Kauno technologijos universitetas

Informatikos fakultetas

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas

Baigiamasis magistro projektas

Gediminas Sviščevskis

Projekto autorius

Prof. Dr. Algimantas Venčkauskas

Vadovas

Kaunas, 2022

Kauno technologijos universitetas

Informatikos fakultetas

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas

Magistro projektas

Informacijos ir informacinių technologijų sauga (6211BX008)

Gediminas Sviščevskis

Projekto autorius

Prof. Algimantas Venčkauskas

Vadovas

Prof. Agnius Liutkevičius

Recenzentas

Kaunas, 2022

Kauno technologijos universitetas

Informatikos fakultetas

Gediminas Sviščevskis

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Gedimino Sviščevskio, baigiamasis projektas tema „Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka)	(parašas)

Sviščevskis Gediminas. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas. Magistro baigiamasis projektas / prof. dr. Algimantas Venčkauskas; Kauno technologijos universitetas, informatikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Informatikos inžinerija (Informatikos mokslai).

Reikšminiai žodžiai: kibernetinis saugumas, kibernetinio saugumo reitingas, kibernetinio saugumo įvertinimas, dinaminis reitingas.

Kaunas, 2022. 64 p.

Santrauka

Kibernetinis saugumas šių dienų pasaulyje tampa vis populiaresnis tarp kasdienių informacinių technologijų naudotojų ir įvairaus dydžio įmonių. Kasmet naujienose pasirodo vis didesni kibernetinio saugumo incidentai, kurių metu nukenčia įmonių reputacija ir įvaizdis, patiriami dideli finansiniai nuostoliai. Tokie įvykiai pritraukia įmonių dėmesį ir verčia ieškoti būdų, kaip įmonės galėtų apsaugoti savo verslų kibernetinę ekosistemą. Vienas iš žingsnių, kuris padeda tai padaryti, yra įmonės kibernetinio saugumo lygio nustatymas. Tam yra daromi įvairūs kibernetinio saugumo auditai, tačiau jie parodo įmonės kibernetinį saugumą tik tam tikru laiko momentu. Siekiant išspręst šią problemą yra kuriamas dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas. Darbe analizuojamas kibernetinio saugumo egzistavimas ir pasireiškimas įmonėse, apibrėžiamas įmonės kibernetinio saugumo reitingas, jo dinamika, kintamieji, vertinimo metrikos, palyginami egzistuojantys kibernetinio saugumo vertinimo ir auditų metodai, keliamos problemos ir naudos. Atlikus analizę buvo pastebėtas realus sistemos, kuri panaudotų dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodą, poreikis. Dėl to buvo suprojektuotas ir realizuotas šį metodą naudojantis sistemos prototipas, kuris pasižymi savo lankstumu, laisva prieiga ir svarbiausia – gebėjimu įvertinti ir stebėti įmonės kibernetinio saugumo situaciją. Taip pat darbe yra atlikti sukurto dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo ir jo sistemos prototipo tyrimai, kurių metu buvo įvertintos šio metodo pritaikymo panaudos galimybės ir pateikti pastebėjimai.

Sviščevskis Gediminas. A Method for Determining the Dynamic Cyber Security Rating of a Company. Master's Final Degree Project / prof. dr. Algimantas Venčkauskas; Faculty of informatics, Kaunas University of Technology.

Study field and area (study field group): Informatics Engineering (Computing).

Keywords: cyber security, cyber security rating, cyber security score, cyber security assessment, dynamic rating, dynamic score.

Kaunas, 2022. 64 p.

Summary

In today's world, cybersecurity is becoming increasingly popular among everyday IT users and businesses of all sizes. Every year, there are more and more cyber security incidents in the news, which damage the reputation and image of companies and cause significant financial losses. Such events attract the attention of companies and force them to look for ways in which companies can protect the cyber ecosystem of their businesses. One of the steps that helps to do this is to determine the level of cyber security in the company. Various cyber security audits are performed for this purpose, but they only show the cyber security of the company at a certain point in time. To solve this problem, a dynamic method of determining the cyber security rating of a company is being developed. The paper analyses the existence and manifestation of cyber security in companies, defines the company's cyber security rating, its dynamics, variables, evaluation metrics, compares existing cyber security evaluation and audit methods, their problems and benefits. The analysis revealed a real need for a system that would use a dynamic approach to determining a company's cyber security rating. As a result, a system prototype using this method has been designed and implemented, which is characterized by its flexibility, free access and, most importantly, the ability to assess and monitor the company's cyber security situation. Also, the research of the developed dynamic method of determining the cyber security rating of the company and its system prototype has been performed, during which the application possibilities of this method have been evaluated and observations have been presented.

Turinys

Lentelių sąrašas **8**
Paveikslų sąrašas **9**
Santrumpų ir terminų sąrašas **10**
Įvadas **12**
1. Dinaminio įmonės kibernetinio saugumo analizė **14**
1.1. Kibernetinis saugumas įmonėje 14
1.1.1. Kibernetinio saugumo supratimas 14
1.1.2. Informacijos saugos politika 14
1.1.3. Kibernetinio saugumo auditai 15
1.2. Dinaminio įmonės kibernetinio saugumo reitingas 17
1.2.1. Kibernetinio saugumo reitingas 17
1.2.2. Kibernetinio saugumo reitingo kintamųjų analizė 17
1.2.3. Kibernetinio saugumo reitingo kintamųjų vertinimo metrikos 18
1.2.4. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo problemos analizė 19
1.3. Kibernetinio saugumo vertinimo metodų analizė 20
1.4. Dinaminio įmonės kibernetinio saugumo reitingo nauda 23
1.5. Esamų kibernetinio saugumo reitingo nustatymo priemonių analizė 23
1.6. Galimų problemos sprendimo metodų nagrinėjimas 25
1.7. Išvados 26
2. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas ir sistema **27**
2.1. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo veikimo konceptas 27
2.1.1. Sistemos veikimo koncepto schema 27
2.1.2. Reitingo skaičiavime naudojamos informacijos surinkimas 28
2.1.3. Dinamiškumo realizavimas sistemoje 28
2.2. Sistemos funkciniai reikalavimai 29
2.2.1. Sistemos panaudojimo atvejų diagrama 29
2.2.2. Pagrindinių panaudos atvejų veiklų diagramos 30
2.3. Reitingo nustatymas 31
2.3.1. Reitingo formatas 32
2.3.2. Reitingo kintamieji 32
2.3.3. Reitingo skaičiavimas 33
2.4. Sistemos architektūra 35
2.5. Duomenų bazės schema 36
2.6. Išvados 38
3. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipas **39**
3.1. Sistemos prototipui pasirinkti įrankiai 39
3.1.1. Žiniatinklio sistemos daliai pasirinkti įrankiai 39
3.1.2. Duomenų surinkimui pasirinktas įrankis 39
3.2. Prototipe naudojamų įrenginių infrastruktūra 40
3.3. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipo diegimas 41
3.3.1. Sistemos diegimo diagrama 41
3.3.2. Konfigūracija 42
3.4. Automatiniu būdu surenkamos informacijos šaltiniai 43
3.5. API apsauga 43

3.5.1. OAuth 2.0 metodologijos pritaikymas API autentifikavimo procese 44
3.5.2. JWT struktūra 44
3.6. Prototipo reitingo skaičiavimo dinamiškumas 45
3.7. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos veikimas 46
3.8. Išvados 56
4. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo tyrimas 57
4.1. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo tikslumas 57
4.2. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo greitaveikos tyrimas ... 57
4.3. Panašių įrankių palyginimas su sukurtu prototipu 59
4.4. Išvados 61
Išvados 62
Literatūros sąrašas 63

Lentelių sąrašas

1 lentelė. Kibernetinio saugumo duomenų surinkimo ir rizikų vertinimo įrankių palyginimas..... 24

Paveikslų sąrašas

1 pav. Galutinio kibernetinio saugumo įvertinimo lentelė 21
2 pav. Kibernetinio saugumo rizikos įvertinimo interviu pavyzdys 22
3 pav. Sistemoje esančių įrenginių pavyzdys 27
4 pav. Dinaminio įmonės kibernetinio saugumo reitingo skaičiavimo sistemos panaudojimo atvejų diagrama 29
5 pav. PA „Surinkti informaciją“ veiklos diagrama 30
6 pav. PA „Skaičiuoti kibernetinio saugumo reitingą“ veiklos diagrama 31
7 pav. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo žingsniai 34
8 pav. Z indekso reikšmės 34
9 pav. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos architektūra 36
10 pav. Duomenų bazės schema 37
11 pav. Užklausos duomenų pavyzdys 40
12 pav. Prototipe naudojamų įrenginių infrastruktūra 41
13 pav. Sukurtos virtualios mašinos „Hyper-V Manager“ programoje 41
14 pav. Sistemos diegimo diagrama 42
15 pav. Naudojami informacijos šaltiniai įrenginiuose 43
16 pav. JWT prieigos rakto antraštė 44
17 pav. JWT prieigos rakto turinys 45
18 pav. JWT prieigos rakto parašo kūrimas 45
19 pav. JWT prieigos rakto pavyzdys 45
20 pav. Kategorijų sąrašo puslapis 47
21 pav. Kategorijos pridėjimo puslapis 47
22 pav. Kategorijų redagavimo puslapis 48
23 pav. „Device security“ kriterijų puslapis 48
24 pav. Kriterijaus pridėjimo puslapis 49
25 pav. Kriterijaus „Operation system security“ redagavimo puslapis 50
26 pav. Kriterijaus „Operation system security“ faktorių puslapis 51
27 pav. Faktoriaus pridėjimo puslapis 51
28 pav. Faktoriaus „Bitlocker“ redagavimo puslapis 52
29 pav. Įrenginių sąrašo puslapis 52
30 pav. Įrenginio pridėjimo puslapis 53
31 pav. Įrenginio redagavimo puslapis 54
32 pav. Agento programinės įrangos terminalo langas 55
33 pav. Pagrindinis sistemos puslapis su pavaizduotu kibernetinio saugumo reitingu 55
34 pav. Duomenų surinkimo greitaveikos grafikas 58

Santrumpų ir terminų sąrašas

Santrumpos:

Prof. – profesorius.

IT – informacinės technologijos.

CSAM – (angl. „Cyber Security Assessment and Management“) sistema, priklausanti Jungtinių Valstijų informacinėms sistemoms, kurios yra susijusios su žiniatinklio kibernetinio saugumo vertinimo ir valdymu.

GAAS – (angl. „Generally Accepted Auditing Standard“) bendrai priimtas audito standartas.

NIST – (angl. „National Institute of Standards and Technology“) nacionalinis standartų ir technologijos institutas.

CVSS – (angl. „Common Vulnerability Scoring System“) viena iš bendrų pažeidžiamumų vertinimo sistemų.

CVE – (angl. „Common Vulnerabilities and Exposures“) programa skirta nustatyti, apibrėžti ir kataloguoti viešai atskleistas kibernetinio saugumo spragas.

OVAL – (angl. „Open Vulnerability and Assessment Language“) atvira pažeidžiamumų ir jų įvertinimo programavimo kalba.

SCAP – (angl. „Security Content Automation Protocol“) saugumo turinio automatizavimo protokolas.

IDS – (angl. „Intrusion Detection System“) įsilaužimų aptikimo sistema.

CSG – (angl. „Cyber Security Game“) kibernetinio saugumo žaidimas, metodo pavadinimas.

API – (angl. „Application Programming Interface“) aplikacijų programavimo sąsaja.

CRUD – (angl. „Create, Read, Update, Delete“) pagrindinės duomenų valdymo funkcijos – sukurti, skaityti, atnaujinti, ištrinti.

SOC – (angl. „Security Operations Center“) saugos operacijų centras.

PCI DSS – (angl. „Payment Card Industry Data Security Standard“) mokėjimo kortelių industrijos duomenų saugumo standartas.

CMMC – (angl. „Cybersecurity Maturity Model Certification“) kibernetinio saugumo brandos modelio sertifikatas.

HITRUST – globali kibernetinio saugumo ir atitikties organizacija.

GDPR – (angl. „General Data Protection Regulation“) bendrasis duomenų apsaugos reglamentas.

CCPA – (angl. „Cybersecurity Response to the California Consumer Privacy Act“) kibernetinio saugumo atsakas į Kalifornijos vartotojų privatumo įstatymą.

ISO – (angl. „International Organization for Standardization“) tarptautinė standartizacijos organizacija.

SaaS – (angl. „Software as a service“) programinė įranga kaip paslauga modelis.

IRP – (angl. „Incident Response Platform“) reagavimo į incidentus platforma.

IP – (angl. „Internet Protocol“) interneto protokolas, adresas.

DNS – (angl. „Domain Name System“) domenų vardų sistema.

ID – (angl. „Identifier“) identifikatorius.

MySQL – viena iš reliacinių duomenų bazių valdymo sistemų, palaikanti daugelį naudotojų, dirbanti SQL kalbos pagrindu.

SQL – (angl. „Structured Query Language“) reliacinių duomenų bazių programavimo kalba.

HTML – (angl. „HyperText Markup Language“) tai kompiuterinė žymėjimo kalba, naudojama pateikti turinį internete.

CSS – (angl. „Cascading Style Sheets“) programavimo kalba, kurią dažniausiai naudojame HTML dokumento stiliui kurti.

PHP – (angl. „Hypertext Preprocessor“) dinaminė interpretuojama programavimo kalba.

JS – (angl. „JavaScript“) objektiškai orientuota programavimo scenarijų programavimo kalba.

JSON – (angl. „JavaScript Object Notation“) atviro standarto formatas, perduodantis duomenų objektus.

SSL – (angl. „Secure Sockets Layer“) protokolas saugiems ryšiams tarp tinkle sujungtų kompiuterių užmegzti.

WMI – (angl. „Windows Management Instrumentation“) tai „Windows“ biblioteka, kuri suteikia operacinės sistemos sąsaja.

JWT – (angl. „JSON Web Tokens“) interneto standartas, skirtas saugiai perduoti duomenis naudojant JSON.

Įvadas

Laikui bėgant technologijos sparčiai vystosi, daugėja informacijos ir įmonėms tenka skirti vis daugiau dėmesio informacijos saugai. Šiais laikais praktiškai visi turime bent dalį informacijos apie save, kuri yra saugoma informacinėse sistemose. Įmonės generuoja dar daugiau informacijos ir dažnai ta informacija būna daug jautresnė. Informacija šiais laikais yra labai vertinga, dėl to pritraukia ir daug blogų ketinimų turinčių žmonių, kurie nori pasinaudoti šia informacija gaunant asmeninės naudos. Taip nuolat yra vykdomos kibernetinės atakos, kurių metų įvyksta finansinės ar duomenų vagystės, sistemų darbo sutrikdymai, duomenų pakeitimai ir kiti nusikalstami veiksmai. Po sėkmingų piktavališkų atakų gali nutikti masiniai padariniai. Nepaisant to, kad įmonės naudoja gerąsias saugumo praktikas jau daugelį metų, kibernetinių atakų kiekis nemažėja. Tam, kad apsisaugotų nuo kibernetinių atakų, įmonės imasi įvairių veiksmų, vienas iš jų – įmonės kibernetinio saugumo įvertinimas. Įmonės pasinaudoja išoriniais ar vidiniais kibernetinio saugumo auditais, kurie įvertina įmonės kibernetinį saugumą. Problema iškyla tame, kad technologijos ir atakų vektoriai keičiasi greičiau, nei įmonės sugeba atlikti kibernetinio saugumo auditus, todėl reikia naujo sprendimo, kuris parodytų įmonės kibernetinio saugumo lygį realiu metu. Kibernetinio saugumo reitingas, kurį būtų galima skaičiuoti dinamiškai ir turėtų suprantamą metriką įmonei, išspręstų šią problemą. Todėl reikia sukurti metodą, kuris skaičiuotų dinamišką įmonės kibernetinio saugumo reitingą ir realizuoti sistemą, kuri galėtų pasinaudoti šiuo metodu ir apskaičiuoti įmonės kibernetinio saugumo reitingą.

Problemos naujumas ir aktualumas

Dinaminio įmonės kibernetinio saugumo reitingas yra naudojamas renkantis partnerius, kibernetiniam draudimui ir padedant įmonei geriau suprasti savo kibernetinės apsaugos galimybes. Pavieniai kibernetinio saugumo įvertinimai parodo įmonės kibernetinio saugumo reitingą tam momentui, bet kibernetinis pasaulis nuolat keičiasi ir įsilaužėliai randa vis naujų atakų vektorių, kaip padaryti įmonėms žalos. Dėl to yra svarbu sugebėti nustatyti dinaminį įmonės kibernetinio saugumo reitingą ir neprarast geros reputacijos bei klientų ar partnerių pasitikėjimo.

Darbo tikslas ir uždaviniai

Darbo tikslas: sukurti metodą, kuris galėtų nustatyti įmonės kibernetinio saugumo reitingą. Šiam tikslui įgyvendinti buvo iškelti šie uždaviniai:

1. Atlikti dinaminio įmonės kibernetinio saugumo reitingo kintamųjų, metrikų, esamų metodų ir priemonių analizę.
2. Sudaryti dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodą atsižvelgus į atliktą analizę.
3. Realizuoti sistemos prototipą, kuris leistų nustatyti įmonės kibernetinio saugumo reitingą.
4. Įvertinti sukurtą kibernetinio saugumo reitingo nustatymo metodą ir apibendrinti gautus rezultatus.

Darbo struktūra

Dokumentą sudaro keturi pagrindiniai skyriai:

1. Dinaminio įmonės kibernetinio saugumo problemos analizė. Analizuojama, kaip kibernetinis saugumas gyvuoja įmonėse, kaip jis yra įvertinimas. Identifikuojami kibernetinio saugumo reitingo kintamieji, metrikos. Palyginami populiaresni kibernetinio saugumo reitingo apskaičiavimo metodai ir naudojamos priemonės.

2. Pasirenkamas geriausias dinaminio įmonės kibernetinio saugumo nustatymo metodas atsižvelgiant į atliktą analizę ir sudaromas metodo programinis prototipas, kurį bus galima panaudoti įvertinant dinaminio įmonės kibernetinio saugumo reitingą.
3. Realizuojamas dinaminio įmonės kibernetinio saugumo reitingo nustatymo programinis prototipas.
4. Pateikiamos galutinės išvados, įvertinamas pasirinktas metodas ir prototipo efektyvumas.

1. Dinaminio įmonės kibernetinio saugumo analizė

Atliekant analizę yra svarbu ištirti, kaip kibernetinis saugumas yra įvertinamas įmonėse, kaip vyksta įvertinimo auditai, kokie metodai yra taikomi. Taip pat, svarbu išanalizuoti kibernetinio saugumo kintamuosius, kuriuos reikia įvertinti, pagal kokią metriką juos vertinti ir jų dinamiškumo aspektą. Taipogi peržiūrėti ir palyginti populiarias kibernetinio saugumo įvertinimo priemones.

1.1. Kibernetinis saugumas įmonėje

Kibernetinis saugumas šių dienų įmonėje yra labai svarbus dėl daugelio priežasčių. Skirtingos įmonės turi skirtingo lygio išvystytą kibernetinį saugumą. Tai priklauso nuo investicijų neskyrimo, lėšų neturėjimo, įmonės verslo veiklos ir tipo, rizikos valdymo metodų ir kitų veiksnių. Todėl reikia suprasti kas yra kibernetinis saugumas, kodėl jis yra svarbus, kaip jis yra vystomas įmonėje bei kas ir kokiais būdais jį patikrina.

1.1.1. Kibernetinio saugumo supratimas

Kibernetinis saugumas dažnai yra perfrazuojamas kaip informacijos saugumas.

Informacinė sauga – tai veiksmų ir specifinių priemonių visuma, kuri yra skirta apsaugoti informaciją nuo neautorizuotos prieigos, sunaikinimo, modifikavimo, atskleidimo ir neteisėto panaudojimo. Informacinė sauga apima duomenų sukūrimo, jų įvesties, apdorojimo ir išvesties procesų apsaugą.

Informacinės saugos tikslas – apsaugoti informacinį turtą ir užtikrinti informacijos konfidencialumą, vientisumą bei prieinamumą. Norint pasiekti, kad informacija būtų saugi, būtina fiksuoti visus įvykius, kurių metu sukuriama ir modifikuojama informacija, prie jos suteikiama prieiga ar atliekami jos platinimo veiksmai.

Informacijos saugumą literatūroje dažniausiai apibūdina trys informacijos saugumo principai: konfidencialumas, vientisumas ir prieinamumas.

Konfidencialumas – tai procesas skirtas užtikrinti, kad su informacija galėtų susipažinti tik tie asmenys, kurie turi teisę su ja susipažinti, ir ji nebus tyčia ar netyčia atskleista kitiems asmenims. Tyčinis ar netyčinis informacijos atskleidimas pašaliniams asmenims yra laikomas konfidencialumo pažeidimu.

Vientisumas – antrasis saugumo principas, kurio pagrindinis tikslas užtikrinti, kad informacija, kuri yra informacinėse sistemose, nebus pakeista nesankcionuotu būdu, sugadinta ar visiškai prarasta. Dalini ar pilni informacijos praradimai ar neleistinas duomenų pakeitimas yra laikomi vientisumo pažeidimais.

Prieinamumas – trečiasis saugumo principas, skelbiantis, kad reikiami informacinių sistemų resursai bet kuriuo metu yra prieinami įgaliotiems asmenims. Pilnas ar dalinis sistemos darbo pažeidimas, dėl kurio informacija yra nepasiekiama visiems ar daliai sistemos naudotojų yra laikomas prieinamumo pažeidimu.

1.1.2. Informacijos saugos politika

Informacijos saugai nuolatos turi būti skiriamas dėmesys. Išvardinti principai yra tiek naudingi, kiek juos palaikys įmonėje dirbantys žmonės. Kad žmonės žinotų kaip elgtis abejotinose situacijose ar

kokių taisyklių laikytis, kad informacijos sauga būtų užtikrinta, įmonėje turi būti formuojama ir ugdoma saugos politika.

Saugumo politika (angl. „information security policy“) – oficialus vadovybės patvirtintas veiksmų ir taisyklių rinkinys, kurių privalo laikytis visi organizacijos darbuotojai bei kiti asmenys, besinaudojantys organizacijos paslaugomis, informacija ir technologijomis. Saugos politikos dokumento apimtis priklauso nuo organizacijos tipo, dydžio, veiklos ir kitų veiksnių.

Saugos politikos tikslas yra sukurti bendrą informacijos saugumo atmosferą organizacijoje, kuri padėtų aptikti ir užkirsti kelią informacijos saugumo pažeidimams, palaikyti organizacijos reputaciją ir laikytis etinių bei teisinių įsipareigojimų bei gerbti klientų teises.

1.1.3. Kibernetinio saugumo auditai

Kad būtų galima įvertinti kibernetinį saugumą yra vykdomi kibernetinio saugumo auditai. Auditus vykdo vidiniai arba išoriniai auditoriai, tai gali būti asmuo arba įmonė, kuri turi sukaupus pakankamai patirties ir žinių, kad galėtų korektiškai įvertinti įmonės kibernetinį saugumą. Priklausomai nuo audito tipo, per auditą gali tikrinti skirtingus dalykus – įvertinti pilną sistemos kibernetinį saugumą, stengtis įsibrauti į sistemą ir atrasti pažeidžiamumus, gali įvertinti atskirus sistemos komponentus, įvertinti kibernetinio saugumo rizikas, teisines atitiktis ir daugelį kitų su kibernetiniu saugumu susijusių dalykų. Kibernetinio saugumo auditų tikslai dažniausiai yra įvertinti įmonės procesus, siekiant atkreipti dėmesį į jautrią informaciją ir sistemas, geriau suprasti įmonės kibernetinių grėsmių bendrą vaizdą ir įvertinti įmonės pasirengimą reaguojant į kibernetinio saugumo įvykius.

„Donaldson et al.“ [12] Nustatė tris skirtingus kibernetinio saugumo auditų tipus:

1. Grėsmių auditai: šie auditai skirti kibernetinėms grėsmėms aptikti IT aplinkoje.
2. Vertinimo auditai: audito metu vertinama kibernetinio saugumo kontrolė, kuri yra susieta su IT karkasais, norminiais reikalavimais, standartais arba ypatingais atvejais – su konkrečia kibernetine grėsme.
3. Patvirtinimo vertinimai: vertinimas atliekamas atsižvelgiant į kibernetinio saugumo kontrolę, siekiant įvertinti šios kontrolės veiksmingumą pagal sukurtus ir dokumentais patvirtinus reikalavimus.

