KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

Dovilė Krivickaitė

Informacinių technologijų saugos politikų įgyvendinimo audito paramos sistema

Baigiamasis magistro projektas

Vadovas
Prof. Algimantas Venčkauskas

KAUNAS, 2020

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

Informacinių technologijų saugos politikų įgyvendinimo audito paramos sistema

Baigiamasis magistro darbas
Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Prof. Algimantas Venčkauskas
(data)
Recenzentas
(parašas) Doc. Stasys Maciulevičius
(data)

Projektą atliko
(parašas) Dovilė Krivickaitė
(data)

KAUNAS, 2020

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Dovilė Krivickaitė

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga, 6211BX008

(Studijų programos pavadinimas, kodas)

„Informacinių technologijų saugos politikų įgyvendinimo audito paramos sistema“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 ___ m. _____ ____ d.

Kaunas

Patvirtinu, kad mano **Dovilės Krivickaitės** baigiamasis projektas tema „Informacinių technologijų saugos politikų įgyvendinimo audito paramos sistema“ yra parašytas visiškai savarankiškai, o 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)*

Krivickaitė, D. **„Informacinių technologijų saugos politikų įgyvendinimo audito paramos sistema**“. Magistro baigiamasis projektas / vadovas prof. Algimantas Venčkauskas; Kauno technologijos universitetas, informatikos fakultetas, kompiuterių katedra.

Mokslo kryptis ir sritis: informatikos inžinerija, informatikos mokslai.

Reikšminiai žodžiai: automatizuotas, sauga, auditas, politikos formalizavimas, duomenų surinkimas.

Kaunas, 2020. 69 p.

SANTRAUKA

Šio darbo tikslas – suprojektuoti automatizuoto IT saugos audito sprendimą, kuris palengvintų audito atlikimo procedūrą bei pagerintų IT saugumą.

IT infrastruktūros audito atlikimo procesas gali tapti labai sudėtingas, kadangi pačią infrastruktūrą gali sudaryti daug skirtingo tipo įrenginių, iš kurių reikia surinkti informaciją, ją susisteminti, palyginti su turimu saugos politikos dokumentu ir, pagal gautą informaciją, paruošti saugos audito ataskaitą. Net jei kalbama apie sąlyginai nedidelę IT infrastruktūrą, audito atlikimo laikas išsiplečia, kadangi, neturint įdiegto automatizuoto audito atlikimo sprendimo, auditoriui tektų fiziškai nuvykti prie kiekvieno įrenginio, pagal jo tipą nuspręsti, kokiu būdu gauti konfigūracinius duomenis, juos palyginti su turimu saugos politikos dokumentu, kartoti šiuos veiksmus su kiekvienu IT infrastruktūroje esančiu įrenginiu ir tik tada paruošti audito ataskaitą. Dėl šių priežasčių, šiame darbe analizuojami sprendimai, kurie padėtų patobulinti šį procesą.

Krivickaitė, Dovilė. Audit Support System for the Implementation of Information Technology Security Policies: Master‘s thesis in Department of Computer Sciences / supervisor prof. Algimantas Venčkauskas. The Faculty of Informatics, Kaunas University of Technology.

Research area and field: Informatics Engineering, Computing.

Key words: automated, security, audit, policy formalization, data collection.

Kaunas, 2020. 69 p.

SUMMARY

The purpose of this thesis is to provide an automated IT security audit solution which will make an audit procedure easier to perform and will improve IT security.

The process of IT infrastructure audit may be quite complicated. Infrastructure that will be audited may have many different types of devices which need to be inspected to get their configuration information. After information is collected, the auditor needs to organise given data and compare it with security policy document. If company does not use automated security audit system, even quite small IT infrastructure’s audit procedure can waste a lot of valuable time. Auditor needs physically visit every device, according to the type of the device determine, how to get configuration files of said device, compare given data with security policy document and only then prepare the audit report. Because of these following reasons solutions to improve this process will be analysed in this paper.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

CCTA
: angl. Central Computer and Telecommunications Agency – centrinė kompiuterių ir telekomunikacijų Jungtinėje Karalystėje agentūra teikianti kompiuterių ir telekomunikacijų paramą vyriausybės departamentams.

CMM
: angl. Capability Maturity Model – pajėgumų brandos modelis yra metodologija, naudojama tobulinti ir tobulinti organizacijos programinės įrangos kūrimo procesą.

COBIT
: angl. Control Objectives for Information and related Technology – informacinių ir susijusių technologijų kontrolės tikslai, nusakantys bendrųjų IT valdymo procesų rinkinį.

CRAMM
: angl. CCTA Risk Analysis and Management Method – centrinės kompiuterių ir telekomunikacijų agentūros rizikos analizės ir valdymo metodas, naudojamas rizikos valdymui.

CSV
: angl. Comma-separated values – kableliais atskirtos reikšmės. Tai bylų formatas, skirtas saugoti duomenims lentelėse.

cURL
: (angl. client URL) – įrankis, skirtas duomenų perdavimui iš serverio arba į jį be vartotojo sąsajos.

DEA
: angl. Data Envelopment Analisis – duomenų aprėpties analizė. Tai metodas, naudojamas įvertinti gamybos ribas ir empiriškai išmatuoti produktyvų sprendimų priėmimo vienetų efektyvumą.

DMTF
: angl. Distributed Management Task Force – pramonės standartų organizacija, kurianti atvirus taikymo standartus, apimančius įvairias kylančias ir tradicines IT infrastruktūras.

DoS
: angl. Denial-of-service – paskirstyta paslaugos trikdymo ataka.

GDPR
: angl. General Data Protection Regulation – bendrasis duomenų apsaugos reglamentas (BDAR).

GUI
: angl. graphical user interface – grafinė naudotojo sąsaja.

HIPPA
: angl. Health Insurance Portability and Accountability – sveikatos draudimo perkeliamumo ir atskaitomybės įstatymas, kuriame reikalaujama sukurti nacionalinius standartus, siekiant apsaugoti neskelbtiną paciento sveikatos informaciją nuo atskleidimo be paciento sutikimo ar žinių.

HTML
: angl. Hyper text Markup Language – Hiperteksto žymėjimo kalba.

IEC
: angl. International Electrotechnical Commission – tarptautinė elektrotechnikos komisija, rengianti ir skelbianti visų elektrinių, elektroninių ir susijusių technologijų tarptautinius standartus, bendrai vadinamus elektrotechnologijomis.

IMAP

angl. Internet Message Access Protocol – elektroninio pašto serverio protokolas, kuris reglamentuoja elektroninių laiškų laikymą ir tvarkymą serverio kompiuteryje, neatsiunčiant jų į gavėjo kompiuterį.

ISACA

angl. Information Systems Audit and Control Association – tarptautinė informacinių sistemų valdymo ir audito asociacija, orientuota į IT valdymą.

ISO

angl. International Organization Standradization – tarptautinė standartizacijos organizacija, jungianti 164 šalių standartų institutus.

ISVS

Informacijos Saugumo valdymo sistema.

ITIL

angl. Information technology Infrastructure Library – informacinių technologijų infrastruktūros biblioteka, orientuota į darbo optimizavimą bei kokybės užtikrinimą IT įmonėse.

JSON

angl. JavaScript Object Notation – atviro standarto formatas, perduodantis duomenų objektus, sudarytus iš atributo ir reikšmės porų, lengvai skaitomame tekste.

LST

Lietuvos standartizacijos departamento leidžiamų standartų žymuo.

NATO

angl. North Atlantic Treaty Organization – Šiaurės Atlanto Sutarties Organizacija. Tai nepriklausomų suverenių valstybių aljansas, kuriame sprendimai priimami bendru sutarimu – konsensusu.

