suderintos taip, kad remtų ir skatintų bendrovės bendruosius tikslus ir uždavinius.

Valdymo ir priežiūra pagrindiniai aspektai apima atsakomybių paskirstymą, informacijos srautų kontrolę, veiklos stebėseną ir laikymąsi nustatytų procedūrų. Tai apima tai, kaip vadovai gauna duomenis, kaip priimami sprendimai, kaip bendrovė bendrauja su pagrindiniais suinteresuotaisiais asmenimis, taip pat ir valdybos sudėtį bei valdymo taisykles. Veiksmingam valdymui reikalingas išsamus organizacijos vaizdas, pasitelkiant duomenis iš vidaus auditų, rizikos vertinimų, atitikties stebėjimo ir kitų įvertinimų strateginiam sprendimų priėmimui informuoti.

Paprastai valdyba yra atsakinga už valdymą, nustatant strategijas, kurios paskirstomos per visą organizaciją. Kiekvienas sprendimas, priimtas pagal valdymo sistemą, veikia visus suinteresuotuosius subjektus, nuo darbuotojų iki investuotojų, klientų iki tiekėjų. Stiprios valdymo programos sukuria skaidrią ir atsakingą infrastruktūrą, kuria naudodamasi organizacija vykdys veikla.

Nuolatinis mokymasis ir prisitaikymas prie besikeičiančios verslo aplinkos yra būtini veiksniai sėkmingai valdymo ir priežiūros praktikai. Valdymo strategijos ir priemonės turi būti lanksčios, kad pritaikytų prie kiekvienos organizacijos specifikos. Pavyzdžiui, įmonė, kuri nekaupia asmens duomenų, neprivalo taip griežtai laikytis Bendrojo duomenų apsaugos reglamento (GDPR) kaip įmonė, tvarkanti didelius asmens duomenų kiekius.

Valdymas pagal GRC modelį kelia reikalavimus, nurodančius, kaip organizacija turėtų veikti, siekiant efektyviai ir etiškai įgyvendinti savo tikslus. Tai sudaro praktinį pagrindą, užtikrinantį, kad verslo veiklos būtų derinamos su strateginiais tikslais, laikantis nustatytų teisinių ir etinių standartų, taip pat būtų efektyviai valdomos ir rizikos.

3.2.2. Strategija ir veiklos užtikrinimas

Šios disciplinos tikslas – užtikrinti, kad organizacijos veikla būtų orientuota į jos strateginius tikslus ir, kad būtų naudojami visi prienami ištekliai siekiant šių tikslų. Tai reiškia, jog šioje srityje svarbiausia yra ne tik išteklių efektyvus naudojimas, bet ir įsitikinimas, jog kiekvienas organizacijos veiksmas prisideda prie bendro tikslo.

Pagrindiniai "Strategijos ir veiklos užtikrinimo" elementai:

- **Strateginės krypties nustatymas**, kuriame aiškiai išdėstomi organizacijos tikslai ir kaip šie tikslai bus pasiekti. Čia svarbus vaidmuo tenka aiškiai suformuluotai misijai ir vizijai.
- **Išteklių efektyvus panaudojimas**, užtikrinant, kad kiekvienas organizacijos turimas išteklius būtų naudojamas kuo produktyviau, remiantis prioritetais ir strateginiais tikslais.
- **Iniciatyvų ir projektų valdymas**, užtikrinant, kad kiekviena veikla būtų aiškiai susieta su organizacijos strateginiais tikslais ir kad būtų stebimas jų įgyvendinimo progresas.
- **Adaptacija ir lankstumas**, leidžiantis organizacijai greitai prisitaikyti prie kintančių aplinkybių ir optimizuoti veiklos procesus atsižvelgiant į naujausias rinkos tendencijas ir iššūkius.

"Strategija ir veiklos užtikrinimas" GRC modelyje skatina strateginį planavimą ir pro-aktyvų veiklos valdymą, užtikrinant, kad kiekvienas organizacijos žingsnis būtų žengtas atsižvelgiant į ilgalaikius tikslus ir viziją. Tai padetų organizacijai ne tik siekti aukštų rezultatų dabartyje, bet ir užtikrinti tvarų augimą bei konkurencingumą ateityje.

3.2.3. Rizika ir sprendimai

Rizikų valdymas ir sprendimai yra skirtas užtikrinti, kad būtų identifikuotos ir tinkamai tvarkomos įvairiausios rizikos, galinčios trukdyti organizacijos tikslams. Šios disciplinos sudaro kelis pagrindinius procesus, kurie padeda organizacijai tvarkyti neapibrėžtumą ir priimti geriausius sprendimus. Be rizikų identifikavimo, įvertinimo ir mažinimo, ši disciplina įtraukia ir sprendimų paramos procesus, kurie leidžia organizacijai veiksmingai reaguoti į iškylančius iššūkius ir pasinaudoti galimybėmis:

- **Rizikos identifikavimas:** Apibūdinamas kaip siekis atpažinti galimas rizikas, su kuriomis organizacija gali susidurti. Tai tiek vidaus, tiek išorės rizikos, pavyzdžiui, finansines, operacines, teisines, reputacinės ar strategines rizikas.
- **Rizikos įvertinimas:** Tai rizikų poveikio ir incidento tikimybės analizė. Šiame etape organizacija įvertina, kaip kiekviena rizika gali paveikti jos veiklą ir kokia tikimybė, kad ši rizika iš tiesų pasireikš.
- **Rizikos mažinimo strategijos:** Remiantis identifikavimo ir įvertinimo rezultatais, suformuojamos rizikos mažinimo ar valdymo strategijos. Tai sudarytų vidinių kontrolės procedūrų stiprinimą, kibernetinio saugumo priemonių diegimą, atsarginių planų kūrimą ar rizikos perkėlimą į draudimą.
- **Rizikos stebėsena ir peržiūra**: Rizikos valdymas yra pastovus procesas, reikalaujantis reguliarios rizikos veiksnių stebėsenos ir strategijų peržiūrėjimo, kad būtų užtikrintas jų aktualumas ir veiksmingumas.
- **Sprendimų paramos mechanizmai:** Tai scenarijų planavimo ir prognozavimo įrankiai, kurie padeda organizacijos vadovams priimti strategiškai svarbius sprendimus, remiantis išsamia rizikos poveikio ir galimybių analize.

Imkime finansų sektoriaus įmonę, kuri susiduria su išorinėmis rizikomis, tokiais kaip rinkos svyravimai ar geopolitinės įtampos, ir vidaus rizikomis, pavyzdžiui, IT sistemų pažeidžiamumais ar darbuotojų klaidomis. Šios rizikos yra identifikuojamos ir vertinamos kaip rizikos valdymo proceso dalis, kuris prasideda nuo rizikos identifikavimo etapo. Šiame etape organizacija nustato visas galimas grėsmes, su kuriomis ji gali susidurti.

Tolesnis etapas – rizikos įvertinimas. Čia analizuojama kiekvienos rizikos tikimybė ir galimas poveikis. Pavyzdžiui, jei IT sistemų pažeidžiamumas būtų išnaudotas kibernetinės atakos, tai gali sukelti didelę grėsmę įmonei, turinčią aukštą tikimybę ir gali lemti reikšmingą finansinį nuostolį.

Toliau remiantis gauta informacija, organizacija rengia rizikos mažinimo planus. Šie planai gali apimti saugumo priemonių stiprinimą, IT infrastruktūros atnaujinimą ar net rizikos perkėlimą draudimo bendrovėms. Pagrindinis rizikų valdymo tikslas nėra visiškai pašalinti rizikas, bet sumažinti jų galimą neigiamą poveikį iki priimtino lygio. Šis procesas reikalauja nuolatinio rizikos stebėjimo ir planų atnaujinimo, kad organizacija galėtų efektyviai prisitaikyti prie kintančių sąlygų ir užtikrinti veiklos stabilumą bei tęstinumą.

3.2.4. Atitiktis ir etika

Atitiktis ir etika GRC 3.5 modelyje yra esminės veiklos dalys, kurios pradedamos nuo aiškaus organizacijos veiklos specifikos supratimo ir atitikties reikalavimų identifikavimo. Pirmasis žingsnis – suprasti, kokių konkrečių įstatymų, reglamentų ir etikos principų laikymosi organizacija privalo siekti, remiantis jos veiklos sritimi ir specifika. Tai padeda išvengti nereikalingo resursų švaistymo ir nukreipia dėmesį į svarbiausias atitikties sritis, sutaupant laiką ir finansus.

Pagrindiniai "Atitikties ir etikos" aspektai yra:

- **Atitikties reikalavimų identifikavimas:** Aiškus organizacijos veiklos specifikos supratimas ir atitinkamų teisinių bei etikos reikalavimų, kurių laikymasis yra privalomas, identifikavimas.
- **Įstatymų ir reglamentų, standartų identifikavimas ir atitikimas:** Užtikrinimas, kad veikla atitiktų visus jai aktualius teisinius ir kitus būtinuosius reikalavimus.
- **Etikos kodekso įgyvendinimas:** Sukūrimas ir diegimas etikos kodekso, atspindinčio organizacijos vertybes ir nustatančio elgesio lūkesčius.
- **Mokymai ir švietimas:** Mokymų programų organizavimas darbuotojams apie atitikties ir etikos svarbą.
- **Vidinės kontrolės ir stebėsenos mechanizmai:** Įdiegimas efektyvių vidinių kontrolės sistemų atitikties ir etikos laikymuisi užtikrinti.

Šis procesas stiprina ne tik teisinį laikymąsi, bet ir organizacijos kultūrą, kurioje skatinama aukšta darbo etika. Tokiu būdu, "Atitiktis ir etika" ne tik apsaugo organizaciją nuo teisinių sankcijų, bet ir skatina teigiamą įvaizdį, stiprina prekės ženklą ir prisideda prie ilgalaikės sėkmės, pabrėžiant atsakingą verslo vystymą.

3.2.5. Saugumas ir tęstinumas

"Saugumo ir Tęstinumo" konceptas GRC 3.5 modelyje apima daug daugiau nei vien turtinės ar informacinės vertės apsaugą; jis įkūnija pačią organizacijos gyvybingumo esmę kritinėse situacijose. Šių disciplinų reikšmė glūdi gebėjime išlaikyti organizacijos veiklos tęstinumą netikėtų įvykių akivaizdoje. Ši sritis reikalauja iš anksto apgalvotos strategijos, kurioje kiekviena detalė – nuo infrastruktūros atsparumo iki darbuotojų parengtumo – yra kruopščiai išplėtota ir įvertinta, siekiant užtikrinti, kad bet kokioje situacijoje organizacija galėtų ne tik išsilaikyti, bet ir tęsti savo veiklą su minimaliais sutrikimais.

Tai, kad "Saugumas ir Tęstinumas" yra neatsiejama bet kurios modernios organizacijos veiklos dalis, akcentuoja ne tik fizinių ar skaitmeninių išteklių apsaugos svarbą, bet ir holistinį požiūrį į organizacijos atsparumą. Organizacijos skiriančios pakankamai dėmesio šiems aspektams, gali ne tik apsisaugoti nuo galimų finansinių nuostolių ar reputacinės žalos, bet ir užsitikrinti, kad jų pagrindinės

vertybės būtų saugios net ir pačiomis sudėtingiausiomis sąlygomis. Gebėjimai greitai atsigauti po įvairių sukrėtimų ne tik stiprina organizacijos įvaizdį, bet ir įtvirtina pasitikėjimo jausmą savo darbuotojams, klientams bei partneriams.

Išsami "Saugumo ir Tęstinumo" planavimo strategija sudaro:

- **Infrastruktūros ir duomenų apsaugos analizė:** Įvertinama, kaip gerai organizacijos fizinė ir skaitmeninė infrastruktūra yra apsaugota nuo potencialių pažeidimų ir nesklandumų, įskaitant duomenų saugumą ir prieigą prie kritinių sistemų.
- **Prevencinių priemonių įgyvendinimą:** Sukuriamos ir taikomos strategijos, skirtos išvengti ar mažinti grėsmių poveikį.
- **Atkūrimo planus:** Paruošiami veiksmų planai, kaip greitai atkurti kritines funkcijas ir paslaugas po sutrikimo.
- **Mokymus ir pratybas:** Organizuojamos mokymų sesijos ir pratybos darbuotojams, siekiant užtikrinti jų pasirengimą veikti pagal planą krizės atveju.

Vis dėlto, "Saugumas ir Tęstinumas" nėra tik apie taktinius planus ir procedūras; tai taip pat apie organizacijos kultūros stiprinimą, kurioje kiekvienas asmuo suvokia savo vaidmenį saugumo grandinėje. Sėkmingas šių disciplinų įgyvendinimas reikalauja nuolatinės vadovų ir darbuotojų įsitraukimo, skaidrumo bei bendradarbiavimo, užtikrinant, kad saugumo ir tęstinumo principai taptų neatsiejama organizacijos veiklos dalimi. Taip "Saugumas ir Tęstinumas" transformuojasi iš iššūkio į galimybę stiprinti organizacijos atsparumą, inovatyvumą ir pasitikėjimą, kartu kuriant tvirtą pagrindą ilgalaikiam augimui ir sėkmei.

3.2.6. Auditas ir užtikrinimas

"Auditas ir Užtikrinimas" atlieka lemiamą vaidmenį užtikrinant organizacijos veiklos atitiktį nusistatytoms normoms, procedūroms ir politikoms. Šios disciplinos yra svarbios skaidrumui, atskaitomybei ir veiklos efektyvumui garantuoti, taip stiprinant pasitikėjimą tarp įvairių suinteresuotųjų šalių, įskaitant organizacijos vadovus, darbuotojus bei akcininkus.

Audito procesai suprantami kaip nepriklausomas, sistemingas vertinimas, kurio tikslas – patikrinti organizacijos atitiktį teisės aktams, standartams bei nustatytoms vidaus procedūroms. Auditas apima ne tik finansų srities tikrinimą, bet ir įvertina procesus, sistemas bei operacijas visose organizacijos veiklos srityse, įskaitant atitiktį ir saugumą, suteikdamas galimybę identifikuoti operatyvinius trūkumus.