Norint korektiškai įvertinti kibernetinį saugumą įmonėje, dažnai atliekami kelių tipų auditai, o populiariausias yra vertinimo auditas. Kadangi technologijos nuolatos evoliucionuoja, įprastiniai auditai, kurie vadovaujasi visuotinai pripažintais audito standartais (GAAS), nėra pajėgūs įvertinti įmonės kibernetinį saugumą. Todėl, remiantis šaltiniu [13] yra palyginti trys vieni populiariausiai naudojamų kibernetinio audito modelių ar karkasų.

Kibernetinio saugumo karkasas sukurtas nacionalinio standartų ir technologijos instituto (NIST) 2017

Kibernetinio saugumo karkasas suteikia bendrą kalbą, skirtą suprasti, valdyti ir dalintis kibernetinio saugumo rizika vidaus ir išorės suinteresuotosioms šalims. Jis gali būti naudojamas atpažinti ir pirmenybę teikti veiksmams, kuriais siekiama sumažinti kibernetinio saugumo riziką ar kaip priemonė, skirta suderinti politikos, verslo ir technologinius metodus valdant šią riziką. Taip pat, jis gali būti naudojamas valdant kibernetinio saugumo riziką per daugelį organizacijų ar koncentruotis

ties kritinių paslaugų teikimų organizacijos viduje. Daugelis organizacijų gali naudoti šį kibernetinio saugumo karkasą skirtingoms priežastims, įskaitant ir profiliavimą.

Kibernetinio saugumo karkaso branduolys yra atsakingas už penkias pagrindines funkcijas – nustatyti, apsaugoti, aptikti, atsakyti ir atstatyti.
Nustatymas – atsakinga už organizacinio supratimo ugdymą, kaip valdyti kibernetinio saugumo riziką, sistemas, personalą, turtą, duomenis ir galimybes.
Apsaugojimas – atsakinga už parengimą ir įgyvendinimą tinkamų apsaugos priemonių, kurios užtikrintų kritinių paslaugų veikimą.
Aptikimas – atsakinga už plėtojimą ir įgyvendinimą atitinkamų procesų, kurie padėtų atpažinti kibernetinio saugumo įvykius.
Atsakymas – atsakinga už sukūrimą atitinkamų veiksmų, kurių būtų galima imtis aptikus kibernetinio saugumo incidentą.
Atstatymas – atsakinga už plėtojimą ir įgyvendinimą procesų, kurie padėtų palaikyti atsparumo planus ir atkurti visas paslaugas ar sistemos komponentus, kurie buvo pažeisti dėl kibernetinio saugumo incidento.

Audito metodologija pagal „Donaldson et al.“ (2015) (The Audit First Methodology: Donaldson et al.)

Šioje metodologijoje atsižvelgiama į kitas kibernetinio saugumo kontrolės priemones ir naudojama prevencinė kontrolė. Šis auditas apima penkis skirtingus etapus:

1. Grėsmės analizė: nustatomos konfidencialumo, vientisumo ir prieinamumo grėsmės, kurios gali turėti įtakos IT ir įmonės duomenims. Grėsmių poveikis ir rodikliai yra apibrėžti.
2. Audito kontrolė: apima grėsmių audito kontrolės planavimą.
3. Teisinė ekspertizė: šis etapas padeda įgyvendinti reikalingas teisines kibernetinio saugumo funkcines sritis:
    1) Sistemų administravimas
    2) Tinklai
    3) Paraiškos
    4) Galiniai taškai, serveriai ir įrenginiai
    5) Tapatybė, tapatybės patvirtinimas ir prieiga
    6) Duomenų apsauga ir kriptografija
    7) Stebėjimas, pažeidžiamumas ir pataisų valdymas
    8) Prieinamumas, atkūrimas po nelaimės ir fizinė apsauga
    9) incidentų valdymas
    10) Tiekimo grandinė ir turto valdymas
    11) Politika, auditas ir mokymai
4. Aptikimo valdikliai: skirti įspėti, aptikti, sustabdyti ir atremti kibernetines atakas.
5. Prevenciniai valdikliai: blokuoja nepageidaujamą veiklą ir neleidžia joms atsirasti.

Kibernetinio saugumo audito modelis (CSAM) pagal „Sabillon et al.“ (2017)

Kibernetinio saugumo audito modelis CSAM gali būti įgyvendintas atlikti vidinius ar išorinius kibernetinio saugumo auditus, taip pat naudojamas kaip dalis didesnio kibernetinio saugumo audito ar vertinti tik specifines įmonės kibernetinio saugumo dalis. Šis audito modelis taip pat naudoja savo

kibernetinio saugumo vertinimo metodą, kuris yra aprašytas prie kibernetinio saugumo vertinimo metodų analizės.

Paminėti kibernetinio saugumo auditai naudoja įvairius kibernetinio saugumo audito tipus ar jų kombinacijas ir skiria dėmesį ne tik kibernetinio saugumo įvertinimui, bet ir grėsmių atpažinimui ir apsisaugojimui nuo jų. Be aprašytų audito modelių yra daugelis kitų, skirtingos įmonės, kurios teikia kibernetinio saugumo audito paslaugas naudoja savo sukurtus ir privačius metodus. Tačiau didžioji dalis kibernetinio saugumo audito modelių yra labai panašūs, skiriasi tik naudojami metodai, be to dažnai persidengia su kitais, nes visi kibernetinio saugumo audito modeliai turi panašius ar vienodus tikslus.

1.2. Dinaminio įmonės kibernetinio saugumo reitingas

Peržvelgus kaip įmonėje veikia kibernetinis saugumas ir kaip bei kokiais būdais jį vertina, galima apibūdinti dinaminį įmonės kibernetinio saugumo reitingą. Reikia identifikuoti kibernetinio saugumo reitingo kintamuosius, kuriuos reikia vertinti, ir pasirinkti tinkamiausias metrikas jiems įvertinti. Taip pat, išanalizuoti šio reitingo dinamiškumo elementą.

1.2.1. Kibernetinio saugumo reitingas

Visų pirma, kibernetinis saugumo reitingas yra duomenimis pagrįstas, objektyvus ir dinamiškas organizacijos kibernetinio saugumo įvertinimas. Panašiai kaip egzistuoja kredito reitingai ir jais siekiama kiekybiškai įvertinti kredito riziką, kibernetinio saugumo reitingu siekiama pateikti kibernetinio saugumo rodiklį. Iš esmės kibernetinio saugumo reitingo ir kibernetinio saugumo auditų tikslas yra panašus, abejais siekiama įvertinti įmonės kibernetinį saugumą. Skirtumas tas, kad kibernetinio saugumo reitingas yra paskaičiuojamas konkrečiai iš įvairiais būdais surinktų duomenų, dėl to yra duomenimis pagrįstas ir kibernetinio saugumo reitingas gali būti nuolat sekamas ir atnaujinamas. Ši kibernetinio saugumo reitingo savybė suteikia dinamiškumo, kurio negauname iš kibernetinio saugumo auditų, kuriuos įmonės darosi kartą per metus ar dar rečiau. Kibernetinio saugumo reitingas yra dažnai nusakomas savo kintamaisiais, pagal ką jis yra paskaičiuojamas. Kintamųjų yra be galo daug ir jie dažniausiai yra priskiriami į kategorijas, kurios jau apima kitus kintamuosius ir atvaizduoja abstraktesnį jų lygį, taip parodydamos įmonės kibernetinio saugumą iš skirtingų pusių. Kibernetinio saugumo reitingas taip pat yra apibūdinamas savo metrika ir taikomu skaičiavimo metodu. Metrika tarp kibernetinio saugumo reitingų įgyvendinimų skiriasi, nes vieni matuoja kibernetinio saugumo rizikas, kiti saugumą. Kas be ko, kibernetinio saugumo reitingo skaičiavimo metodas yra vienas svarbiausių aspektų, nes galima turėti visus duomenis ir norimas metrikas, bet nesugebėti tiksliai ir efektyviai apskaičiuoti įmonės kibernetinio saugumo. Taigi, kibernetinio saugumo reitingas yra visuma kintamųjų, kurie kibernetinio saugumo reitingo skaičiavimo metodu yra įvertinti pagal pasirinktas metrikas ir šiuo atveju nustato ir atvaizduoja įmonės kibernetinį saugumą.

1.2.2. Kibernetinio saugumo reitingo kintamųjų analizė

Norint nustatyti dinaminį įmonės kibernetinio saugumo reitingą, pirmiausia reikia nustatyti kibernetinio saugumo įmonėje kintamuosius, kurie bus vertinami. Kintamųjų įmonėje priklausomai nuo jos dydžio ir naudojamų technologijų gali būti be galo daug, todėl kintamieji yra grupuojami į kategorijas. Prieš tai aptarti metodai bendrai yra išskyrę septyniolika pagrindinių kategorijų, kurios yra vertinamos darant išsamų kibernetinio saugumo auditą:

1. Valdymas ir strategija
2. Įstatymai ir atitikties užtikrinimas (angl. „compliance“)
3. Kibernetinis turtas
4. Kibernetinės rizikos
5. Karkasai ir reguliacijos
6. Architektūra ir tinklas
7. Informacija, informacinės sistemos ir aplikacijos
8. Pažeidžiamumų identifikacija
9. Grėsmių žvalgyba
10. Incidentų valdymas
11. Skaitmeninė kriminalistika
12. Sąmoningumo ugdymas
13. Kibernetinis užtikrinimas
14. Aktyvi kibernetinė gynyba
15. Besivystančios technologijos
16. Atkūrimo planai
17. Personalas

Kiekviena iš šių kategorijų gali turėti žemesnio lygių kategorijų ir įvairių įmonės kibernetinio saugumo aspektų, kuriuos reikia vertinti. Vieni kintamieji yra pakankamai statiniai ir informaciją apie juos galima surinkti automatizuotais būdais, kitiems reikia žmogaus indėlio. Priklausomai nuo įmonės dydžio, vykdomos veiklos ir kitų veiksnių, ne visi kintamieji yra aktualūs ar reikalingi įvertinti įmonės kibernetinį saugumą.

1.2.3. Kibernetinio saugumo reitingo kintamųjų vertinimo metrikos

Žemiau paminėtos kibernetinio saugumo reitingo kintamųjų vertinimo metrikos yra globaliai naudojami standartai arba naudojami populiariausiuose metoduose ar įrankiuose, kurie vertina kibernetinį saugumą arba kibernetines rizikas.

CVSS

Bendra pažeidžiamumo vertinimo sistema (CVSS) suteikia būdą užfiksuoti pagrindines pažeidžiamumo savybes ir suteikia jam skaitinę reikšmę, kuri atspindi jo pažeidžiamumo lygį. Skaitinis balas gali vėliau būti paverstas kokybiniu įvertinimu (pvz., žemas, vidutinis, aukštas), kad organizacijos galėtų tinkamai įvertinti ir nustatyti prioritetus savo pažeidžiamumo valdymo procesams. Bendra pažeidžiamumo vertinimo sistema yra paskelbta kaip standartas, kurį naudoja organizacijos visame pasaulyje. Plačiausiai paplitus versija CVSS2, o naujausia versija yra CVSS3.1.

CVE

Bendrieji pažeidžiamumai ir ekspozicijos (CVE) yra viešai žinomų kibernetinio saugumo pažeidžiamumų bendrų identifikatorių sąrašas. CVE įrašų naudojimas užtikrina pasitikėjimą diskutuojant ar dalinantis informaciją apie programinės ar aparatinės įrangos pažeidžiamumus, suteikia pagrindą įrankių vertinimui ir įgalina automatizuotus duomenų mainus.

CVE ypatybės:

1. Vienas identifikatorius vienam pažeidžiamumui

2. Vienas standartizuotas kiekvieno pažeidžiamumo aprašymas
3. Labiau naudojamas kaip žodynas, o ne duomenų bazė
4. Sąveikos ir geresnio saugumo padengimas
5. Nemokamas viešai atsisiųsti ir naudoti
6. Paslaugų, įrankių ir duomenų bazių vertinimo pagrindas
7. Plačiai naudojamas ir patvirtintas CVE numeracijos tarnybų ir kitų organizacijų, kurios naudoją CVE savo paslaugose ar produktuose.

OVAL

Atvira pažeidžiamumo ir įvertinimo kalba (OVAL) yra tarptautinis informacijos saugumo bendruomenės standartas, skirtas skatinti atvirą ir viešai prieinamą saugos turinį ir standartizuoti šios informacijos perdavimą per visą saugos priemonių ir paslaugų spektrą. Ji taip pat yra nemokama, globaliai naudojama ir viešai prieinama.

Įrankiai ir paslaugos, kurie naudoja OVAL trims sistemos vertinimo etapams – atvaizduojant sistemos informaciją, išreiškiant konkrečias mašinos būsenas ir pranešant vertinimo rezultatus – teikia įmonės tikslią, nuoseklią ir naudingą informaciją, kuri padeda pagerinti įmonėms savo saugumą. Naudojant OVAL taip pat užtikrinama patikima ir atkuriama informacijos užtikrinimo metrika ir užtikrinama saugumo priemonių ir paslaugų sąveika ir automatika.

SCAP

Saugumo turinio automatizavimo protokolas (SCAP) yra metodas, skirtas naudoti specifinius standartus, leidžiančius automatizuoti organizacijoje naudojamų sistemų pažeidžiamumo valdymą, matavimą ir atitikties politikos vertinimą.

Metasploit

„Metasploit“ projektas yra kompiuterio saugos projektas, teikiantis informaciją apie saugos spragas ir pagalbines priemones skverbties tikrinimui ir IDS parašo plėtrai.

Kitos kibernetinio saugumo reitingo kintamųjų vertinimo metrikos yra paprastesnės, subjektyviai pasirenkamos. Tokių metrikų pavyzdžiai: verslo vienetai, verslo išlaidos, kritiškumas, pagrindinis poveikis, padarinių žala.

Paminėtos kibernetinio saugumo vertinimo metrikos pasižymi tuo, kad visą informaciją iš šių metrikų galima paimti automatizuotu būdu. Taip pat, didžioji dalis metrikų vertina pažeidžiamumus, o ne kibernetinį saugumą. Nors nemaža dalis metrikų persidengia, ir vertina tuos pačius pažeidžiamumus ir jų aspektus, yra geras pasirinkimas įmonei ar naudotojui susidaryti nuomonę apie pažeidžiamumą ir kylančias rizikas. Naudojant šių metrikų duomenų bazes galima gauti informaciją apie naujausius pažeidžiamus ir atitinkamai įvertinti įmonės kibernetinį saugumą.

1.2.4. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo problemos analizė

Dinaminis kibernetinio saugumo reitingo nustatymas yra sudėtingas, o kartais pilnai neįmanomas procesas, o jo nebuvimas kelią riziką įmonei. Dinamiškumo elementas gali būti apibrėžiamas taip, kad laikui bėgant, keičiasi sprendimai, atsinaujina sistemos, atsiranda naujų puolimo vektorių, bet įmonė nėra įsivertinusi savo kibernetinio saugumo reitingo iš naujo kai tik nutinka įvykis, kuris daro įtaką kibernetinio saugumo reitingui. Taip atsiranda rizika, kad tuo laiko momentu, kada įmonė nėra

atsinaujinusi savo kibernetinio saugumo reitingo, ji potencialiai yra pažeidžiama ir reitingas yra nekorektiškas.

Kibernetinių įvykių įmonės kasdienėje veikloje nutinka daug ir reikia atpažinti, ar tai įvykis, kuris daro įtaką įmonės kibernetiniam saugumui. Pirmoji problema, su kuria yra susiduriama, kaip surinkti informaciją apie visus kibernetinius įvykius, kurie nutinka įmonės veikloje. Antroji problema – kaip nustatyti, ar nutikęs kibernetinis įvykis daro įtaką įmonės kibernetiniam saugumui. Pavyzdžiui, nutinka įvykis, kai iš darbo išeina ar yra atleidžiamas darbuotojas, kuris turėjo prieigą prie daug vertingos ir jautrios informacijos. Automatizuoti tokį įvykį yra praktiškai neįmanoma ir turi būti atsakingas žmogus, kuris suveda šią informaciją į kibernetinio saugumo vertinimo sistemą. Kitas atvejis, kai yra naudojamas privatus sprendimas ar technologija įmonės viduje ir informacijos apie šias informacines sistemas nėra jokiose viešose duomenų bazėse. Tokiu atveju yra neįmanoma gauti naujausios informacijos apie galimus pažeidžiamumus.

Taigi, dinaminis įmonės kibernetinio saugumo vertinimas yra aktuali problema, neturinti vieningo sprendimo, todėl reikia veiksmingo metodo ar priemonės, kuri užtikrintų dinaminį įmonės kibernetinio saugumo įvertinimą.

1.3. Kibernetinio saugumo vertinimo metodų analizė

Kibernetinis saugumas dažniausiai būna vertinamas kibernetinio saugumo audito metu, tačiau įvairūs auditai ir įmonės naudoja skirtingus kibernetinio saugumo vertinimo metodus ar jų kombinacijas. Įmonės dažnai naudoja kibernetinio saugumo karkasus, kurie yra pritaikyti pagal įmonės poreikius arba yra privatūs, todėl vertinimo metodas turi į tai atsižvelgti ir būti lankstus bei universalus.

Žemiau aprašyti keli populiariausi skirtingi vertinimo metodai.

CSAM [12]

Šis metodas skaičiuoja kibernetinį saugumo vertinimą pagal 17 sričių, kurias įmonė turi atsižvelgti galvojant apie savo kibernetinį saugumą. Kiekviena sritis turi kelias žemesnio lygio sritis ir daug klausimų. Į klausimą galima atsakyti „sutinku“, „iš dalies sutinku“, „nesutinku“. Pagal atsakymus ir atsakytų klausimų kiekį yra nustatomas kiekvienos srities įvertinimas skalėje nuo 0 iki 100. Tada yra paimamas visų sričių įvertinimų vidurkis ir gaunamas galutinis įmonės įvertinimas. Pagal gautą bendrą įvertinimą įmonė yra klasifikuojama į vieną iš keturių grupių:

1. Nesubrendus (0-30 balų).
   Organizacija neketina valdyti savo kibernetinio saugumo. Kritinių kibernetinio saugumo sričių kontrolė neegzistuoja arba yra labai silpna. Organizacija neįgyvendino išsamios kibernetinio saugumo programos.
2. Besivystanti (31-70 balų).
   Organizacija pradeda sutelkti dėmesį į kibernetinio saugumo reikalus. Jei technologijos yra įdiegtos, organizacija turi sutelkti dėmesį į pagrindines kibernetinio turto apsaugos sritis. Dėmesys turi būti sutelktas į personalą, procesus, kontrolę ir reglamentus.
3. Subrendus (71-90 balų).
   Nors organizacija turi brandžią aplinką, reikia patobulinti pagrindines sritis, kurios buvo nustatytos su trūkumais.
4. Pažangi (91-100 balų).

Organizacija puikiai įgyvendino geriausią kibernetinio saugumo praktiką. Visada yra kur tobulėti. Nuolat peržiūrėti kibernetinio saugumo procesus atlikdami auditus.

Šio metodo įvertinimų lentelės pavyzdys (1 pav.). Metodas gali būti dalinai automatizuojamas, yra lengvai suprantamas ir gali būti atliekamas įprasto IT darbuotojo, neprireikiant išskirtinių žinių ar gebėjimų.

Cybersecurity Audit Model (CSAM)						
No.	Domain	Ratings				Score
		I	D	M	A	
2	Governance and Strategy	☐	☒	☐	☐	35%
3	Legal and Compliance	☐	☐	☒	☐	90%
4	Cyber Assets	☒	☐	☐	☐	30%
5	Cyber Risks	☐	☒	☐	☐	60%
6	Frameworks and Regulations	☒	☐	☐	☐	30%
7	Architecture and Networks	☐	☒	☐	☐	67%
8	Information, Systems and Apps.	☐	☒	☐	☐	55%
9	Vulnerability Identification	☒	☐	☐	☐	30%
10	Threat Intelligence	☐	☒	☐	☐	60%
11	Incident Management	☒	☐	☐	☐	10%
12	Digital Forensics	☒	☐	☐	☐	30%
13	Awareness Education	☐	☒	☐	☐	60%
14	Cyber Insurance	☐	☐	☒	☐	90%
15	Active Cyber Defense	☒	☐	☐	☐	5%
16	Evolving Technologies	☐	☐	☐	☒	100%
17	Disaster Recovery	☒	☐	☐	☐	30%
18	Personnel	☐	☐	☒	☐	77%
Final Cybersecurity Maturity Rating		☐	☒	☐	☐	**51%**

1 pav. Galutinio kibernetinio saugumo įvertinimo lentelė

[1] Kiekybinė CVSS pagrįsta kibernetinio saugumo rizikos vertinimo metodika IT sistemoms

Metodas remiasi kiekybiniu CVSS vertinimo metodu. Naudojamas į turtą ir pažeidžiamumus orientuotas analizės metodas. Atlikus analizę, atliekamas rizikos įvertinimo procesas, kuris susideda iš šių žingsnių:

1. Nustatyti grėsmės šaltinius.
2. Nustatyti pažeidžiamumus.
3. Nustatyti jų atsiradimo tikimybę.
4. Nustatyti poveikio dydį.
5. Nustatyti galutinę riziką.

Pirmam ir antram žingsniams yra naudojami įvairūs duomenų skenavimo ir surinkimo įrankiai. O 3-5 žingsniuose skaičiavimus atlieka žmogus pagal duotą CVSS vertinimo metriką. Šis metodas gali būti dalinai automatizuojamas, tačiau įvertinti grėsmių atsiradimo tikimybes ir poveikio dydžius reikia išsamios duomenų bazės, kuri galėtų realiu metu duoti informaciją apie naujausius pažeidžiamumus.

[2] Interviu grįstas kibernetinio saugumo vertinimas

Šis metodas dažniausiai naudojamas kibernetinio saugumo auditorių ir turi bendrų bruožų su pirmuoju metodu. Naudojant šį metodą auditorius ar kitas žmogus, kuris turi sukaupęs didelę patirtį kibernetinio saugumo srityje ir yra šios srities ekspertas daro interviu su įmonės atstovu kibernetiniam saugumui. Interviu metu praeinama po pagrindines sritis ir prie kiekvienos srities yra užduodama nuo keliolikos iki kelių šimtų klausimų. Dažniausiai kiekviena didžioji sritis yra apkalbama per skirtingus interviu. Sričių pavyzdžiai gali keistis priklausomai nuo įmonės dydžio, veiklos ir kitų veiksnių. Kibernetinio saugumo rizikos įvertinimo interviu pavyzdys (2 pav.).

Level	Questions	Time	Unit
Business information	16	1 hour	Service
Process/people	300	3 hours	Process
Applications	250	3 hours	Application
Software components	200	2 hours	Type of asset
Infrastructure	200	2 hours	Type of asset
Facilities	100	1 hours	Facility

2 pav. Kibernetinio saugumo rizikos įvertinimo interviu pavyzdys

Po interviu auditorius ar kibernetinio saugumo ekspertas padeda atpažinti didžiausią riziką turinčias vietas ir ką reikėtų patobulinti, subjektyviai įvertina įmonės kibernetinio saugumo lygį. Procesas užtrunka ilgai ir yra gan subjektyvus, labai remiasi auditoriaus kibernetinio saugumo išmanymo lygiu.

Kibernetinio saugumo rizikos valdymo požiūris iš žaidimų teorinės pusės

Kibernetinio saugumo žaidimas (CSG) – tai metodas, įdiegtas programinėje įrangoje, kuris kiekybiškai nustato kibernetinio saugumo riziką ir naudoja šią metriką, kad nustatytų optimalų saugumo metodų pritaikymą bet kuriam investicijų lygiui. Rizikos balas apskaičiuojamas naudojant misijos poveikio modelį kibernetinių incidentų pasekmėms apskaičiuoti ir derinant tai su tikimybe, kad atakos bus sėkmingos. Išpuolių sėkmės tikimybė apskaičiuojama taikant grėsmės modelį sistemos topologijos modeliui ir gynėjo modeliui. Kibernetinio saugumo žaidime atsižvelgiama į plačiai paplitusias kibernetinių sistemų tarpusavio sąsajas, kai gynėjai turi apginti visus kelių pakopų atakos kelius, o užpuolikui reikia tik vieno, kad pavyktų. Jame naudojamas žaidimų teorinis sprendimas, naudojant žaidimo formuluotę, kuri nustato gynybos strategijas, kad sumažintų maksimalią kibernetinę riziką. Šis modelis pasižymi tuo, kad yra skirtas įvertinti kibernetinio saugumo riziką atskiriems ir smulkesniems įmonės komponentams, tačiau gali būti pilnai automatizuojamas.