NIST

angl. National Institute of Standards and Technology – Nacionalinis standartų ir technologijos institutas. Tai fizinių mokslų laboratorija ir JAV prekybos departamento nereglamentuojanti agentūra, kurios misija yra skatinti naujoves ir pramonės konkurencingumą.

PCI DSS

angl. Payment Card Industry Data Security Standard – banko kortelių duomenų apsaugos standartas, taikomas duomenų saugyklų infrastruktūrai.

POP3

angl. Post Office Protocol Version 3 – trečios versijos protokolas, naudojamas elektroninių laiškų gavimui iš serverio.

syslog

žinučių registravimo standartas, kuris suteikia galimybę atskirti programinę įrangą, kuri generuoja pranešimus, sistemą, kuri juos saugo, ir programinę įrangą, kuri juos analizuoja.

SMTP

angl. Simple Mail Transfer Protocol – paprastas pašto perdavimo protokolas. SMTP yra TCP / IP protokolo taikymo sluoksnio dalis, kuris naudoją procesą, vadinamą saugoti ir persiųsti – SMTP perkelia el. paštą tinkluose ir per juos.

SNMP

angl. Simple Network Management Protocol – paprastas tinklo stebėjimo protokolas, skirtas tinkle veikiantiems įrenginiams stebėti ir valdyti.

SPF

angl. Sender Policy Framework – metodas, skirtas kovoti su SPAM laiškų siuntimu.

TCP
angl. Transmission Control Protocol – perdavimo valdymo protokolas, kurio pagalba aplikacijos gali sukurti jungtis tarp viena kitos ir dalintis duomenimis.

TR
angl. technical report – tarptautinės standartizacijos organizacijos teikiamas leidinių tipas, kuriuose aprašomi duomenys, gauti atlikus apklausas, išnagrinėjus informacines ataskaitas ir kt.

UDP
angl. User Data Protocol – TCP/IP perdavimo protokolas, naudojamas norint užmegzti ryšius tarp nedidelių delsos ir nuostolių toleruojančių programų tarp interneto ar programinės įrangos.

USB
angl. Universal Serial Bus – universalioji jungtis, leidžianti kompiuteriui susisiekti su periferiniais ir kitais prietaisais.

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

XML
angl. Extensible Markup Language - bendros paskirties duomenų struktūrų bei jų turinio aprašomoji kalba.

ĮVADAS

Šis darbas priklauso informacijos ir informacinių technologijų saugos studijų programai.

Darbo problematika ir aktualumas

IT infrastruktūros saugos auditas yra vienas iš svarbiausių ir geriausiai atspindinčių IT saugos būseną įmonėje, procesų. Tačiau jį atlikti nėra itin lengva: reikalingas tinkamai paruoštas saugos politikos dokumentas, kuriame apibrėžti saugos objektai ir kaip jie turi būti apsaugoti. Turint šį dokumentą, galima atlikti IT infrastruktūros vertinimą, tačiau tiriant net ir sąlyginai mažą IT infrastruktūrą, duomenų surinkimas jos vertinimui gali būti komplikuotas, kadangi ją sudaro skirtingų tipų įrenginiai, iš kurių informacija turi būti surenkama individualiai.

Dėl šios priežasties buvo nuspręsta apžvelgti automatizuoto IT infrastruktūros audito galimybes bei realizuoti sprendimą, padėsiantį atlikti IT infrastruktūros auditą.

Darbo tikslas ir uždaviniai

Darbo tikslas – sukurti IT saugos politikų įgyvendinimo audito paramos sistemos prototipą, kuris palengvintų IT infrastruktūros saugos audito atlikimo procesą.

Darbo uždaviniai:

- išanalizuoti IT infrastruktūros saugos audito atlikimo problemas ir rasti tinkamiausius būdus joms išspręsti;
- remiantis atlikta analize, suprojektuoti IT saugos politikų įgyvendinimo audito paramos sistemą;
- realizuoti minėtos sistemos prototipą;
- atlikti realizuoto sistemos prototipo tyrimą;
- įvertinti konkrečios įmonės IT infrastruktūros saugą, naudojantis realizuotu prototipu.

Darbo rezultatai ir jų svarba

Darbo atlikimo metu bus suprojektuota automatizuoto IT infrastruktūros saugos audito sistema, kurios pagrindu bus realizuotas prototipas. Naudojantis prototipu bus atliktas konkrečios įmonės IT infrastruktūros saugos auditas ir taip bus įvertinta IT saugos būsena joje.

Darbo struktūra

Šį dokumentą sudaro lentelių bei paveikslų turinys, kuriuose pateikiama dokumente minimų paveikslų ir lentelių informaciją (pavadinimas ir vieta dokumente), terminų ir santrumpų žodynas, kuriame pateikiamos tekste naudojamų terminų ir santrumpų reikšmės bei paaiškinimai. Toliau seka keturi pagrindiniai dokumento skyriai: analizės skyrius, kuriame išanalizuotos IT saugos audito problemos, sistemos projekto skyrius, kuriame aprašoma suprojektuota automatizuoto IT saugos audito sistema, sistemos prototipo skyrius, kuriame aprašoma, kaip buvo realizuotas IT saugos audito sistemos prototipas ir prototipo tyrimo skyrius, kuriame apžvelgiamas prototipo funkcionalumas, gaunamų duomenų kokybė bei įvertinamas konkrečios IT įmonės infrastruktūros saugumas. Dokumento pabaigoje pateikiamas literatūros, kuria buvo naudotasi rašant šį dokumentą, sąrašas, bei priedai.

1. PROBLEMINĖS SRITIES ANALIZĖ

1.1. Analizės tikslas

Tikslas – ištyrus IT infrastuktūros saugos audito problemas, rasti tinkamiausius būdus joms išspręsti ir pritaikyti juos projektuojant IT saugos politikų įgyvendinimo audito paramos sistemą.

1.2. Tyrimo objektas, sritis ir problema

Siekiant užtikrinti informacinių technologijų infrastuktūros saugą yra būtina turėti saugos politiką, kurioje aiškiai būtų apibrėžta kas ir kaip turi būti saugoma. Tačiau vien saugos politikos turėjimas neapsaugo nuo netinkamo naudojimosi informacinių technologijų infrastruktūros mazgais: nors vartotojai yra susipažinę su keliamais saugumo reikalavimais, tai dar nereiškia, kad jie tikrai jų laikysis. Todėl norint įsitinkinti, kad saugos politika veikia tinkamai, būtina pasinaudoti auditoriaus paslaugomis.

Saugos auditoriaus tikslas yra patikrinti ar tai, kas parašyta saugos politikoje, sutampa su veiksmais, kuriuos atlieka vartotojai, ir, atlikus tyrimą, pateikti užsakovui ataskaitą apie informacinių technologijų infrastruktūros būklę. Tačiau net ir vidutinės ar mažos įmonės informacinių technologijų infrastruktūros auditas gali tapti tikru galvos skausmu jei turimoje infrastuktūroje nėra automatizuoto duomenų surinkimo iš visų turimos infrastruktūros mazgų. Negana to, kad jų gali būti labai daug, jų būna ir labai įvairių, ir siekiant patikrinti tą patį saugos politikos punktą visiems įrenginiams, gali atimti labai daug auditoriaus laiko.

Taigi apibendrinant, informacinių technologijų infrastruktūroje yra daug mazgų, iš kurių reikia surinkti informaciją saugos auditui atlikti, tačiau tos informacijos surinkimą būtina automatizuoti sklandesniam auditoriaus darbui.