Užtikrinimo veikla yra procesas, kurio metu sekama, kaip visi organizacijos procesai ir sistemos veikia pagal iš anksto nustatytas direktyvas, užtikrinant jų efektyvumą, saugumą ir atitiktį privalomiems standartams. Užtikrinimo veiklą sudaro reguliarūs vidaus patikrinimai, rizikos vertinimus ir kontrolės priemonių efektyvumo analizę.

Rizikos valdymo auditas tikrina, ar esami organizacijos rizikos valdymo metodai yra pakankamai efektyvūs potencialių grėsmių prevencijai ir minimizavimui. Atitikties auditas analizuoja, kaip organizacija atitinka privalomus teisinius reikalavimus, pramonės standartus ir vidines taisykles, siekdama išvengti galimų sankcijų ir reputacinės žalos. Saugumo auditas tikrina, ar organizacijos fizinės ir informacinės apsaugos priemonės atitinka aukščiausius saugumo standartus ir yra tinkamos apsaugoti organizacijos turtą ir duomenis.

Reguliariai vykdomi audito ir užtikrinimo procesai ne tik padeda identifikuoti veiklos trūkumus, bet ir parodo organizacijos pasiryžimą veikti pagal aukščiausius standartus. Toks nuoseklus įsipareigojimas laikytis nustatytų principų neabejotinai prisideda prie organizacijos ilgalaikės sėkmės ir sustiprina pasitikėjimą tarp visų suinteresuotųjų šalių, padėdamas pagrindą atsakingam ir etiškam verslo vystymui.

3.3. Kibernetinio saugumo modelio verslui sukūrimas ir plėtra

Kibernetinis saugumas, kaip buvo aptarta ankstesniuose darbo skyriuose, yra nepaprastai svarbus veiksnys, turintis tiesioginį poveikį įmonių tvarumui ir augimui, ir jo svarba tik didėja, atsižvelgiant į sparčiai besivystančias technologijas ir vis sudėtingesnes kibernetines grėsmes.

Analizuojant verslo modeliavimo aspektus, buvo nustatyta, kad šiuolaikinės organizacijos naudoja įvairius modelius ir strategijas, kad pasiektų pelningumą, konkurencingumą ir augimą rinkoje. Tačiau, kaip buvo aptarta skyriuje "Verslo modeliavimo teoriniai aspektai", vienas iš esminių iššūkių yra efektyviai integruoti kibernetinį saugumą į šiuos modelius, kad būtų galima ne tik apsaugoti įmonės duomenis ir sistemas, bet ir užtikrinti tvarų verslo plėtros modelį.

Vertinant kibernetinio saugumo iššūkius, aprašytus skyriuje "Kibernetinio saugumo iššūkiai ir sprendimai versle", buvo atkreiptas dėmesys į tai, kad kibernetinės grėsmės ir atakos yra vis sudėtingesnės ir išradingesnės. Taip pat buvo išnagrinėti pagrindiniai kibernetinio saugumo standartai ir kontrolės priemonės, pateikti skyriuje "Kibernetinio saugumo principai ir apsaugos metodai", kurie yra būtini siekiant sukurti veiksmingą saugumo modelį.

Taigi, remiantis sukaupta informacija ir išanalizavus kibernetines atakas bei jų veikimo principus, šiame skyriuje siekiama sulieti visus šiuos aspektus į vieną holistinį modelį, pasitelkiant GRC (angl.k Governance, Risk Management, and Compliance) - Valdymo, Rizikos Valdymo ir Atitikties metodiką. GRC metodika pasirinkta dėl jos gebėjimo integruoti valdymo praktikas, rizikos valdymą bei teisinių reglamentų aspektus į vieną struktūrizuotą ir sistemingą procesą.

3.3.1. Verslo modelio drobė kaip struktūrinis pagrindas

"Verslo modelio drobė" (Business Model Canvas, BMC), sukurta A. Osterwalderio, yra vienas iš lanksčiausių ir efektyviausių įrankių verslo modeliavimui. Šis metodas suteikia aiškią struktūrą, padalijant verslo idėjas ir procesus į devynis pagrindinius segmentus: Klientų Segmentus, Siūlomą Vertę, Kanalus, Klientų Santykius, Pajamų Srautus, Pagrindinius Išteklius, Pagrindines Veiklas, Pagrindinius Partnerius ir Sąnaudų Struktūrą. Ši metodika leidžia verslams ne tik išsamiai įsivertinti ir planuoti savo veiklą, bet ir atskleisti svarbiausias sąveikas tarp skirtingų verslo komponentų.

Integruojant BMC į mūsų kibernetinio saugumo strategiją, kiekvienas verslo modelio segmentas bus praturtintas kibernetinio saugumo elementais. Tai užtikrins, kad kibernetinio saugumo praktikos taptų integralia verslo strategijos ir kasdienės veiklos dalimi, suteikianti kiekvienam verslo aspektui aiškią ir sistemingą saugumo dimensiją.

Pavyzdžiui, integravus kibernetinį saugumą į segmentą "Siūloma Vertė", galime išryškinti, kaip saugumo aspektai gali padidinti produkto ar paslaugos vertę klientams. Segmentas "Pagrindinė Veikla" leis išanalizuoti, kaip saugumo veiklos integruojamos į įprastą verslo veikimą. Toks metodinis požiūris ne tik užtikrintų kiekvieno verslo aspekto apsaugą, bet ir skatintų saugumo iniciatyvas, kurios prisideda prie bendro verslo efektyvumo ir konkurencinio pranašumo rinkoje.

Pasirinkus "Business Model Canvas" kaip pagrindą, mūsų modelis tampa ne tik struktūrizuotu, bet ir dinamišku įrankiu. Jis leidžia organizacijoms greitai reaguoti į kibernetinės saugumo aplinkos pokyčius, išlaikant aiškią verslo kryptį. Taip BMC tampa ne tik modeliavimo pagrindu, bet ir tiltu, jungiančiu verslo plėtrą su kibernetinio saugumo užtikrinimu.

3.3.2. Kibernetinio saugumo integracija į verslo segmentus

Integruojant saugumo principus į visus "Business Model Canvas" (BMC) segmentus, galima sukurti veiksmingą ir atsparų kibernetinio saugumo modelį versle. Toks metodas leidžia ne tik apsaugoti organizacijos veiklą nuo kibernetinių grėsmių, bet ir stiprinti verslo modelį, įdiegiant patikimumo ir saugumo kultūrą.

Klientų Segmentai: Įtraukiant saugumo reikalavimus į klientų segmentavimą, galima atsižvelgti į skirtingas klientų grupių lūkesčius. Verslo klientams gali būti reikalingi aukštesni duomenų apsaugos standartai, o individualiems vartotojams svarbesni gali būti asmeninio privatumo užtikrinimo aspektai.

Siūloma Vertė: Integravus aukšto lygio kibernetinį saugumą į siūlomą vertę, šis aspektas tampa neatsiejama produkto ar paslaugos dalimi, suteikiančia klientams papildomą pasitikėjimo ir lojalumo

jausmą. Pabrėžiant saugumo savybes savo produktuose ir paslaugose, organizacijos gali išsiskirti rinkoje, suteikiant savo siūlomai vertei konkurencinį privalumą.

Kanalai: Saugant visus klientų įsigijimo ir sąveikos kanalus, organizacija ne tik apsaugo klientų duomenis nuo neteisėtos prieigos, bet ir užtikrina aukštos kokybės, sklandžią vartotojų patirtį.

Santykiai su Klientais: Įtraukiant kibernetinį saugumą į visus klientų santykių aspektus, užtikrinama, kad klientų duomenys yra tvarkomi ir saugomi pagal aukščiausius standartus.

Pajamų Srautai: Užtikrinant, kad mokėjimo procesai bei kiti pajamų generavimo kanalai yra saugūs, sumažėja finansinių nuostolių ir reputacijos žala.

Pagrindiniai Ištekliai: Saugumo technologijos, procesai ir ekspertizė yra esminiai organizacijos ištekliai. Jų nuolatinis tobulinimas ir atnaujinimas yra būtinas, siekiant efektyviai apsisaugoti nuo esamų ir būsimų kibernetinių grėsmių.

Pagrindinės Veiklos: Integruojant saugumo principus į pagrindines veiklas, užtikrinama, kad visos organizacijos operacijos vyktų saugioje aplinkoje. Tai mažina riziką ir užtikrina verslo operacijų stabilumą, apsaugant nuo galimų saugumo incidentų.

Pagrindiniai Partneriai: Vertinant partnerių ir tiekėjų saugumo praktikas, užtikrinama, kad visi su jais susiję verslo procesai yra apsaugoti. Bendradarbiavimas su partneriais, kurie laikosi aukštų saugumo standartų, garantuoja bendrą verslo saugumą.

Sąnaudų Struktūra: Saugumo investicijos organizacijoje turėtų būti traktuojamos ne kaip papildomos išlaidos, bet kaip būtina verslo veiklos dalis. Saugumo išlaidos laikomos investicija, kuri padeda užtikrinti organizacijos tvarumą ir patikimumą, padedant išvengti potencialių nuostolių.

Integravus kibernetinio saugumo elementus į visus "BMC" segmentus, organizacijos sukuria tvirtą saugumo kultūrą, kuri ne tik apsaugo verslą nuo kibernetinių grėsmių, bet ir skatina inovacijas bei augimą saugioje aplinkoje.

3.3.3. Kibernetinio saugumo įvertinimo įrankis BMC segmentams pagal GRC disciplinas

Analizuojant mokslinę literatūrą ir esamas GRC (valdymo, rizikos valdymo ir atitikties) strategijas, nustatėme pagrindinius principus, reikalingus kibernetinio saugumo efektyviam įtraukimui į verslo strategijas. Išnagrinėjus turimą medžiagą paaiškėjo, kad, nepaisant plačiai pripažintos kibernetinio saugumo svarbos, daug organizacijų dar nepilnai įtraukia šiuos aspektus į savo verslo procesus. Remiantis gilia GRC disciplinų žinių analize, siūlome struktūrizuotą klausimyną, kuris padėtų organizacijoms aiškiau identifikuoti, kaip kibernetinio saugumo praktikas galima integravimo į kiekvieną "Business Model Canvas" segmentą.

Siekiant tai pasiekti, verta adresuoti po tris klausimus kiekvienam BMC segmentui, kurie yra struktūruoti taip, kad atsakydami į juos, verslininkai ir organizacijų vadovai galėtų gilintis į kiekvieno segmento specifiką ir suvokti, kokios saugumo priemonės ir procesai yra reikalingi optimaliam saugumo lygiui užtikrinti (**žr. 5 lentelę**).

5. Lentelė. Kibernetinio saugumo integracijos įvertinimo klausimynas

BMC Segmentas	**Valdymas**	**Rizikos valdymas**	**Atitiktis**
Klientų segmentai	Kaip įvairūs kibernetinio saugumo būdai pritaikomi atsižvelgiant į klientų segmentų specifiką?	Kokias specifines kibernetines grėsmes pastebite skirtinguose klientų segmentuose?	Kaip informuojate klientus apie saugumo politikas ir jų teises?
Siūloma vertė	Kaip kibernetinio saugumo strategijos įtraukiamos į jūsų siūlomas prekes ar paslaugas?	Kokios grėsmės kyla jūsų siūlomai vertei ir kaip jas šalinamas?	Kaip užtikrinamas atitikimas saugumo standartams jūsų siūlomoje vertėje?
Pristatymo kanalai	Kaip saugumo politika yra įgyvendinama per visus klientų sąveikos kanalus?	Kokios kibernetinės grėsmės susijusios su jūsų naudojamais pristatymo kanalais?	Kaip užtikrinate, kad jūsų kanalai atitinka saugumo reglamentus?
Klientų santykiai	Kaip valdote ir apsaugote klientų duomenis ?	Kokias grėsmes klientų duomenų saugumui kelia jūsų sąveikos su jais?	Kaip jūsų klientų duomenų saugojimas atitinka duomenų apsaugos įstatymus?
Pajamų srautai	Kokį poveikį kibernetinis saugumas daro jūsų pajamų srautams?	Kokios kibernetinės grėsmės gali paveikti jūsų pajamų srautus?	Kaip pajamų generavimas suderinatas su saugumo ir privatumo reikalavimais?
Pagrindiniai ištekliai	Kaip saugote ir valdote savo pagrindinius išteklius?	Kaip identifikuojate ir tvarkote su pagrindiniais ištekliais susijusias rizikas?	Ar mūsų pagrindiniai ištekliai ir jų naudojimas atitinka saugumo standartus?

Pagrindinės veiklos	Kaip saugumo strategijos integruojamos į pagrindines veiklas?	Kokios yra pagrindinės kibernetinės rizikos mūsų veikloje ir kaip mes jas mažiname?	Kaip užtikrinama, kad pagrindinės veiklos atitiktų saugumo reglamentus?
Pagrindiniai partneriai	Kaip įtraukiate saugumo aspektus bendradarbiaujant su partneriais?	Kaip vertinate ir tvarkote su partneriais susijusias rizikas?	Kaip užtikrinate, kad partneriai laikytųsi saugumo standartų?
Sąnaudų struktūra	Kaip kibernetinis saugumas veikia mūsų sąnaudų struktūrą ir biudžetą?	Kaip mes planuojame ir valdome išlaidas, susijusias su kibernetinio saugumo užtikrinimu?	Ar saugumo išlaidos atitinka teisinius reikalavimus?

2. Šaltinis: Sudaryta autoriaus naudojant BMC ir GRC modelius

Atsakydami į šiuos klausimus, verslininkai tūrėtų gauti gilesni supratimą apie tai, kaip kibernetinio saugumo aspektai yra į įtraukti į verslo strategijas ir operacijas.

Šio klausimyno kūrimo procesas atskleidė, kad, nors standartiniai GCR klausimai yra geras pradžios taškas, tam tikrais atvejais gali prireikti išplėstinės analizės, remiantis GRC 3.5 modeliu. Šis modelis suteikia dar išsamesnį ir individualizuotą požiūrį į kibernetinio saugumo integravimą, leisdamas organizacijoms giliau nagrinėti specifines rizikas, valdymo strategijas ir atitikties reikalavimus, pritaikytus prie jų unikalių aplinkybių.

Kaip pavyzdžiui pateikiamas išplėstinis klausimynas pagal GRC 3.5 modelį tik „***Klientų segmentai***“ skyriui:

Valdymas: Kaip mūsų organizacija pritaiko saugumo strategijas, atsižvelgdama į skirtingų klientų segmentų poreikius ir lūkesčius?