Apžvelgus kibernetinio saugumo vertinimo metodus, pastebėta, kad jie gali būti skirstomi į dvi grupes – vieni metodai vertina įmonės kibernetinį saugumą, o kiti vertina įmonės kibernetinio saugumo pažeidžiamumą ir rizikas. Viename aukštas balas reiškia saugią įmonės kibernetinę aplinką, kitame reiškia, kad ta aplinka gali turėti daug pažeidžiamumų ir yra rizikinga. Daugelis metodų pajėgia

automatizuoti tik atskiras įmonės kibernetinio saugumo vertinimo dalis ir negali įvertinti visos įmonės bendro kibernetinio saugumo.

1.4. Dinaminio įmonės kibernetinio saugumo reitingo nauda

Saugumo reitingai leidžia įmonėms nuolat stebėti savo kibernetinę ekosistemą, nereikalaujant savęs apsunkinti brangiais ir daug laiko reikalaujančiais saugumo metodais. Geras saugumo įvertinimas yra organizacinis turtas, kuris gali atverti verslo galimybes ir partnerystes. Prasti saugumo reitingai rodo, kad organizacijos duomenims gresia pavojus, pabrėžiant kritines saugumo spragas. Kaip kredito reitingai suteikia įžvalgų apie organizacijos finansinį stabilumą, kibernetinio saugumo reitingai suteikia įžvalgų apie kibernetinio saugumo būklę ir organizacijos praktiką. Dėl šios priežasties saugos reitingų naudojimas turi daug pranašumų įmonių organizacijoms.

Toliau pateikiami trys saugumo reitingo naudos įmonėse elementai:

Nuolatinis kibernetinio saugumo stebėjimas

Saugumo reitingas suteikia organizacijoms vidinį vaizdą apie jų IT infrastruktūrą, leidžiant jiems nuolat stebėti savo saugumo padėtį. Tai reiškia efektyvesnį grėsmių nustatymą ir šalinimą, supaprastinant rizikos valdymo procesus. Turėdamos saugumo reitingus, įmonės gali būti labiau užtikrintos kovojant su vis atsirandančia kibernetine rizika.

Sprendimų priėmimo patobulinimas

Išsamiai apžvelgdamos savo kibernetinę sveikatą, organizacijos gali priimti labiau pagrįstus sprendimus dėl savo kibernetinio saugumo. Saugumo reitingas taip pat naudingas versle, kai reikia atlikti tinkamą kibernetinio saugumo patikrinimą ir perduoti šiuos duomenimis verslo partneriams ar įmonės viduje. Galiausiai, saugumo reitingai leidžia priimti duomenimis pagrįstus verslo ar IT sprendimus.

Geriau valdoma trečiųjų šalių rizika

Kadangi vis daugiau organizacijų remiasi trečiosiomis šalimis versle, atsiranda vis didesnė rizika informacijos saugumui bei didesnis poreikis šios rizikos valdymui. Saugumo reitingas padeda įmonėms nustatyti kibernetinio saugumo riziką jų tiekėjų ekosistemoje ir sudaryti trečiųjų šalių rizikos portfelius. Veiksmingai valdydama trečiąsias šalis, įmonė gali greitai nustatyti ir spręsti susijusias problemas bei rizikas.

Dinaminio įmonės kibernetinio saugumo reitingas suteikia organizacijoms galimybę nuolat stebėti savo kibernetinio saugumo ekosistemą, efektyviau nustatyti ir šalinti grėsmes bei priimti duomenimis pagrįstus verslo sprendimus.

1.5. Esamų kibernetinio saugumo reitingo nustatymo priemonių analizė

Atlikus rinkos analizę pastebėta, kad nėra visiškai automatizuotų įrankių, kurie nustato įmonės kibernetinio saugumą reitingą. Yra tik tokie įrankiai, kurie padeda surinkti informaciją iš informacinių sistemų ir įvertinti rizikas iš prieš tai paminėtų metrikų duomenų bazių.

Remiantis [11] šaltiniu, buvo pasirinkti 9 gan populiarūs kibernetinio saugumo duomenų surinkimo ir kibernetinių rizikų vertinimo įrankiai. Šios priemonės buvo analizuojamos remiantis šiais

kriterijais, kurie remiantis šaltiniu [11] buvo svarbiausi tokio tipo įrankių palyginimui: kibernetinio saugumo metrika, standartai ir palaikomos rizikos strategijos. Įrankių palyginimo lentelė (1 lentelė).

1 lentelė. Kibernetinio saugumo duomenų surinkimo ir rizikų vertinimo įrankių palyginimas

Įrankiai	Metrika	Rizikos įvertinimo strategija
Nessus Home	CVSS2, CVSS3	Rezultatai, pagrįsti pažeidžiamumas (pvz., žemas, vidutinis, didelis, kritinis)
Saint8	Verslo vienetas, kritiškumas, Verslo išlaidos, CVSS	Prioritetų nustatymas ir išteklių naudojimas - turtas, pagrįstas svarbia metrika organizacijai
EyeRetina	Poveikis verslui, pagrindinis poveikis, Metasploit, Exploit-db, CVSS	Reali rizika kritiniam turtui ir panaudojimas
GFILanguard	OVAL, CVE	Saugumo problemos vertinamos pagal jų sunkumo lygį ir kiekvienam kompiuteriui yra suteikiama rizika ir pažeidžiamumo įvertinimas.
nCircle® IP360	CVE, CVSS, OVAL, SCAP	Pirmenybę teikia pažeidžiamumui, valdo riziką ir pagerina saugumo efektyvumą derinant verslo kontekstas su pažeidžiamumo žvalgyba.
Security System Analyzer	CVE, CVSS, OVAL, SCAP	-
OpenVAs	OVAL	Pažeidžiamumo rezultatai buvo prioritetiniai pagal poveikį sistemoms.
QualysGuard	CVSS, CVE, SCAP, Padarinių žala	Rizika pagrįstas požiūris į prioritetų nustatymą, pastangų skyrimas ištaisyti pažeidžiamumus, kurie turėtų įtakos verslui.
Nexpose	CVE, CVSS, SCAP	Reali rizika, laikina pridėtinė, laikina pasverta, PCI ASV 2.0

Nors dauguma įrankių naudoja CVSS metriką prioritetams nustatyti ir rizikai valdyti, kai kurie iš jų įtraukia ir kitą įmonei svarbią metriką. Pavyzdžiui, „Saint8“ apima verslo vieneto, kritiškumo ir verslo išlaidų metrikas, siekiant sužinoti pažeidžiamumo poveikį verslui. „EyeRetina“ naudoja verslo poveikio, pagrindinio poveikio, „Metasploit“ ir „Exploit-db“ kaip kitą metriką rizikai įvertinti, o „QualysGuard“ naudoja padarinių žalą remiantis CVSS balu. Galima pabrėžti, kad kai kurios priemonės nustato savo rizikos vertinimo strategiją palaikyti sprendimų priėmimą. Tarp jų yra „nCircle® IP360“, kuris sujungia verslo kontekstą su pažeidžiamumų žvalgyba, „Saint8“, kuris

susieja ne tik bazinę, bet ir aplinkos metriką realiai rizikai įvertinti ir „Nexpose“, kuris apima įvairias rizikos strategijas, pritaikytas verslo poreikiams.

1.6. Galimų problemos sprendimo metodų nagrinėjimas

Atlikus kibernetinio saugumo metodų, priemonių ir reitingo analizę yra pastebėta eilė problemų, kurių esami sprendimai ar priemonės neišsprendžia, todėl reikia kurti naują metodą, kuris išspręstų atrastas problemas. Taigi, šiame skyrelyje bus aprašytos savybės, kuriomis turėtų pasižymėti naujas metodas ar šio metodo sistemos prototipas ir procesai, kuriuos įmonė turėtų įgyvendinti.

Visų pirmiausia, surinkti visą įmonės kibernetinių įvykių informaciją vien automatizuotu būdu nėra įmanoma naudojantis esamais įrankiais. Vienas iš sprendimų būdų yra sukurti sistemos programavimo sąsaja (API), kuria galėtų pasinaudoti įmonės pačios paduodančios reikalingą informaciją. Kitas būdas būtų sukurti naudotojo sąsają, kurioje atsakingas įmonės darbuotojas rankiniu būdu įvestų reikalingą informaciją. Dalį kibernetinio saugumo informacijos taip pat galima surinkti ir naudojant jau paminėtus įrankius.

Tarp analizės metu identifikuotų problemų buvo ir privačios, įmonės poreikiams pritaikytos vidinės sistemos. Kad būtų galima pilnai įvertinti tokio tipo įmonės dinaminį kibernetinį saugumą, reikia pilno įmonės įsitraukimo į procesus, kurie turi būti sukurti, norint korektiškai įvertinti dinaminį įmonės kibernetinį saugumą. Tokiu atveju naujojo metodo sistema turėtų būti vystoma ne tik įmonės išorėje bet ir viduje. Dinaminis įmonės kibernetinis saugumo įvertinimas nereiškia realiu laiko momentu atlikto įvertinimo, o labiau automatizuoto įvertinimo, kurio efektyvumas priklauso nuo laiko tarpo, per kurį įvyksta įvertinimas. Taigi, įmonė turėtų sudaryti procesus, kurie būtų atsakingi už informacijos pateikimą naujojo dinaminio kibernetinio saugumo reitingo įvertinimo metodo programinei realizacijai. Šitaip būtų užtikrintas įmonės kibernetinio saugumo reitingo dinamiškumo elementas.

Naujasis dinaminio įmones kibernetinio saugumo reitingo įvertinimo metodas turėtų nuolat atnaujinti savo duomenis apie sistemos pažeidžiamumus ir rizikas naudojantis viešomis metrikų duomenų bazėmis. Tiksliausiam įmonės kibernetinio saugumo reitingui nustatyti, reikia atsižvelgti ne į vieną, bet į daugelį patvirtintų metrikų ir jų įvertinimų. Taip bus užtikrintas nešališkas kibernetinio saugumo reitingo vertinimas. Ši dalis gali būti pilnai automatizuota. Sistema, prie pradedant naudoti, turėtų būti sukaupus išsamų kintamųjų aprašymą. Jį galima sukaupti padarius pirmą pilną įmonės kibernetinio saugumo auditą ir įvesti gautą informaciją į sistemą. Taip pat, įmonės kibernetinio saugumo reitingas turėtų atsižvelgti į pažeidžiamumų rizikos analizę skaičiuojant galutinį reitingą.

Naujasis metodo sistemos prototipas turėtų būti universalus ir lankstus, kad jį galėtų naudoti įvairaus dydžio įmonės ir galėtų būti pritaikytas pagal įmonės investicijas. Taip pat, šis prototipas turėtų būti kiek įmanoma daugiau automatizuotas su kuo mažesniu žmogiškuoju faktoriumi. Reikalui esant, realizuojant šį metodą būtų įmanoma sukurti nutolusią kibernetinio saugumo duomenų apdorojimo sistemą, kuri pasitelkus mašininį mokymą galėtų tobulinti pati save ir taip suteikti daugiau informacijos vertinant dinaminį įmonės kibernetinio saugumo reitingą.

Taigi, sukūrus kibernetinio saugumo vertinimo sistemą, kuri pasižymėtų minėtomis savybėmis, ir būtų naudojama įmonės aplinkoje, kuri turi sukūrus atitinkamus procesus, užtikrinančius sistemos dinamiškumo elementą ir veikimo korektiškumą, galima paskaičiuoti dinaminį įmonės kibernetinio saugumą reitingą.

1.7. Išvados

1. Atlikus kibernetinio saugumo vertinimo metodų analizę, buvo pastebėta, jog nei vienas metodas nėra pilnai automatizuotas ir dažnai nėra pakankamai lankstus, kad jį galėtų įgyvendinti įvairaus dydžio įmonės.
2. Atlikus dinaminio įmonės kibernetinio saugumo reitingo analizę, buvo išskirta 17 pagrindinių kintamųjų, kurie turėtų būti vertinami bei 5 vienos populiariausių metrikų, kurios gali būti pilnai automatizuojamos ir turi išsamius vertinimo kriterijus bei aprašus. Taip pat buvo nustatytos dinamiškumo problemos, su kuriomis susiduria esami metodai.
3. Atlikus esamų kibernetinių saugumo reitingo nustatymo priemonių analizę, buvo nustatyta, jog nėra įrankio, kuris automatiškai įvertintų įmonės bendrą kibernetinio saugumo reitingą. Yra tik tokios priemonės, kurios sugeba surinkti įmonės kibernetinio saugumo duomenis ir įvykdyti rizikų analizę.
4. Išnagrinėjus galimus problemos sprendimo metodus buvo nuspręsta, kad reikia sukurti naują metodą, kuris išspręstų minėtas problemas, būtų dinamiškas ir galėtų paskaičiuoti įmonės kibernetinio saugumo reitingą. Taip pat nuspręsta realizuoti jo prototipą, kad būtų galima įvertinti gautus rezultatus.

2. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas ir sistema

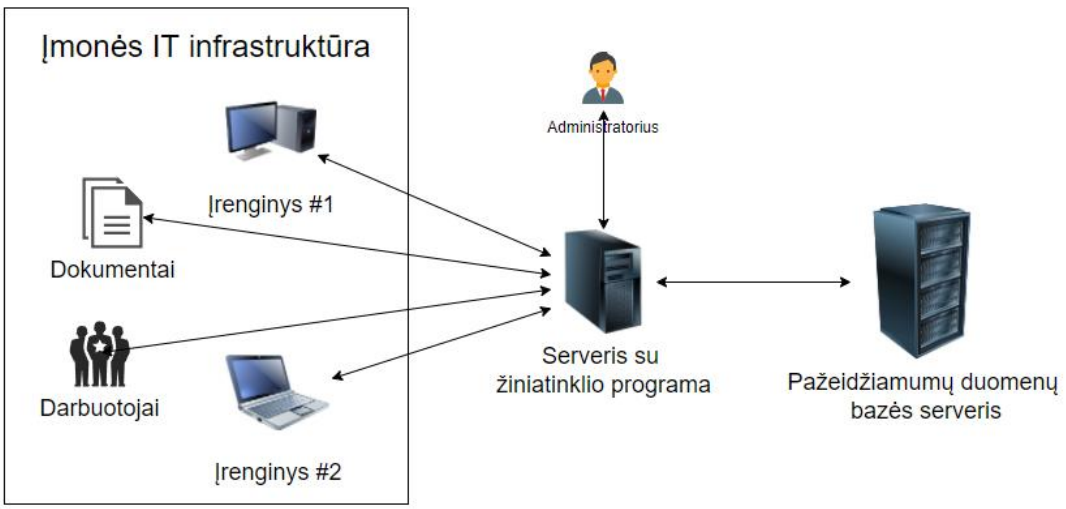
Atlikus probleminės srities analizę pastebėta, kad tiriamieji įrankiai ar metodai nėra pakankamai lankstūs ir automatizuoti bei nėra dinamiški. Taip pat dauguma įrankių įvertina vienetines kibernetinio saugumo sritis arba įvertina tik egzistuojančias rizikas, todėl atsižvelgiant į šiuos trūkumus yra kuriama sistema, kuri naudos dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodą. Šiame skyriuje bus aprašomas kuriamas metodas ir sistema.

2.1. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo veikimo konceptas

Šiame skyrelyje yra aprašyta ir detaliai paaiškinta kaip veiks dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas projektuojamoje sistemoje.

2.1.1. Sistemos veikimo koncepto schema

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos veikimas susideda iš kelių pagrindinių etapų – duomenų surinkimo ir reitingo įvertinimo. Duomenys bus saugomi serveryje, kuriame yra patalpinta žiniatinklio programa ir duomenų bazė. Įmonės įrenginiuose bus įrašyta programinė įranga – agentas, kuris periodiškai ir dinamiškai sugebės siųsti informaciją apie įrenginį tiesiai į serverį ir taip bus renkama informacija automatiniu būdu. Taip pat, informaciją bus galima įvesti ir rankiniu būdu, ką darys sistemos administratoriai, surenkami informaciją ne tik apie įmonės įrenginius, bet ir apie naudojamas politikas ir praktikas įmonėje, informaciją apie darbuotojų išsilavinimą ir turimus sertifikatus. Toks duomenų rinkimas suteikia didelį lankstumą įmonei ir sugebėjimą didžiąją dalį informacijos rinkimo automatizuoti, išlaikomas dinamiškumo aspektas. Visa komunikacija tarp įrenginių yra šifruota ir apsaugota. Serveryje esanti žiniatinklio programa gavusi informaciją, ją apdoroja ir tikrina su naujausia informacija iš nutolusios pažeidžiamumų duomenų bazės. Reitingas yra nuolatos perskaičiuojamas ir rezultate yra gaunama sistema, kuri gali įvertinti pasikeitusį įmonės kibernetinio saugumo reitingą pasikeitus vos vienam reitingo kintamajam ir nereikia daryti papildomų auditų, kurie viską vertintų iš naujo ir sugaištų daug įmonės resursų. Ši sistema suteiks galimybę gauti realų įmonės kibernetinio saugumo reitingą periodiškai ir dinamiškai, o ne tik tada, kada yra gaunami reitingai būtent tai laiko žymei, kada yra daromas auditas. Sistemos veikimo koncepto schema pavaizduota 3 pav.



3 pav. Sistemoje esančių įrenginių pavyzdys

2.1.2. Reitingo skaičiavime naudojamos informacijos surinkimas

Visų pirma, surinkta informacija keliaus į serverį, kuriame vyks informacijos apdorojimo ir reitingo įvertinimo procedūros. Duomenys bus surenkami keliais būdais. Būdai skirstomi į automatinius ir rankinius.

Automatiniai informacijos surinkimo metodai pasinaudotų programine įranga – agentu, kuris būtų sudiegtas į kiekvieną įmonėje naudojamą įrenginį. Ši programinė įranga automatiškai periodiškai siunčia informaciją apie tą įrenginį. Agento programinė įranga yra sukurta naudojantis .NET programine kalba ir susijusiomis bibliotekomis. Taip pat būtų pasinaudota tinklo veiklos stebėsena žinant visus įmonės naudojamus interneto adresus. Tinklo stebėsenai būtų galima panaudoti nmap programą. Tinklo veiklos stebėsenos žurnalas būtų tinkamas pavyzdys kaip būtų galima pasyviai perduoti informaciją į serverį. Reikalui esant, sistema pati galėtų bandyti padaryti užklausą į kompiuterį dėl reikiamos informacijos.

Rankiniai informacijos surinkimo metodai turėti padengti tas vietas, kurių negalima automatizuoti. Tai būtų įmonės naudojamos programinė įranga ir jos konfigūracijos, kurių negalima gauti automatiniu būdu, informacijos saugos politikos praktikos ir procedūros, kiti dokumentai, informacija apie darbuotojų išsilavinimą ir turimus sertifikatus ir kita informacija, kuri gali daryti įtakos kibernetinio saugumo reitingo skaičiavimui. Pavyzdžiui, įmonės slaptažodžių politika, darbinių kompiuterių išsinešimas iš darbo patalpų ir t.t. Rankiniu būdu informaciją bus galima įvesti tiesiai į reitingo įvertinimo sistemą, kur priėjimą turės sistemos administratorius.

Tarp informacijos surinkimo patenka ne tik įmonės darbuotojų ar įrenginių informacija. Informacija apie naujausius kibernetinio saugumo pažeidžiamumus bei jų įvertinimus iš nutolusios duomenų bazės taip pat bus surenkama automatiškai.

2.1.3. Dinamiškumo realizavimas sistemoje

Dinamiškumas yra vienas svarbiausių šio metodo bruožų, kuris leidžia kuriamam prototipui išsiskirti nuo kitų alternatyvų. Šiame prototipe planuojama padaryti automatinį informacijos surinkimą pagal tvarkaraštį ir pagal įvykį.

Informacijos surinkimas pagal tvarkaraštį yra plačiai naudojamas smulkaus ir vidutinio dydžio programose. Šio metodo implementacija dažniausiai remiasi procesu, kuris tikrina laiką ir atlieka atitinkamas užduotis pagal iš anksto sudarytą tvarkaraštį. Šiame prototipe tai bus realizuota šiek tiek kitaip, kad būtų suteikiama daugiau lankstumo, bet vis tiek išlaikant metodo esmę. Pagrindiniame serveryje bus API prieigos taškas, į kurį kreipiantis, individualus įrenginys paduos savo įrenginio identifikacinį kodą ir gaus instrukcijas, ką reikia daryti – šiuo atveju – siųsti įrenginio informaciją. Poreikiui esant, šioje vietoje galima pridėti papildomų funkcijų į tvarkaraštį ir patobulinti sistemą pagal savo poreikius. Dažniausiai šis metodas susiduria su problemomis, kai informacija yra nustojama padavinėti reguliariai, tačiau kuriamas prototipas neturės šios problemos, nes informacijai nustojus padavinėti, pavyzdžiui tokiais atvejais kai įrenginys yra išjungtas, sistema vis tiek galės paskaičiuoti kibernetinio saugumo reitingą su paskutiniais gautais įrenginio duomenimis.

Kitas metodas yra surinkti informaciją pagal įvykį. Tai yra sudėtingesnis, plačiai naudojamas didesnėse programose metodas. Šio metodo implementacija dažniausiai remiasi procesu, kuris nuolatos laukia kokio nors iš anksto aprašyto įvykio ir tai atsitikus įvykdo aprašytą logiką. Šiame

prototipe bus naudojamas įrenginio įjungimo įvykis ir ant šio įvykio bus siunčiama įrenginio informaciją į pagrindinį serverį. Poreikiui esant, galima patobulinti šio prototipo vietą ir aprašyti daugiau įvykių, į kuriuos agento programa galėtų reaguoti.

Toks prototipo realizavimas pasinaudojus automatiniu informacijos surinkimu pagal tvarkaraštį ir pagal įvyki leis sukurti stiprų dinamiškumo lygį sistemoje, kuris suteiks daug lankstumo pritaikyti sistemą pagal savo poreikius.

2.2. Sistemos funkciniai reikalavimai

Šiame skyrelyje yra aprašytos pagrindinės sistemos funkcijos, pavaizduota panaudojimų atvejų diagrama ir esminių sistemos panaudos atvejų veiklos diagramos.