1.3. IT saugos politika

Viena iš svarbiausių informacijos saugumo kontrolės priemonių yra informacijos saugumo politika. Tačiau šį itin svarbų dokumentą ne visada lengva sukurti. Tai lemia, kad politikos autoriai nagrinėja esamus šaltinius bei remiasi gerosiomis praktikomis. Vienas iš šaltinių yra įvairūs tarptautiniai informacijos saugumo standartai kurie yra pradinis taškas nustatant, kokią informacijos saugumo politiką reikėtų sudaryti. Tačiau nereikėtų pasikliauti vien tik jais – jie nėra išsamūs ir yra linkę daugiau dėmesio skirti procesams, kurių reikia norint sėkmingai įgyvendinti informacijos saugumo politiką. Kur kas svarbiau, kad informacijos saugumo politika atitiktų organizacijos kultūrą, todėl turi būti kuriama atsižvelgiant į tai.

Siekiant užtikrinti efektyvų informacijos saugumo veikimą organizacijoje, yra įvairių kontrolės priemonių ir priemonių, kurios gali būti įgyvendintos ir kurias tikrai reikia įgyvendinti. Šios kontrolės ir priemonės svyruoja nuo techninių sprendimų ir sutartinių reglamentų iki organizacijos supratimo apie esamą riziką, grėsmes ir pažeidžiamumą. Žinoma, išskirtinė šių kontrolės priemonių reikšmė yra informacijos saugumo politika. Informacijos saugumo politika yra informacijos apie organizaciją nukreipimo dokumentas. Tai dokumentas, kuriame nurodomas vadovybės įsipareigojimas ir palaikymas informacijos saugumo srityje, taip pat apibrėžiamas vaidmuo, kurį informacijos saugumas turi atlikti, siekiant ir palaikant organizacijos viziją ir misiją. Iš esmės sakoma, kad informacijos saugumo politika paaiškina informacijos saugumo poreikį ir jo sąvokas visiems organizacijos informacijos išteklių vartotojams. Tai turėtų papildyti organizacijos verslo tikslus ir atspindėti vadovybės norą valdyti organizaciją kontroliuojamu ir saugiu būdu. Tačiau diegiant saugos

sprendimus nereikėtų persistengti, kadangi per didelis noras apsisaugoti gali padaryti daugiau žalos negu naudos. Todėl, remiantis gerosiomis praktikomis, bus aptarti keli galimi saugos politikos punktai ir apžvelgti aspektai, į kuriuos būtina atkreipti dėmesį kuriant saugos politikos dokumentą.

1.3.1. Saugos politikos samprata, sudėtinės dalys ir rengimo tvarka

Informacijos saugos politika – tai aukšto lygio planas, kuriame aprašomi saugos tikslai ir uždaviniai [1]. Politikos dokumente neaprašomos direktyvos, instrukcijos ar kitos valdymo priemonės – jame aprašoma sauga bendrai, taisyklių pavidalu, be specifinių būdų taisyklių laikymuisi užtikrinti. Saugos politikos dokumentas iš esmės reikalingas tam, kad būtų galima užtikrinti kokybišką įmonės procesų valdymą, kuris garantuos nuoseklumą sprendžiant apsaugos klausimus. Taisyklės turi būti aprašytos prieš atsirandant saugumo problemoms, jų probleminė sritis turi būti nuodugniai ištirta įvertinant riziką. Prieš pradedant jas rengti, privalu nustatyti visos saugos politikos dokumento tikslus: reikia aprašyti, ką ir kodėl norima apsaugoti. Tai gali būti aparatinės ar programinės įrangos saugos užtikrinimas, informacijos prieinamumo apsauga, tinklų apsauga ir kt. Dėl paprastesnio taisyklių dokumento naudojimosi, galima išskaidyti jį į kelis atskirus dokumentus. Sukūrus pirminį taisyklių rinkinį, jis turi būti objektyviai įvertinamas ir tik galutinai jas išbaigus ir vadovybei patvirtinus, galima pradėti jas įgyvendinti.

1.3.2. Informacijos saugos objektai, subjektai. Saugos taisyklių turinys

Įmonės procesams įgyvendinti yra reikalinga programinė ir aparatinė įrangos. Taigi kuriant saugos politikos dokumentą, būtina aprašyti, kurias konkrečiai iš šių sistemos dalių reikia apsaugoti. Vienas iš svarbių punktų – sistema turi būti inventorizuota. Inventorizacija, kaip ir informacijos saugos taisyklės, turi apimti ne tik aparatines priemones ir programinę įrangą [1]. Į šį procesą įeina ir dokumentai, aprašantys technologinius įmonės procesus, organizavimo ypatumus bei sričių, kurios gali būti atakuojamos, sąrašas ir informacija apie įmonės personalą.

Kai jau turimas sąrašas išteklių, kuriuos reikia apsaugoti, būtina apsibrėžti nuo ko jie bus saugomi. Iš esmės svarbiausia turimus išteklius apsaugoti nuo nesankcionuotos prieigos, nuo netyčinio informacijos atskleidimo bei nuo programinės įrangos ir vartotojo klaidų. Toliau saugos taisyklėse turi būti aprašyta, kaip bus apsaugoti įmonės turimi duomenys, kad jais nebūtų neleistinai disponuojama. Kaip pavyzdys, į saugos taisykles gali būti įtraukti tokie punktai apie paskirstytos intelektinės nuosavybės apsaugą [1]:

- kompanijos informacijos naudojimas ne dalykiniais tikslais;
- intelektinės nuosavybės naudojimo reikalavimų nustatymas;
- informacijos perdavimas trečiajai šaliai;
- atviros informacijos apsauga.

Saugos taisyklėse taip pat būtina aprašyti atsarginio kopijavimo, archyvavimo ir naikinimo taisykles. Prieš jas aprašant įmonės atsakingi asmenys turėtų nustatyti kai kurias papildomas taisykles, kaip pavyzdžiui, kokius duomenis ir kaip dažnai juos kopijuoti, kur saugoti atsarginę kopiją, kam suteikti prieigą prie atsarginių kopijų ir panašiai. Kitas svarbus aspektas – duomenų naikinimas. Labai svarbu yra aprašyti procedūras, kaip tie duomenys bus naikinami, siekiant užtikrinti, jog sunaikintų duomenų nebus įmanoma atkurti.

1.3.3. Saugumo taisyklių rengimas

Fizinis saugumas

Šių taisyklių aprašymas gali būti vienas lengvesnių, tačiau vis vien būtina paminėti kelis svarbius aspektus. Svarbu nepamiršti įrengti ir saugos taisyklėse aprašyti tinkamų spynų, durų ar kitų užrakinimo prietaisų, kad būtų galima fiziškai apsaugoti išteklius nuo tyčinio ar netyčinio modifikavimo. Taip pat reikėtų nustatyti sąlygas, kurias turi tenkinti turimos įmonės patalpos: pradedant apsauga nuo elektros šuolių ir baigiant oro temperatūra, vesti inventorizacinę įrangos apskaitą, kurios taisyklėse būtų aprašyta visa turima įranga nurodant jos buvimo vietą bei parengti prieigos prie patalpų ar aparatinės įrangos taisykles, kuriose būtų aprašyta, kas ir kokiomis sąlygomis gali prieiti prie išteklių.

Autentifikavimas ir tinklo saugumas

Tinklo sauga apibrėžia santykį tarp informacijos ir tarp tų, kurie ja naudojasi. Pagrindinis prieigos valdymo punktas yra vartotojo autentifikavimas. Tai toks apsaugos būdas, kai pagal vartotojo nustatytas privilegijas yra gaunama atitinkama prieiga prie išteklių ar tinklo. Kalbant apie tinklo saugos taisykles, jose turi būti aprašoma tinklo architektūra ir adresavimas, prieigos prie tinklo valdymas, registracijos ir slaptažodžių sauga.