Rizikos Valdymas: Kaip mes identifikuojame ir vertiname specifines kibernetinio saugumo rizikas, susijusias su kiekvienu klientų segmentu?

Atitiktis: Kaip užtikriname, kad visi klientų segmentai yra tvarkomi laikantis atitinkamų duomenų apsaugos ir privatumo reglamentų?

Auditas: Kokius periodinius saugumo auditus atliekame skirtinguose klientų segmentuose, siekiant įvertinti saugumo politikų veiksmingumą ir atitiktį?

Organizacinis atsparumas: Kaip mūsų organizacija užtikrina atsparumą saugumo incidentams skirtinguose klientų segmentuose, ir kaip tai veikia mūsų bendrą atsparumą?

Atkūrimas po incidentų: Kokias atkūrimo strategijas ir planus turime, jei kibernetinis saugumo incidentas paveiktų specifinius klientų segmentus?

Remiantis išplėstiniu GRC 3.5 modeliu, gali būti sukurtas platesnis klausimynas, padedantis dar plačiau integruoti kibernetinio saugumo principus į "BMC", suteikiantis galimybę bet kuriam asmeniui, neturinčiam net gilių IT srities žinių, efektyviai įvertinti organizacijos kibernetinį atsparumą.

4. KIBERNETINIO SAUGUMO INTEGRACIJA Į VERSLO MODELIAVIMĄ: TYRIMO METODOLOGIJA

Šiame skyriuje pateikiama išsami magistro baigiamojo darbo empirinės dalies metodologija, atspindinti ryšį tarp empirinio tyrimo ir teorinės darbo dalies. Aptariama pasirinkta tyrimo strategija, taip pat naudoti duomenų rinkimo metodai ir dalyvių atrankos procesas, įskaitant dalyvavusių asmenų charakteristikas. Detaliai pristatomi duomenų rinkimo instrumentai, paaiškinamas duomenų rinkimo procesas, bei išdėstyti duomenų apdorojimo metodai ir analizės strategija, leidžianti išgryninti svarbiausius tyrimo rezultatus. Pateikiama informacija apie tyrimą ribojusius veiksnius, tyrimo validumą kurių buvo laikomasi atliekant tyrimą.

Tyrimo objektas – įmonių, veikiančių Lietuvoje ir užsienyje, praktinė patirtis ir iššūkiai integruojant kibernetinio saugumo strategijas į jų verslo modelius, atsižvelgiant į specifinius rinkos ir teisinio reglamentavimo reikalavimus

Tyrimo tikslas – empiriškai ištirti kibernetinio saugumo integracijos į verslo modeliavimą procesus bei galimybes.

Tyrimo uždaviniai:

1. **Literatūros ir dokumentų analizė:** Analizuoti esamą literatūrą ir dokumentus apie kibernetinio saugumo integravimą į verslo modelius, nustatant svarbiausius integracijos principus ir strategijas.
2. **Modelio kūrimas:** Sukurti kibernetinio saugumo integracijos metodiką, remiantis BMC+GRC aspektais, siekiant sistemingai įdiegti saugumo elementus į verslo strategiją.
3. **Ekspertų interviu analizė**: Įvertinti duomenis gautus iš ekspertų interviu, siekiant nustatyti, kaip efektyviai kibernetinis saugumas integruojamas į įvairias verslo situacijas.
4. **Rekomendacijų formulavimas:** Remiantis tyrimo rezultatais, formuluoti rekomendacijas kibernetinio saugumo integracijai į verslo modelius tobulinimui.

4.1. Metodologijos pasirinkimas ir tyrimo metodai

Metodologijos pasirinkimas. Siekiant išsamiai ištirti kibernetinio saugumo integracijos į verslo modeliavimą procesus, šiame magistro darbe bus pasitelkiamas ***kokybinis tyrimo metodas***, kuris leis įsigilinti į sudėtingas ir dažnai subtilesnes sąveikas tarp minėtų sričių. Kokybinio tyrimo metodo pasirinkimas yra grindžiamas siekiu atskleisti ne tik paviršutiniškas sąsajas, bet ir gauti gilesnį, prasmingesnį supratimą apie tai, kaip verslo subjektai Lietuvoje integruoja kibernetinio saugumo

aspektus į savo veiklos modelius, taip pat koks yra šios integracijos poveikis verslo strategijoms, operacijoms ir bendrai saugumo kultūrai.

Šiame darbe taikoma A. Bryman kokybinių tyrimų metodologija (Bryman, 2001), kuri buvo pritaikyta remiantis A. Augustinaičio ir kitų mokslininkų siūlomomis ekspertinio vertinimo procedūromis (Augustinaitis ir kt., 2009). Pagal šią metodologiją, kokybinis tyrimas yra grindžiamas skerspjūvio nuostata, apimant tik vieną empirinį ciklą. Toks metodologinis požiūris leidžia detaliai analizuoti ir vertinti kibernetinio saugumo integraciją į verslo modelius, užtikrinant, kad gauti duomenys atspindėtų realias verslo praktikas ir jų iššūkius.

Norint užtikrinti kokybinio tyrimo patikimumą ir tinkamumą, buvo taikomi mokslinėje literatūroje aptariami principai: tikrumas, perkeliamumas ir įtikinamumas, kaip nurodyta V. Žydžiūnaitės ir S. Sabaliausko (2017) darbuose. Šie principai yra būtini norint įsitikinti, kad tyrimo rezultatai bus patikimi ir galėtų būti pritaikomi platesnėje konteksto aplinkoje. Tyrimo tikslas – sukurti konceptualų kibernetinio saugumo valdymo modelį, integruojant BMC+GRC aspektus, remiantis gautomis ekspertų įžvalgomis ir patarimais. Sukurtas modelis bus siūlomas kaip pagrindas tolesniems tyrimams ir praktiniam taikymui, siekiant ištirti jo efektyvumą ir pritaikomumą įvairiose verslo situacijose.

Tyrimo metodai. Tyrimas – tai tam tikras procesas, kuris susideda iš kelių sudedamųjų dalių:

1. **Teorinių įžvalgų formavimas**: Perskaityta, analizuota ir susisteminta mokslinė literatūra, įstatymai bei dokumentai, tiesiogiai susiję su kibernetinio saugumo ir verslo modeliavimo tematika, leido geriau suprasti, kaip organizacijos integruoja kibernetinio saugumo aspektus į savo veiklos modelius.
2. **Interviu tyrimo metodikos ruošimas.** Rengiama metodika atskleidžianti kibernetinio saugumo integracijos ypatybes į verslo modelius, sukuriamas klausimynas, atrenkami ekspertai ir sudaroma tyrimo eiga.
3. **Duomenų rinkimas:** Struktūruotų interviu pagalba organizuojamas duomenų rinkimas, jų sisteminimas ir gautų atsakymų analizė.
4. **Rezultatų interpretavimas:** Pagrindinių tyrimo rezultatų apibendrinimas, formuojant bendrą ekspertų nuomonę.
5. **Rezultatų ir išvadų pateikimas:** Galutinių išvadų ir praktinių rekomendacijų pristatymas, remiantis duomenų analize ir interpretacija.

Teorinių įžvalgų formavimas: Kadangi šis tyrimas orientuotas į kibernetinio saugumo aspektų integraciją, ekspertų apklausos anketa bus sudaryta remiantis išsamiu teoriniu ir praktiniu literatūros nagrinėjimu, siekiant užtikrinti, jog kiekvienas klausimas atitiktų tyrimo tikslus. Klausimų

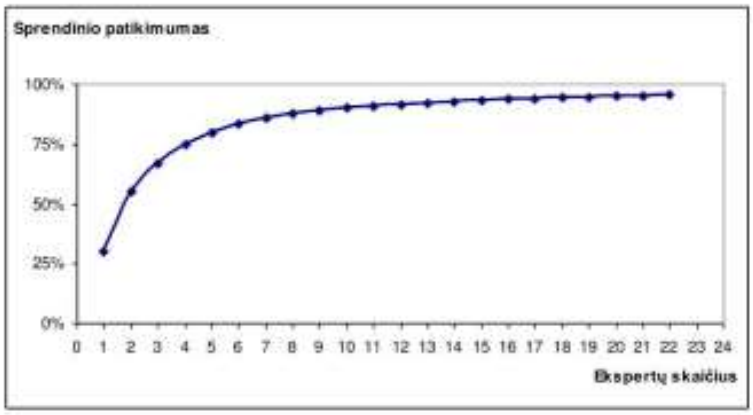
formulavimas buvo grindžiamas teoriniais modeliais, kurie aptariami mokslinėje literatūroje, ir praktiniais kibernetinio saugumo iššūkiais, su kuriais susiduria įmonės. Klausimai buvo kruopščiai atrinkti, kad atspindėtų skirtingas kibernetinio saugumo integracijos dimensijas – nuo verslo valdymo ir procedūrų iki technologinių sprendimų ir žmogiškųjų išteklių valdymo.

Duomenų analizės procese bus taikoma kokybinė turinio analizė, kurios tikslas – struktūruoti, koduoti ir interpretuoti gautą medžiagą, atskleidžiant esmines temas, kategorijas ir prasmes. Toks analizės metodas yra ypač tinkamas kokybiniams duomenims išgryninti svarbiausias įžvalgas ir tendencijas, susijusias su kibernetinio saugumo integravimu į verslo praktikas.

Remiantis išsamia duomenų analize, bus pateiktos praktinės rekomendacijos verslo subjektams. Kurios nurodys konkrečias strategijas ir veiksmus, kuriuos įmonės galės taikyti, siekiant efektyviau integruoti kibernetinio saugumo aspektus į savo veiklos modelius. Tyrimas taip pat atvers kelius tolesnėms diskusijoms ir moksliniams tyrinėjimams šioje svarbioje ir aktualioje srityje, teikdamas ne tik akademinę, bet ir praktinę vertę.

Tyrimo imtis: Ekspertinio tyrimo imties formavimas buvo grindžiamas teoriniais pagrindais, išplėtotais klasikinėje testų teorijoje, kurios principai atskleidžia, kad ekspertų skaičiaus ir jų priimtų sprendimų patikimumas yra susiję greitai mažėjančia netiesine funkcija. Remiantis A. Augustinaičio et al. (2009) ir kitų mokslininkų (A.Baležentis ir M.Žalimaitė 2011) darbais, buvo nustatyta, kad ekspertų vertinimų patikimumas nežymiai priklauso nuo jų skaičiaus didėjimo. Atlikus analizę, paaiškėjo, kad nedidelė ekspertų grupės suteikiamos įžvalgos gali būti lygiavertės didesnės grupės išvadoms, kaip pabrėžia Libby ir Blashfield (1978) bei patvirtina A.Augustinaitis (2009). Šių mokslininkų rekomenduojamas optimalus imties dydis, vykdant ekspertinius vertinimus, yra nuo penkių iki devynių ekspertų.

10 Pav. Ekspertų skaičiaus įtaka vertinimo patikimumui



Šaltinis: A.Augustinaitis ir kt. (2009)

Todėl buvo nuspręsta apklausti septynis kibernetinio saugumo ekspertus, naudojant pusiau struktūrizuotą interviu metodą. Pasirinkus būtent šį ekspertų skaičių, buvo siekiama užtikrinti duomenų gausą ir įvairumą, kad galima būtų gauti išsamią ir prasmingą informaciją.

4.2. Ekspertų atrankos procesas

Ekspertų atrankos procesas buvo grindžiamas klasikinės testų teorijos principais, siekiant užtikrinti aukštą pasirinktų ekspertų patikimumą ir jų pateikiamų išvadų kokybę. Tyrimui atrinkta ***septynių ekspertų grupė***, kurių kiekvieno patirtis kibernetinio saugumo srityje viršija dešimt metų.

Šie specialistai atstovauja įvairioms sritims: nuo Lietuvos valstybinių įstaigų ir gynybos sektoriaus iki didelių tarptautinių korporacijų, veikiančių finansų sektoriuje, bei įmonių vadovų, turinčių reikšmingą patirtį su serverių ir debesijos sprendimais. Atrinkti ekspertai suteikia galimybę giliau analizuoti kibernetinio saugumo integracijos į verslo modelius niuansus ir garantuoja, kad tyrimo rezultatai būtų realistiški ir praktiškai pritaikomi.

Tyrimo organizavimas. Tyrimas vyko 2024 m. balandžio mėnesį. Ekspertų atranka buvo atlikta naudojant tikslinę atranką, siekiant įtraukti asmenis su giliomis žiniomis ir praktine patirtimi kibernetinio saugumo integracijos į verslą srityje. Ekspertų paieška organizuota per profesinę bendruomenę, naudojant sniego gniūžtės metodą, kuris leidžia plėsti respondentų ratą remiantis pradinių dalyvių rekomendacijomis.

Interviu su ekspertais buvo iš anksto suplanuoti, susiderinant dėl patogaus laiko ir komunikacijos būdo. Atsižvelgiant į dalyvių pageidavimus, interviu buvo vykdomi žodžiu arba raštu. Žodiniai interviu, trukę nuo 30 iki 90 minučių, vyko naudojant skaitmenines komunikacijos priemones, užtikrinančias aukštą vaizdo ir garso kokybę, o gauti atsakymai buvo iškart transkribuojami. Kiti ekspertai atsakymus į iš anksto paruoštus klausimus pateikė elektroniniu paštu.

Per interviu buvo siekiama suprasti, kaip įmonės įgyvendina kibernetinio saugumo metodus, kokia įtaka tai daro jų verslo modeliams ir kokiais būdais stiprinama bendra saugumo kultūra. Klausimynas buvo sudarytas remiantis moksliniais tyrimais ir teoriniais modeliais, kad atsakymai atskleistų kibernetinio saugumo integravimo galimybes ir svarbą tyrimo kontekste. Tokiu būdu buvo įmanoma išsamiai įvertinti, kaip organizacijos pritaiko saugumo strategijas, nustatyti veiksmų efektyvumą ir atpažinti galimas klaidas, kurios vėliau padėjo formuluoti praktines rekomendacijas ir akademines diskusijas.