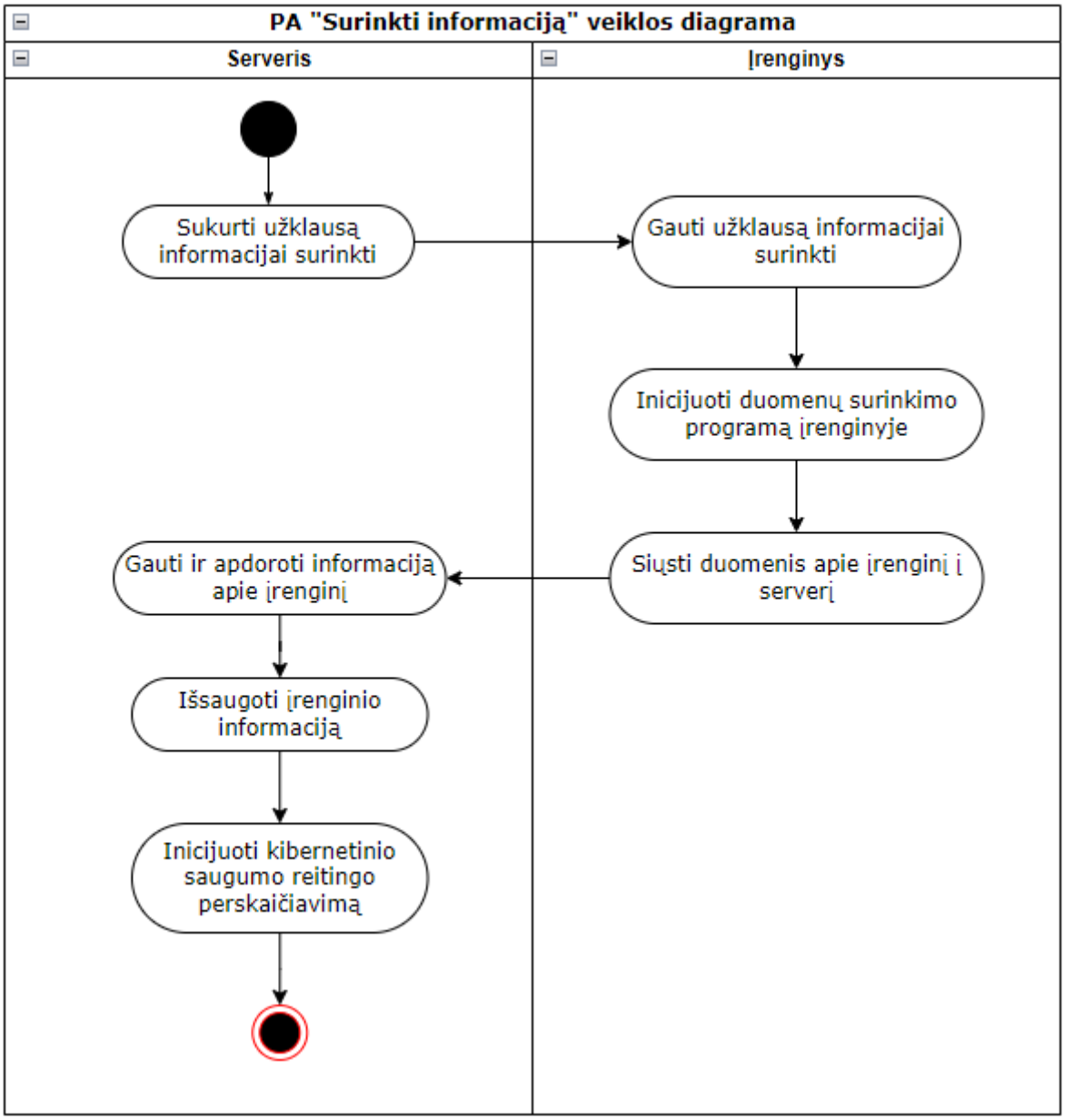
2.2.1. Sistemos panaudojimo atvejų diagrama

Sistemos aktorius sudaro IT darbuotojas ir pati sistema. IT darbuotojas gali valdyti kategorijas, kriterijus bei konfigūracijas. Valdymas reiškia, kad aktorius gali atlikti visus CRUD veiksmus. Sistema gali skaičiuoti kibernetinio saugumo reitingą, tikrinti pažeidžiamumus nutolusioje duomenų bazėje, surinkti informaciją ir atvaizduoti informaciją apie reitingą ir jo skaičiavimą. Sistemos funkcinių reikalavimų schema pavaizduota 4 pav.

4 pav. Dinaminio įmonės kibernetinio saugumo reitingo skaičiavimo sistemos panaudojimo atvejų diagrama

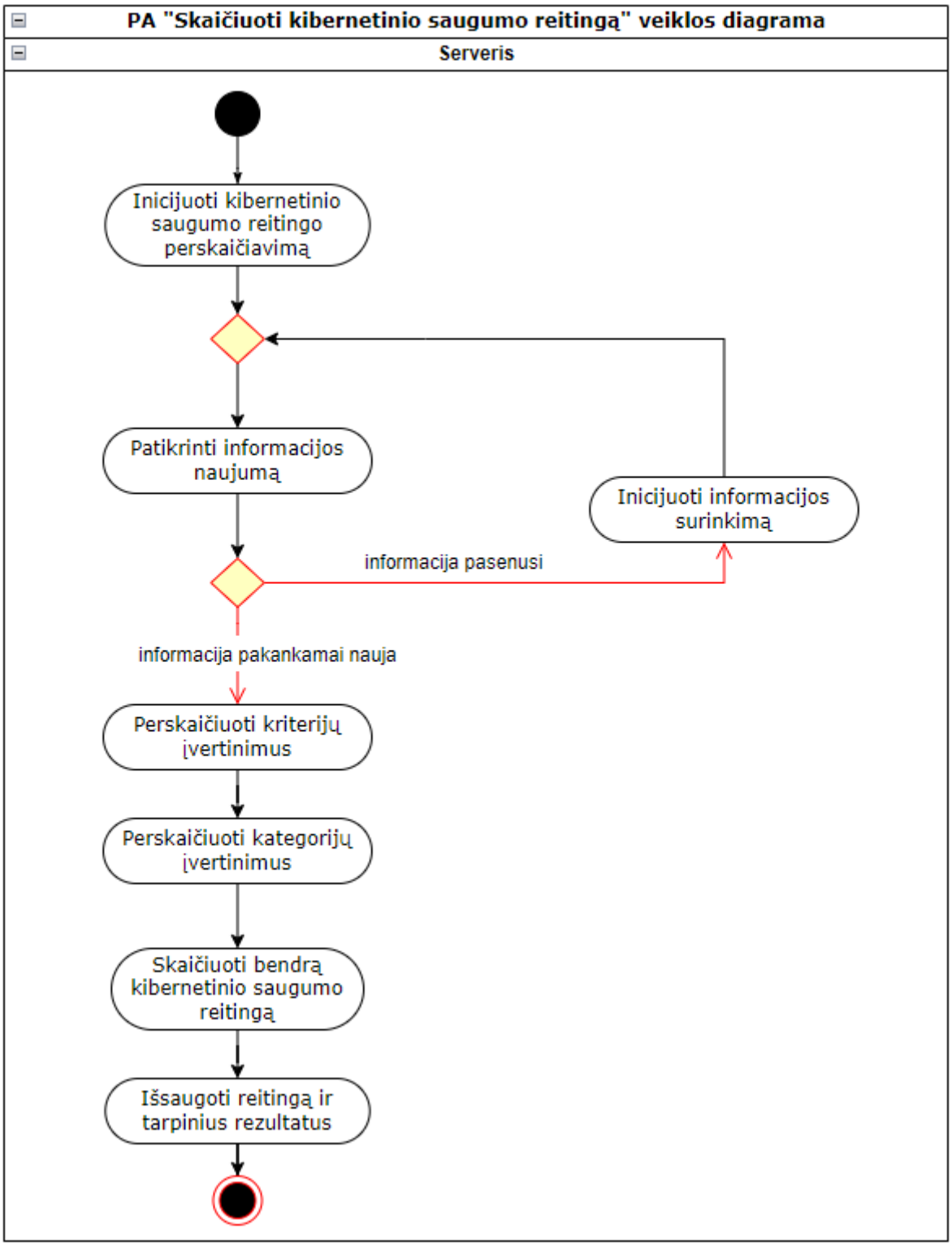
2.2.2. Pagrindinių panaudos atvejų veiklų diagramos

Panaudojimo atvejo „Surinkti informaciją“ veiklos diagrama pavaizduota 5 pav.



5 pav. PA „Surinkti informaciją“ veiklos diagrama

Panaudojimo atvejo „Skaičiuoti kibernetinio saugumo reitingą“ veiklos diagrama pavaizduota 6 pav.



6 pav. PA „Skaičiuoti kibernetinio saugumo reitingą“ veiklos diagrama

2.3. Reitingo nustatymas

Reitingo nustatymui bus naudojamas kiekybinis svorinis metodas. Metodo tikslas yra įvertinti įmonės kibernetinį saugumą tiksliai, dinamiškai ir suteikti lankstumo.

2.3.1. Reitingo formatas

Reitingas bus matuojamas skalėje nuo 0 iki 10, o po kablelio bus daugiausiai 2 skaitmenys. Tokia vertinimo skalė parinkta dėl vientisumo priežasčių, nes dauguma pažeidžiamumų duomenų bazių pažeidžiamumus vertina dešimtbalėje sistemoje. Tokią skalę yra lengva suprasti, o jos didinimas ar mažinimas nesuteiktų papildomo tikslumo arba jį net sumažina. Metodas vertins įmonės kibernetinį saugumą, bet ne riziką. Tai reiškia, kad aukštas balas atitinka aukšto lygio įmonės kibernetinį saugumą, o žemas balas atitinka stipriai pažeidžiamą įmonės kibernetinį saugumą. Kad būtų galima geriau suprasti gautą rezultatą, reitingą reikėtų interpretuoti pagal analizėje nagrinėtą CSAM kibernetinio saugumo įmonėje vertinimo metodologiją. Vadovaujantis šia metodologija, įmonė yra priskiriama vienai iš šių grupių pagal gautą reitingą:

1. Nesubrendus (0.00 – 3.00 balai)

Įmonė neketina valdyti savo kibernetinio saugumo. Kritinių kibernetinio saugumo sričių kontrolė neegzistuoja arba yra labai silpna. Įmonė neįgyvendino išsamios kibernetinio saugumo programos.

2. Besivystanti (3.01 – 7.00 balai)

Įmonė pradeda sutelkti dėmesį į kibernetinio saugumo reikalus. Jei technologijos yra įdiegtos, įmonė turi sutelkti dėmesį į pagrindines kibernetinio turto apsaugos sritis. Dėmesys turi būti sutelktas į personalą, procesus, kontrolę ir reglamentus.

3. Subrendus (7.01 – 9.00 balai)

Nors įmonė turi brandžią aplinką, reikia patobulinti pagrindines sritis, kurios buvo nustatytos su trūkumais.

4. Pažangi (9.01 – 10.00 balų)

Įmonė puikiai įgyvendino geriausią kibernetinio saugumo praktiką. Visada yra kur tobulėti. Nuolat peržiūrėti kibernetinio saugumo procesus atlikdami auditus.

2.3.2. Reitingo kintamieji

Prieš pradedant naudotis sistema yra nustatomos įmonei aktualios kategorijos ir kriterijai arba kitaip tariant kintamieji, kurie bus vertinami. Jų kiekis priklauso nuo įmonės dydžio ir kibernetinio saugumo brandumo. Metodo standartiniame plane bus naudojami tik pagrindiniai kintamieji, į kuriuos turėtų būti atsižvelgiama, jeigu įmonė susiduria su informacinėmis technologijomis. Įmonė naudodama šią sistemą turi kriterijus nusistatyti pagal save, priklausomai nuo savo poreikių ir jeigu įmonės viduje nėra kibernetinio saugumo eksperto, rekomenduojama pasidaryti kibernetinio saugumo auditą, pagal kurį būtų galima nesudėtingai sukonfigūruoti sistemą. Taip pat, visa informacija apie kintamuosius gali būti įvesta rankiniu būdu, o automatiniu būdu galima surinkti informaciją iš įmonės infrastruktūros – apie sistemas, įrenginius, tinklą ir kitą trečios šalies programinę įrangą. Automatiniui surinkimui reikalinga įdiegta programinė įranga – agentas, kiekviename įrenginyje.

Pagrindinės kategorijos su kriterijais numatytoje konfigūracijoje:

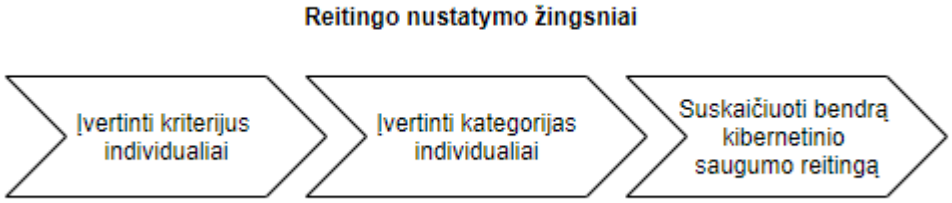
1. Įrenginių sauga
    1.1. Operacinės sistemos sauga
    1.2. Ugniasienė ir įrenginio tinklo apsauga
    1.3. Aparatinės įrangos sauga
2. Tinklo sauga
    2.1. DNS konfigūracija

2.2. IP reputacija
2.3. IP įtraukimas į baltuosius/juoduosius sąrašus
2.4. Ugniasienė
2.5. Nuotolinė prieiga
2.6. Prieigos kontrolė
3. Darbuotojai
3.1. Mobilių įrenginių naudojimas
3.2. Pakankamai prieinami IT resursai
3.3. Darbuotojų kvalifikacija
3.4. Reguliariai atliekami darbo su duomenimis mokymai
4. Sertifikatai ir atitiktis
4.1. SOC 2 parengtis
4.2. PCI DSS atitiktis
4.3. CMMC atitiktis
4.4. HITRUST sertifikatas
4.5. GDPR atitiktis
4.6. CCPA parengtis
4.7. ISO 27001 sertifikatas
5. Politika ir procedūros
5.1. Informacijos saugos politika
1.1. Duomenų dalinimosi politika
1.2. Mobilių įrenginių naudojimosi politika
1.3. IT operacijų ir administravimo politika
1.4. Asmeninių ir mobilių įrenginių politika
1.5. Nuotolinės prieigos politika
1.6. SaaS ir debesų kompiuterijos politika
1.7. Incidentų reagavimo politika (IRP)
1.8. El. pašto naudojimo ir komunikacijos politika
1.9. Tapatybės prieigos ir valdymo politika
1.10. Atkūrimo po nelaimių politika
1.11. Duomenų klasifikavimo politika
2. Fizinė apsauga
2.1. Uždaros grandinės stebėjimo kameros
2.2. Judesio ir (arba) šiluminės signalizacijos sistemos
2.3. Apsaugos darbuotojai
2.4. ID su darbuotojų nuotraukomis
2.5. Prieiga naudojant biometrinius duomenis

Jeigu yra galimybė informaciją surinkti automatiniu būdu, tie kriterijai po savimi turi faktorius – dar žemesnę „subkategoriją“, kuri leidžia konfigūruoti automatiniu būdu surenkamą informaciją ir lanksčiau valdyti pasirinkto kriterijus apsaugos įvertinimą.

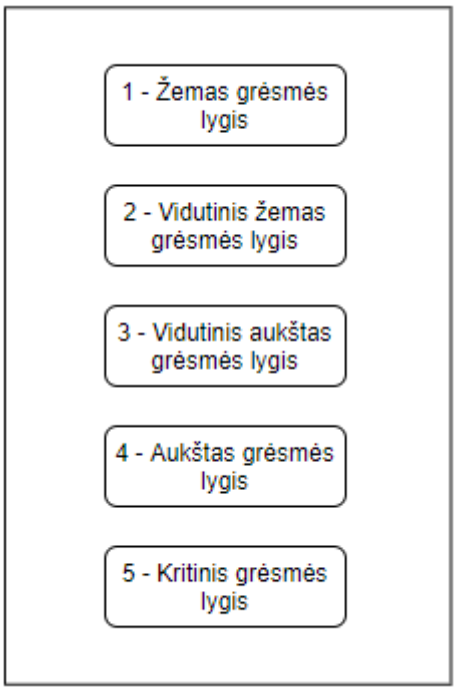
2.3.3. Reitingo skaičiavimas

Reitingas yra suskaičiuojamas per tris žingsnius (7 pav.).



7 pav. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo žingsniai

Formulėse naudojamas z indeksas yra naudojamas kaip svoris, kuris leidžia vienus kriterijus ar kategorijas padaryti svarbesnius nei kiti kriterijai ar kategorijos. Jį pilnai redaguoti tiek kriterijams tiek kategorijoms. Šis indeksas visada yra sveikas skaičius ir yra vertinamas nuo 1 iki 5. Svoriai kategorijoms yra parenkami atlikus kategorijų analizę, remiantis pažeidžiamumų duomenų bazių suteikta informacija apie pažeidžiamumų kiekį ir kritiškumą atitinkamose kategorijose ir naudojant ekspertines žinias. Z indekso reikšmės pavaizduotos 8 pav.



8 pav. Z indekso reikšmės

Pirmiausia yra įvertinami individualūs kriterijai. Kriterijaus pradinis vertinimas k yra skaičiuojamas pagal jo tiesioginį rankiniu būdu nustatyta įvertinimą arba jo faktorių įvertinimus. Kriterijaus individualus įvertinimas KR yra skaičiuojamas pagal paėmus kriterijaus pažeidžiamumo įvertinimą k iš pažeidžiamumų duomenų bazės (dešimtbalėje sistemoje) ir padauginus iš z indekso. Z indeksas šioje situacijoje yra kriterijaus standartizavimo pataisymas, nes ne visi kriterijai yra lygiaverčiai kibernetinio saugumo atžvilgiu.

$$KR = k \times z_{KR}$$

Toliau yra įvertinama kiekviena kategorija individualiai. Kriterijus visada priklauso vienai kategorijai, o kategorija turi bent vieną ar daugiau kriterijų. Kategorijos yra nurodytos analizės dalyje,

jų buvo identifikuota 17, tačiau jeigu yra reikalas jas išskirstyti smulkiau ar pridėti naujų kategorijų, tą galima padaryti pasinaudojus interneto svetaine. Kategorijos įvertinimas skaičiuojamas susumavus kriterijaus individualaus įvertinimo KR ir kategorijos standartizavimo pataisymo sandaugas. Z indeksas šioje situacijoje yra kategorijos standartizavimo pataisymas, nes ne visos kategorijos yra lygiavertės kibernetinio saugumo atžvilgiu.

$$KA = \sum KR \times z_{KA}$$

Kitame žingsnyje yra apverčiamas kategorijos įvertis, jog jis rodytų saugumą, o ne pažeidžiamumo lygį. Normalizuojamos visos kategorijos, kad individualios kategorijos reikšmė būtų dešimtbalėje sistemoje. Normalizuota kategorijos reikšmė KA_n yra gaunamas padalinus kategorijos individualų įvertinimą iš kategorijos standartizavimo pataisymo ir kriterijų standartizavo pataisymų sumos sandaugos.

$$KA_n = \frac{KA}{Z_{KA} \times \sum Z_{KR}}$$

Galutinis reitingas R yra lygus kategorijų aritmetiniam vidurkiui.

$$R = \frac{\sum KA}{N_{KA}}$$

Galutinis reitingas R parodo skaičių nuo 0 iki 10 kiek saugus yra įmonės kibernetinis saugumas.

2.4. Sistemos architektūra

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos architektūra (9 pav.) pagrinde susideda iš serverio ir kliento (įmonės) įrenginių bei viešai prieinamos pažeidžiamumų duomenų bazės.

Kliento įrenginyje bus vienas komponentas:

Duomenų surinkimo ir perdavimo programa bus atsakinga už informacijos surinkimo etapą. Ji automatiškai surinks informaciją apie kliento įrenginį atsiųs į serverį naudojant saugų https protokolą. Duomenis bus siunčiami įrenginiui (dažniausiai kompiuteriui) įsijungus, kas pasirinktą laiko tarpą, informacijai pasikeitus ar serveriui atsiuntus užklausą su prašymu atsiųsti naują informaciją.

Serveryje bus keturi komponentai:

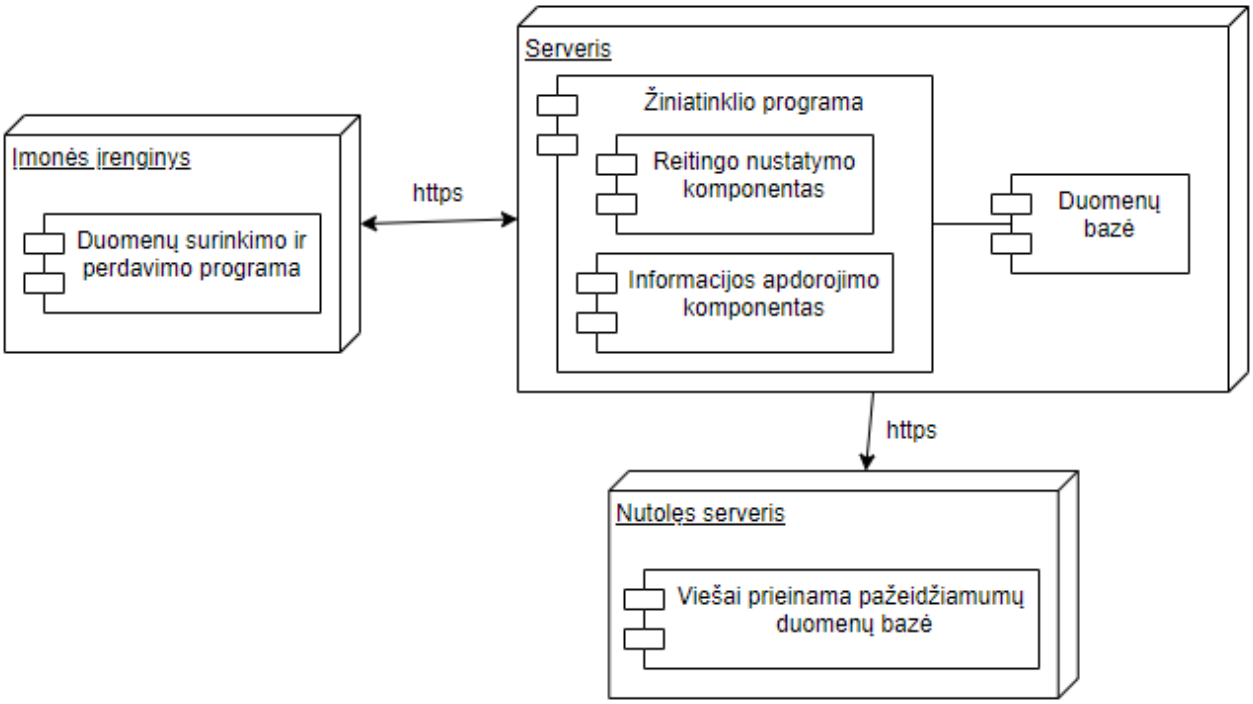
Informacijos apdorojimo komponentas – atsakingas už informacijos apdorojimo etapą. Šiame etape surinkta informacija bus suformatuota taip, kad būtų tinkama perduoti reitingo nustatymo komponentui. Plačiau kas bus daroma šiame komponente yra aprašyta prie informacijos apdorojimo etapo.

Reitingo nustatymo komponentas – naudojantis sukurto metodo algoritmu nustatys įmonės kibernetinio saugumo lygį. Plačiau aprašomas bus prie reitingo nustatymo etapo.

Interneto svetainė – vieta, kur įmonės atsakingas žmogus už kibernetinį saugumą galės valdyti dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemą. Į tai įeina sistemos konfigūracija, duomenų padavimas, reitingo peržiūrėjimas, ataskaitų generavimas. Taip pat, poreikiui esant, ši interneto svetainė galės veikti tik vidiniame tinkle ir informaciją apie pažeidžiamumus bus galima importuoti rankiniu būdu, kas užtikrintų dar didesnį saugumo lygį.

Duomenų bazėje bus saugoma surinkta informacija apie įmonės įrenginius, tinklo infrastruktūrą, sistemos konfigūracijos, duomenys apie kibernetinio saugumo reitingą ir su juo susiję istoriniai pažeidžiamumai.