Interneto saugumas

Šių taisyklių kūrimas yra vienas sudėtingesnių žingsnių, kadangi technologijos vystosi labai greitai ir aprašyti visas naujas technologijas yra labai sunku. Todėl rekomenduojama turimas technologijas suskirstyti į logines grupes pagal jų panaudojimo sritį. Jos galėtų būti tokios [1]:

1. prieiga prie interneto;
2. administravimo pareigos;
3. vartotojų pareigos;
4. taisyklės dirbant žiniatinklyje;
5. virtualūs privatūs tinklai;
6. modemai;
7. atviro rakto infrastruktūros ir kitų kontrolės priemonių taikymas;
8. elektroninė prekyba.

Elektroninio pašto saugumas

Kuriant elektroninio pašto saugumo taisykles, patariama, kad pagrindinės darbo taisyklės ir instrukcijos, kuriomis turi vadovautis vartotojai, pirmiausia būtų surašytos elektroninio pašto saugumo taisyklėse [1]. Saugos taisyklėse svarbu aprašyti, kaip tinkamai administruoti elektroninį paštą: kontroliuoti jo srautą, jį archyvuoti bei skenuoti, apriboti pranešimo dydį, naudoti šifravimą bei skaitmeninį parašą.

Apsauga nuo virusų

Saugos nuo virusų taisyklėse turėtų būti aprašomi reikalavimai visiems įmonės darbuotojams saugoti duomenis. Apibrėžiant apsaugą turėtų būti nurodomas apsaugos metodas, o ne konkretus programinės ar aparatinės įrangos produktas. Taip pat prie reikalavimų turėtų būti apibrėžtas trečiųjų šalių programinės įrangos naudojimas.

1.4. IT saugos audito metodai ir įrankiai

Surinkus duomenis apie informacinių technologijų infrastruktūrą, galima atlikti saugos auditą. Auditas yra įrankių ir veiksmų kompleksas, kuriame be auditoriaus veiksme dalyvauja ir audituojamos įmonės atstovai. Siekiant jį atlikti, rekomenduojama remtis gerosiomis saugos atlikimo praktikomis, kurių vienas iš šaltinių galėtų būti standartai, kuriuose aprašomi įvairūs audito atlikimo modeliai.

1.4.1. IT saugos audito metodai

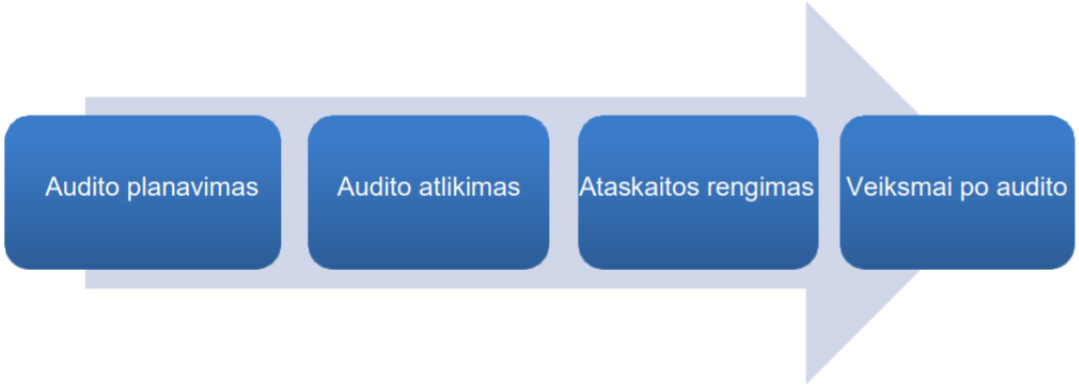
Saugos audito metodus galima skirstyti dviem būdais: pagal audito technikas (rankinis, statinis, dinaminis) arba pagal audituojamas sistemų funkcijas ar dalis (skvarbos, interneto programų ar duomenų bazių). Atliekant auditą pasirinktu metodu jis turėtų gebėti įvertinti vidaus kontrolę, apimančią visus audituojamos infrastruktūros mazgus.

Atliekant auditą nenaudojant automatizuotų priemonių, duomenys renkami kalbinant įmonės darbuotojus, pateikiant jiems įvairius klausimynus žodžiu ar raštu. Visa surinkta informacija yra vertinama auditoriaus sukaupta patirtimi.

Atliekant auditą automatizuotomis priemonėmis yra naudojami įvairūs įrankiai, kurie surenka ir analizuoja duomenis bei paruošia išanalizuotų duomenų ataskaitą. Analizei vykdyti yra naudojamos žiniomis paremtos sistemos, kurios analizuoja duomenis pagal savo turimą žinių bazę.

1.4.2. IT saugos audito procesas

Toliau esančiame 1.1 pav. pavaizduotas saugos audito procesas. Audito planavimo etape surenkama informaciją apie sistemą ir įvertinamos galimos rizikos.



1.1 pav. IT saugos audito procesas [2]

Audito atlikimo etape surenkami rizikų įkalčiai ir įvertinamas informacijos saugumo valdymas, o ataskaitos rengimo žingsnyje aprašomas minėtas vertinimas su įkalčiais. Toliau bus aptartas kiekvienas audito etapas išsamiau.

Audito planavimas

Audito planavimo tikslas yra nustatyti audito tikslus ir jo apimtį. Siekdamas juos nustatyti, auditorius pirmiausia surenka informaciją, susijusią su audito planavimu, per pokalbius ir dokumentų peržiūras. Pavyzdžiui, jei audituojama organizacija turi kritinių žiniatinklio paslaugų, audito tikslas yra apsaugoti paslaugas nuo kenkėjiškų išpuolių, o audito apimtis yra jame veikiančios sistemos, įskaitant tuos, kurie administruoja sistemas. Auditorius apklausia administratorius ir peržiūri internetinių sistemų tinklo schemą. Tada auditorius įvertina riziką remdamasis surinkta informacija. Jei nustatoma tam tikra rizika, auditorius renka daugiau informacijos apie ją. Jei sistemoje randama keletas pažeidžiamų komponentų, auditorius paprašo administratoriaus išsamios informacijos apie komponentus. Surinkus daugiau informacijos gali paaiškėti dar viena rizika.

Būtina pabrėžti, kad planavimas yra vienas svarbesnių saugos audito žingsnių: jei auditorius, kurdamas audito planą, nenustato kritinės rizikos, vėlesniuose etapuose rizika nėra svarstoma, dėl kurios audituojama įmonė gali patirti nuostolių.

Audito atlikimas

Audito metu auditorius renka įrodymus apie riziką, kuri vertinama planuojant, apklausiant daugiau žmonių, peržiūrint išsamius dokumentus ir naudojantis rizikos nustatymo priemonėmis. Auditorius gali tikrinti komponentų parametrų vertes, remdamasis kontroliniais sąrašais, ir vykdo nekenksmingas atakas, kad atskleistų pažeidžiamumą. Šio proceso metu įvertinamas informacijos saugumo valdymas įmonėje.

Surinkti audito įrodymai gali būti skirstomi pagal jų surinkimo būdą. Audito įrodymų rūšių ir įvairių metodų ryšys pavaizduotas 1.1 lentelėje.

1.1 lentelė. Audito įrodymų rūšių ir įvairių metodų ryšys [2]

Audito įrodymai	**Duomenų rinkimo būdai**
Žodiniai audito įrodymai	Interviu. Apklausos, klausimynai. Tikslinės darbo grupės. Kontrolinės grupės.
Dokumentiniai įrodymai	Dokumentų peržiūra. Bylų peržiūra. Esamos statistikos naudojimas. Esamų duomenų bazių naudojimas.
Daiktiniai įrodymai	Žmonių stebėjimas. Objektų ir procesų patikros. Eksperimentai, pavyzdžiui, susiję su kompiuterinių duomenų saugumu.
Analitiniai įrodymai	Pavyzdžiui: kiekybinių duomenų rinkimo metodai; DEA metodas, regresinė analizė; skaičiavimai, palyginimai, informacijos skaidymas į komponentus, racionalūs argumentai.