Tyrimo etika. Tyrimo metu buvo griežtai laikomasi etikos principų, užtikrinant, kad visi dalyviai būtų informuoti ir sutikę dalyvauti tyrime. Šie principai apėmė:

- Savanoriškumas dalyvauti tyrime**.** Visi tyrimo dalyviai buvo išsamiai informuoti apie tyrimo tikslus ir procedūras bei turėjo teisę bet kuriuo metu atsisakyti dalyvavimo tyrime be jokių pasekmių.
- Informacijos apie tyrimo panaudojimą teikimas. Dalyviams buvo paaiškinta, kad jų pateikti duomenys bus naudojami tik moksliniams tikslams. Tyrimo tikslas ir duomenų naudojimo

ribos buvo nurodyti, siekiant užtikrinti duomenų konfidencialumą ir tinkamą jų panaudojimą, paaiškinant, kaip informacija bus saugoma ir panaudota.

- Laisvė atsakinėti į klausimus. Tyrimo dalyviai turėjo visišką laisvę atsakinėti į pateiktus klausimus, o jų atsakymai buvo vertinami kaip svarbus įnašas į bendrus tyrimo rezultatus.

Duomenų konfidencialumo užtikrinimas. Ekspertai, dalyvavę tyrime ir dirbantys aukštose pozicijose svarbiose įmonėse, pabrėžė ypatingą anonimiškumo svarbą. Jie buvo susirūpinę, kad jų tapatybės atskleidimas galėtų kelti abejonių dėl jų įmonių kibernetinio saugumo patikimumo. Šis susirūpinimas buvo ypač išreikštas ekspertų, dirbančių nacionalinio saugumo ar kritinės infrastruktūros apsaugos sektoriuose, taip pat tarptautinėse korporacijose, veikiančiose finansų sektoriuje. Vadovai, atsakingi už sudėtingus serverių ir debesijos sprendimus, taip pat siekė išvengti bet kokio asmeninės informacijos paviešinimo, kad būtų apsaugotas jų pačių ir jų klientų konfidencialumas.

Atsižvelgiant į šiuos reikalavimus ir laikantis aukščiausių tyrimų etikos standartų, remiantis Kardelio (2019) bei Žydžiūnaitės ir Sabaliausko (2017) rekomendacijomis dėl dalyvių teisių į privatumą, buvo nuspręsta kiekvienam ekspertui suteikti unikalų kodą. Ši praktika leido ne tik užtikrinti dalyvių tapatybės anonimiškumą, bet ir išlaikyti tyrimo duomenų objektyvumą bei patikimumą, tuo pačiu metu apsaugant ekspertų profesinę reputaciją ir jų atstovaujamų organizacijų kibernetinio saugumo statusą.

6 lentelė. Ekspertų unikalus kodai ir interviu informacija

Eksperto unikalusis kodas	Interviu trukmė (min)	Interviu data	Apklausos tipas
E1	**--**	**2024-04-7**	Raštu
E2	**90**	**2024-04-12**	Žodžiu
E3	**54**	**2024-04-12**	Žodžiu
E4	**30**	**2024-04-14**	Žodžiu
E5	**--**	**2024-04-14**	Raštu
E6	**--**	**2024-04-15**	Raštu
E7	**--**	**2024-04-17**	Raštu

Šaltinis: Sudaryta autoriaus

Tyrimo klausimyno sudarymas. Siekiant išsamiai suprasti kibernetinio saugumo integraciją į verslo modelius, magistro darbe buvo sukurtas pusiau struktūrizuotas klausimynas, kurį sudarė 12 detalių klausimų (žiūrėti 1 Priedas). Klausimynas buvo parengtas remiantis giluminės analizės principais, kuri apėmė mokslinę literatūrą, teisės aktus ir praktinių veiklų dokumentaciją. Ši analizė

padėjo identifikuoti esminius kibernetinio saugumo iššūkius ir strategijas, kurie tapo klausimyno pagrindu. Kiekvienas klausimas buvo kruopščiai suformuluotas siekiant paskatinti ekspertus dalintis ne tik faktiniais duomenimis, bet ir asmeninėmis įžvalgomis bei patirtimi, skatinant atvirą ir turiningą diskusiją.

Interviu metu, jei reikėjo aiškinimo arba atsakymai atskleidė naujas perspektyvas, buvo pateikiami papildomi klausimai. Ši lanksti metodika leido ekspertams išsamiai ir nuodugniai išdėstyti savo mintis, užtikrinant, kad informacija būtų turininga ir atspindėtų tikrąsias verslo praktikas bei iššūkius. Toks metodas, remiantis kokybinio tyrimo principais, ne tik struktūrizavo informaciją, bet ir išryškino svarbias temas bei kategorijas, palengvinant svarbių įžvalgų ir tendencijų išskyrimą, susijusių su kibernetinio saugumo integracija į verslo modeliavimo procesus. Gautų duomenų analizės pagrindu bus suformuluotos praktinės rekomendacijos verslo subjektams, apimančios strategijas ir veiksmus kibernetinio saugumo efektyviai integracijai.

4.3. Tyrimo rezultatų interpretavimas

Šiame skyriuje pateikiami pagrindiniai empirinio tyrimo rezultatai, susiję su kibernetinio saugumo integracija į verslo modeliavimą. Tyrimo metu buvo detaliai analizuoti surinkti duomenys, siekiant išgryninti ekspertų nuomones ir suprasti, kaip siūlomas BMC+GRC klausimynas gali būti efektyviai pritaikytas realiose verslo aplinkose. Remiantis gautomis ekspertų įžvalgomis, buvo suformuluotos rekomendacijos klausimyno tobulinimui ir praktiniam pritaikymui, užtikrinant, kad klausimynas atitiktų realios verslo praktikos poreikius ir padėtų įmonėms geriau integruoti kibernetinio saugumo strategijas.

Ekspertų įžvalgų analizė: Tyrimo metu vykdyta ekspertų apklausa leido išsamiai surinkti jų nuomones, siekiant išsiaiškinti, kaip įmonės integruoja kibernetinio saugumo strategijas į savo verslo procesus. Išanalizavus ekspertų atsakymus, buvo identifikuotos pagrindinės temos: saugumo technologijų integravimas, darbuotojų suvokimo stiprinimas, ir organizacinės kultūros kūrimas. Šios temos padėjo suformuoti aiškesnį vaizdą apie tai, kaip kibernetinis saugumas ir verslo strategijos veiksmingai dera, sukuriant tiek saugumo, tiek verslo tikslų įgyvendinimą.

Rekomendacijos dėl modelio tobulinimo: Gauti atsakymai patvirtino, kad BMC+GRC klausimynas yra veiksmingas įrankis saugumo ir verslo strategijų įvertinimui. Vis dėlto, ekspertai pateikė keletą rekomendacijų, kaip šį klausimyną galima tobulinti, kad jis būtų dar efektyvesnis:

- **Technologijų integracija**: Rekomenduojama įtraukti naujausias technologijas į klausimyną, kurios padėtų efektyviau sekti ir neutralizuoti grėsmes bei užtikrintų nuolatinę

organizacijos apsaugą. Šis atnaujinimas leistų organizacijoms greičiau reaguoti į naujas grėsmes ir užtikrinti, kad saugumo priemonės yra aukščiausio lygio.

- **Mokymų programos:** Plėtoti ir įgyvendinti mokymų programas darbuotojams, kad jie galėtų efektyviau identifikuoti ir reaguoti į kibernetinio saugumo iššūkius.
- **Procesų integracija:** Užtikrinti, kad kibernetinis saugumas taptų integralia verslo procesų dalimi, nuo strateginio planavimo iki įgyvendinimo.

Ekspertų įžvalgos apie integracijos pritaikomumą: Klausimyno universalumas ir lankstumas buvo išskirti kaip pagrindiniai jo privalumai. Jis taip gali būti pritaikytas įvairioms organizacinėms struktūroms ir atitikti skirtingus rinkos reikalavimus, sėkmingai leidžiantis suderinti saugumo ir verslo aspektus. Remiantis gauta ekspertų įžvalgų analize, buvo suformuluotos praktinės rekomendacijos, kaip efektyviausiai naudoti klausimyną. Tyrimo rezultatai rodo, kad klausimynas yra vertingas įrankis ne tik akademinėje, bet ir praktinėje srityje, skatinantis tolesnius tyrimus ir diskusijas dėl kibernetinio saugumo ir verslo modeliavimo sėkmingos integracijos.

5. KIBERNETINIO SAUGUMO INTEGRACIJA Į VERSLO MODELIAVIMĄ: TYRIMO ANALIZĖ

Analizuojant apklausų ir interviu metu gautus duomenis, jie buvo kategorizuoti remiantis iš anksto apibrėžtu teoriniu modeliu. Skyrius baigiasi gautų rezultatų sinteze, pabrėžiant pagrindines išvadas ir rekomendacijas, kurios padės tobulinti kibernetinio saugumo strategijas.

Išsiaiškinus empiriniame tyrime dalyvavusių ekspertų nuomonę apie kibernetinio saugumo suvokimą, standartus ir kitus aspektus, ekspertams buvo pateiktas BMC+GRC klausimynas. Surinkus atsiliepimus apie šio klausimyno naudingumą ir praktinį panaudojimą, akivaizdu, kad yra poreikis sukurti dinamišką ir pritaikomą kibernetinio saugumo modelį, kuris tiktų įvairaus dydžio įmonėms. Nors ekspertai nebuvo iš anksto giliai susipažinę su A. Osterwalderio BMC modeliu, jie pripažino, kad ši struktūra suskirstytą į devynis segmentus padeda aiškiau matyti, kaip kibernetinis saugumas galėtų būti integruotas į skirtingas verslo sritis.

Tyrimo metu ekspertai buvo paprašyti ne tik įvertinti esamas kibernetinio saugumo valdymo priemones savo organizacijose, bet ir nurodyti galimas papildomas priemones, kurios galėtų efektyviai pagerinti kibernetinio saugumo valdymą. Šios įžvalgos buvo labai svarbios formuojant praktines rekomendacijas, kaip organizacijos galėtų geriau valdyti kibernetinio saugumo rizikas ir atitikti teisės aktų reikalavimus.

Gauti duomenys ir ekspertų atsiliepimai rodo, kad sėkmingai integruojant kibernetinio saugumo principus į verslo modelius, būtina atsižvelgti ne tik į technines bei technologines naujoves, bet ir į organizacijos kultūrą, darbuotojų švietimą bei procesų valdymą. Šie aspektai yra ypatingai svarbūs kuriant visapusiškai pritaikomą kibernetinio saugumo sistemą, kuri galėtų lanksčiai prisitaikyti prie nuolat kintančių rinkos sąlygų ir technologinės pažangos.

5.1. Ekspertų nuomonės vertinimo tyrimo rezultatai

Ekspertų nuomonės apie kibernetinį saugumą buvo sistemingai sugrupuotos į logiškas kategorijas, atsižvelgiant į magistrinio darbo temą, kuri yra orientuota į kibernetinio saugumo iššūkius ir integraciją į verslo procesus.

Apklausos pradžioje, siekiant nustatyti diskusijos toną ir kontekstą, visiems ekspertams buvo užduotas atviras klausimas: „**kaip jie apibūdintų kibernetinio saugumo sąvoką?**“ Šis klausimas padėjo pradėti diskusiją, leidžiant ekspertams išdėstyti savo bendras įžvalgas apie kibernetinio saugumo svarbą ir poveikį jų organizacijų veiklai. Taip buvo sudaryta galimybė giliau suprasti ekspertų požiūrius ir jų patirtį, kas yra būtina tolesnei analizei ir išvadų formavimui.

Kibernetinio saugumo suvokimas:

Ekspertai pateikė įvairias nuomones apie tai, kas sudaro kibernetinį saugumą jų sektoriuje. Pavyzdžiui, ekspertas E1 akcentavo, kad kibernetinis saugumas yra „*klientų duomenų, informacijos ir verslo tęstinumo apsauga*“, o ekspertas E2 pabrėžė saugumo procedūrų ir technologijų visumą, skirta apsaugoti objektų išteklius nuo kibernetinių grėsmių. Šios nuomones atskleidė, kaip skirtingai kibernetinio saugumo sąvoka gali būti interpretuojama priklausomai nuo patirties dirbant vienoje ar kitoje pramonės srityje ir žinoma, nuo asmeninės patirties.

Analizuojant kitų ekspertų atsakymus, išaiškėjo, kad kibernetinis saugumas neapsiriboja vien tik technologijomis; jis taip pat apima organizacinius procesus ir darbuotojų švietimą. Ekspertas E3 pabrėžė: "Saugumas mūsų įmonėje prasideda nuo darbuotojų mokymų ir baigiasi išsamiu rizikų auditu," o E4 komentarai atskleidė: "Mes tvarkome svarbius miesto infrastruktūros aspektus, todėl mūsų esminė atsakomybė – užtikrinti, kad visi veiklos procesai veiktų patikimai ir saugiai". Todėl jų nuomone, efektyvi kibernetinio saugumo strategija privalėtų apimti ne tik technologines priemones, bet ir žmogiškųjų išteklių valdymą bei procesų tobulinimą.

Atsižvelgiant į ekspertų pateiktas įžvalgas, tampa aišku, kad kibernetinis saugumas yra kompleksinė sritis, reikalaujanti nuolatinio dėmesio ir prisitaikymo prie besikeičiančių sąlygų. Todėl būtina ne tik sekti naujausias technologijas ir grėsmių valdymo praktikas, bet ir nuolat šviesti ir įtraukti darbuotojus į saugumo procesus, stiprinant bendrą organizacijos atsparumą kibernetinėms grėsmėms.

5.2. Kibernetinio saugumo integracijos į verslo procesus sisteminė analizė

Pradiniuose apklausos etapuose ekspertų požiūriai atskleidė, kaip įvairiai kibernetinis saugumas suvokiamas, priklausomai nuo jų asmeninės patirties ir veiklos sričių. Įvairūs požiūriai padėjo nustatyti diskusijos gaires ir atskleidė, kad kibernetinio saugumo suvokimas yra labai platus. Siekiant užtikrinti aiškią ir struktūrizuotą duomenų analizę, visa medžiaga buvo sistemingai išdėstyta pagal penkias pagrindines kategorijas.

Kiekviena kategorija atspindi svarbius kibernetinio saugumo aspektus, kurie yra būtini organizacijų veiklos efektyvumui ir saugumui užtikrinti. Toks metodinis duomenų susistemintas leido efektyviau išanalizuoti ir suprasti, kokie kibernetinio saugumo elementai yra labiausiai reikšmingi įvairių sričių ekspertams.