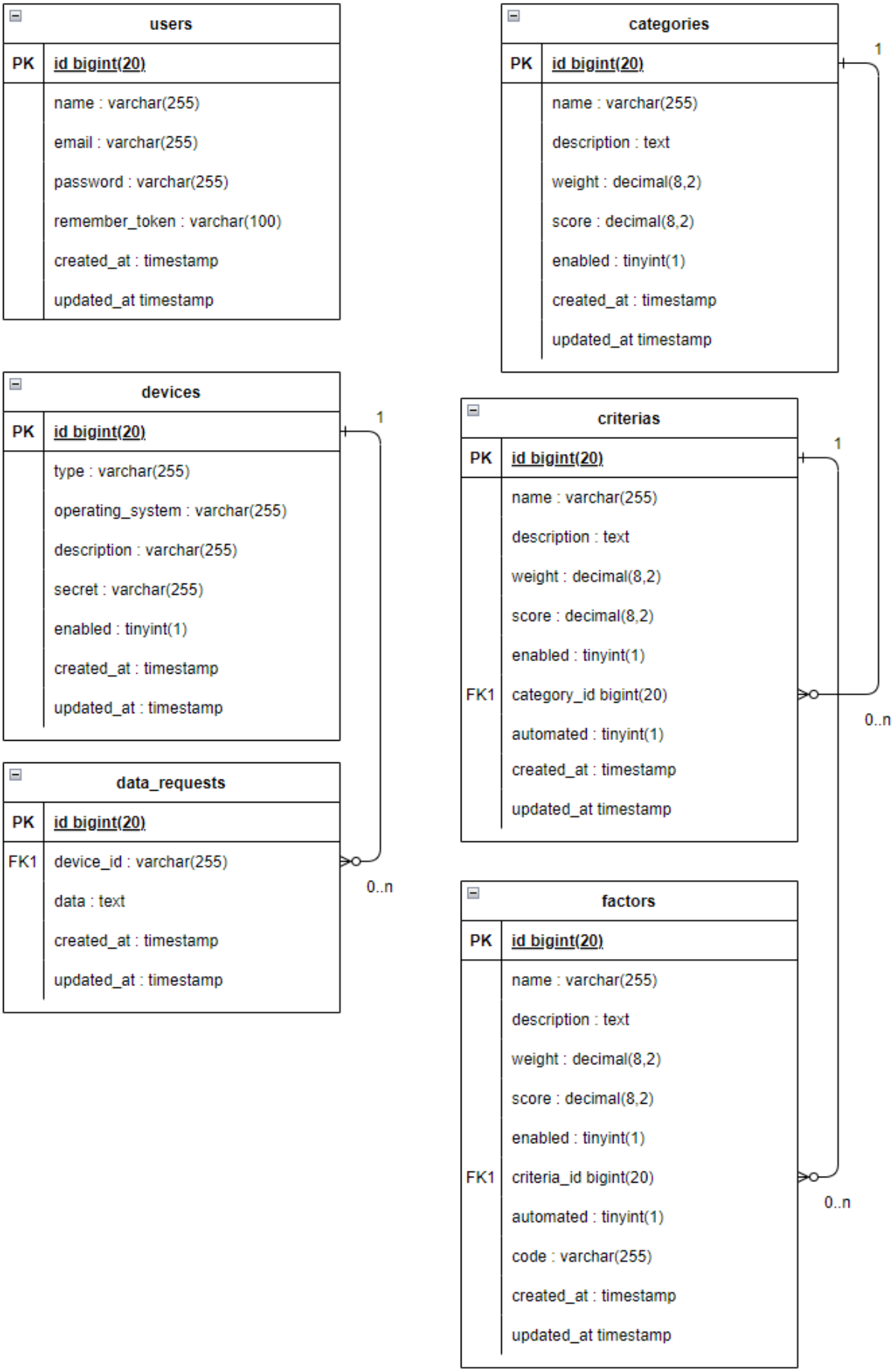
Serveris taip pat bendraus su nutolusia viešai prieinama pažeidžiamumų duomenų baze https protokolu, kad būtų galima gauti naujausią informaciją apie pavojų keliančius pažeidžiamus automatiškai. Pažeidžiamumų duomenų bazė gali būti CVE, CVSS ar Metasploit, priklausomai nuo konfigūracijos.



9 pav. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos architektūra

2.5. Duomenų bazės schema

Šiame skyrelyje pateikiama projektuojamos sistemos duomenų bazės schema (10 pav.). Duomenų bazės schemą sudaro šios lentelės: naudotojai, įrenginiai, duomenų užklausos kategorijos, kriterijai ir faktoriai (angl. „users“, „devices“, „data_requests“, „categories“, „criterias“, „factors“). Naudotojų lentelėje saugoma naudotojų informacija. Naudotojų yra viena rūšis, administratoriai, kurie prižiūri ir naudojasi sistema. Įrenginių lentelėje yra išsaugomi individualūs įmonės įrenginiai, kuriuose yra surašyta agento programinė įranga, kuri surenka informaciją. Duomenų užklausos lentelėje yra saugoma ta surinkta informacija, kuri yra susieta su konkrečiu įrenginiu. Kategorijų, kriterijų ir faktorių lentelėse yra saugomi sukonfigūruoti kintamieji, kurie daro įtaką kibernetinio saugumo reitingo vertinimui.



10 pav. Duomenų bazės schema

2.6. Išvados

1. Sukurtas dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas, kuris gali įvertinti įmonės kibernetinį saugumą tiksliai, dinamiškai ir lanksčiai.
2. Atliktas reikalavimų specifikavimas, kurio metu apibrėžti funkciniai reikalavimai ir sistemos architektūra.
3. Suprojektuota sistema, kuri realizuotų pasiūlytą dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodą.

3. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipas

Kad būtų galima pavaizduoti dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo veikimą, nuspręsta sukurti sistemos prototipą, kuris realizuotų šį metodą. Šis prototipas bus realizuotas kaip žiniatinklio programa, kad būtų lengviau pademonstruoti jo veikimą. Sistemos prototipas kuriamas su idėja, jog jis būtų naudojamas įmonės viduje, o ne išorėje, kaip trečios šalies programa, kuria naudotųsi daug skirtingų įmonių. Svarbus pastebėjimas – prototipas yra skirtas pavaizduoti sukurto metodo veikimą, o ne praktiškai naudoti įmonėse su dabartinėmis funkcijomis.

3.1. Sistemos prototipui pasirinkti įrankiai

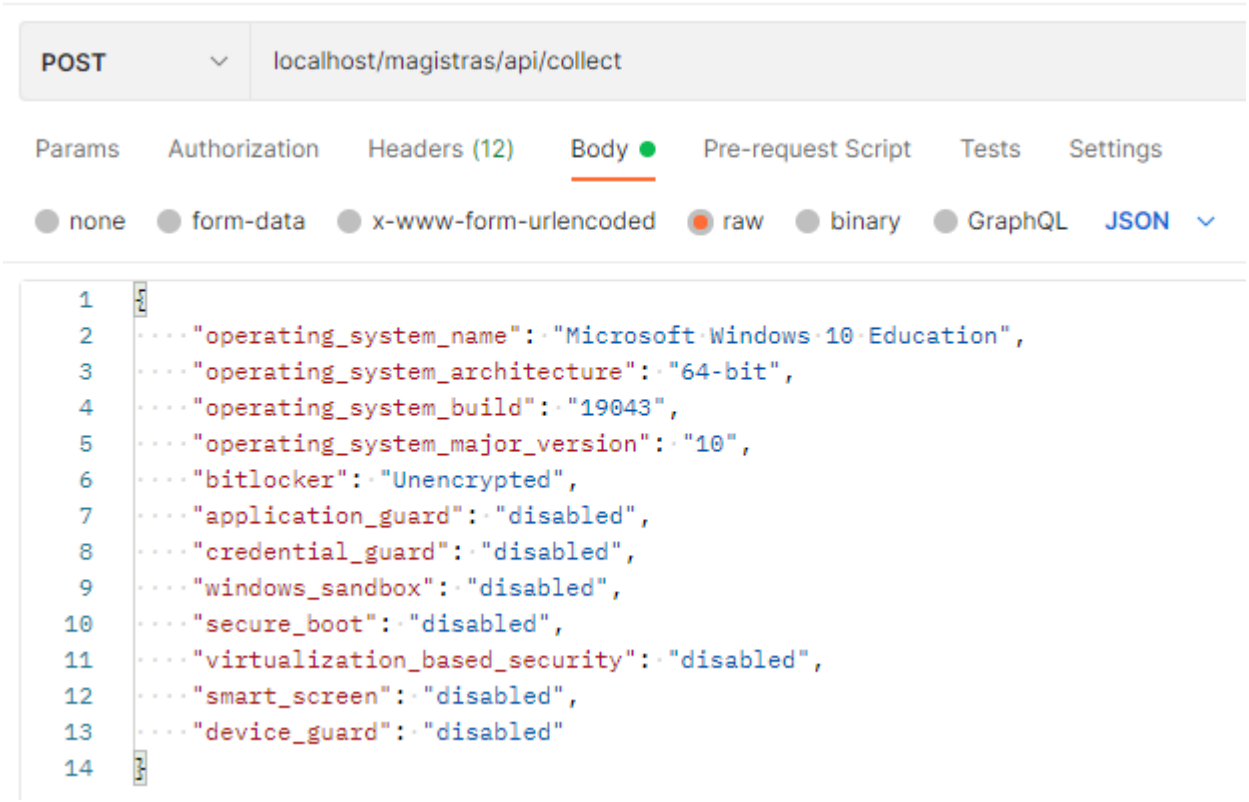
Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipui realizuoti yra reikalinga sistema, kurioje bus patalpinta metodo logika ir duomenų surinkimo programa, kuri iš įvairių įrenginių surinks reikalingą informaciją, kuri padėtų sistemai įvertinti kibernetinio saugumo reitingą.

3.1.1. Žiniatinklio sistemos daliai pasirinkti įrankiai

Kuriama sistema yra žiniatinklio programa ir ji yra pasirinkta daryti su „Laravel“ PHP kalbos karkasu. Duomenų bazėj pasirinkta MySQL kalba, kadangi Laravel karkasas ją palaiko didžiausiu prioritetu. Naudotojo sąsajai pasirinktos standartinės front-end kalbos – HTML, CSS ir JS, nes žiniatinklio naudotojo sąsajai nėra teikiamas didelis prioritetas, nes esmė yra realizuoti patį metodą. Pačiame serveryje bus CentOS 7 operacinė sistema. Ji pasirinkta todėl, kad sukuria lengvą aplinką, kurioje galima valdyti serverį.

3.1.2. Duomenų surinkimui pasirinktas įrankis

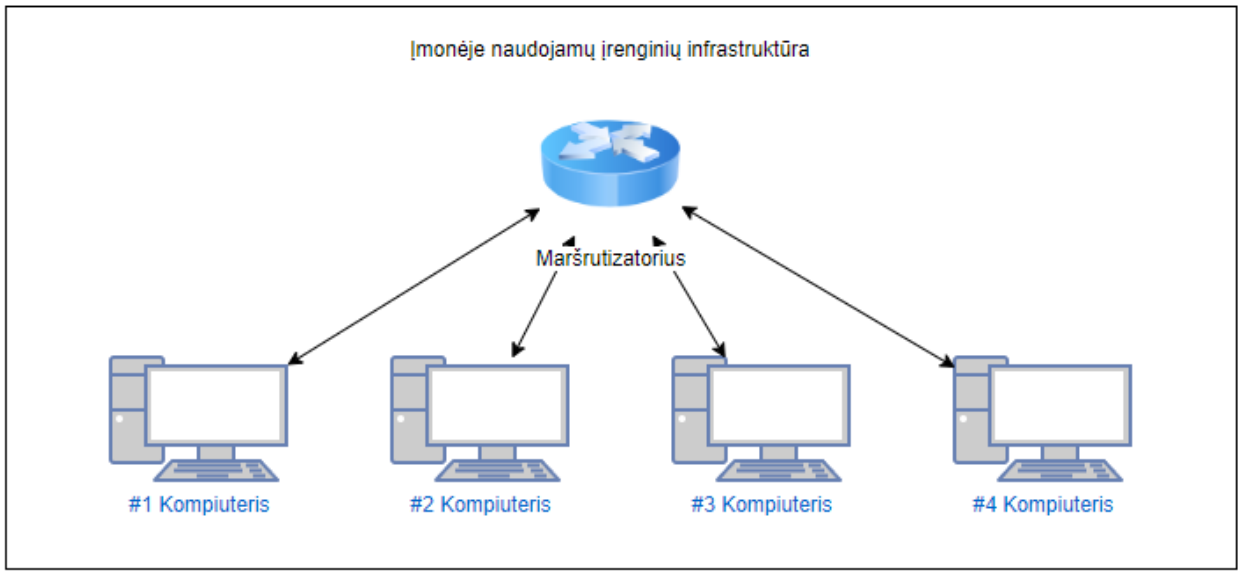
Prototipo realizavimui pasirinkta duomenų surinkimą daryti tik iš Windows šeimos operacinių sistemų (7 ir vėlesnių versijų). Duomenų surinkimui pasirinkta „.NET“ konsolinė programa, kuri surinktų duomenis ir juos išsiųstų į sistemą. Ši programa surinktų informaciją (11 pav.) apie operacinę sistemą, veikiančius procesus, prijungtus įrenginius ir tinklo parametrus.



11 pav. Užklausos duomenų pavyzdys

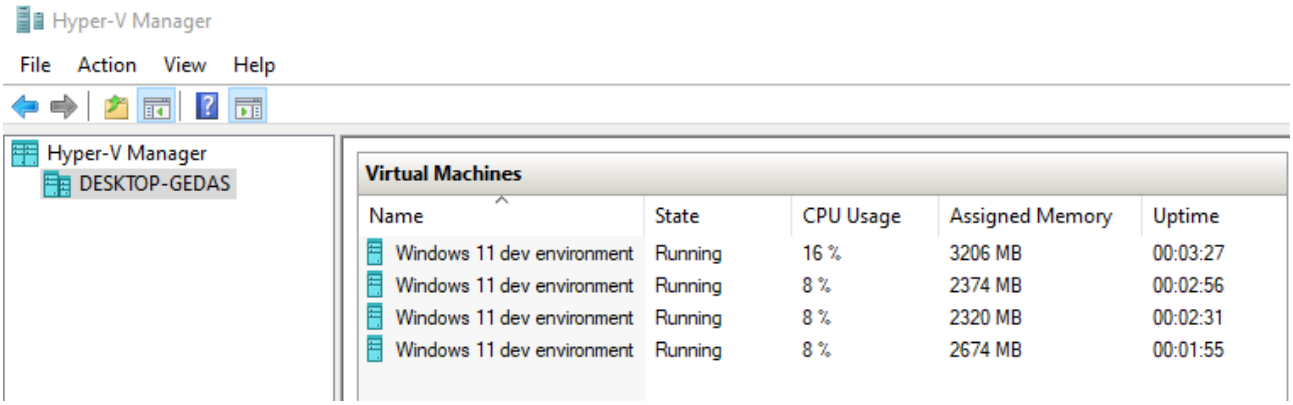
3.2. Prototipe naudojamų įrenginių infrastruktūra

Tam, kad būtų galima pratestuoti prototipo veikimą, buvo sukurta dirbtinės įmonės naudojamų įrenginių infrastruktūra. Sistema yra projektuojama taikant pagrinde į nedideles ir vidutinio dydžio įmones, todėl buvo simuliuota ir atitinkama įrenginių infrastruktūra (12 pav.). Įmonėje naudojami keturi kompiuteriai, prijungti prie maršrutizatoriaus. Visuose kompiuteriuose yra įrašyta Windows 10 operacinė sistema. Kompiuterių aparatinė įranga nėra tiek svarbi, nes vieninteliai reikalavimai testavimui yra galimybė paleisti agento programą ir prieigą prie interneto. Kad būtų galima paleisti agento programą, kompiuteryje turi būti Windows operacinės sistemos šeimos dalimi ir turėti įrašytą „.NET 6“ vykdymo biblioteką, kuri yra palaikoma nuo Windows 10 OS 1607 versijos.



12 pav. Prototipe naudojamų įrenginių infrastruktūra

Kadangi tai yra dirbtina įmonė, ši infrastruktūra yra sukurta naudojantis virtualių mašinų pagalba. Tam pagelbėjo „Hyper-V Manager“ įrankis, su kuriuo buvo sukurtos keturios virtualios mašinos (13 pav.). Į jas buvo įrašyta agento programa ir atitinkamai sukonfigūruoti saugos nustatymai būsimiems testavimams.



13 pav. Sukurtos virtualios mašinos „Hyper-V Manager“ programoje

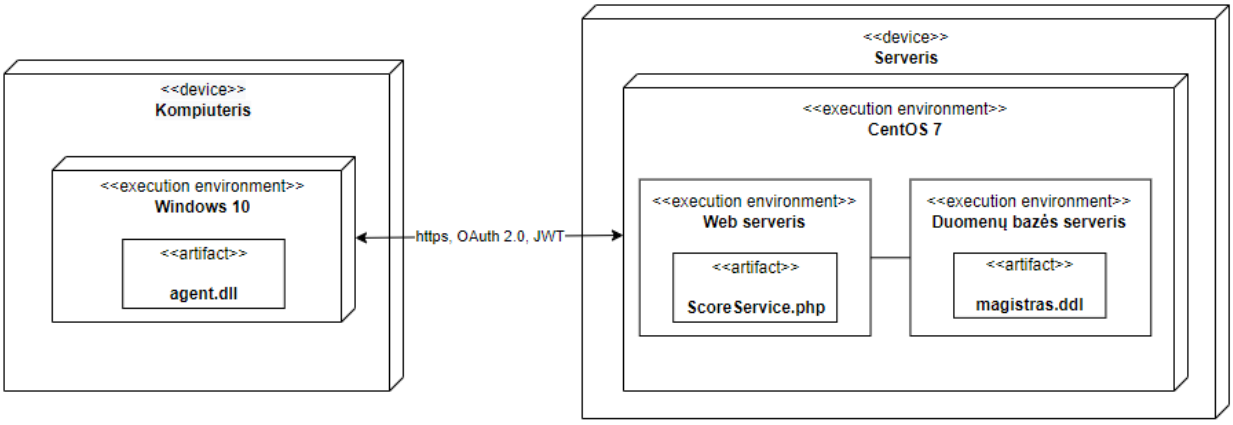
3.3. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipo diegimas

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipo diegimas susideda iš kelių dalių. Pirmiausia yra įrašoma sistemos programinė įranga. Tada kiekvienam įmonės įrenginyje turi būti įdiegta duomenų surinkimo programa, kuri siųs šią informaciją kibernetinio saugumo reitingo nustatymo sistemai. Tada sistemoje reikia sukonfigūruoti nustatymus, kurie geriausiai atitinka įmonės kibernetinio saugumo profilį.

3.3.1. Sistemos diegimo diagrama

Sistemos diegimo diagramoje (14 pav.) pavaizduoti du pagrindiniai įrenginiai, juose įrašytos operacinės sistemos ir pagrindiniai sistemos artefaktai. Sistema bus įdiegta serveryje, kuriame yra įrašyta „CentOS 7“ operacinė sistema. Jame bus web ir duomenų bazės lokalūs serveriai. Web serveryje bus „ScoreService.php“ artefaktas, kuris bus atsakingas už duomenų apdorojimo ir reitingo

nustatymo logiką. Web serveryje taip pat bus talpinama žiniatinklio programa su grafine naudotojo sąsaja. Duomenys siunčiami iš agento į web serverį bus šifruojami naudojant SSL sertifikatus. Papildomai apsaugai bus naudojama OAuth 2.0 metodologija ir „JSON Web Tokens“ formatas.



14 pav. Sistemos diegimo diagrama

3.3.2. Konfigūracija

Norint pradėti naudotis sukurta sistema pirma reikia ją sukonfigūruoti pagal savo lūkesčius ir galimybes. Mažesnei įmonei yra atitinkamai mažiau pavojaus vektorių ir kibernetinio saugumo kriterijų, kuriuos reikia tenkinti negu didesnei įmonei.

Analizės dalyje buvo paminėta 17 kategorijų, po kuriomis gali pakliūti praktiškai visi kriterijai. Kriterijai bus naudojami reitingo nustatymui. Taigi, pradžioj reikia nustatyti savo įmonei aktualias kategorijas ir kriterijus. Iš anksto bus parūpinta standartinė konfigūracija, kuri leis iš karto naudotis sistema. Tačiau, kad įmonės kibernetinio saugumo reitingas būtų įvertintas tiksliai, patariama sukonfigūruoti sistemą pagal savo poreikius. Taip pat, jeigu nebuvo darytas kibernetinio saugumo auditas, ar buvo, bet seniai, patariama jį pasidaryti prieš pradedant sistemos konfigūravimą, kad būtų aiškesnė įmonės kibernetinio saugumo padėtis ir šios sistemos naudojimo tikslai.

Konfigūracijos etapai:
1. Kriterijų nustatymai

Kriterijų nustatymai yra pats svarbiausias žingsnis, nes pagal juos yra skaičiuojamas įmonės kibernetinio saugumo reitingas. Standartinėje konfigūracijoje yra nustatytos pagrindinės 17 kategorijų, po kuriomis yra jau sukurti ir taip pat gali būti papildyti kriterijai. Kategorijas ir kriterijus laisvai galima pridėti ar pašalinti. Kriterijai gali būti įvairių tipų, kas leidžia konfigūruoti sistemą dar detaliau.

2. Duomenų surinkimo ir apdorojimo nustatymai

Duomenų surinkimo ir apdorojimo nustatymai yra svarbūs tuo, kad jie leidžia automatizuoti visą šitą procesą vietoj to, kad reikėtų visus duomenis suvedinėti ranka. Tai daro didelę įtaką sistemos dinamiškumo aspektui. Norint duomenis surinkti automatiškai, tam reikalinga programinė įranga (agentas) įrašyta į norimus įmonės įrenginius. Kiekvienas agentas įrašytas į įrenginį turi to įrenginio identifikacinį kodą ir paslaptį. Šie kintamieji naudojami tikslingai rinkti informaciją ir ją rinkti

saugiai. Prototipo atveju bus dirbama dirbtinėje įmonės infrastruktūroje su virtualiomis mašinomis. Duomenis taip pat visada bus galima įrašyti rankiniu būdu.

3. Dinamiškumo nustatymas

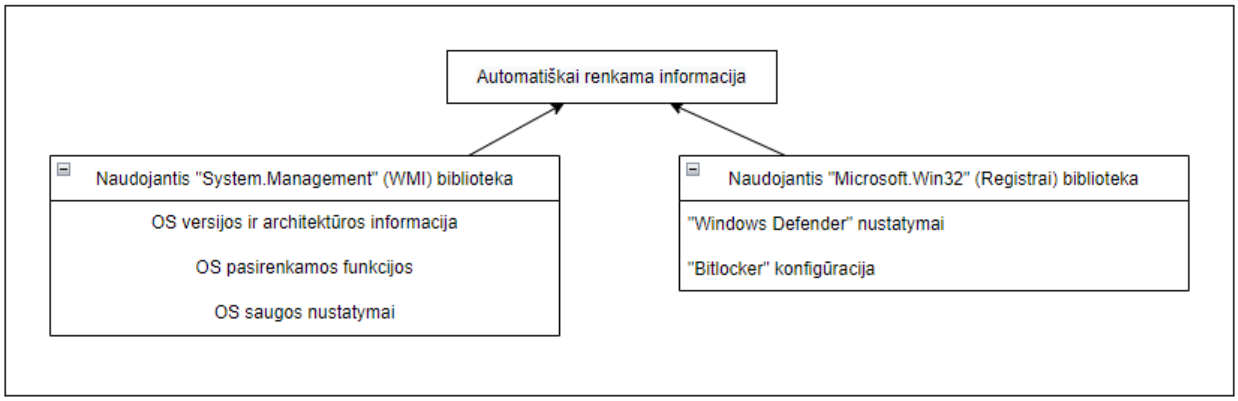
Dinamiškumas gali būti apibrėžiamas keliais būdais. Jį gali lemti keli nustatymai – kas kiek laiko duomenys yra surenkami ir atsiunčiami į sistemą, kas kiek laiko yra atnaujinama informacija, kuri gali būti atnaujinta tik rankiniu būdu, ar reikia laukti duomenų iš kelių skirtingų informacijos šaltinių, kad būtų paskaičiuotas kibernetinio saugumo reitingas ir kas kiek laiko skaičiuojamas kibernetinio saugumo reitingas.

4. Įrenginių pridėjimas

Įrenginių informacijos pridėjimas yra papildomas pasirinkimas konfigūracijoje, kurį užpildžius kibernetinio saugumo reitingas paskaičiuojamas tiksliau. Pridėjus įrenginius galima jiems pridėti papildomos informacijos. Tai yra ypač naudinga jeigu įrenginio naudotojas per tą įrenginį turi prieigą prie daug jautrios informacijos ar įrenginys turi specifinių saugumo pasirinkimų, kurių neišeitų pridėti per kriterijus. Taip pat jis yra skirtas ir įrenginiams, į kuriuos nėra įrašyta programinė įranga, kuri automatiškai gali surinkti ir atsiųsti duomenis į serverį, kas vėlgi pagelbsti įvertinant kibernetinio saugumo reitingą.

3.4. Automatiniu būdu surenkamos informacijos šaltiniai

Automatiniu būdu informacija iš įrenginių yra surenkama pasinaudojant „System.Management“ („Windows Management Instrumentation“) biblioteką ir „Microsoft.Win32“ biblioteką, kad būtų galima prieiti registrų informaciją. Naudojantis WMI biblioteka yra automatiškai surenkama informacija apie operacinės sistemos versiją ir architektūrą, kokios yra įgalintos pasirenkamos (neprivalomos) funkcijos ir kokie saugos nustatymai yra sukonfigūruoti. Naudojantis registrų informacija yra tikrinami „Windows Defender“ nustatymai ir „Bitlocker“ konfigūracija.