Auditorius privalo surinkti pakankamai tinkamų audito įrodymų, kad galėtų suformuluoti audito tikslus ir audito klausimus, atitinkančius audito pastebėjimus, išvadas bei pateikti rekomendacijas [2].

Ataskaitos rengimas

Galiausiai, auditorius parengia ataskaitą apie riziką su įrodymais. Kadangi ataskaita naudojama tobulinant informacijos saugumo valdymą, turinys apima tai, kas būtina jai pagerinti. Ataskaitoje pateikiamos ne tik audito išvados, bet ir informacija iš įmonės išorės, pavyzdžiui, informacijos saugumo tendencija.

Surašant audito ataskaitą, labai svarbu, kad audito grupė, priežiūros ir kokybės kontrolės vertintojai kritiškai apsvarstytų išvadas, atsižvelgdami į audito pastebėjimus, įrodymus, duomenis ir kriterijus. Pastebėjimai ir išvados turi būti paremti pakankamais ir tinkamais įrodymais. Jeigu yra pateikiamos rekomendacijos, jos turi būti susietos su pastebėjimais ir išvadomis. Taip pat yra svarbios tinkamos procedūros, skirtos išaiškinimui ir faktų patvirtinimui su audituojamu subjektu [2].

Veiksmai po audito

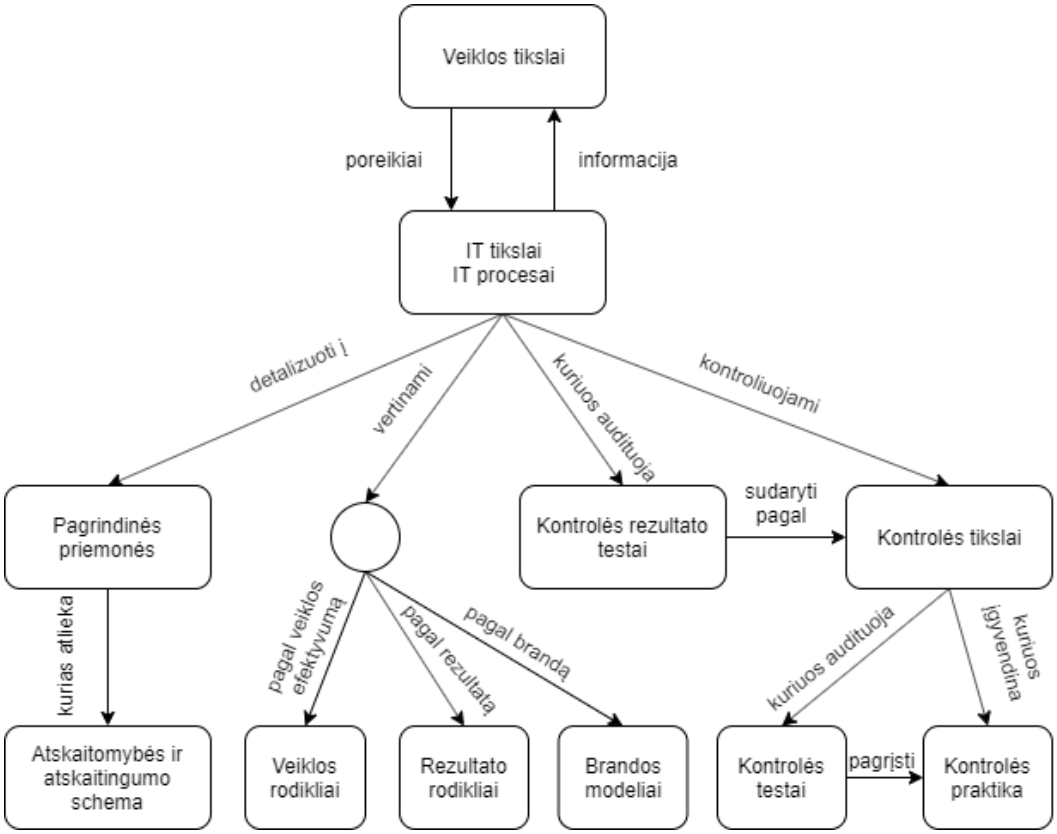
Ataskaitos paskelbimas nėra audito proceso pabaiga. Ją paskelbus, turi būti stebimas audito poveikis audituojamai sistemai. Ataskaitos pagrindinis tikslas yra ištirti būdus, kuriais yra kuriamos ir teikiamos paslaugos bei pateikti rekomendacijų, skirtų pagerinti šias paslaugas ekonomiškumo, efektyvumo ir rezultatyvumo aspektais [2].

1.4.2.1. Standartai, apibrėžiantys informacijos saugą

Siekiant užtikrinti duomenų konfidencialumą, 1997 m. rugsėjo 4 d. nutarimu nr. 952, Lietuvos Respublikos Vyriausybė įdiegė pirmuosius bendruosius duomenų saugos reikalavimus bei nuostatas [3]. Dokumente akcentuojama, kad duomenų valdytojas, formuluodamas specialius duomenų apsaugos priemonių reikalavimus, turėtų remtis ISO 11442, ISO/IEC TR 13335-1 bei ISO/TR 13569 standartais. Nors šis nutarimas jau nebegalioja, jį pakeitęs 2013 m. liepos 24 d. nutarimas nr. 716 vis tiek rekomenduoja remtis standartais: LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, apibūdinančiais saugų elektroninės informacijos tvarkymą [4].

1.4.2.2. COBIT metodika

Paprastesniam ir efektyvesniam standartų naudojimui įmonėse galima diegti metodikas, kuriose naudojami įvairūs, tarpusavyje derantys standartai. Vienas iš pavyzdžių – „COBIT“ instrumentas. COBIT yra ISACA metodika ir gerosios praktikos rinkinys, padedanti organizacijoms siekti IT valdymui ir vadovavimui keliamų tikslų, t. y. sukurti optimalią vertę naudojant IT, išlaikant pusiausvyrą tarp siekiamos naudos, optimalaus rizikos valdymo ir išteklių naudojimo [5]. Ryšiai tarp COBIT komponentų yra pavaizduoti 1.2 pav.



1.2 pav. Ryšiai tarp „Cobit“ komponentų

Naudojant COBIT metodiką ir įmonės struktūrą, lengva nustatyti, kurie iš šių procesų ir kokiu mastu yra svarbūs. Brandos vertinimas grindžiamas CMM modeliu, tik COBIT modelyje kiekvienam procesui labai išsamiai apibūdinami ir paaiškinami įvertinimai. IT valdymo procesų brandos įvertinimas yra nuo 0 iki 5 [6]:

0 – procesų nėra, IT valdymo procesai neegzistuoja.

1 – pradiniai procesai. Vadovybė nežino IT valdymo svarbos. Nėra oficialių procedūrų, informacinių technologijų valdymas ir priežiūra dažniausiai grindžiami individualiai ir nekontroliuojant, o veiksmų imamasi kiekvienu atveju atskirai. Nėra nei standartų, nei įmonės taisyklių, nei įsipareigojimų ar atsakomybės šiuo klausimu. IT valdymas ir jo veiklos vertinimas yra procesai, vykdomi tik IT skyriuje, valdymas yra pasyvus.