1. **Kibernetinio saugumo integracija į verslo procesus** (Klausimai: 2, 5) – Šioje kategorijoje aptariama, kaip kibernetinis saugumas yra įtraukiamas į įmonių verslo strategijas ir kaip jis veikia sprendimų priėmimą bei kasdienę veiklą.

2. **Kibernetinio saugumo rizikos valdymas** (Klausimai: 3, 6, 7, 9) – Buvo nagrinėjama, kaip įmonės identifikuoja ir valdo kibernetines grėsmes, kurios gali kilti dėl įvairių veiklos aspektų.
3. **Saugumo protokolų ir politikos taikymas** (Klausimai: 4, 12) – Analizuojama, kaip įmonės laikosi teisinių reikalavimų ir kaip jos įgyvendina savo saugumo politikas, siekiant užtikrinti duomenų apsaugą ir atitikimą teisiniam reguliavimui ir standartams.
4. **Organizacinė kultūra ir darbuotojų švietimas** (Klausimas: 11) – Ši kategorija atskleidžia, kaip organizacijos skatina saugumo sąmoningumą tarp savo darbuotojų ir kaip švietimas yra integruotas į saugumo strategijas.
5. **BMC+GRC Klausimyno naudingumo analizė** (Klausimas: 10) – Ekspertų buvo paklaustą apie tokio klausimyno naudingumą, trūkumus ir privalumus.

5.3. Ekspertų nuomonės apie kibernetinį saugumą: apklausos atsakymai

Kibernetinio saugumo į verslo procesus. Šiame skyriuje analizuojamas ekspertų požiūris apie kibernetinio saugumo integraciją į įmonių verslo veiklas ir strategijas, remiantis atsakymais į apklausos klausimus 2, ir 5. Atsakymai į šiuos klausimus atskleidžia, kaip skirtingų sektorių organizacijos pritaiko kibernetinio saugumo praktikas, užtikrinant jų verslo tęstinumą ir sprendimų priėmimo efektyvumą.

Atsakydamas į klausimą „**Kaip Jūsų įmonėje įgyvendinamas kibernetinis saugumas?**“ Ekspertas E1 pabrėžė, kad kibernetinis saugumas yra savaime įliejamas į organizacijos veiklą ir procesus, kuomet tenka dirbti finansų rinkoje kuri yra stipriai reguliuojama įstatymų ir standartų. „*Paprastai kibernetinis saugumas, kuomet dirbi finansų rinkoje su kliento duomenimis būna įlietas į verslo esybę*“.

Eksperto E7 nuomone, panaši. Jis taip pat pabrėžia, kad kibernetinio saugumo svarba labai priklauso nuo veiklos rūšies. “*Mūsų organizacija įdiegė sistemas, skirtas Creative Commons licencijų valdymui, dar žinomos kaip DRM kurios yra svarbios reguliuojant kūrybinio turinio platinimą. DRM (angl.k. Digital Rights Management) integracija yra sudėtinga, tačiau būtina, siekiant užtikrinti teisėtą ir saugų jūsų kūrybinio turinio naudojimą*“. Abiejų ekspertu nuomone kibernetinis saugumas ir verslo veiklos planavimas yra neatsiejami. Norint pradėti bet kokią komercinę veiklą nuo pirmųjų sekundžių asmuo susiduria su duomenų perdavimų, standartais, reikalavimais ir pan.

Ekspertas E2 atkreipė dėmesį, kad įmonės nepakankamai rūpinasi savo kibernetiniu saugumu tol, kol nenutinka incidentai. „*...Duomenų atkurti nepavyko, turėjo sistemas kurti nuo pradžių. Tai tik tada jie ir susirūpino, kaip dar labiau užtikrinti saugumą*.“ Tuo pačiu metu pridūrė „*Realiai manau garantuotos apsaugos nėra, visada kažkas gali nutikti*.**“**. Suponuodamas, kad šiais laikais kiekviena įmonė privalo vertinti kibernetinių incidentų rizikas visada.

Ekspertas E6 pabrėžė, kad vadovų iniciatyva ir įsipareigojimas užtikrinti aukščiausius saugumo standartus yra labai svarbūs kibernetiniam saugumui. Jis sakė: „*Kibernetinis saugumas yra neatsiejama mūsų verslo strategijos dalis. Vadovybės įsipareigojimas užtikrinti aukščiausius saugumo standartus įpareigoja mums efektyviai valdyti grėsmes ir užtikrinti klientų pasitikėjimą.“* Jis pabrėžė žmogiškojo faktoriaus svarbą kibernetinio saugumo srityje ir nurodė, kad stiprus vadovavimas ir reikalavimai gali paveikti kibernetinio saugumo įdiegimo ir atsparumo lygį. Ekspertas E3 akcentavo kibernetinio saugumo strategijų pritaikymo prie kintančios rinkos svarbą. Jis sakė: „*Mūsų įmonėje kibernetinis saugumas nėra statinis elementas; tai nuolat besikeičiantis procesas, atsižvelgiant į naujas technologijas ir rinkos pokyčius. Reguliariai atnaujiname mūsų saugumo protokolus ir įgyvendiname aktyvias priemones prieš galimas grėsmes*.“

Vertinant šiuos atsakymus, tapo aišku, kad kibernetinio saugumo integracija į verslo procesus nėra tik technologinis iššūkis, bet taip pat reikalauja aukšto vadovų dėmesio ir organizacijos kultūros pritaikymo. Vadovų įsipareigojimai užtikrinti aukščiausius saugumo standartus, kaip pabrėžė ekspertas E6, yra kritiškai svarbūs efektyviai kibernetinio saugumo integracijai, kuri padeda valdyti rizikas ir užtikrinti organizacijos saugumą. Tai rodo, kad kibernetinis saugumas yra ne tik apsaugos priemonė, bet ir strateginis veiksnys, tiesiogiai įtakojantis verslo tęstinumą ir sėkmę.

Kibernetinio saugumo rizikos valdymas. Skyriuje gilinamasi į ekspertų požiūrį, kaip jie identifikuoja ir valdo kibernetinio saugumo rizikas įvairiuose verslo sektoriuose, remdamiesi atsakymais į apklausos klausimus 3, 6, 7 ir 9.

Ekspertas E1 iš didelės įmonės pabrėžė, kad dėl didelio masto veiklos jie susiduria su padidėjusiomis rizikomis. Jis atkreipė dėmesį, kad jų įmonėje net paprasta vagystė gali būti analizuojama per įvairius scenarijus, iš kurių vienas gali evoliucionuoti į kibernetinį incidentą. „*Mes mokomės iš klaidų ir įgyvendiname išsamias prevencijos priemones*," - sakė jis. Be to, jis paminėjo, kad jų įmonė privalo laikytis tarptautinių standartų, pavyzdžiui, PCI ir NIST, kurie nustato būtinybę įgyvendinti konkrečias apsaugos priemones. Ekspertas taip pat atskleidė, kad rizikos valdymo strategijos dažnai yra formuojamos atsižvelgiant į „priimtiną rizikos lygį“. Jis paaiškino, kad net turint pakankamą biudžetą, pirmenybė teikiama apsisaugojimui nuo dažniausiai pasitaikančių grėsmių. Tai reiškia, kad pradinis biudžetas skiriamas esminėms saugumo priemonėms, o likęs biudžetas naudojamas atsižvelgiant į tai, ką galima įdiegti nedelsiant, o kas gali palaukti.

E2 ekspertas atskleidė, kad dažnai rizikos vertinimas vyksta tik įvykus incidentui, o tai yra problema visame sektoriuje. "*Lietuvoje trūksta supratimo apie kibernetinę riziką, viskas daroma jau po incidento*" – sakė jis, pabrėždamas prevencinių veiksmų svarbą. E3 identifikavo duomenų nutekėjimą ir praradimą kaip svarbiausias, ir dažniausiai pasitaikančiais rizikas finansų sektoriuje. „*Institucijos privalo saugoti klientų duomenis, todėl yra kuriami ir nuolat tobulinami veiklos tęstinumo ir IT rizikų valdymo planai“*.

E4 ir E5 ekspertų dėmesys koncentravosi į panašius dalykus susiedami rizikų valdymą su duomenų atstatymo efektyvumu. E4: "*Mes stengiamės diegti rimtas prieigos kontrolės sistemas ir reguliariai atnaujiname savo sistemas*". E5 išskyrė DDoS atakas ir klientų duomenų vagystes kaip pagrindines grėsmes, su kuriomis jo organizacija susiduria. „*Taikomas daugiasluoksnis prieinamumo modelis, įskaitant fizines ir programines apsaugas, bei nuolatiniai duomenų atsarginių kopijų kūrimo ir atkūrimo planai.*“ Šios dvi nuomonės panašios paminėdamos, kad infrastruktūra būtina apsaugoti ne tik prieš incidentus, bet ir privalu turėti efektyvius veiklos tęstinumą užtikrinančius įrankius.

E7 ekspertas atkreipė dėmesį į kibernetinio saugumo ir intelektinės nuosavybės tarpusavio ryšį: "*Mes diegiame pažangias šifravimo technologijas ir dvigubą autentifikaciją, užtikrinant mokėjimų ir turinio saugumą. Be to, naudojame trečiųjų šalių DRM [39]paslaugas nelegaliam turinio platinimui stebėti.*" – teigė ekspertas, pabrėždamas tarptautinio bendradarbiavimo svarbą.

Šių atsakymų analizė atskleidžia, kad efektyvus rizikos valdymas reikalauja integruotos strategijos, įtraukiančios technologines naujoves, organizacines procedūras ir tarptautinį bendradarbiavimą, siekiant užtikrinti visapusišką saugumo užtikrinimą.

Saugumo protokolų ir politikos taikymas. Šiame skyriuje aptariame, kaip įmonės užtikrina teisinių reikalavimų laikymąsi ir kaip jos įgyvendina savo saugumo politikas. Ekspertų atsakymai į apklausos klausimus 4 ir 12 atskleidžia, kad įmonės skirtingai taiko saugumo protokolus, priklausomai nuo teisinių standartų ir specifikos savo veiklos sektoriuje.

Ekspertas E1 išryškino tarptautinių standartų, tokie kaip NIST ir PCI DSS, svarbą, nurodydamas, jog jie palengvina tarp organizacinį bendradarbiavimą ir informacijos mainus kibernetinio saugumo srityje. Tačiau pabrėžė, kad šių standartų taikymas gali kelti iššūkių, kai kalbama apie skirtingų šalių teisinius reglamentus: "*Informacijos mainai tarp mūsų įmonių biurų, esančių Europos Sąjungoje ir JAV, yra gana paprasti ir efektyviai kontroliuojami dėl panašių teisinių standartų. Tačiau, pereinant prie šalių, tokių kaip Kinija ar Brazilija, tenka susidurti su nacionaliniais saugumo reglamentais, kurie ne tik neatitinka tarptautinių standartų, bet ir sukelia papildomą administracinę naštą*." Ekspertas 4 dirbantis tarptautinėje rinkoje pateikė panašų atsakymą: "*Mūsų organizacija veikia keliuose kontinentuose, ir kiekviena regioninė rinka turi savo specifikas į kurias privalome atsižvelgti formuodami saugumo politikas. Tai apima viską nuo duomenų apsaugos standartų iki specifinių operacinių protokolų, kurie užtikrina, kad veikla ne tik efektyvi, bet ir atitinka vietos įstatymus*." Šie dviejų ekspertų pateikti pavyzdžiai patvirtina literatūros analizės metu išryškintą idėją, kad įgyvendinant tam tikrus teisinius reglamentus ar standartus, organizacija automatiškai veikia kaip standartų skleidėjas savo veiklos sektoriuje. Toks modelis leidžia standartams plisti tarp įmonių, kurios bendradarbiauja ar yra tarpusavyje susijusios komercinėmis ar operacinėmis veiklomis. Organizacijoms dažnai yra

[39] Kūrinių apsaugos valdymo programa (anglų.k digital rights management)

efektyviau ir ekonomiškiau standartizuoti operacijų procedūras, nei nuolat jas pritaikyti atskirais atvejais.

Ekspertai E7 ir E3 pabrėžė, kad GDPR yra vienas iš svarbiausių reglamentų, veikiančių jų organizacijas. E7 minėjo: "*Mes privalome laikytis GDPR reglamentų, kurie yra būtini mūsų duomenų apsaugos strategijai. Tai reikalauja nuolatinio mūsų IT ir teisinių komandų bendradarbiavimo, užtikrinant, kad mūsų veikla atitiktų šiuos standartus*." E3 pridūrė: "*GDPR, įgyvendinimas reikalauja nuolatinio mūsų procesų ir sistemų atnaujinimo, kad užtikrintume pilną atitikimą*."

Ekspertų įžvalgos pabrėžia, kad saugumo protokolų ir politikų taikymas yra kompleksinis procesas, reikalaujantis nuolatinio dėmesio ir prisitaikymo prie kintančių teisinių reikalavimų bei technologinių aplinkybių. Įmonės turi integruoti tarptautinius ir nacionalinius standartus, o tai kartais sukuria papildomas administracines naštas ir teisinių nesuderinamumų iššūkius.

Organizacinė kultūra ir darbuotojų švietimas. Ekspertų atsakymai į 11-ąjį klausimą atskleidžia, kaip organizacinė kultūra ir švietimo programos yra įtraukiamos į kibernetinio saugumo praktikas.

Ekspertas E1 pabrėžė, kad mokymai yra būtini, kad kiekvienas darbuotojas suvoktų savo atsakomybę ir būtų gerai informuotas apie galimas grėsmes: "*Rengiame privalomus mokymus visiems darbuotojams, per kuriuos simuliuojamos įvairios kibernetinės atakos, pvz., 'spear phishing', ir stebimas darbuotojų atsakas. Taip pat vykdome mokymus, kurie, nors ir ne visiškai orientuoti į kibernetinį saugumą, vis tiek prisideda prie bendros įmonės saugumo*." Jis taip pat minėjo lojalumo programas, kurios skatina darbuotojų sąmoningumą ir atsakomybę už saugumą.