15 pav. Naudojami informacijos šaltiniai įrenginiuose

3.5. API apsauga

Įmonės IT infrastruktūros duomenys yra labai jautri informacija, kuri gali sukelti neigiamų padarinių patekus į pakenkti norinčių asmenų rankas. Kibernetinio saugumo reitingo nustatymo sistema šią informaciją gauna per API užklausas iš įmonės IT infrastruktūros įrenginių. Tam, kad apsaugoti šią informaciją, buvo realizuota API apsauga, kuri remiasi OAuth 2.0 metodologija ir JWT API formatu.

3.5.1. OAuth 2.0 metodologijos pritaikymas API autentifikavimo procese

OAuth 2.0 yra plačiai naudojamas prieigos prie API autentifikavimo metodas. Kadangi kuriama dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistema bus naudojama įmonės viduje, API prieiga yra uždara – tik įmonės IT infrastruktūros įrenginiai gali bendrauti su pagrindiniu sistemos serveriu, kur yra API galutiniai prieigos taškai. Dėl kaupiamos informacijos pobūdžio yra reikalingas tik autentifikavimo procesas, kuris leis patvirtint, jog tai tikrai yra įrenginys, priklausantis įmonei.

OAuth 2.0 metodas kalbant apie API prieigos taškus nurodo, jog reikia identifikuoti užklausos siuntėją, kas gali būti padaryta pasirinkus iš keleto nurodytų būdų ir suteikti jam autorizacijos prieigos raktą, kurį vėliau sistemos tarpusavyje naudotų saugiam duomenų apsikeitimui. Kadangi dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistema yra kuriama, kad būtų naudojama įmonės viduje, dėl to autentikavimo procesas palengvėja. Įmonės IT personalas, atsakingas už įrenginių priežiūra ir parengimą darbui, pirma įrašo agento programinę įrangą, kuri yra skirta siųsti informaciją į pagrindinį sistemos serverį. Taigi, tuo pačiu metu kai yra įrašoma agento programinė įranga, taip pat yra sukuriamas identifikacinis įrenginio numeris, kuris yra iš karto pridedamas į kibernetinio saugumo reitingo nustatymo sistemą ir sugeneruojama kiekvienam įrenginiui individuali paslaptis, kuri vėliau yra panaudojama JWT prieigos rakte.

3.5.2. JWT struktūra

JWT yra JSON žiniatinklio prieigos rakto standartas, kuris apibrėžia kompaktišką ir savarankišką būdą saugiai perduoti informaciją kaip JSON objektą. Tokio tipo prieigos raktas leidžia užtikrint, jog įmonės IT infrastruktūros informacija siunčiama užšifruota viešomis ir privačiomis raktų poromis bei patikrinti, jog turinys buvo nepakeistas.

JWT susideda iš trijų dalių – antraštės, turinio ir parašo. JWT prieigos rakto dalys yra atskiriamos taškais.

Pirmojoje dalyje – antraštėje yra patalpinta informacija apie prieigos rakto tipą ir koks šifravimo algoritmas yra naudojamas. Realizacijoje naudojama antraštė pavaizduota 16 pav. Prieš siunčiant, antraštė yra užšifruojama Base64Url šifruote ir patampa pirmąja JWT prieigos rakto dalimi.

```
{
    "alg": "HS256",
    "type": "JWT"
}
```

16 pav. JWT prieigos rakto antraštė

Antroji JWT prieigos rakto dalis yra turinys. Šio prototipo atveju JWT naudojamas tik kaip saugios struktūros perdavimo įrankis, dėl to jame yra talpinama įrenginio informacija, kuri atrodo kaip pavaizduota 17 pav. Turinio dalis taip pat yra užkoduojama Base64Url šifruote ir tik tada patampa JWT prieigos rakto antrąja dalimi.

```
{
    "operating_system_name": "Microsoft Windows 10 Education",
    "operating_system_architecture": "64-bit",
    "operating_system_build": "19043",
    "operating_system_major_version": "10",
    "bitlocker": "Unencrypted",
    "application_guard": "disabled",
    "credential_guard": "disabled",
    "windows_sandbox": "disabled",
    "secure_boot": "disabled",
    "virtualization_based_security": "disabled",
    "smart_screen": "disabled",
    "device_guard": "disabled"
}
```


17 pav. JWT prieigos rakto turinys

Paskutinę JWT prieigos rakto dalį sudaro parašas. Parašas yra sukuriamas paėmus užkoduotą antraštės dalį su užkoduota turinio dalimi ir jas kartu užšifravus panaudojant antraštėje nurodytą šifravimo algoritmą ir panaudojant paslaptį. Ši veiksmų eiga užrašyta kodu atrodytų taip, kaip pavaizduota 18 pav.

```
HMACSHA256(
  base64UrlEncode(antraste) + "." +
  base64UrlEncode(turinys),
  paslaptis)
```

18 pav. JWT prieigos rakto parašo kūrimas

Galutinis užšifruotas ir pilnas JWT prieigos raktas atrodo kaip pateikta 19 pav., kur kiekviena spalva reiškia skirtingą prieigos rakto dalį.


```
eyJhbGciOiJIUzI1NiIsInR5cGUiOiJKV1QifQ.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ik1
hZ2lzdHJvIGRhcmJhcyIsImlhdCI6MTUxNjIzOT
AyMn0.t68cxEgkt5Xl5R9YIauJtOo6mrhbxFo3V
dO3w4b0djg
```


19 pav. JWT prieigos rakto pavyzdys

3.6. Prototipo reitingo skaičiavimo dinamiškumas

Kuriamoje dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemoje buvo projektuojama skaičiuoti reitingą dinamiškai keliais būdais, tai yra pagal įvykį ir tvarkaraštį. Taigi galutinis realizuotos sistemos dinamiškumas apibrėžiamas kaip ir kada reitingas yra paskaičiuojamas. Šiuo metu sistemoje kibernetinio saugumo reitingą galima paskaičiuoti 4 būdais ar laikais (visada naudojamas tas pats metodas):

1. Atsidarius pagrindinį puslapį.

Atsidarius pagrindinį puslapį yra paskaičiuojamas kibernetinio saugumo reitingas imant tik kategorijų įvertinimus.

2. Paspaudus mygtuką „paskaičiuoti reitingą“ pagrindiniame puslapyje.

Paspaudus šį mygtuką yra perskaičiuojami visi lygiai – kategorijos, kriterijai ir faktoriai. Faktoriai paskaičiuojami (jeigu yra automatizuoti) iš įrenginių surinktos informacijos, o tiksliau iš kiekvieno įrenginio paskutinio atsiųsto duomenų rinkinio. Tada yra paskaičiuojami visi kriterijai pagal jau atnaujintus faktorius ir galiausiai yra atnaujinami kategorijų įverčiai pagal šviežiai paskaičiuotus kriterijų reitingus. Kadangi ši užduotis gali užtrukti sąlyginai ilgiau, ant mygtuko paspaudimo yra iškviečiamas reitingo skaičiavimo darbas, kuris visus šiuos veiksmus atlieka sistemos fone. Vėliau užtenka tiesiog perkrauti puslapį praėjus atitinkamai laiko ir jau bus rodomas naujai paskaičiuotas reitingas.

3. Atnaujinus kategoriją, kriterijų ar faktorių rankiniu būdu.

Kai yra atnaujinama informacija susijusi su kibernetinio saugumo reitingo kintamaisiais, yra taip atnaujinamas reitingas kintamojo esančio aukščiau abstraktumo lygyje. Tai yra, kai atnaujinamas faktorius, tuo pat metu yra atnaujinamas to individualaus faktoriaus kriterijaus įvertis ir tuo pačiu to kriterijaus kategorijos įvertis. Taigi atnaujintus kibernetinio saugumo reitingo kintamąjį rankiniu būdu, visada gausime šviežiausią reitingą pagrindiniame puslapyje, nereikės laukti kada suveiks užduotis eilėje ar mygtuko paspaudimo.

4. Kas 30 sekundžių suveikus kibernetinio saugumo reitingo skaičiavimo užduočiai eilėje.

Paskutinis ir greičiausiai pagrindinis atvejis yra tada, kai įmonės kibernetinio saugumo reitingas yra pats paskaičiuojamas kas 30 sekundžių suveikus užduočiai, kuri skaičiuoją šį reitingą, užduočių eilėje.

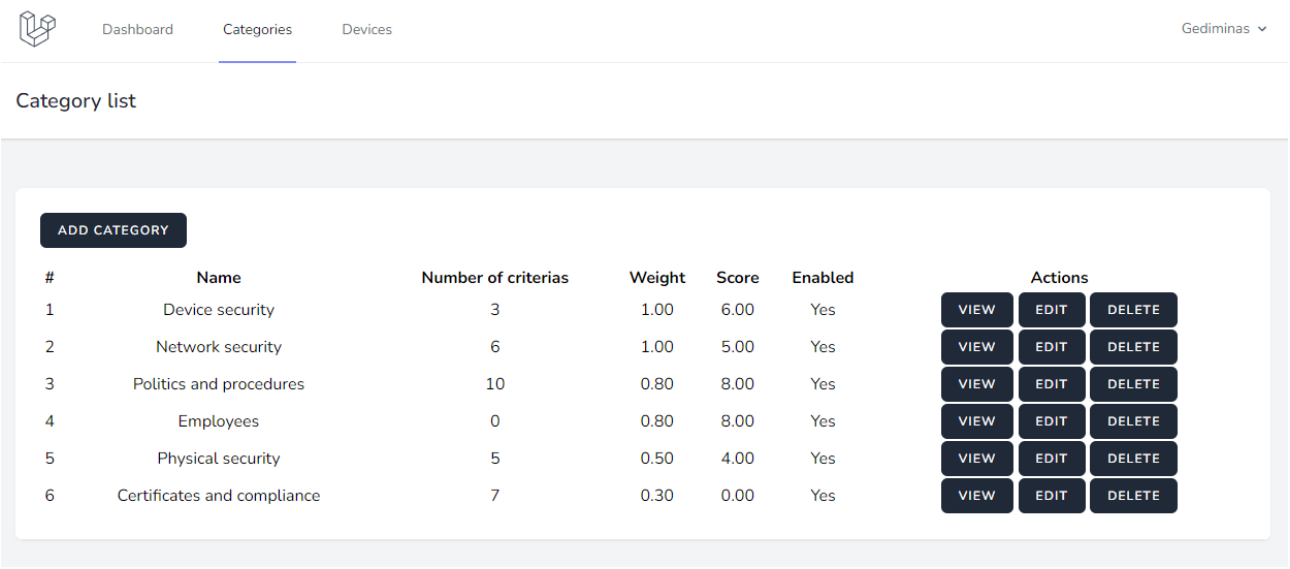
Kadangi duomenų surinkimas taip pat daro didelę įtaką kibernetinio saugumo reitingo skaičiavimui ir turi savo dinamiką, buvo realizuota keletas funkcijų, kurios leidžia dar lanksčiau naudotis šia sistema. Visų pirma tai prie kiekvieno įrenginio buvo realizuotas mygtukas, kurį paspaudus galima gauti to įrenginio informaciją ant kitos gautos jo užklausos, kai yra klausiama veiksmų eiga tvarkaraštyje. Su šia funkcija galima nelaukti kitos užklausos, kuri siųstų duomenis pagal nustatytą laiką ar keisti nustatymų kada norime gauti įrenginio informaciją. Taip pat buvo realizuota ir galimybė keisti individualaus įrenginio duomenų surinkimo laiko nustatymą, kas kiek laiko bus siunčiami duomenys.

3.7. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos veikimas

Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos veikimą galima atvaizduoti ir aprašyti praėjus pagrindinius tris sistemos veikimo etapus – konfigūravimą, duomenų surinkimą ir kibernetinio saugumo reitingo apskaičiavimą.

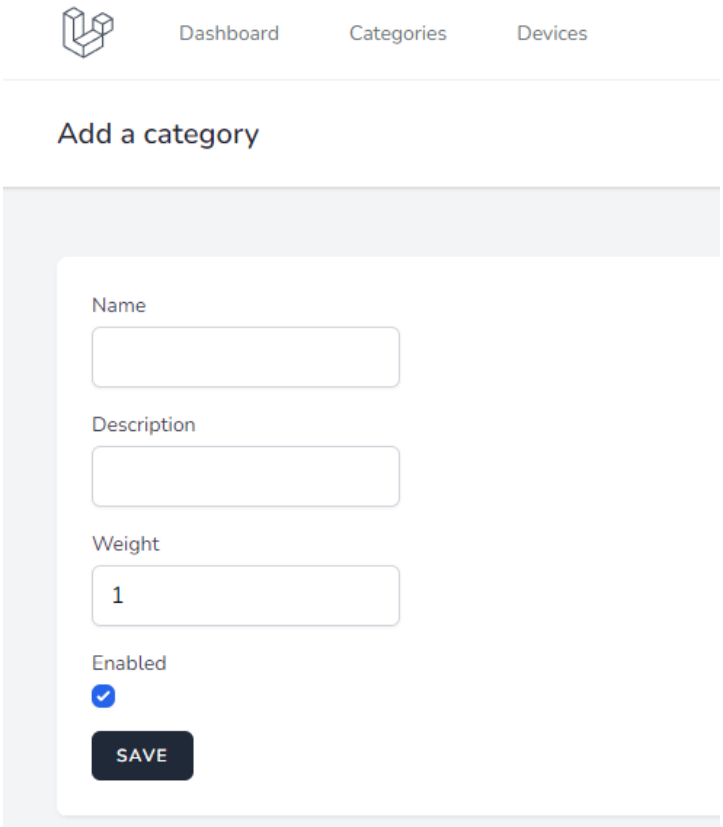
1. Konfigūravimas

Per konfigūravimą etapą visų pirmiausia reikia nustatyti kintamuosius, kad būtų galima paskaičiuoti tikslesnį ir aktualesnį kibernetinio saugumo reitingą. Taigi, kintamųjų nustatymas yra pradedamas nuo kategorijų peržiūros ir atnaujinimo. Kategorijų sąrašas su pagrindinėmis funkcijomis – peržiūrėjimo, redagavimo, ištrynimo ir pridėjimo yra pavaizduotas 20 pav. Sąraše taip pat galima matyti kategorijos pavadinimą, jai priklausančių kriterijų skaičių, svorį, reitingą ir ar ji yra aktyvi.



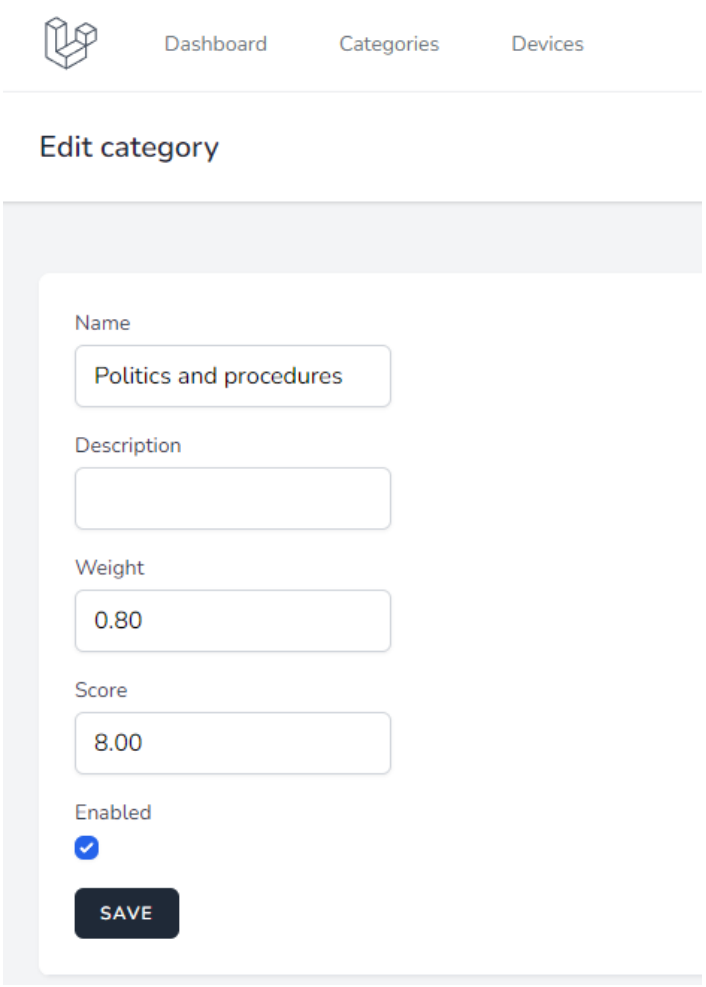
20 pav. Kategorijų sąrašo puslapis

Paspaudus ant mygtuko „Add category“ atidaromas naujas langas (21 pav.), kuriame galima pridėti naują kategoriją. Kad būtų sukurta kategorija, privalomai turi būti užpildytas vardo laukelis ir svorio laukelis. Aprašymas yra neprivalomas, o „Enabled“ laukelis standartiškai būna įjungtas, kas reiškia, jog ir kategorija yra aktyvi.



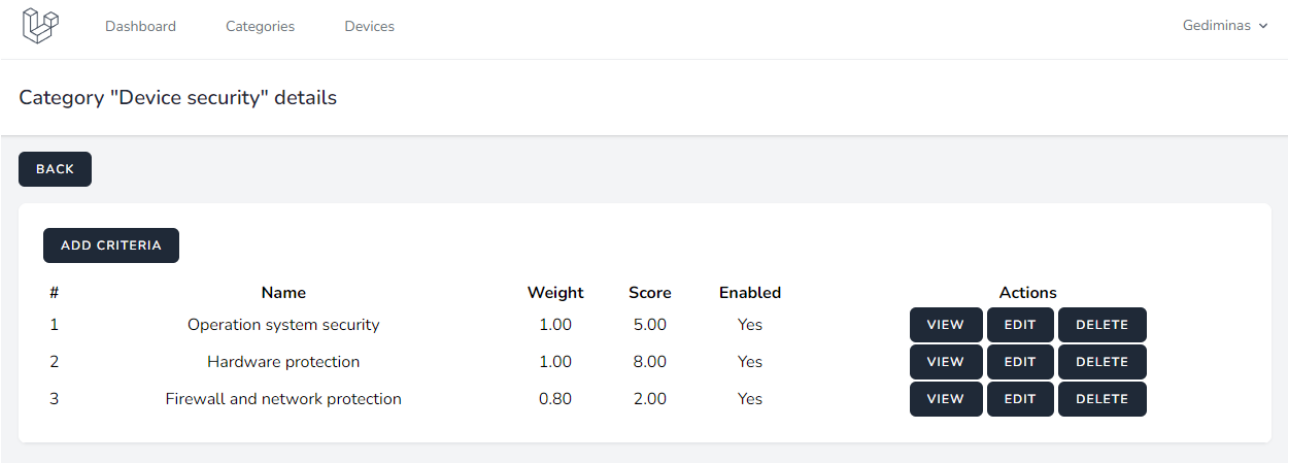
21 pav. Kategorijos pridėjimo puslapis

Kategorijų puslapyje paspaudus mygtuką „Edit“ atidaromas puslapis (22 pav.), kuriame galima redaguoti jau egzistuojančią kategoriją. Šioje formoje yra duoti tokie patys laukai kaip ir sukūrimo formoje, tačiau yra galimybė tuo pačiu nustatyti šios kategorijos reitingą.



22 pav. Kategorijų redagavimo puslapis

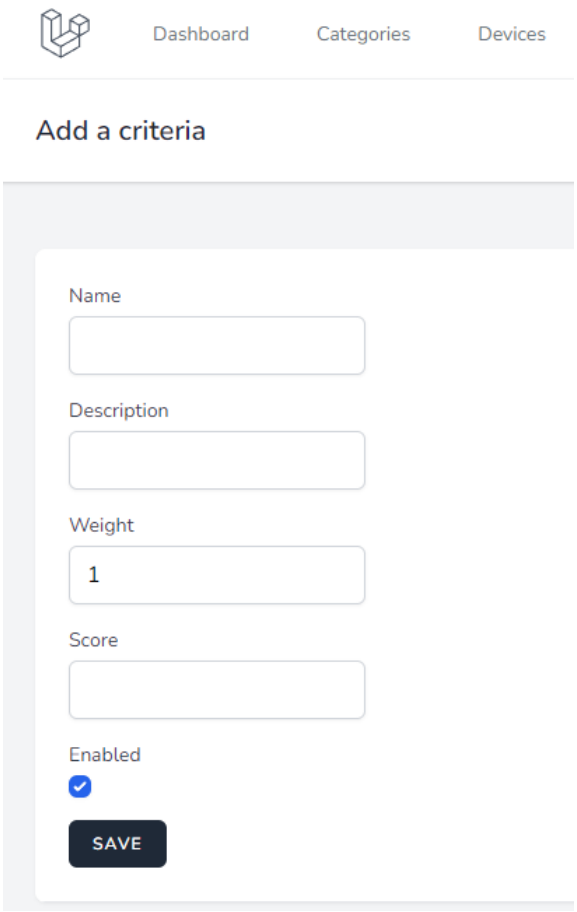
Paspaudus mygtuką „Show“ prie „Device security“ kategorijos, atidarome detalesnį vaizdą – šios kategorijos kriterijų puslapį (23 pav.). Jame yra tokios pat funkcijos kaip ir kategorijų puslapyje – kriterijų pridėjimo, peržiūrėjimo, redagavimo ir ištrynimo. Sąraše pavaizduoti kriterijų pavadinimai, svoriai, reitingai ir aktyvumas.



23 pav. „Device security“ kriterijų puslapis

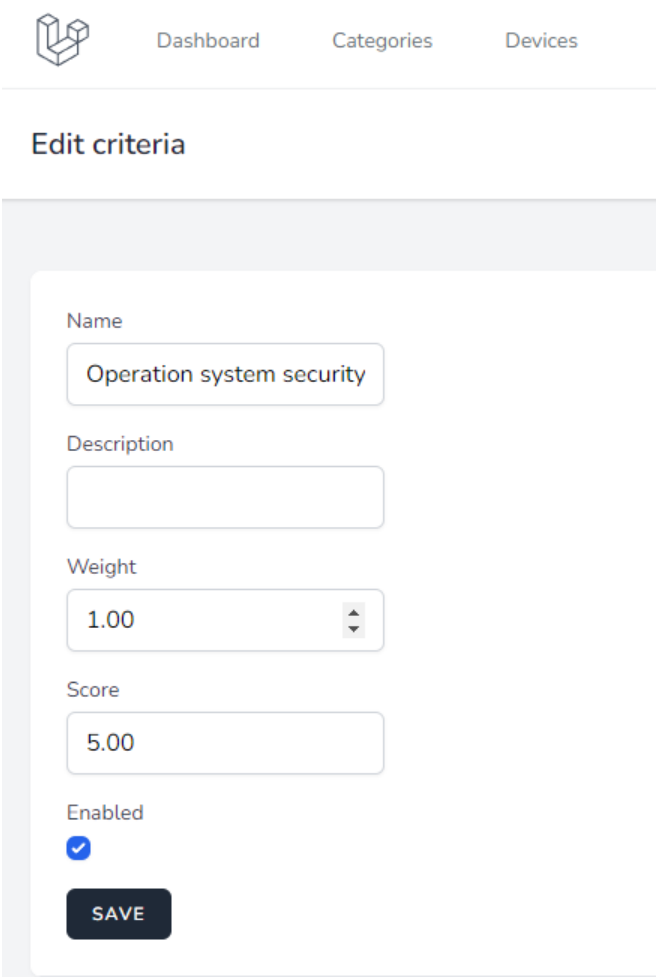
Paspaudus ant mygtuko „Add criteria“ yra atidaromas puslapis (24 pav.), kuriame galima pridėti kriterijų. Formoje atvaizduoti tokie patys laukai kaip ir kategorijos pridėjimo formoje, nes kriterijus

iš esmės yra informacinis vienetas panašus į kategoriją, tačiau daugiau konkretesnis. Kategoriją galima laikyti kaip kriterijų grupę. Sėkmingai išsaugojus kriterijų, jis iš karto išsaugomas prie kategorijos, iš kurios puslapio buvo ateita.