2 – pasikartojantys procesai. IT valdymo procesai egzistuoja, tačiau jie nekoordinuojami ir daugiausia inicijuojami IT ar kokio kito operacinio lygio skyriaus. Dažnai atsitinka, kad daugelis žmonių atlieka tą pačią užduotį (pareigų atskyrimo klausimas); nėra sistemos priežiūros, koordinavimo ar standartizuotų procedūrų. Atsakomybė paliekama pavieniams asmenims; įmonės politika neegzistuoja arba nėra pateikiama darbuotojams.

3 – apibrėžti procesai. IT valdymo procedūros yra aprašytos ir dokumentuojamos bei nuolat tobulinamos oficialių mokymų metu. Nors formaliai procedūros ir bendros taisyklės egzistuoja, jos

nėra modernios ar pritaikytos įmonės verslo specifikai ir atspindi tik esamų procedūrų įforminimą. Nepaisant to, kad yra procedūrų, už kurių vykdymą atsakingi konkretūs asmenys, nėra sistemos priežiūros, taigi, mažai tikėtina, kad pavyks nustatyti šio klausimo anomalijas.

4 – valdomi procesai. Išskyrus įmonės politiką ir procedūras, yra galimybė nuolat stebėti procesų vykdymą, įvertinti jų efektyvumą ir atlikti reikiamus pataisymus atsižvelgiant į poreikius. Procesai ir veikla nuolat tobulinami. Nustatomi labai sudėtingi IT valdymo tikslai, glaudžiai suderinti su verslo tikslais. Matuojant veiklos rezultatus ir atliekant IT auditą, naudojami patvirtinti metodai ir sistemos (COBIT, ITIL ir kt.).

5 – optimizuoti procesai. IT valdymo procesai atliekami optimaliame lygyje. IT, kaip verslo funkcijos, našumas ir efektyvumas yra nuolat matuojamas, o rezultatai lyginami su gerosiomis praktikomis ir kitomis organizacijomis. Taikomas visiškas IT valdymo principų skaidrumas. Įmonės vadovai faktiškai prižiūri informacines technologijas, naudodamiesi daugybe oficialių mechanizmų. Informacinės technologijos yra naudojamos strateginiam tikslui pasiekti, nes pagrindiniai verslo šaltiniai ir informacinė veikla (investicijos, projektai, rizika ir kt.) yra optimaliai veikianti ir atitinka realius verslo prioritetus.

1.4.2.3. Tarptautinės standartizacijos organizacijos (ISO) standartai

ISO/IEC 27000 serijos standartai dar vadinami ISVS šeimos standartais. Juose aprašomos rekomendacijos, kurios yra sudarytos remiantis geriausiomis ISVS praktikomis [7]. Šie standartai yra plačios apimties bei gali būti taikomi įvairioms organizacijoms.

Šiuo metu ISO/IEC 27000 seriją sudaro šeši viešai publikuojami standartai:

- ISO/IEC 27000 – ISVS apžvalga ir žodynas. Šis standartas apibūdina ISVS valdymą, rekomendacijos panašios į kituose ISO standartuose esančias, pavyzdžiui, ISO 9000 ir ISO 14000.
- ISO/IEC 27001 – ISVS reikalavimai. ISO/IEC 27001 aprašo valdymo sistemą, skirtą informacijos saugumui valdyti, ir pateikia konkrečius reikalavimus. Įmones, kurios atitinka reikalavimus, gali sertifikuoti akredituota sertifikavimo įstaiga, sėkmingai atlikusi auditą.
- ISO/IEC 27002 – informacijos saugos valdymo praktikų rinkinys. ISO/IEC 27002 pateikia geriausių praktikų rekomendacijas dėl informacijos saugumo kontrolės, skirtos naudoti tiems, kurie atsakingi už informacijos saugumo valdymo sistemų inicijavimą, įgyvendinimą ar priežiūrą.
- ISO/IEC 27003 – ISVS įgyvendinimo gairės. Standarte orientuojamasi į kritinius aspektus būtinus sėkmingam ISVS sukūrimui ir įgyvendinimui.
- ISO/IEC 27004 – informacijos saugos valdymo priemonės. Šiame standarte aprašoma, kaip reikėtų įvertinti ISVS efektyvumą.
- ISO/IEC 27005 – informacijos saugos incidentų valdymas. Šis standartas aprašo informacijos rizikų vertinimo ir valdymo metodus bei yra labai naudingas ISO 27001 planavimo fazėje.
- ISO/IEC 27006 – reikalavimai organizacijoms, atliekančioms auditą bei sertifikuojančioms informacijos saugos valdymo sistemas.

1.4.3. IT saugos audito įrankiai

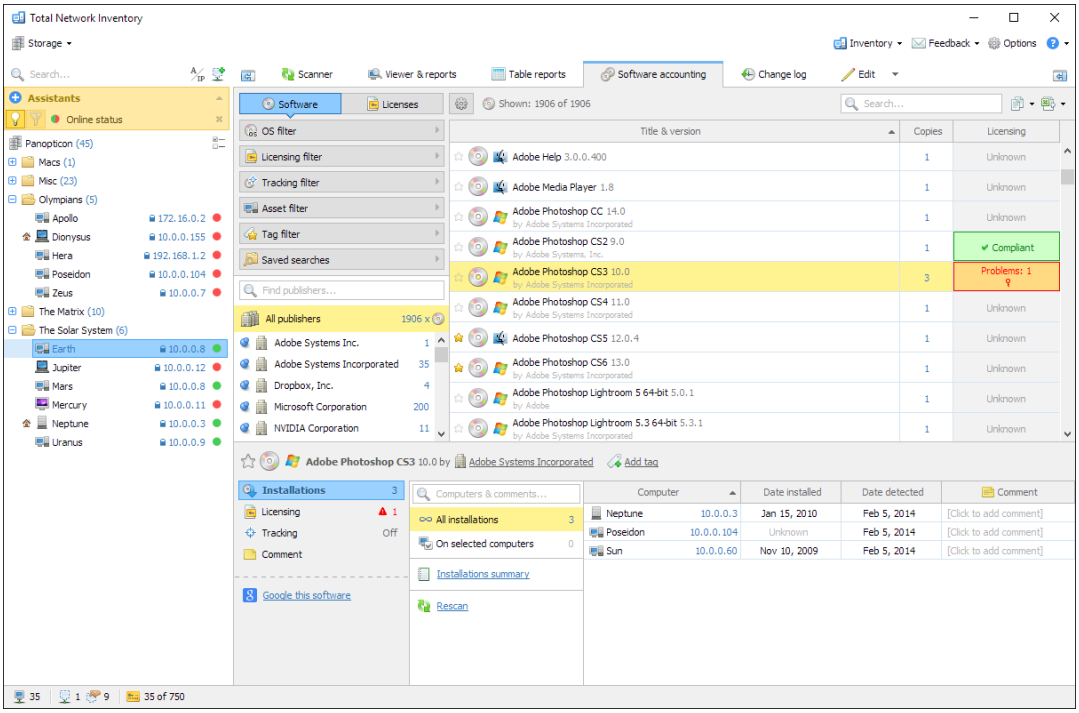
1.4.3.1. „Risk Watch“ rizikų valdymo sistema

„Risk Watch“ yra rizikos valdymo ir atitikties tikrinimo įrankis, kuriame pagrindinis dėmesys skiriamas fiziniam bei kibernetiniam saugumui ir saugos politikos atitikčiai nustatyti. Įrankis turi nemažai automatizacijos funkcijų tam, kad audito atlikimas užtruktų trumpiau: auditoriai prietaisų skydelyje gali matyti informaciją realiu laiku, kurti audito ataskaitas ar bendrauti su darbuotojais elektroninėmis žinutėmis [8].