Ekspertai E3 ir E4 akcentavo nuolatinių mokymų svarbą. Ekspertas E3 minėjo: "*Nuolatiniai mokymai padeda darbuotojams suvokti ir praktiškai taikyti saugumo žinias kasdieninėje veikloje, ypač reaguojant į įtartinus laiškus ar potencialias grėsmes. Ši praktika ne tik stiprina saugumo kultūrą, bet ir padeda formuoti atsakomybės jausmą.“* E4 ekspertas pridūrė: "*Darbuotojai dalyvauja saugumo seminaruose, kurie ne tik pateikia teorinę medžiagą, bet ir skatina diskusijas apie geriausias praktikas. Vertiname mokymų efektyvumą stebėdami, kaip mažėja saugumo pažeidimai ir kaip greitai darbuotojai reaguoja į naujai atsirandančias grėsmes*."

Ekspertas E5 paaiškino, kad jų įmonė vykdo periodiškus mokymus, kurie apima praktines užduotis: "*Nauji darbuotojai pradeda nuo pradinio saugumo kurso, o vėliau periodiškai atnaujina žinias. Vykdomos įvairios praktinės užduotys, pvz., simuliavimas atakų, leidžiančios darbuotojams išbandyti reakcijas į kritines situacijas."*

Ekspertas E7 minėjo, kaip nuolatinis švietimas prisideda prie darbuotojų saugumo sąmonės kūrimo: "*Visi mūsų darbuotojai, nuo administracijos iki aukščiausios vadovybės, dalyvauja mūsų saugumo mokymų cikluose, kurie yra interaktyvūs ir pateikia realius pavyzdžius, su testais, padedančiais geriau suprasti ir taikyti saugumo principus*."

Remiantis aptartų ekspertų įžvalgomis, akivaizdu, kad nuolatinis darbuotojų mokymas ir teisingai formuojama organizacinė kultūra yra pagrindiniai veiksniai, užtikrinantys efektyvų kibernetinio saugumo valdymą. Tinkamai įgyvendintos švietimo programos ir darbuotojų įtraukimas į saugumo procesus ne tik padeda išvengti incidentų, bet ir stiprina bendrą organizacijos atsparumą kibernetinėms grėsmėms.

BMC+GRC Klausimyno naudingumo analizė

Vertinant ekspertų atsiliepimus apie „Kibernetinio Saugumo Integracijos Klausimyną“, išryškėja, kad šis įrankis ne tik suteikia galimybę sistemingai įvertinti esamas saugumo praktikas, bet ir padeda atskleisti, kaip galima tobulinti kibernetinio saugumo integravimą į įmonės operacijas. Ekspertų teigimu, šis klausimynas atveria naujas perspektyvas dėl kibernetinio saugumo ir verslo procesų sąsajų, ypač atkreipiant dėmesį į tai, kad daugelis iš jų iki šiol nebuvo susidūrę su A. Osterwalderio Verslo modeliavimo drobe ar GRC (Valdymo, Rizikos valdymo ir Atitikties) modeliu. Todėl klausimynas sulaukė itin palankių įvertinimų ne vien dėl savo klausimų struktūros, bet ir dėl inovatyvaus požiūrio į verslo segmentų analizę ir saugumo valdymo integraciją, kuri buvo naujovė daugumai ekspertų.

Daugiausia informacijos suteikė ekspertas E1, kurio patirtis yra didžiausia iš visų apklausoje dalyvavusių dalyvių. Ekspertui paliko didelį įspūdį verslo modelio segmentų analizė, ir jis labai teigiamai atsiliepė apie lentelėje esamus klausimus, pabrėždamas jų svarbą bei naudingumą verslui. Ekspertas E1 pabrėžė, kad klausimynas efektyviai suskirstytas į verslo sritis, atspindinčias esminius verslo konceptus, ir išskyrė valdymo, rizikos valdymo bei atitikties komponentus kaip ypač svarbius saugumo vertinimo elementus. Ekspertas atkreipė dėmesį į tai, kad mažesnis dėmesys valdymo aspektams gali lemti didesnes rizikas ir atitikties trūkumą, pabrėždamas, kad šių aspektų aiškesnis išdėstymas padidintų modelio efektyvumą.

Be to, E1 pasiūlė praturtinti klausimyną praktiniais pasiūlymais, kurie būtų priskirti kiekvienam segmentui, siekiant atitikti kibernetinio saugumo reikalavimus. Jis pasiūlė įtraukti papildomą stulpelį, kuriame būtų nurodyti būtini veiksmai saugumo atitikčiai užtikrinti. "*Pridėjus praktinius veiksmus, kurie turėtų būti atlikti siekiant užtikrinti atitiktį, klausimynas ne tik padėtų identifikuoti esamas problemas, bet ir pateiktų aiškias gaires, kaip šias problemas spręsti*," sakė E1. Tokia naujovė padėtų organizacijoms ne tik vertinti, bet ir aktyviai tobulinti savo kibernetinio saugumo praktikas, teikdama aiškią struktūrą ir konkrečias gaires problemų sprendimui.

Ekspertas E4, įvertinęs klausimyną kaip naudingą įrankį, taip pat išreiškė idėją dėl tolesnės jo plėtros: "*Klausimynas galėtų būti praplėstas įtraukiant scenarijus, kurie simuliuotų įvairius kibernetinio saugumo incidentus. Tai padėtų organizacijoms ne tik teoriškai vertinti savo pasiruošimą, bet ir praktiškai testuoti savo reakcijas į įmanomas grėsmes*."

Ekspertas E3, kuris dirba itin reguliuojamoje sferoje, išreiškė nuomonę, jog klausimynas galėtų būti išsamesnis. Jis paaiškino: "*Man, dirbančiam tokioje sudėtingoje reguliavimo aplinkoje, šis*

klausimynas pasirodė šiek tiek per glaustas. Visgi, mano patirtis yra ne visiškai tipinė, ir suprantu, kad daugumai kitų pramonės šakų jis turėtų būti visiškai pakankamas. Tačiau norėčiau matyti, kad klausimynas būtų adaptuotas ir pritaikytas specifiškai tokiems sektoriams kaip mano, kur detalesnė informacija ir gilesnis išnagrinėjimas yra būtini saugumo užtikrinimui."

Apibendrinant ekspertų atsiliepimus, „BMC+GRC Kibernetinio Saugumo Integracijos Klausimynas" pasirodė kaip vertingas įrankis, atskleidžiantis saugumo integracijos į verslo procesus galimybes. Nors klausimynas buvo palankiai įvertintas dėl savo struktūros ir naujoviškumo, atsirado pasiūlymų jį dar tobulinti, įtraukiant įmonės veiklos specifiką ir praktinius elementus, kurie padėtų organizacijoms geriau pasiruošti ir reaguoti į kibernetines grėsmes realiomis sąlygomis. Gauti įvertinimai taps pagrindu kuriant hipotetinį kibernetinio saugumo verslo sprendimų modelį, siekiant ne tik identifikuoti potencialias saugumo spragas, bet ir aktyviai dirbti su jų prevencija ir šalinimu.

5.4. Integravimas GRC į BMC: Hipotetinio kibernetinio saugumo verslo sprendimų modelio kūrimas

Atsižvelgiant į magistro darbe atliktą išsamų teorinį tyrimą, apklausus ekspertus ir įvertinus jų įžvalgas, išaiškėjo, kad kibernetinis saugumas yra itin svarbus visose organizacijos segmentuose. Efektyvus ir gerai apsaugotas verslas pasižymi ne tik puikiais techniniais sprendimais, bet tai pat brandžia kibernetine kultūrą, kurioje įtraukti žmogiškieji ištekliai yra puikiai apmokyti ir gerai valdomi, reaguoti tinkamai į kibernetines grėsmes.

Šiame skyriuje pristatomas metodas, kaip kibernetinio saugumo principai, remiantis GRC (valdymo, rizikos valdymo ir atitikties) dimensijomis, gali būti integruoti į verslo modelio drobės (BMC) segmentus, įskaitant naujai įtrauktą žmogiškųjų išteklių segmentą. Metodas yra atspindėtas lentelėje, kuri parodo, kaip kiekvienas GRC aspektas pritaikomas skirtingiems BMC segmentams, pabrėžiant žmogiškųjų išteklių vaidmenį kibernetinio saugumo strategijoje.

7. Lentelė. Hipotetinio saugumo verslo modelis naudojant BMC ir GRC

BMC Segmentas	**Valdymas**	**Rizikos valdymas**	**Atitiktis**
Klientų segmentai	Nustatyti asmeninių duomenų apsaugos politiką	Analizuoti duomenų pažeidimų riziką kiekviename segmente	Užtikrinti atitiktį su GDPR ir kitais privalomais reglamentais

Siūloma vertė	Integruoti kibernetinio saugumo funkcijas į produktus	Vertinti saugumo sprendimų poveikį bendrovei	Pagal poreikį taikyti pramonės saugumo standartus ISO27001, NIST ir tt.
Pristatymo kanalai	Įdiegti duomenų šifravimą ir kitas saugumo technologijas	Vertinti ir mažinti kanalų pažeidžiamumą	Įgyvendinti saugumo auditus ir atitikties tikrinimus
Klientų santykiai	Užtikrinti skaidrumą duomenų naudojime	Vertinti ir mažinti duomenų nutekėjimo riziką	Užtikrinti, kad klientų aptarnavimas atitiktų privatumo įstatymus
Pajamų srautai	Apsaugoti finansinius duomenis nuo kibernetinių atakų	Įvertinti finansinę riziką susijusią su saugumo pažeidimais	Užtikrinti atitiktį su finansų sektoriaus reglamentais
Pagrindiniai ištekliai	Taikyti pažangias apsaugos technologijas	Stiprinti fizinių ir virtualių išteklių saugumą analizuojant ir taikant rizikų prevenciją	Laikytis turtų saugojimo ir naudojimo reglamentų
Pagrindinės veiklos	Integruoti saugumo protokolus į kasdienę veiklą	Mažinti operacinės veiklos rizikas	Užtikrinti, kad veikla atitinka nacionalinius saugumo standartus
Pagrindiniai partneriai	Reikalauti saugumo standartų iš partnerių	Vertinti partnerių veiklos riziką	Užtikrinti sutarčių su partneriais atitiktį saugumo reikalavimams
Sąnaudų struktūra	Optimaliai paskirstyti išlaidas saugumo priemonėms	Įvertinti saugumo investicijų grąžą	Užtikrinti, kad saugumo išlaidos atitinka biudžetines gaires
Žmogiškieji ištekliai	Įtraukti saugumo kultūrą į organizacijos vertybes	Stiprinti žmogiškųjų išteklių saugumo žinias ir įgūdžius	Užtikrinti reguliarius mokymus ir atitiktį su darbo saugos normomis

Šaltinis: Sudaryta autoriaus naudojant BMC ir GRC modelius

Pateiktoje lentelėje įvardinama, kaip kibernetinis saugumas galėtų būti integruojamas į kiekvieną verslo segmentą. Prieš tai atlikto tyrimo rezultatai parodė, kad žmogiškieji ištekliai yra vienas svarbiausių reiškinių kibernetinio saugumo politikos formavimui ir jos veiksmingam įgyvendinimui

praktikoje. Į šį segmentą įtraukiamas poreikis nustatyti kibernetinio saugumo kultūra įmonėje, , paskirstyti atsakomybes, organizuoti mokymus ir darbuotojų įtraukimą į įmonės saugumo procesus.

Sukurtas hipotetinis saugumo modelis yra dinamiškas ir lankstus, leidžiantis ne tik sumanyti, kokiais techniniais veiksmais apsaugoti atskirus verslo elementus, bet ir suteikiantis visišką laisvę pritaikyti tarptautinius standartus pagal poreikį. Skirtingai nei apklausos metu kalbinti ekspertai įsivaizdavo, šis modelis nepasiūlo alternatyvos populiariesiems kibernetinio saugumo standartams, o veikiau pateikia strategines gaires, kurios leidžia lanksčiai nuspręsti, kokias saugumo priemones reikia įdiegti, atsižvelgiant į tikrąją verslo poreikių specifiką.

BMC+GRC klausimynas, įvertintas ekspertų ankstesniuose tyrimo etapuose, išsiskiria ne tik kaip modelio pagalbinis kūrimo įrankis, bet ir kaip metodas jo patikrinimui. Remiantis hipotetiniu modeliu, kuris grindžiamas siūlomų metodų taikymu ir lankstumu, aiškiai matomas jo pritaikomumas ir pridėtinė vertė, o tai leidžia modeliui išsiskirti palyginti su dažnai ribotais ir standartizuotais metodais, suteikiant galimybę lanksčiau reaguoti į iššūkius ir adaptuotis prie kintančių sąlygų.