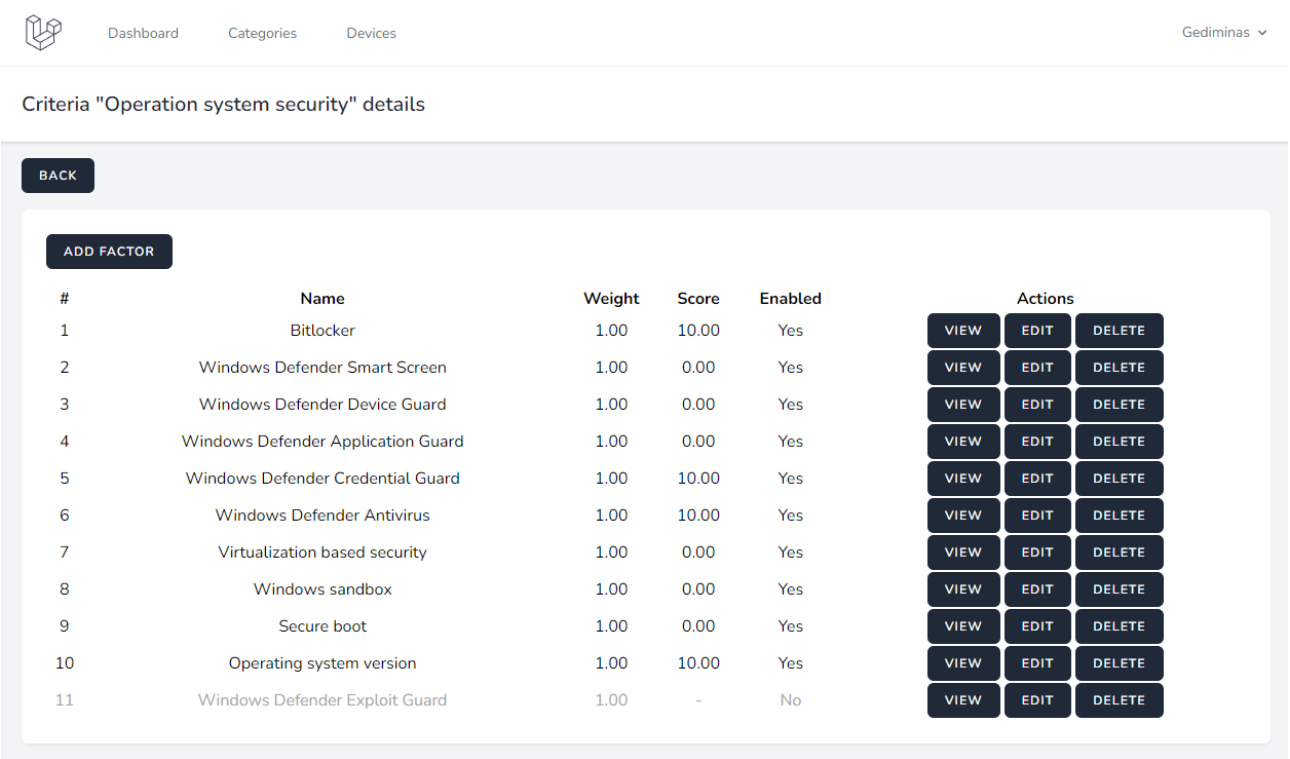
24 pav. Kriterijaus pridėjimo puslapis

Paspaudus mygtuką „Edit“ prie kriterijaus „Operation system security“, atidaromas šio kriterijaus redagavimo puslapis (25 pav.). Jame redagavimo forma yra identiška kategorijų redagavimo formai. Esminis dalykas, kad čia galima atnaujinti kriterijaus reitingą.



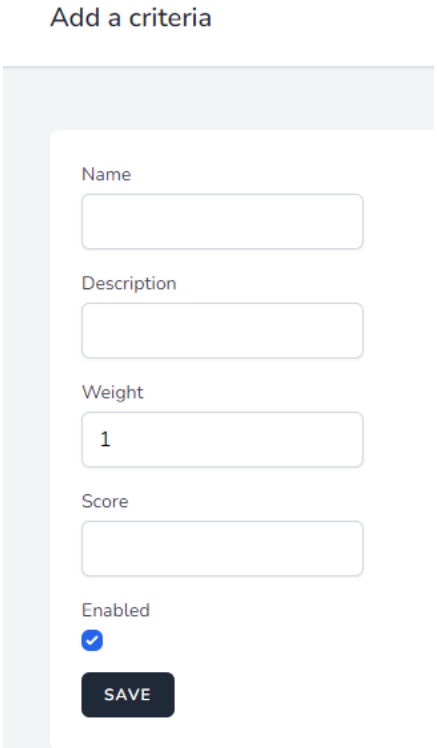
25 pav. Kriterijaus „Operation system security“ redagavimo puslapis

Paspaudus „Show“ mygtuką šalia „Operation system security“ kriterijaus, atidaromas šio kriterijaus faktorių puslapis (26 pav.). Čia taipogi yra tos pačios funkcijos kaip ir prie kategorijų ir kriterijų, tačiau čia yra žemiausias abstrakcijos lygis. Faktoriai dažniausiai yra naudojami automatiškai surenkant informaciją. Tai yra kiekvieno įrenginio surinktos informacijos rezultatas.



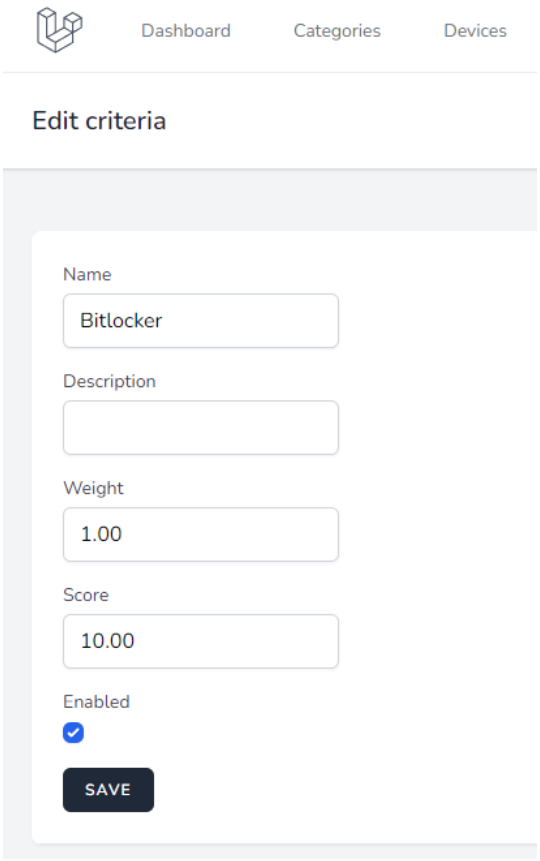
26 pav. Kriterijaus „Operation system security“ faktorių puslapis

Paspaudus ant „Add factor“ mygtuko, atsidaro puslapis (27 pav.), kuriame galima pridėti faktorių. Formos laukai yra identiški kategorijoms ir kriterijams.



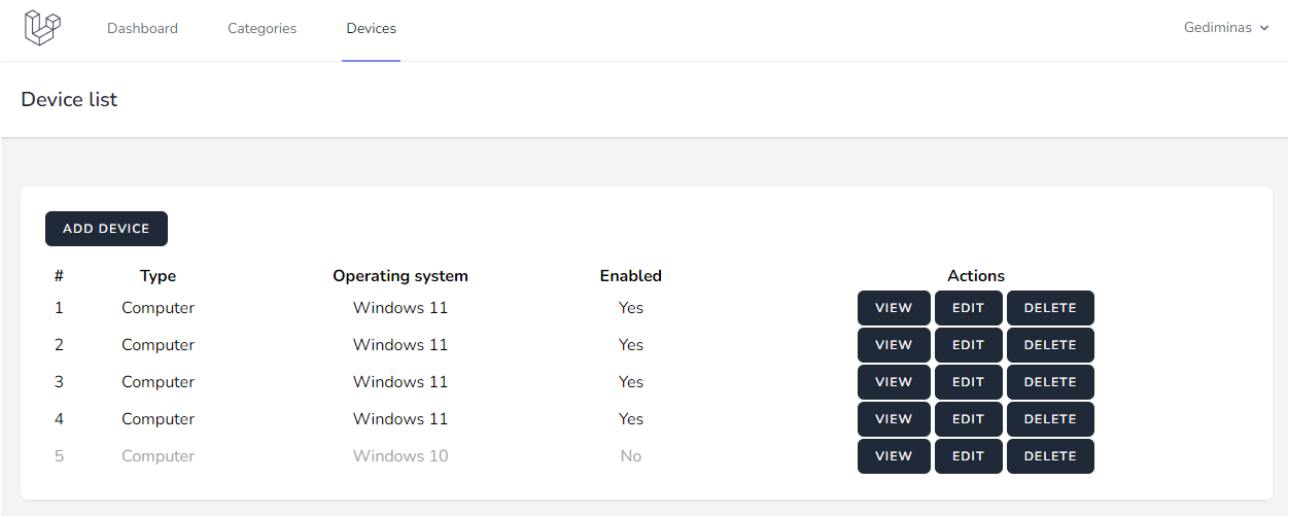
27 pav. Faktoriaus pridėjimo puslapis

Paspaudus ant „Edit“ mygtuko šalia „Bitlocker“ faktoriaus, atsidaro jo redagavimo puslapis (28 pav.). Šis puslapis yra taipogi identiškas kategorijoms ir kriterijams, tačiau sistema yra projektuota su tikslu, jog faktoriai bus surenkami automatiškai, tad jų redaguoti neturėtų prireikti.



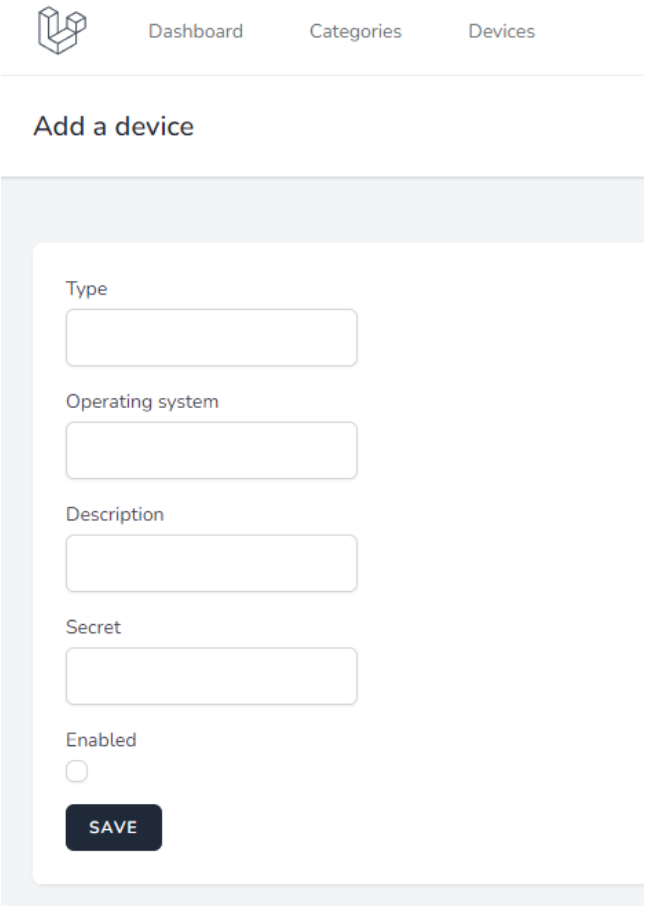
28 pav. Faktoriaus „Bitlocker“ redagavimo puslapis

Kitas konfigūracijos žingsnis yra pridėti įrenginius. Realizacijoje buvo panaudota 4 virtualių kompiuterių struktūra, kurie taip pat matosi įrenginių sąraše (29 pav.). Penktasis, neaktyvus kompiuteris, yra kompiuteris, kuriame buvo kuriama ši sistema.



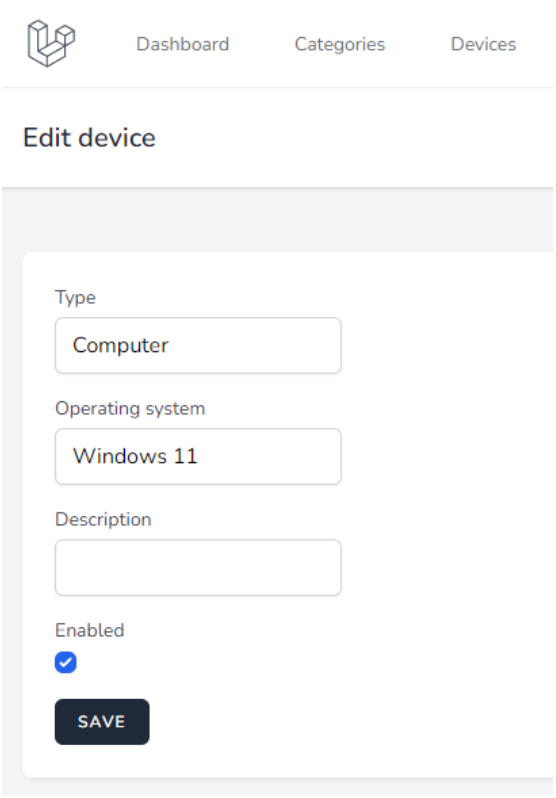
29 pav. Įrenginių sąrašo puslapis

Paspaudus ant mygtuko „Add device“ galima pridėti įrenginį. Šiame puslapyje (30 pav.) privalomi formos laukai yra įrenginio tipas, operacinė sistema ir paslaptis, kuri yra panaudojama agento programinėje įrangoje siunčiant API užklausas iš ir į tą įrenginį. Įrenginio aprašymo laukelis nėra privalomas.



30 pav. Įrenginio pridėjimo puslapis

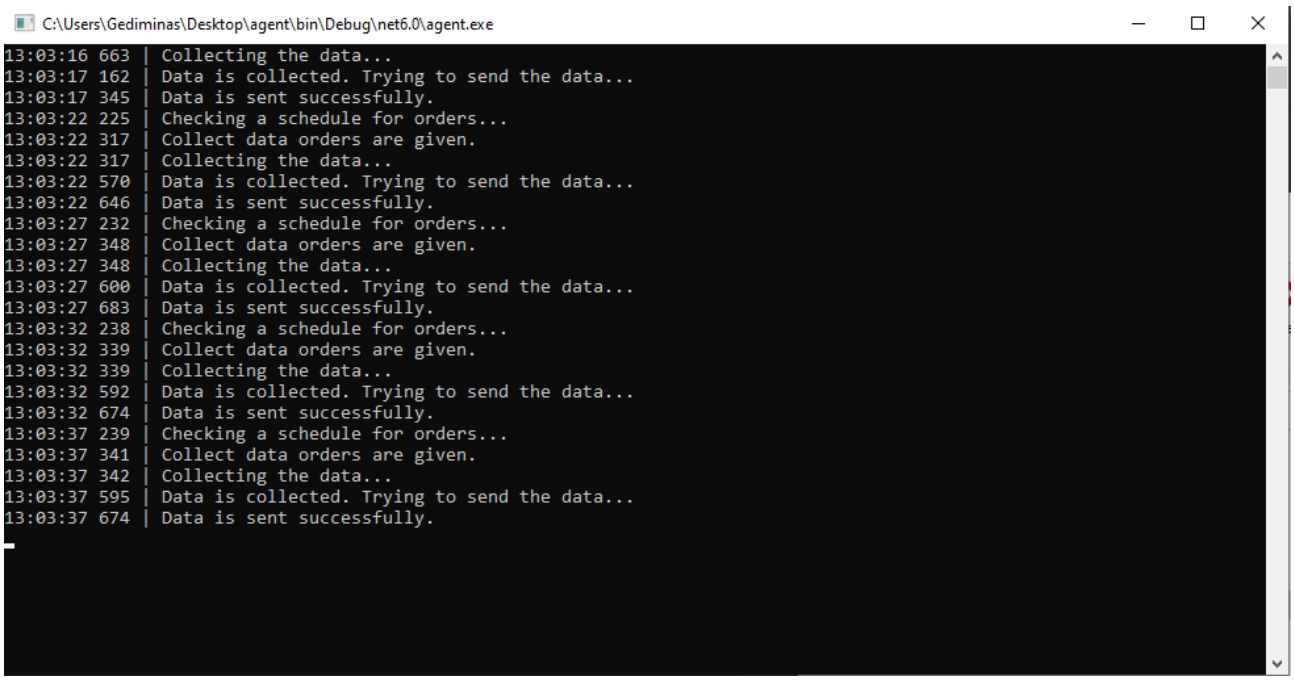
Paspaudus ant „Edit“ mygtuko, galima redaguoti įrenginio informaciją. Šiame puslapyje (31 pav.) yra duoti tokie patys formos laukai kaip ir pridėjimo formoje, tačiau nebegalima keisti paslapties, nes jos keitimas nebeleistų agento programinės įrangos surinktai įrenginio informacijai pasiekti sistemos.



31 pav. Įrenginio redagavimo puslapis

2. Duomenų surinkimas

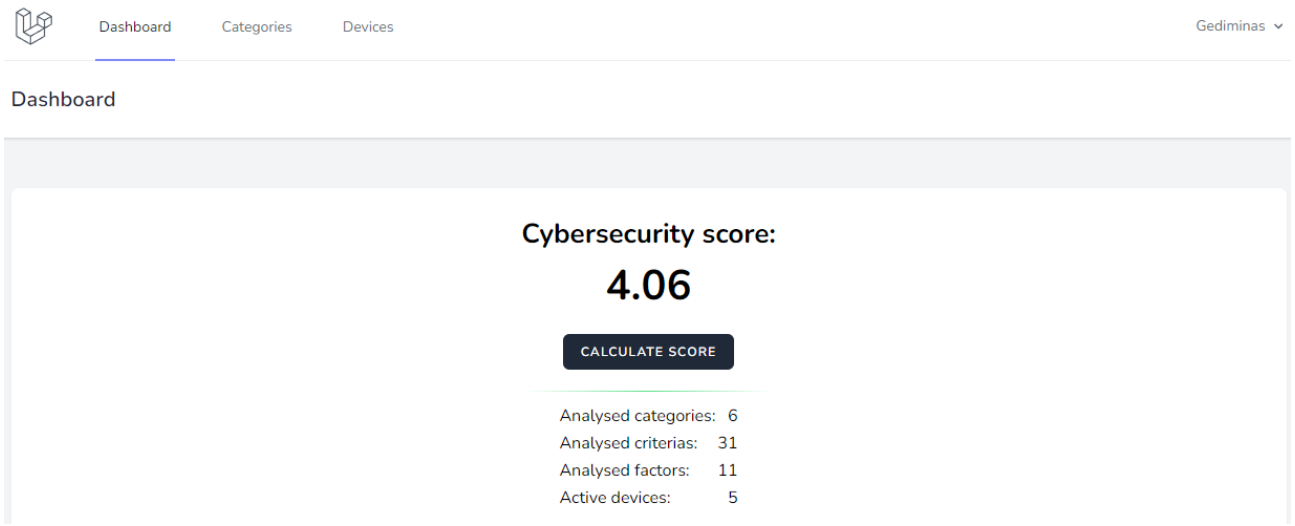
Duomenų surinkime yra naudojama agento tipo programinė įranga, kuri yra įrašoma į kiekvieną įrenginį. Paleidus šią programą yra atidaromas terminalo langas (32 pav.), kuriame yra išvedamas informacinis tekstas apie programos veikimą. Jame galima pamatyti skirtingų tipų žinutes – apie duomenų surinkimą, apie sėkmingai surinktus duomenis ir bandymą siųsti juos į serverį, apie sėkmingai išsiųstus duomenis, apie tvarkaraščio tikrinimą ir apie gautus nurodymus patikrinus tvarkaraštį. Taip pat prie kiekvienos žinutės yra parašomas dabartinis laikas su milisekundžių tikslumu. Šiame terminalo pavyzdyje taip pat galima pastebėti, kad iš karto jį paleidus, buvo siunčiami duomenys (dinamiškumas pagal įvykį) ir vėliau buvo tikrinamas tvarkaraštis (dinamiškumas pagal tvarkaraštį) dėl tolimesnių instrukcijų.



32 pav. Agento programinės įrangos terminalo langas

3. Kibernetinio saugumo reitingo nustatymas

Pagrindiniame puslapyje (33 pav.) yra rodomas įmonės kibernetinio saugumo reitingas. Rodomas ką tik atnaujinta informacija, nes kibernetinio saugumo reitingas yra perskaičiuojamas pagal kategorijas tik atėjus į puslapį. Paspaudus „Calculate score“ mygtuką galima iškviesti užduotį eilėje, kuri atnaujintų reitingą iš pagrindų, tai yra nuo pat faktorių iki kategorijų ir taip būtų pilnai atnaujinta informacija. Tai yra daroma kas puse minutės sistemos fone net ir nepaspaudus mygtuko, jog būtų užtikrinta šviežia informacija.



33 pav. Pagrindinis sistemos puslapis su pavaizduotu kibernetinio saugumo reitingu

3.8. Išvados

1. Realizuota prototipo sistema ir sukurta dirbtinės įmonės infrastruktūra, kurių pagalba yra pavaizduojama dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistema ir jos veikimas.
2. Aprašyta realizuoto prototipo diegimo diagrama ir konfigūracija, kuri yra reikalinga sistemos paleidimui.
3. Realizuota naudojamų API prieigos taškų apsauga remiantis OAuth 2.0 metodologija ir JWT API formatu.

4. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo tyrimas

Šiame skyriuje bus tiriamas dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo panaudojamumas ir veiksmingumas, taip pat tiriamas sukurtas prototipas, jo tikslumas, greitaveika, resursų naudojimas. Taip pat prototipas bus palygintas su panašiais jau egzistuojančiais įrankiais.

4.1. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo tikslumas

Kibernetinio saugumo reitingo tikslumas yra viena svarbiausių charakteristikų kalbant apie jo nustatymo metodo veiksmingumą. Kadangi vienu skaičiumi apsakyti įmonės kibernetinį saugumą yra sudėtinga, tam projektavimo skyriuje buvo aprašyti rezultatų rėžiai, kurie apibūdina įmonės kibernetinį saugumą, kai gautas kibernetinio saugumo reitingas patenka tarp jų. Žinoma, to dažniausiai nepakanka, dėl to buvo įvesti individualūs kintamieji, kurie padeda geriau paaiškinti gautą reitingo reikšmę. Tie kintamieji susideda iš kategorijų, kriterijų ir faktorių abstraktumo mažėjimo tvarka. Kadangi reitingas yra skaičiuojamas remiantis šiais kintamaisiais, jų pagalba galima nusakyti kodėl buvo gautas vienoks ar kitoks kibernetinio saugumo reitingas, kokios yra stipriosios ir silpnosios įmonės kibernetinio saugumo pusės.

Taip pat įtaką tikslumui gali daryti pats duomenų surinkimas, manualinis ir automatinis. Svarbu kad kiekvienas įrenginys turėtų įrašytą agento programinę įrangą, kuri galėtų dalį duomenų surinkti automatiškai. Taip pat, reikėtų nepamiršti atnaujinti informacijos sistemoje rankiniu būdu po atliktų pakeitimų įmonės IT infrastruktūroje, kurie gali daryti įtaką kibernetiniam saugumui.

Vienas iš rekomenduojamų būdų padidinti dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo tikslumą yra pasidaryti įmonės kibernetinio saugumo auditą. Audito metu būtų naudinga įvertinto įmonės kibernetinio saugumo būklę pagal pagrindinius pažeidžiamumo faktorius – atakos paviršių, atakos vektorius, darbo faktorių. Tokiu būdu bus galima taisyklingai sukonfigūruoti sistemą ir palyginti audito gautą rezultatą su sistemos apskaičiuotu kibernetinio saugumo reitingu. Šie veiksmai padės suteikti atitinkamus svorinius parametrus kategorijoms, kriterijams ir faktoriams ir didesnį tikslumą kibernetinio saugumo reitingui.