Naudojant šią sistemą pirmiausia reikėtų apsibrėžti punktus, kurie bus vertinami, o tada – pasirinkti klausimus, kurie bus vertinime. Įrankis taip pat siūlo integraciją su daugiau nei 35 įvairiais dokumentais, tokiais kaip NIST, HIPPA ar ISO, tad klausimus galima pasirinkti ir pagal naudojamą standartą ar dokumentą [9]. Paskutinis žingsnis, kurį reikia atlikti – įvykdyti patį auditą. Įrankis leidžia duomenis surinkti iš vartotojų automatizuotai ir neprisijungus prie tinklo. Atlikus vertinimą iš karto yra pasiūlomas problemos sprendimas: auditoriui pateikiamas sąrašas, ką galima atlikti, kad būtų pagerinta esama situacija. Šitokiu būdu ši programinė įranga padeda nustatyti valdymo klaidas bei didelę turto riziką. Tačiau pats auditas atliekamas klausimyno pagrindu, todėl gauti tikslią IT infrastruktūros mazgų informaciją, kaip pavyzdžiui įdiegtų programų ar prieigos kontrolės sąrašai, nėra įmanoma.

1.4.3.2. „PC system audit“ įrankis

Šis įrankis yra skirtas atlikti sistemos auditą vietiniame tinkle. Jo pagalba galima surinkti tinklo saugos, kompiuterinės įrangos bei jose esančios programinės įrangos informaciją iš skirtingų tipų įrenginių. Įrankis taip pat aptinka licencijų problemas ir suteikia galimybę peržiūrėti išsamią audito įrenginių informaciją. [10]. Duomenys, kuriuos galima gauti naudojantis šia programine įranga, pavaizduoti 1.3 pav.



1.3 pav. „PC system audit“ programos gaunamos informacijos pavyzdys

Vienas iš pagrindinių šios programinės įrangos pliusų – automatinis įrenginių tinkle aptikimas. Tokiu būdu nereikia programinės įrangos diegti atskiruose mazguose: atliekant auditą

skenuojamas visas tinklas ir duomenys surenkami iš aktyvių įrenginių. Tačiau gaunama informacija yra gana ribota saugos audito požiūriu: įrankis surenka įdiegtos programinės įrangos informaciją ir aparatinės įrangos komponentų informaciją.

1.4.3.3. „CRAMM“ rizikos valdymo metodas ir įrankis

„CRAMM“ yra rizikos analizės metodas, kurį sukūrė Didžiosios Britanijos vyriausybinė organizacija CCTA. Tuo pačiu pavadinimu pavadintas ir įrankis, skirtas atlikti analizę šiuo metodu. [11]

Analizė šiuo metodu susideda iš trijų dalių, kurių kiekviena paremta objektyviais klausimynais ir gairėmis. Pirmųjų dviejų etapų pagalba nustatoma ir analizuojama sistemos rizika, o trečiajame – pateikiamos rekomendacijos, kaip reikėtų valdyti šią riziką [12]. Detalesnis jų aprašymas pateikiamas 1.2 lent.

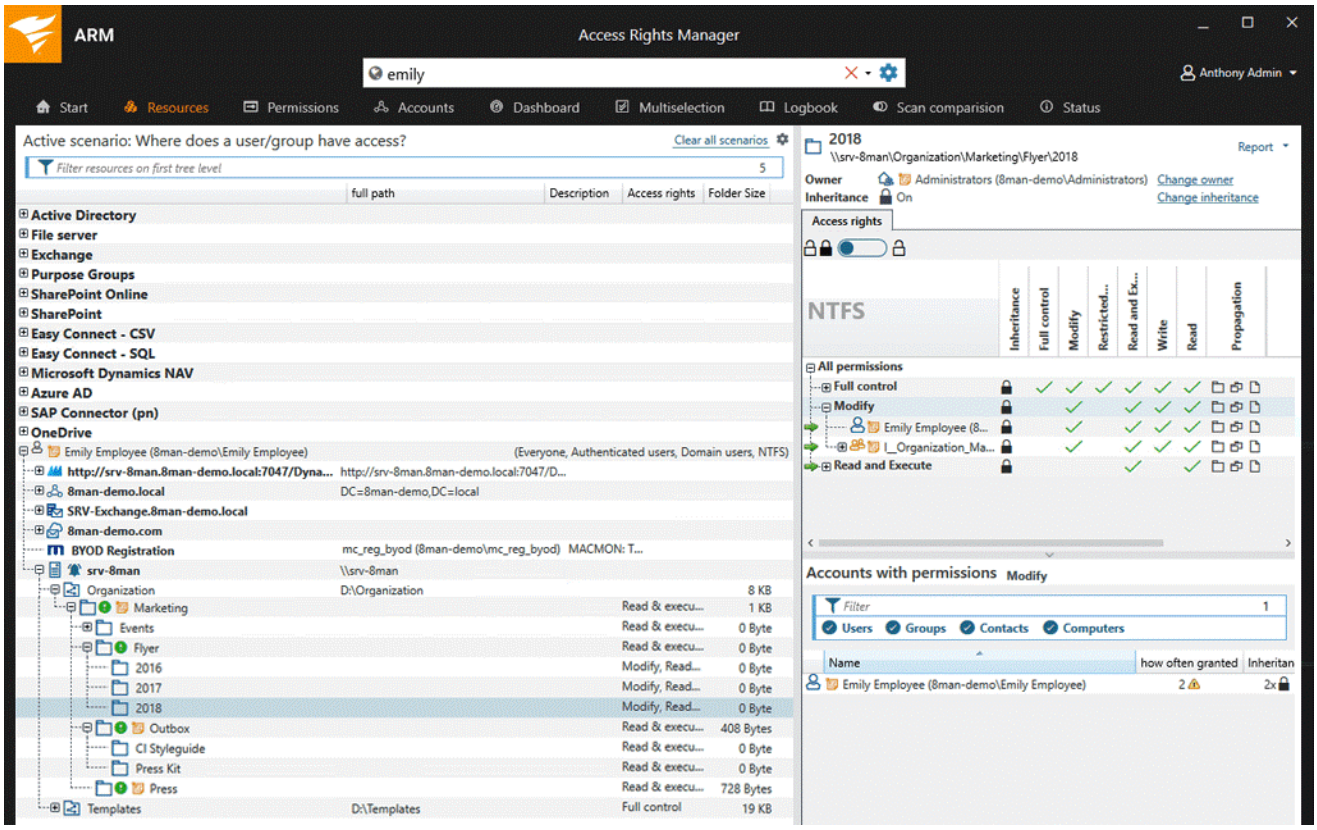
1.2 lent. Rizikos analizės, atliekamos „CRAMM“ metodu, etapai

Pirmasis etapas Saugumo tikslų nustatymas	Rizikos vertinimo ribų apibrėžimas.
	Fizinio turto, kuris yra sistemos dalis, nustatymas ir vertinimas.
	Duomenų, kuriuos turi vartotojai, vertės ir galimo poveikio verslui, kurį gali sukelti neprieinamumas, sunaikinimas, atskleidimas ar pakeitimas, nustatymas.
	Programinės įrangos, kuri yra sistemos dalis, nustatymas ir vertinimas.
Antrasis etapas Siūlomos sistemos rizikos ir saugumo reikalavimų vertinimas	Grėsmių, galinčių turėti įtakos sistemai, tipo ir lygio nustatymas ir įvertinimas.
	Sistemos pažeidžiamumą nustatytoms grėsmėms įvertinimas.
	Griežtumo ir pažeidžiamumo vertinimų derinimas su turto vertėmis, apskaičiuojant rizikos rodiklius.
Trečiasis etapas Atsakomųjų priemonių, kurios būtų proporcingos 2 etape apskaičiuotoms rizikos priemonėms, identifikavimas ir parinkimas	CRAMM turi didelę atsakomųjų priemonių biblioteką, susidedančią iš daugiau nei 3000 išsamių atsakomųjų priemonių, suskirstytų į daugiau nei septyniasdešimt loginių grupių.