IŠVADOS IR REKOMENDACIJOS

Magistro darbe nagrinėjamas kibernetinis saugumas ir jo integracija į verslo modelius per A. Osterwalderio sukurto Verslo Modelio Drobės (BMC) ir Valdymo, Rizikos bei Atitikties (GRC) principus. Tyrimo metu sukurtas hipotetinis kibernetinio saugumo modelis leidžia sistemingai įtraukti saugumo aspektus į verslo procesus, didinant rizikų valdymo efektyvumą ir užtikrinant atitiktį teisiniams reikalavimams. Analizė, apimanti mokslinės literatūros peržiūrą, teorinius svarstymus ir ekspertų įžvalgas, pabrėžė žmogiškųjų išteklių svarbą kibernetinio saugumo strategijose ir atskleidžė būdus, kaip organizacijos gali efektyviau integruoti saugumo principus į savo veiklą. Tyrimas atskleidė pagrindines išvadas:

1. **Verslo modelio drobės (BMC) taikymas:** Verslo Modelio Drobės (BMC) modelis sukurtas A. Osterwalderio gali būti lengvai pritaikomas verslo modeliavime, dėl savo aiškios ir struktūrizuotos sandaros. BMC išsiskiria kaip ypač tinkamas įrankis kibernetinio saugumo aspektų integravimui į verslo strategijas. Tyrimas atskleidė, kad BMC modelis yra viena patogiausių priemonių organizacijoms, kurios siekia ne tik sistemingai valdyti saugumo priemones, bet ir užtikrinti verslo procesų efektyvumą ir pritaikomumą.
2. **Kibernetinio saugumo apibrėžimai ir svarba:** Antrajame etape išsamiai detaliai išnagrinėta kibernetinio saugumo sąvoka, išsamiai apžvelgiant kibernetines grėsmes ir jų atakų vektorius. Išvados rodo, kad organizacijos, kurios sistemingai formuluoją ir įgyvendina kibernetinio saugumo politikas, yra žymiai geriau pasirengusios atremti kibernetines atakas ir mažinti su jomis susijusius nuostolius.
3. **Kibernetinio saugumo standartai:** Tyrimo metu buvo gilinamasi į svarbius kibernetinio saugumo standartus, tokius kaip ISO/IEC 27001, NIST Cybersecurity Framework, PCI DSS, ir CIS controls. Šie standartai yra itin svarbūs užtikrinant, kad organizacijų saugumo praktikos atitiktų tiek nacionalinius, tiek tarptautinius saugumo reikalavimus. Jie teikia struktūrizuotą pagrindą saugumo politikų kūrimui ir jų įgyvendinimui, leidžiant organizacijoms efektyviai valdyti saugumo rizikas ir aktyviai reaguoti į kylančias grėsmes. Analizė atskleidė, kad šių standartų integravimas į organizacijų kasdienę veiklą ne tik padeda užtikrinti aukštesnį atsparumo lygį kibernetinėms atakoms, bet ir stiprina bendrą saugumo kultūrą.
4. **Teisinio reguliavimo įtaka:** Tyrimo metu atliktas Europos Sąjungos ir kitų jurisdikcijų teisinio reguliavimo poveikio vertinimas parodė, kad teisės aktai yra būtini kibernetinio saugumo strategijų elementai. Teisinės normos, pavyzdžiui, bendrasis duomenų apsaugos reglamentas (GDPR), kuriuo keliami aukšti reikalavimai duomenų tvarkymui ir saugumui, priverčia organizacijas įgyvendinti atitinkamas saugumo priemones. Šie reglamentai ne tik

sudaro saugumo praktikų pagrindą, bet ir verčia organizacijas nuolat tobulinti savo saugumo procesus, siekiant išvengti finansinių sankcijų ir išlaikyti aukštą pasitikėjimo lygį tarp klientų ir partnerių.

5. **Valdymo, rizikos valdymo ir atitikties (GRC) principų integracija:** GRC principų taikymas parodė, kad valdymo, rizikos valdymo ir atitikties principų įtraukimas į organizacijų kasdienybę ne tik padeda užtikrinti nuoseklų ir efektyvų saugumo valdymą, bet ir suteikia reikalingus įrankius adekvačiai reaguoti į nuolat kintančias kibernetines grėsmes.
6. **Ekspertų įžvalgos:** Ekspertų interviu, atlikti šio tyrimo metu, buvo ypatingai naudingi atskleidžiant esminius trūkumus žmogiškųjų išteklių valdyme tiek BMC, tiek GRC modeliuose. Ekspertai vieningai pabrėžė, kad žmogiškieji ištekliai yra esminiai ne tik saugumo incidentų prevencijai, bet ir operatyviam reagavimui į juos. Jie akcentavo, kad efektyvus saugumo politikų įgyvendinimas yra neįmanomas be kompetentingų, gerai informuotų ir saugumo sąmoningumu pasižyminčių darbuotojų. Ekspertų teigimu, kvalifikuoti darbuotojai suteikia organizacijai būtiną lankstumą ir reikalingą greitį spręsti kibernetinio saugumo iššūkius. Taip pat pabrėžiama, kad šių darbuotojų mokymai ir nuolatinis švietimas yra kritiniai dalykai užtikrinant, kad saugumo procedūros būtų įgyvendinamos laiku ir efektyviai, užtikrinant organizacijos apsaugą ir atsparumą kibernetinėms grėsmėms.
7. **Žmogiškųjų išteklių integracija:** Remiantis ekspertų rekomendacijomis, BMC modelis buvo papildytas žmogiškųjų išteklių segmentu, kuris pabrėžia mokymų ir sąmoningumo ugdymo svarbą organizacijoje. Šia integracija siekiama užtikrinti, kad kiekvienas darbuotojas būtų tinkamai supažindintas su saugumo rizikomis, jų prevencijos metodais ir reagavimo procedūromis. Toks papildymas neabejotinai sustiprintų organizacijos atsparumą kibernetinėms grėsmėms, padidintų darbuotojų įsitraukimą ir atsakomybę už kibernetinį saugumą. Tai ne tik padėtų formuoti atsakingą požiūrį į saugumą organizacijoje, bet ir skatintų kibernetinio saugumą kultūrą bendrai.
8. **Hipotetinio kibernetinio saugumo modelio sukūrimas:** Magistriniame darbe sukurtas modelis, remiantis BMC ir GRC principais, aiškiai parodo, kaip įmanoma lanksčiai integruoti kibernetinio saugumo aspektus į skirtingas verslo modelio sritis. Modelis apima saugumo strategijų diegimą visose svarbiose verslo srityse, nuo klientų santykių iki žmogiškųjų išteklių, užtikrinant, kad kibernetinis saugumas tampa integraliu visos organizacijos veiklos elementu.
9. **Modelio plėtros perspektyvos**: Sukurtas kibernetinio saugumo modelis, remiantis BMC ir GRC principais, yra tvirtas pagrindas tolesnei plėtrai ir adaptacijai skirtingose organizacijose ir verslo aplinkose. Modelis sukurtas taip, kad būtų lankstus ir galėtų prisitaikyti prie naujų technologijų, saugumo iššūkių ir teisinių reikalavimų pokyčių.

Rekomendacijos:

1. **Kibernetinio saugumo integracija naudojant BMC ir GRC 3.5 modelius:** Kaip išsamiai aptarta darbe prie GRC klausimyno skyriuje, buvo pasiūlyta naudoti atnaujintą GRC 3.5 modelį, kuris detaliai išskiria Valdymo, Rizikų valdymo ir Atitikties komponentus į išplėstas subkategorijas: Valdymo ir priežiūros, Strategijos ir veiklos užtikrinimo, Rizikos ir sprendimų, Atitikties ir etikos, Saugumo ir tęstinumo, Audito ir užtikrinimo. Išplėstas metodas leistų dar efektyviau įdiegti kibernetinio saugumo priemones, sukuriant ***šešis konkretaus kibernetinio saugumo pasiūlymus*** kiekvienam Verslo Modelio Drobės segmentui.
2. **Mokymų ir sąmoningumo didinimas**: Reguliariai organizuoti mokymus ir informavimo kampanijas visiems darbuotojams, siekiant didinti jų sąmoningumą apie kibernetines grėsmes ir atitinkamas prevencijos bei reagavimo strategijas.
3. **Standartų ir teisinių reikalavimų laikymasis:** Vykdant kibernetinio saugumo veiklas, būtina laikytis nacionalinių ir tarptautinių standartų bei teisinių reikalavimų, tokių kaip ISO/IEC 27001, GDPR, kad užtikrinti atitiktį ir įstatymų laikymąsi.
4. **Kibernetinio saugumo politikų ir procedūrų nuolatinis atnaujinimas:** Ypatingas dėmesys turėtų būti skiriamas kibernetinio saugumo politikų atnaujinimui, kad jos visada atitiktų naujausias technologijas ir atspindėtų besikeičiančias grėsmes.
5. **Rizikos vertinimas ir valdymas:** Svarbu aiškiai identifikuoti potencialias grėsmes bei įgyvendinti efektyvias rizikos mažinimo strategijas.
6. **Tarpsektorinis ir tarptautinis bendradarbiavimas:** Skatinti tarpsektorinį ir tarptautinį bendradarbiavimą, keitimąsi patirtimi ir informacija apie grėsmes bei jų neutralizavimo būdus. Toks bendradarbiavimas padėtų stiprinti bendrą saugumo tinklą ir skatintų efektyvesnį atsaką į grėsmes.
7. **Technologinės naujovės ir atnaujinimai:** Prioretizuoti investicijas į naujausias saugumo technologijas ir reguliarius sistemų atnaujinimus, tokiu būdų išlaikant aukščiausią saugumo lygį.
8. **Strateginio planavimo ir adaptacijos svarba:** Lanksčių saugumo strategijų diegimas, kurios gebėtų ne tik reaguoti į esamas grėsmes, bet ir numatytų būsimuosius iššūkius.

LITERATŪROS SĄRAŠAS

1. Vitalija Bagdžiūnienė „Įmonių Veiklos Planavimas ir Analizė“ p.8 (2011)
2. Vytautas Bujauskas, Leonas Simanauskas ir Rimvydas Skyrius „Kompiuterinis sprendimų modeliavimas p.12-13 (2009)
3. Remigijus Kinderis „Verslo Modeliai – Jų Semantinė Raiška ir Struktūra“ (2012). Prieiga per internetą: https://www.researchgate.net/publication/336148442_VERSLO_MODELIAI_-_JU_SEMANTINE_RAISKA_IR_STRUKTURA
4. Remigijus Kinderis, Giedrius Jucevičius „Verslo modelio inovacijos: tipologijos ir dimensijos vadybos teorijoje“ Ekonomika ir vadyba: aktualijos ir perspektyvos. ISSN 1648-9098. (2013)
5. Aurelija Burinskienė, Diana Daškevič „Verslo Modeliai prekybos įmonėse“ Prieiga per internetą: https://www.researchgate.net/publication/315627073_Verslo_modeliai_prekybos_imonese
6. Chesbrough, H., Rosenbloom, R. S., The Role of the Business Model in Capturing Value from Innovation: Evidence from Xerox Corporation’s Technology Spinoff Companies. (2002). Prieiga per internetą: https://www.researchgate.net/publication/247989217_The_Role_of_the_Business_Model_in_Capturing_Value_from_Innovation_Evidence_from_Xerox_Corporation's_Technology_Spin-Off_Companies
7. Joan Magretta „Why Business Models Matter“ (2002) Priega per internetą: https://hbr.org/2002/05/why-business-models-matter
8. Alexander Osterwalder „The Business Model Ontology – A propositions in a design science approach“ (2004) Priega per interneta: https://www.researchgate.net/publication/33681401_The_Business_Model_Ontology_-_A_Proposition_in_a_Design_Science_Approach
9. C. Trimble „More thant a field trip“ The business mocel canvas as support for the field site visits in marketing courses“ p.92 (2015). Prieiga per internetą: https://www.mmaglobal.org/_files/ugd/3968ca_1bcb1e204edc4f9988242dedafa96f20.pdf#page=107
10. H. Chesbrough „Busines model inovation: It‘s not just about technology“ (2007) Prieiga per internetą: https://www.emerald.com/insight/content/doi/10.1108/10878570710833714/full/html?skipTracking=true

11. D. Teece „Business Models, Business Strategy and Innovation“ (2010) Prieiga per internetą: https://www.researchgate.net/publication/222880471_Business_Models_Business_Strategy_and_Innovation
12. Alexander Osterwalder, Yves Pigneur, Tucci, C. L.,“Clarifying business models: origins, present, and future of the concept“ (2005). Prieiga per internetą: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3016&context=cais
13. Alexander Osterwalder, Yves Pigneur „Busines Model Generation“ (2010) prieiga per internetą: https://www.google.lt/books/edition/Business_Model_Generation/Bjj8G3ttLWUC?hl=en&gbpv=1&printsec=frontcover
14. Charles Baden-Fuller, Marry S.Morgan „Business Models as Models“ (2010) Prieiga per interntą: https://www.researchgate.net/publication/48911606_Business_Models_as_Models
15. Gerard George, Adam Jay Block „The Business Model in Practice and Its Implications for Entrepreneurship Research“ (2009) Prieiga per internetą: https://www.researchgate.net/publication/228215619_The_Business_Model_in_Practice_and_Its_Implications_for_Entrepreneurship_Research
16. Ramon Casadesus-Masanell, Joan E. Ricart „From Strategy to Business Models and onto tactics“ (2010) Prieiga per internetą: https://www.researchgate.net/publication/222219462_From_Strategy_to_Business_Models_and_onto_Tactics
17. Raphael Amit, Christoph Zott „Business Model Innovation Strategy: Transformational Concepts and Tools for Entrepreneurial Leaders„ (2020) Prieiga per internetą: https://books.google.lt/books?id=PV-wzAEACAAJ&pg=PA14&source=gbs_selected_pages&cad=1#v=onepage&q&f=false
18. B.W. Wirtz „Business Model Management, Design - Process – Instruments“ (2020) Prieiga per internetą: https://www.researchgate.net/publication/345175886_Business_Model_Management_Design_-_Process_-_Instruments
19. Steve Jobs iPhone presentation (2007) video: https://www.youtube.com/watch?v=4mvHgLy_YV8
20. Suhr Hansen (2021) „The story of how Netflix became the world’s most successful subscription company“ Prieiga per internetą: https://subscrybe.com/netflix-subscription-success/
21. Carolina Milanesi „Amazon’s Business Is Growing And Diversifying And So Is Its Sustainability Strategy“ (2022) Priega per internetą:

https://www.forbes.com/sites/carolinamilanesi/2022/08/01/safamazons-business-is-growing-and-diversifying-and-so-is-its-sustainability-strategy/

22. Par-Jorgen Parson „Spotify — The impossible success story“ (2018)) Prieiga per internetą: https://medium.com/@Pjparson/spotify-the-impossible-success-story-316a1062d79e
23. Darius Štitilis „Kibernetinio saugumo teisinis reguliavimas: Kibernetinio saugumo strategijos“ (2013). Priega per internetą: https://www.researchgate.net/publication/273219228_Kibernetinio_saugumo_teisinis_reguliavimas_kibernetinio_saugumo_strategijos
24. Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, Inga Malinauskaitė-van de Castel „Rekomendacijos Lietuvos Respublikos Kibernetinio Saugumo Įstatymui“ (2017) Prieiga per internetą: https://cris.mruni.eu/server/api/core/bitstreams/203f299e-dc63-41e0-b6ee-36321e70e3b4/content
25. R.A. Kemmerer „Cybersecurity“ (2003) 25th International Conference on Software Engineering, 2003. Proceedings „Introduction“. Prieiga per internetą: Cybersecurity | IEEE Conference Publication | IEEE Xplore
26. E. Courty: „The story of the first ever computer virus: Creeper“ (2023), Prieiga per internetą: https://medium.com/@edouard.courty/the-story-of-the-first-ever-computer-virus-creeper-f7fcf8cb7fc4
27. K. Zetter „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid“ (2016), Prieiga per internetą: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
28. KAM, LR Vyriausybė „Dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo“ (2018) Kibernetinio saugumo įstatymo nutarimas 818, 5 straipsnio 1 punktas. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595
29. KAM, LR Vyriausybė „Lietuvos nacionalinė kibernetinio saugumo strategija“ 2018, prieiga per internetą: https://kam.lt/leidiniai/nacionaline-kibernetinio-saugumo-strategija/
30. KAM, LR Vyriausybė „Lietuvos respublikos įstatymo nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnio, 5 skyriaus pavadinimo, priedo pakeitimo ir įstatymo papildymo 17 straipsniu ir 6 skyriumi įstatymas“ (2018), Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595
31. ES Direktyva (ES) 2016/1148, *OL L 194, 2016 7 19, p. 1–30* (2016) Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016L1148