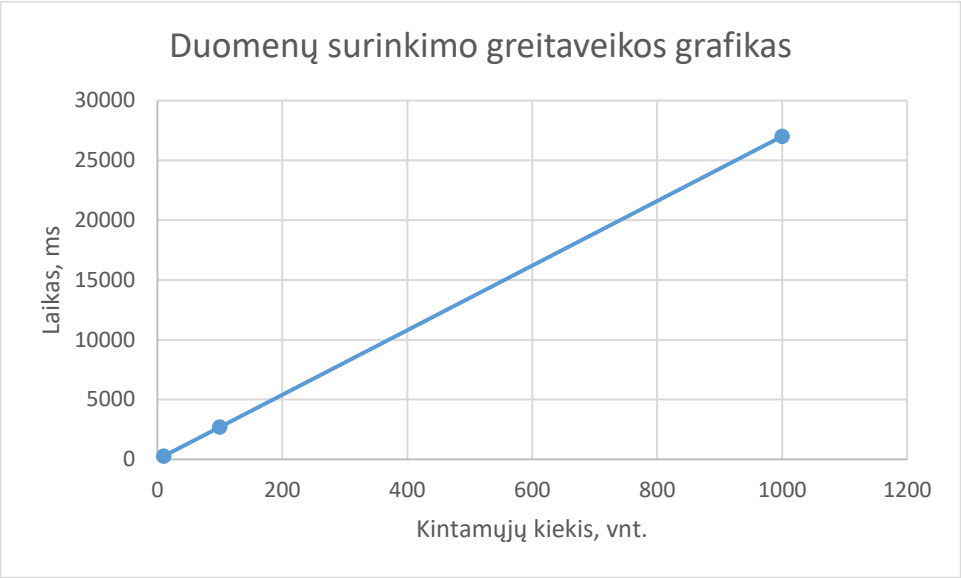
4.2. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo greitaveikos tyrimas

Greitaveika yra viena iš pagrindinių charakteristikų kalbant apie programas. Nagrinėjant šią specifinę sistemą galima greitai pastebėti, jog jos greitaveika yra labai svarbi visame kibernetinio saugumo reitingo nustatymo procese. Greitaveiką šioje sistemoje galime pamatuoti keturiais etapais:

1. Duomenų surinkimas
2. Duomenų persiuntimas
3. Duomenų apdorojimas
4. Reitingo skaičiavimas

Kadangi greitaveika visuose etapuose taipogi priklauso ir nuo įrenginio aparatinės įrangos pajėgumų, todėl bus iš anksto apibrėžta aplinka, kurioje vyks tyrimai. Aktuali ir svarbi aparatinė įranga testuojamame įrenginyje:
Procesorius: „AMD Ryzen 5 3600“ 6 – branduolių
Atmintis: 32 GB DDR4 RAM
Diskas: 1 TB M.2 SSD „ADATA SX6000PNP“

Duomenų surinkimo etape laikas yra tiesiogiai priklausomas nuo surenkamų duomenų – jų tipų, kiekio, iš kur ir kokiu būdu jie yra traukiami. Kadangi duomenų tipas, iš kur ir kokiu būdu jie yra traukiami yra aprašyta realizacijos skyriuje – naudojantis „WMI“ biblioteka ir registrų įrašais, bus tiriama kaip programos greitis skirsis keičiant surenkamų duomenų kiekį. Kadangi tai vėl galės priklausyti nuo individualios įmonės poreikių, tačiau duotas duomenų surinkimo greitaveikos grafikas () turėtų padėti susidaryti bendrą vaizdą kaip plačiai programa gali būti naudojama.



34 pav. Duomenų surinkimo greitaveikos grafikas

Grafikui sudaryti ir išmatuoti duomenų surinkimo greitaveiką buvo taikoma tokia metodologija: duomenų surinkimas išmatuotas su 3 skirtingais kiekiais duomenų – su 10. 100 ir 1000 duomenų kintamųjų. Kiekvienas duomenų kiekis buvo matuojamas 10 kartų ir imamas gautas laiko vidurkis. Gauti rezultatai buvo 274,5 ms su 10 kintamųjų, 697,8 ms su 100 kintamųjų ir 27 s su 1000 kintamųjų. Daugiausia laiko užtrunka WMI klasėje rašomos užklausos, kurios ir sudaro daugiau nei 99% viso laiko. Dažnu atveju WMI klasėje rašoma užklausa ištraukia daugiau informacijos negu reikia, testavimu metu pakartotinai yra inicializuojamos klasės, tai rašomas užklausas tikrai galima optimizuoti ir tai turėtų būti kreipiamas dėmesys, jei įmonė turės daugiau nei 100 kintamųjų. Taip pat galima būtų pasiieškot alternatyvių būdų surinkti informaciją, kuri šiuo metu yra surenkama naudojant WMI biblioteką.

Duomenų persiuntimą šiame tyrime galima ignoruoti, nes testavimas vyksta ant lokalios sistemos, kur nėra jokio žymaus vėlavimo. O siunčiant duomenis į serverį, greitis pagrinde priklausys nuo interneto greičio, kur turint 100 mbps standartinį greitį, duomenys bus greitai nusiunčiami net turint ir 1000 kintamųjų, kadangi jie neužima daug vietos. Saugant 1000 kintamųjų į failą JSON formatu, failo dydis siekia iki 50 KB.

Toliau buvo tiriamas duomenų apdorojimas serveryje. Duomenys patekę į apdorojimo metodą yra sulyginami su egzistuojančiais faktoriais, apdirbami (jeigu reikia) ir išsaugomi. Pamatavus šį laikotarpį, vidutiniškai tai užtrunka tik 20 milisekundžių (0,02 s) naudojant 10 kintamųjų. Šis laikas nesikeistų taip ženkliai net ir padavus daugiau kintamųjų. Vertinant blogiausiu atveju tai užtruktų tiesiškai daugiau nuo naudojamų kintamųjų ir užtruktų 2 sekundes su 1000 kintamųjų. Tačiau

pakartotinai būtų galima išsaugoti naudojamas duomenų bazės užklausas į talpyklas (angl. „cache“), su kuriomis greitis būtų ženkliai padidintas.

Paskutinis greitaveikos testavimo etapas yra pačio kibernetinio saugumo reitingo skaičiavimo laiko matavimas. Kadangi skaičiavime yra naudojamos pagrinde vien vidurkio skaičiavimo funkcijos, laiką labiausiai uždelsia visų kategorijų, kriterijų ir faktorių ištraukimas ir kiekvieno atitinkamai vidurkio apskaičiavimas. Savaime suprantama, kuo daugiau šių kintamųjų, tuo ilgiau užtruks ir galima teigti jog tai būtų tiesinė priklausomybė. Tačiau duomenų bazės užklausų kiekis nesikeičia, keistųsi tik įrašų kiekis (kintamųjų), dėl to greitis daug nesikeis. Dabartiniais duomenimis, su 40 kintamųjų, kurie buvo suvesti ne tik automatiniu, bet ir rankiniu būdu, kibernetinio saugumo reitingo apskaičiavimas užtrunka 100 milisekundžių (0,1 sekundės). Taip pat buvo sukurta fiktyvių kintamųjų, kurie būtų įtraukiami į skaičiavimą. Su 1000 kintamųjų, sistema apskaičiuoja kibernetinio saugumo reitingą per 220 milisekundžių (0,22 sekundės). Taipogi pakartotinai saugant tą pačią informaciją galima naudoti tas pačias talpyklas (angl. „cache“), kurios ženkliai pagreitins apskaičiavimo procesą.

Ištyrus sistemos greitaveiką skirtinguose etapuose, galima pastebėti jog ilgiausiai užtrunka duomenų surinkimas, dėl naudojamos WMI bibliotekos. Kadangi kintamųjų kiekis automatiškai reiškia ir informacijos dydį, su kuria yra dirbama, visų sistemos etapų greitaveika priklauso nuo kintamųjų kiekio tiesine priklausomybe. Bendrai sudėjus, sistema su dabartiniais duomenimis (apie 40 kintamųjų) nuo duomenų surinkimo iki kibernetinio reitingo apskaičiavimo suveikia per 820 milisekundžių (0,82 sekundės), kai tuo tarpu naudojant 1000 kintamųjų suveikia per maždaug 30 sekundžių, iš kurių 27 yra WMI bibliotekos duomenų surinkimas. Žiūrint į bendrą vaizdą, jeigu būtų atliktos minimalios optimizacijos ir pakeista WMI biblioteka, sistema veiktų pakankamai greitai netgi su dideliu kiekiu kintamųjų, kas leistų sistemą naudoti ir toms įmonėms, kurios turi didesnius poreikius.

4.3. Panašių įrankių palyginimas su sukurtu prototipu

Šiame skyrelyje bus palyginti vieni geriausių jau egzistuojančių sprendimų ir jų taikyta metodika su dinaminiu įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipu.

Vienas iš šių sprendimu yra įmonės „ESET“ antivirusinė. Šis produktas yra labiau taikytas didelėms įmonėms, tačiau siūlo tą patį produktą su apribotomis funkcijomis ir žemesne kaina ir smulkesniems verslams. Jų sistema veikia ant trijų operacinių sistemų šeimų, tai yra „Windows“, „macOS“ ir „Android“. Pati kompanija egzistuoja jau daugiau kaip 30 metų. Vieni iš populiariausių sistemos pranašumų rinkoje yra tai, kad jie siūlo patogų ir greitą sistemos diegimą, reikalauja nedidelių sistemos resursų, kad programa veiktų, siūlo techninę pagalbą įvairiomis kalbomis, pagrinde tomis, kuriose šalyse vykdo savo veiklą, tarp jų yra ir lietuvių kalba. Pati antivirusinė siūlo atskirą monitoringo platformą, kurioje galima stebėti visus įrenginius ir naudojamas saugos priemones bei matyti statistiką. Į įmonės kompiuterius yra įrašoma pati antivirusinė programa, kuri skenuoja įrenginį ir siunčią tą informaciją į pagrindinį serverį. Antivirusinė taip pat apsaugo įrenginį nuo potencialių grėsmių, suteikia debesijos paslaugų, pašto ir failų serverių apsaugą. Taip pat yra galimybė papildomai pasinaudoti pilnu disko šifravimu. Šios funkcijos atitinkamai prieinamos skirtingose paslaugų paketuose ir savaime suprantama, kuo paslaugų paketas siūlo daugiau funkcijų, tuo didesnė kaina. Vienas esminių dalykų, šitie pasiūlymai, skirti smulkesniems verslams turi įrenginių limitą, kuriose gali veikti antivirusinė ir leidžia apsaugoti tik 100 arba mažiau įrenginių. Kaina taip pat priklauso ir nuo įrenginių kiekio. Lyginant šią sistemą su sukurta dinaminio įmonės kibernetinio

saugumo reitingo nustatymo sistema, veikimas yra gan panašus, tačiau su kitokiu tikslu. Antivirusinė bando įrenginį apsaugoti ir dirba su pačios nustatytais ir paslaugos teikėjo atnaujinamais grėsmių faktoriais, kurių neleidžia redaguoti. Susidaryti įspūdį apie esančią kibernetinio saugumo situaciją įmonėje galima peržvelgiant monitoringo platformą, kurioje panašiai kaip ir sukurtame prototipe kibernetinis saugumas yra vertinamas kategorijomis, tačiau be konkrečių reitingų.

Dar vienas artimiausias sprendimas yra įmonės „SecurityScorecard“ teikiama įmonių kibernetinio saugumo reitingo nustatymo paslauga. Ši įmonė remiasi dideliais duomenimis (angl. „big data“) ir nuolat tobulina savo kibernetinio saugumo reitingo nustatymo algoritmus. Šiuo metu jie reitingą vertiną pagal 10 modulių, kurie susideda iš tinklo apsaugos, DNS sveikatingumo, saugumo pakeitimų kokybė, prieigos taškų apsauga, IP reputacija, aplikacijų apsauga, administracinių portalų apsaugos konfigūracijos, informacijos ieškojimas įsilaužėlių forumuose, informacijos nutekinimas, socialinė inžinerija. Kiekvienas modulis savyje turi daugiau smulkesnių kintamųjų, pagal ką yra nustatomas reitingas, tačiau tai nėra atskleidžiama viešai. Vienas iš esminių skirtumų lyginant šį sprendimą su kitomis sistemomis, „SecurityScorecard“ stengiasi vertinti įmonės kibernetinio saugumo reitingą tik iš išorės, o ne vidaus. Tai reiškia, kad visi prieinami resursai, kurie gali daryti įtaką reitingui yra prieinami tik iš išorės ir tai nebūtinai yra tikslus įmonės kibernetinio saugumo reitingo nustatymas.

Palyginus minėtų sprendimų teikiamą naudą, galima įvertinti dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos teigiamas ir neigiamas puses.

Visų pirma, tai yra nemokamas, taikytinas į mažas ar vidutinio dydžio įmones. Kibernetinis saugumas šiais laikais kainuoja nemažai ir prieš tai lyginti sprendimai dažniausiai siūlo gan nemažą kainą už padorią kokybę. Tačiau smulkesni verslai ne visada sugeba skirti pakankamai lėšų įsigyjant tokius įrankius, o dideli verslai gali sau leisti nepagailėti pinigų ir reikalui esant naudoti didelį arsenalą įrankių užtikrinant kibernetinį saugumą įmonėje.

Kitas svarbus skirtumas yra suteikiamas lankstumas valdant įrankį. Su šiame darbe aprašyta ir sukurta sistema galima laisvai konfigūruoti praktiškai viską šioje sistemoje ir nuo to gan stipriai priklauso teikiama nauda ir galimi rezultatai. Tai ypač svarbu tokioje sferoje kaip kibernetinis saugumas, nes šiais laikais jo aplinka sparčiai keičiasi, ir vieną dieną svarbūs faktoriai kibernetiniam saugumui gali būti nebe tokie svarbūs kitą dieną bei gali atsirasti naujų grėsmių. Reitingo tikslumas tiesiogiai priklauso nuo kintamųjų, kuriuos galima lengvai keisti pagal savo poreikius. Kad įmonės galėtų geriau pasinaudoti šio darbo sprendimu ir būtų didesnis skaidrumas, kaip viskas veikia, įrankis yra padarytas atvirojo kodo. Kadangi tai yra atvirojo kodo sistema, įmonė naujų reitingo kintamųjų informacijos traukimą gali automatizuoti. Vienintelis reikalavimas įmonei būtų turėti bent vieną atsakingą IT darbuotoją, kuris galėtų naudoti šį įrankį, kadangi tam reikia minimalių kibernetinio saugumo žinių. Lyginant su panašiais sprendimais, jie siūlo iš anksto apibrėžta produktą, kuriame galima įjungti arba išjungti esamas funkcijas. Taipogi trūksta skaidrumo, kaip kibernetinis saugumas yra įvertinamas.

Nors dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistema yra taikyta į nedideles ar vidutinio dydžio įmones, rasti naudos ir ja pasinaudoti gali beveik bet kurio profilio įmonė. Jeigu įmonė turi labai paprastą IT infrastruktūrą, šiuo įrankiu taipogi bus labai lengva naudotis ir bus gaunamas dinaminis įmonės kibernetinio saugumo reitingas. Jeigu įmonė yra labai nišinė ir IT infrastruktūra yra labai sudėtinga, suteikiamas įrankio lankstumas vertinant kibernetinį saugumą turėtų būti pilnai pakankamas.

Ši sistema padeda prižiūrėti esamą kibernetinio saugumo situaciją įmonėje. Pats kibernetinio saugumo reitingas jau iš savęs atlieka šią pareiga, tačiau net jį ir pašalinus, įmonės kibernetinio

saugumo apžvalga pagal kategorijų įvertinimus tai puikiai atlieka. Iš esmės atlikus kibernetinio saugumo auditą įmonėms būna sunku sekti jų situaciją iki kito audito, kaip jie patobulėja per tą laiką ir ar neatsiranda naujų spragų. Tačiau su šia sistema tai padaryti yra gan nesudėtinga dėl įrankio dinamiškumo ir tai leidžia turėti nuolatinę kibernetinio saugumo patikrą. Taipogi, šioje sistemoje įvesta informacija ženkliai palengvins įmonei atliekant kibernetinio saugumo rizikų įvertinimo procedūras ir netgi padės reikaluose su kibernetinio saugumo draudimu.

Dar vienas svarbus pastebėjimas lyginant su kitais sprendimais yra tai, kad ši sistema vertina įmonės kibernetinį saugumą, bet ne riziką ar kitus galimus kibernetinio saugumo parametrus. Kiti sprendimai dažniausiai vertina įmonės kibernetinio saugumo rizikas, tačiau jos neparodo įmonės tikrojo kibernetinio saugumo, nes įmonė gali jau saugotis nuo aprašytų bei nežinomų rizikų.

4.4. Išvados

1. Tyrimo metu buvo atlikta dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo tikslumo kokybinė analizė, kurios metu buvo įvertinta, jog šio metodo tikslumas gali būti labai aukšto lygio, tačiau tam reikia ir atitinkamo išsilavinimo IT žmogaus, kuris sugebėtų naudotis šiuo metodu. Kuo sudėtingesnė įmonės IT infrastruktūra, tuo daugiau žinių ir pastangų reikia įdėti naudojantis šiuo metodu.
2. Tyrimo metu buvo atliktas dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistemos prototipo greitaveikos testas, kuriuo metu buvo ištirti skirtingi sistemos veikimo etapai. Gauti rezultatai rodo, jog sistemos greitaveika yra pakankama naudoti įmonėse, tačiau reikėtų pakeisti „WMI“ biblioteką.
3. Dinaminio įmonės kibernetinio saugumo reitingo nustatymo sistema buvo palyginta su panašiais rinkoje egzistuojančiais sprendimais. Šios analizės metu buvo pastebėta, jog tokia sistema, kuri pasižymi savo lankstumu, atviru kodu, gebėjimu nenutraukiamai stebėti ir vertinti įmonės kibernetinį saugumą turi plačias panaudojimo galimybes ir turėtų savo vertę rinkoje.

Išvados

1. Atlikus probleminės srities analizę buvo nustatyta, jog nei vienas analizuotas kibernetinio saugumo auditavimo ar vertinimo metodas nesuteikia pakankamai lankstumo ar galimybių automatizuoti įmonės kibernetinio saugumo įvertinimo procesą. Dėl to, norint išspręsti šias problemas, reikia kurti naują įmonės kibernetinio saugumo reitingo nustatymo metodą, kuris pasižymėtų savo dinamika ir lankstumu.
2. Sukurtas dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodas, kuris išsprendžia analizėje nagrinėtas problemas. Kad būtų pavaizduotas sukurto metodo veikimas, buvo nuspręsta sukurti sistemą, kuri naudotų šį metodą. Projektuojant sistemą buvo atlikti reikalavimų specifikavimai, apibrėžti funkciniai reikalavimai ir sistemos architektūra.
3. Realizuota prototipo sistema, kuri naudoja sukurtą dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodą. Taip pat buvo sukurta dirbtinė įmonės infrastruktūra, kurios pagalba buvo pavaizduotas ir aprašytas sukurto prototipo veikimas.
4. Atlikti dinaminio įmonės kibernetinio saugumo reitingo nustatymo metodo ir sistemos prototipo tyrimai parodė, jog šio metodo tikslumas ir sistemos greitaveika yra pilnai patenkinama. Taip pat palyginus panašius rinkos sprendimus pastebėta, jog ši sistema padėtų įmonėms įsivertinti savo kibernetinį saugumą ir jos kuriama nauda turėtų savo vertę rinkoje.

Literatūros sąrašas

1. G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadão, I. Yevseyeva, ir V. Basto-Fernandes, „A Comparison of Cybersecurity Risk Analysis Tools“, *Procedia Computer Science*, t. 121, p. 568–575, saus. 2017, nuoroda: http://www.sciencedirect.com/science/article/pii/S1877050917322755 (žiūrėta 2020 m. gruodžio 8 d.).
2. R. Sabillon, J. Serra-Ruiz, V. Cavaller, ir J. Cano, „A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)“, *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, lapkr. 2017, p. 253–259. nuoroda: 10.1109/INCISCOS.2017.20 (žiūrėta 2020 m. gruodžio 8 d.).
3. S. Musman ir A. Turner, „A game theoretic approach to cyber security risk management“, *Journal of Defense Modeling & Simulation*, t. 15, nr. 2, p. 127–146, bal. 2018, nuoroda: https://doi.org/10.1177/1548512917699724 (žiūrėta 2020 m. gruodžio 8 d.).
4. R. Sabillon ir R. Sabillon, „A Practical Model to Perform Comprehensive Cybersecurity Audits“, *Enfoque UTE*, t. 9, nr. 1, p. 127–137, kovo 2018, nuoroda: http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S1390-65422018000100127&lng=en&nrm=iso&tlng=en (žiūrėta 2020 m. gruodžio 8 d.).
5. M. U. Aksu *ir kt.*, „A quantitative CVSS-based cyber security risk assessment methodology for IT systems“, *2017 International Carnahan Conference on Security Technology (ICCST)*, spal. 2017, p. 1–8. nuoroda: 10.1109/CCST.2017.8167819 (žiūrėta 2020 m. gruodžio 8 d.).
6. S. Y. Enoch, M. Ge, J. B. Hong, H. Alzaid, ir D. S. Kim, „A systematic evaluation of cybersecurity metrics for dynamic networks“, *Computer Networks*, t. 144, p. 216–229, spal. 2018, nuoroda: http://www.sciencedirect.com/science/article/pii/S1389128618306285 (žiūrėta 2020 m. gruodžio 8 d.).
7. „CISTAR Cybersecurity Scorecard“. https://hammer.figshare.com/articles/CISTAR_Cybersecurity_Scorecard/11312150/1 (žiūrėta 2020 m. gruodžio 8 d.).
8. W. G. No ir M. A. Vasarhelyi, „Cybersecurity and Continuous Assurance“, *Journal of Emerging Technologies in Accounting*, t. 14, nr. 1, p. 1–12, liep. 2017, nuoroda: https://doi.org/10.2308/jeta-10539 (žiūrėta 2020 m. gruodžio 8 d.).
9. T. Hamid, D. Al-Jumeily, ir J. Mustafina, „Evaluation of the Dynamic Cybersecurity Risk Using the Entropy Weight Method“, *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, ir B. Akhgar, Sud. Cham: Springer International Publishing, 2018, p. 271–287. nuoroda: https://doi.org/10.1007/978-3-319-60137-3_13 (žiūrėta 2020 m. gruodžio 8 d.).
10. M. Evans, L. A. Maglaras, Y. He, ir H. Janicke, „Human behaviour as an aspect of cybersecurity assurance“, *Security and Communication Networks*, t. 9, nr. 17, p. 4667–4679, 2016, nuoroda: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1657 (žiūrėta 2020 m. gruodžio 8 d.).
11. A. A. Ganin *ir kt.*, „Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management“, *Risk Analysis*, t. 40, nr. 1, p. 183–199, 2020, nuoroda: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12891 (žiūrėta 2020 m. gruodžio 8 d.).
12. Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, ir S. Huang, „Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems“, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, t. 46, nr. 10, p. 1429–1444, spal. 2016, nuoroda: 10.1109/TSMC.2015.2503399 (žiūrėta 2020 m. gruodžio 8 d.).

13. K. N. Zakaria, S. H. Othman, ir A. Zainal, „Review of Cybersecurity Audit Management and Execution Approaches“, *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, gruodž. 2019, p. 1–6. nuoroda: 10.1109/ICRIIS48246.2019.9073641 (žiūrėta 2020 m. gruodžio 8 d.).
14. „Risk assessment by dynamic representation of vulnerability, exploitation, and impact“. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/9458/945809/Risk-assessment-by-dynamic-representation-of-vulnerability-exploitation-and-impact/10.1117/12.2177405.full?SSO=1 (žiūrėta 2020 m. gruodžio 8 d.).
15. M. Guarascio, C. A. Brebbia, F. Garzia, ir M. Lombardi, *Safety and Security Studies*. WIT Press, 2018. (žiūrėta 2020 m. gruodžio 8 d.).
16. L. Allodi ir F. Massacci, „Security Events and Vulnerability Data for Cybersecurity Risk Estimation“, *Risk Analysis*, t. 37, nr. 8, p. 1606–1627, 2017, nuoroda: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12864 (žiūrėta 2020 m. gruodžio 8 d.).
17. L. Langer, P. Smith, ir M. Hutle, „Smart grid cybersecurity risk assessment“, *2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*, rugs. 2015, p. 475–482. nuoroda: 10.1109/SEDST.2015.7315255 (žiūrėta 2020 m. gruodžio 8 d.).
18. M. H. T. de Boer, B. J. Bakker, E. Boertjes, M. Wilmer, S. Raaijmakers, ir R. van der Kleij, „Text Mining in Cybersecurity: Exploring Threats and Opportunities“, *Multimodal Technologies and Interaction*, t. 3, nr. 3, Art. nr. 3, rugs. 2019, nuoroda: http://creativecommons.org/licenses/by/3.0/ (žiūrėta 2020 m. gruodžio 8 d.).