32. ES Direktyva (ES) 2019/881, (2019) Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32019R0881
33. ES Direktyva (ES) NIS 2.0 2022/2555, (2023) Prieiga per internetą: https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive
34. Star Adviser (2011) „Kaneohe woman indicted in 'ghost payroll' scheme". Priega internetu: https://www.staradvertiser.com/2011/12/28/breaking-news/kaneohe-woman-indicted-in-ghost-payroll-scheme/
35. Pravin Gupta „Salami attack: What it is and how to avoid it?" (2023). Prieiga internetu: https://codedamn.com/news/cyber-security/salami-attack-what-it-is-and-how-to-avoid-it
36. Los Angeles Times „EBAY case leads FBI probe on „Shill" bidding. (2000). Priega per internetą: https://www.latimes.com/archives/la-xpm-2000-jun-08-fi-38885-story.html
37. M. Stephens, C. Hymas, The Telegraph, (2023) „Scams demanding payment for phantom goods soar to 450,000 a year". Prieiga per internetą: https://www.telegraph.co.uk/news/2023/04/27/scams-demanding-payment-phantom-goods-soar-450000-year/
38. Kevin Mitnick (2021) "Interview With Renowned Hacker Kevin Mitnick". Interviu internete: https://www.youtube.com/watch?app=desktop&v=QCU4nkgfg4U
39. J.Reitman, Rolling Stone magazine (2012), „The Rise and Fall of Jeremy Hammond: Enemy of the State". Prieiga per internetą: https://www.rollingstone.com/culture/culture-news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-183599/
40. P. Nicholson „Five most famous DDoS attacks and then some" (2022). Prieiga per internetą: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/#:~:text=The%20CloudFlare%20DDoS%20Attack%20in,gigabits%20per%20second%20of%20traffic.
41. S. Gallagher „Biggest DDoS ever aimed at Cloudflare's content delivery network" (2014). Priega per internetą: https://arstechnica.com/information-technology/2014/02/biggest-ddos-ever-aimed-at-cloudflares-content-delivery-network/
42. A. Bizga, „Bitdefender", „FIFA World Cup 2022: Scammers phish for personal data and Microsoft login credentials, Bitdefender Antispam Lab warns". Priega per internetą: https://www.bitdefender.com/blog/hotforsecurity/fifa-world-cup-2022-scammers-phish-for-personal-data-and-microsoft-login-credentials-bitdefender-antispam-lab-warns/
43. J. Kelley „A World Cup of Phishing and Cyberattacks" (2022). Prieiga per internetą: https://www.f5.com/company/blog/a-world-cup-of-phishing-and-cyberattacks

44. BBC (2017) „Massive ransomware infection hits computers in 99 countries“. Prieiga per internetą: https://www.bbc.com/news/technology-39901382
45. H.Marin, A.Matosov, E.Rodionov, Virus Bulletin (2010), prieiga per internetą: https://www.virusbulletin.com/virusbulletin/2010/10/rooting-about-tdss
46. BBC (2017) „NHS 'could have prevented' WannaCry ransomware attack“. Priega per internetą: https://www.bbc.com/news/technology-41753022
47. S. Larson „Why WannaCry ransomware took down so many businesses“ (2017) priega per internetą: https://money.cnn.com/2017/05/17/technology/wannacry-ransomware-business-security/index.html
48. BBC „Stuxnet 'hit' Iran nuclear plans“ (2010). Priega per internetą: https://www.bbc.com/news/technology-11809827
49. BBC „Code clues point to Stuxnet maker“ (2010). Priega per interntą: https://www.bbc.com/news/technology-11795076
50. A.Orlando „The Story of the 414s: The Milwaukee Teenagers Who Became Hacking Pioneers“ (2020). Prieiga per internetą: https://www.discovermagazine.com/technology/the-story-of-the-414s-the-milwaukee-teenagers-who-became-hacking-pioneers
51. Lockheed Martin, E.M. Hutchins, J.M. Cloppert, R.M. Amin, 2009, „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains“. Prieiga per internetą: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
52. Casey Crane (2023) straipsnis „A Look at 30 Key Cyber Crime Statistics“. Prieiga per internetą: https://www.thesslstore.com/blog/cyber-crime-statistics/
53. Bruce Lyon „Risk Assessment standarts and definitions“ (2021). Prieiga per internetą: https://www.researchgate.net/publication/357146623_Risk_Assessment_Standards_and_Definitions
54. PCI DSS (2024). Prieiga per internetą: https://www.pcisecuritystandards.org/
55. S. Licke „Complying with the PCI DSS Standard“ (2024). Priega per internetą: https://www.researchgate.net/publication/377456787_Complying_with_the_PCI_DSS_Standard
56. Mandy Huth „Security Frameworks Fundamentals: PCI DSS and Credit Card payments“ (2023). Prieiga per internetą: https://www.linkedin.com/learning/security-frameworks-fundamentals/cis-security-controls?u=2056964
57. CIS Kontrolė (2024). Prieiga per internetą: https://www.cisecurity.org/

58. Mandy Huth „Security Frameworks Fundamentals: CIS security Controls (2023). Prieiga per internetą: https://www.linkedin.com/learning/security-frameworks-fundamentals/cis-security-controls?u=2056964
59. NIST (2024). Prieiga per internetą: https://www.nist.gov/
60. FedRAMP (2024). Prieiga per internetą: https://www.fedramp.gov/
61. NIST 80-53. (2024) Prieiga per internetą: https://csrc.nist.gov/publications/sp800
62. Ronald Woerner „Implementing the NIST Risk Management Framework“ (2020). Prieiga per internetą: https://www.linkedin.com/learning/implementing-the-nist-risk-management-framework/reducing-risks-using-the-nist-risk-management-framework?u=2056964
63. ISO 27001:2022 (2024) Priega per internetą: https://www.iso.org/standard/27001
64. ISO 27001:2022 (2024) Prieiga per internetą: https://www.itgovernance.co.uk/iso27001
65. ISO 27002:2022 (2024) Prieiga per internetą: https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates
66. Ta-Seen Junaid „ISO 27001 (2023): Information Security Management Systems“ prieiga per internetą: https://www.researchgate.net/publication/367166657_ISO_27001_Information_Security_Management_Systems
67. Senesh Wijayarathne „ISO 27001 Implementations“ (2022) prieiga per internetą: https://www.researchgate.net/publication/372523436_ISO_27001_Implementation
68. March Menninger „ISO 27001:2013-Compliant Cybersecurity: Getting Started“ Prieiga per internetą: https://www.linkedin.com/learning/iso-27001-2013-compliant-cybersecurity-getting-started/the-international-standard-for-information-security?u=2056964
69. Malcom Shore „Cybersecurity Foundations: Frameworks for protection agains Cyber Threats“ (2023). Prieiga per internetą: https://www.linkedin.com/learning/cybersecurity-foundations-22006082/what-you-should-know?autoSkip=true&resume=false&u=2056964
70. Mandy Muth „Security Frameworks Fundamentals: Framework Comparison“ (2023). Priega per internetą: https://www.linkedin.com/learning/security-frameworks-fundamentals/how-the-frameworks-compare?resume=false&u=2056964
71. O. Kibik, O. Taran-Lala, V. Saienko, T Metil, T. Umanets, I.Maksymchuk „Vectors for Enterprise Development in the Context of the Digitalization of the Economy“ (2022), Volume 13, Issue 2, pages: 384-395| https://doi.org/10.18662/po/13.2/460
72. Mitchell, S. GRC360: A framework to help organisations drive principled performance. Int J Discl Gov 4, 279–296 (2007). Prieiga per internetą: https://doi.org/10.1057/palgrave.jdg.2050066

73. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 Prieiga per internetą: https://eur-lex.europa.eu/eli/reg/2016/679/oj
74. OCEG Red Book 2024 Prieiga per internetą: https://www.oceg.org/grc-capability-model-red-book/
75. P.Vincente, M.Silva „A Business Viewpoint for Integrated IT Governance, Risk and Compliance.“ In: 2011 IEEE World Congress on Services (SERVICES). pp. 422–428 (2011)
76. N. Racz, E. Weippl, A. Seufert. „A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)“ Prieiga per interntą: https://www.researchgate.net/publication/221521336_A_Frame_of_Reference_for_Research_of_Integrated_Governance_Risk_and_Compliance_GRC
77. A. Gericke, H-G. Fill, D. Karagiannis, R. Winter „Situational Method Engineering for Governance, Risk and Compliance Information Systems“ (2009) Prieiga per interntą: https://www.researchgate.net/publication/44939592_Situational_Method_Engineering_for_Governance_Risk_and_Compliance_Information_Systems
78. A. Bryman „Social Research Methods. Oxford University Press. Oxford.“ (2001).
79. Augustinaitis, A.; Rudzkienė, V.; Petrauskas, R.A.; Dagytė, I.; Martinaitytė E.; Leichteris E.; Malinauskienė E.; Višnevska V.; Žilionienė I. (2009). Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas. Monografija. Vilnius: MRU, 352 p.
80. A.Baležentis, M. Žalimaitė „Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje : Lietuvos inovatyvių įmonių vertinimas“ (2011), Nr. 3 (27), p. 23-31
81. K. Kardelis „Mokslinių tyrimų metodologija ir metodai“ (2019) MP3 Garso įrašas
82. V. Žydžiūnaitė ir S. Sabaliauskas „Kokybiniai tyrimai. Principai r metodai“, (p. 332–367), (2017)
83. Libby, R., & Blashfield, R. K. (1978). Performance of a composite as a function of the number of judges. Organizational Behavior and Human Performance, 21(2), 121-129. https://doi.org/10.1016/0030-5073(78)90044-2

SANTRAUKA

Magistriniame darbe "Kibernetinio saugumo verslo sprendimų modeliavimas ir plėtra" analizuojamas kibernetinio saugumo integravimas į verslo procesus naudojant A. Osterwalderio sukurtą Verslo Modelio Drobę (BMC) ir GRC (Valdymo, Rizikos ir Atitikties) principus. Tyrimo tikslas – sukurti hipotetinį modelį, kuris leistų įmonėms efektyviai valdyti saugumo rizikas ir užtikrinti atitiktį teisiniams reikalavimams, tuo pačiu skatinti tvarią kibernetinio saugumo strategijų integraciją.

Darbe atliekama išsami teorinė ir praktinė kibernetinio saugumo literatūros analizė, apžvelgiami svarbiausi kibernetinio saugumo standartai, tokie kaip ISO/IEC 27001, NIST ir PCI DSS, ir jų taikymo praktika. Be to, nagrinėjamas teisinis reguliavimas, pabrėžiant ES Bendrojo duomenų apsaugos reglamento (GDPR) ir kitų svarbių teisės aktų įtaką kibernetinio saugumo politikoms.

Analizė parodė, kad efektyvi kibernetinio saugumo integracija reikalauja ne tik technologinių sprendimų, bet ir žmogiškųjų išteklių, procesų ir politikų derinimo. Magistriniame darbe pateikti įrodymai, kad žmogiškieji ištekliai yra neatskiriama sėkmingo kibernetinio saugumo strategijos dalis, reikalaujanti nuolatinio mokymo, įtraukties ir saugumo sąmoningumo kėlimo visuose organizacijos lygmenyse.

Hipotetinis modelis, sukurtas tyrimo metu, suteikia organizacijoms metodinį pagrindą, kaip sistemingai įgyvendinti kibernetinio saugumo strategijas, atitinkančias tiek operacines, tiek strategines verslo reikmes. Modelis efektyviai padeda vertinti kibernetinio saugumo rizikas, taikyti atitikties standartus ir užtikrinti duomenų apsaugą, įgyvendinant kibernetinio saugumo priemones.

Šis magistro darbas yra reikšmingas indėlis į kibernetinio saugumo ir verslo modelių integravimo sritį, pateikiantis praktinės vertės sprendimus, pritaikomus įvairiose pramonės šakose. Jis išryškina kibernetinio saugumo reikšmę kaip būtiną verslo plėtros ir inovacijų dalį šiuolaikinėje verslo aplinkoje.

SUMMARY

In the master's thesis "Modeling and Development of Cybersecurity Business Solutions," the integration of cybersecurity into business processes is analyzed using the Business Model Canvas (BMC) and GRC (Governance, Risk, and Compliance) principles developed by A. Osterwalder and S. Mitchell. The aim of the study is to create a hypothetical model that would allow companies to effectively manage security risks and ensure compliance with legal requirements, while promoting sustainable integration of cybersecurity strategies.

The thesis includes a detailed theoretical and practical analysis of cybersecurity literature, reviews key cybersecurity standards such as ISO/IEC 27001, NIST, and PCI DSS, and their practical application. Additionally, legal regulation is examined, emphasizing the impact of the EU General Data Protection Regulation (GDPR) and other significant legal acts on cybersecurity policies.

The analysis showed that effective integration of cybersecurity requires not only technological solutions but also the alignment of human resources, processes, and policies. The master's thesis presents evidence that human resources are an integral part of a successful cybersecurity strategy, requiring continuous training, inclusion, and raising security awareness at all organizational levels.

The hypothetical model developed during the study provides organizations with a methodological basis on how to systematically implement cybersecurity strategies that meet both operational and strategic business needs. The model effectively helps identify cybersecurity risks, apply compliance standards, and ensure data protection through the implementation of cybersecurity measures.

This master's thesis is a significant contribution to the field of cybersecurity and business model integration, offering practical value solutions that can be applied across various industry sectors. It highlights the importance of cybersecurity as an essential part of business development and innovation in the modern business environment.

PRIEDAI

1. Apklausos anketa