Šis metodas ypač tinka didelėms organizacijoms – jį naudoja NATO, Danijos karinės pajėgos, „Unisys“ ir kitos. Pats įrankis turi įvairius skirtingus modulius, kurie suskirstyti pagal standartų reikalavimus. Saugos politikos atitikmens punktas randamas BS 7799 modulyje, tad jis ir galėtų būti naudojamas IT saugos audito atlikimui. Šiame įrankyje randamas didelis kiekis parengtų klausimynų, kurių pagalba galima atlikti automatizuotą saugos auditą, tačiau automatinio duomenų surinkimo iš IT infrastruktūros įrenginių įrankis nepalaiko.

1.4.3.4. „Solarwinds Access Rights Manager“ įrankis

Šis įrankis sukurtas padėti IT saugos administratoriams laikytis norminių reikalavimų, tokių kaip GDPR, PCI DSS ir HIPPA. Jis suteikia galimybę analizuoti vartotojo autorizacijos ir prieigos prie sistemų, duomenų ir failų leidimus. Įrankyje pateikiamas išsamus vaizdas apie vartotojų prieigas prie aktyvaus katalogo (*angl. active directory*), mainų taško (*angl. exchange share point*) ir failų serverių [13]. Taip pat jis automatiškai dokumentuoja atliktus veiksmus, kurie pasitarnauja atliekant sistemų auditą.

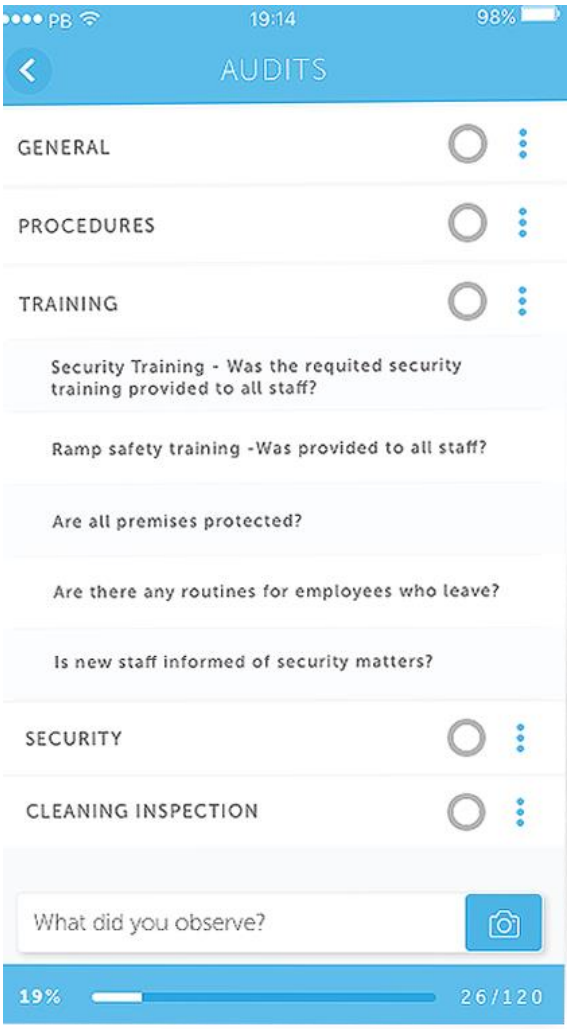


1.4 pav. Prieigos kontrolės sąrašo valdymo langas „Solarwinds Access Rights Manager“ įrankyje

Tačiau įrankis nepritaikytas platesniam duomenų, tokių kaip įdiegtos programinės įrangos, gavimui. Taip pat įrankis neatlieka audito remiantis saugos politikos dokumentu, tad norint naudoti jį IT saugos auditui atlikti, jis turėtų būti derinamas su kitais įrankiais.

1.4.3.5. „audits.io“ sistema

„Plan Brothers“ įmonės sukurtas produktas „audits.io“ skirtas atlikti automatizuotam auditui klausimynų pagrindu [14]. Šiame įrankyje, atliekant auditą, galima naudotis jau sukurtais klausimynų šablonais, arba susikurti savo klausimyną. Klausimyno pavyzdys pateiktas 1.5 pav.



1.5 pav. „audits.io“ įrankio klausimyno pavyzdys

Kadangi šis įrankis auditą atlieka klausimyno pagrindu, nėra galimybės gauti konkrečios IT infrastruktūros mazgų informacijos, tačiau jame įrankyje pateikiamos išsami audito ataskaitos, kurios skirstomos pagal audito atlikimo vietą.

1.5. IT saugos politikos įgyvendinimo audito automatizavimas

Viena iš svarbiausių audito atlikimo dalių – duomenų surinkimas. Jie gali būti renkami neautomatizuotu būdu – atliekant pokalbius su įmonės darbuotojais, paprašant jų atlikti paruoštas apklausas, analizuojant įvairius įmonės dokumentus ir kt., arba automatizuotu būdu – naudojant įrankius, kurie ženkliai palengvina auditoriaus darbą ir sumažina audito atlikimo laiką. Didelė tikimybė, kad vieno įrankio nepakaks, nes ir pats saugos auditas apima daug skirtingų informacinės technologijos saugos sričių, kaip, pavyzdžiui, tinklo sauga, duomenų prieigos sauga, įrangos sauga ir pan.

Žurnalų duomenys yra neįkainojami įsilaužimo aptikimui ir saugumo analizei. Žurnalizavimo paslaugos suteikia apsaugą žurnalų duomenims, kuriuose yra vertingos informacijos apie sistemas,

tinklus ir programas. Žurnalų duomenų rinkimas yra atskaitomybės ir audito paslaugų pagrindas [15]. Duomenų rinkimo metodai leidžia įrašyti vartotojo veiklą, sekti bandymus atlikti autentifikavimą ir kitus saugos įvykius. Dėl didėjančio grėsmių tinklams ir sistemoms, padidėja saugos žurnalų skaičius. Taigi žurnalų valdymas yra gyvybiškai svarbi organizacijos tinklo valdymo ir sistemos administravimo dalis. Tačiau daugelis įmonių, dirbančių paskirstytoje aplinkoje, susiduria su šiomis problemomis: žurnalo generavimas ir saugojimas, žurnalo apsauga ir žurnalo analizė. Kita problema yra užtikrinti, kad saugumo, sistemos ir tinklo administratoriai veiksmingai analizuotų žurnalo duomenis [16]. Saugos žurnalo valdymas yra būtinas norint įterpti įvykių sekimo teiginius, kurie duos reikiamų rezultatų. Šiuolaikinės programos atsekamumui naudoja tokius registravimo sprendimus kaip „NLog“, „C# Logger“ ar kt. Audito žurnalas turi būti apsaugotas nuo neteisėtų subjektų, o visi su saugumu susiję įvykiai turi būti užregistruoti [17]. Žurnalo įvykiai turėtų būti siunčiami saugiu ryšiu ir pažymėti unikalia tapatybe. Taigi, jei žurnalo įvykiai yra saugomi tinkamai, jie gali pasitarnauti atliekant IT saugos auditą.

Vienas iš galimų audito sistemos modelių aprašytas Olof Söderström ir Esmiralda Moradian straipsnyje [18]. Tokią sistemą sudaro vienas centralizuotas serveris, esantis saugioje vietoje, sujungtas su vidinėmis palaikomos sistemos tinklo dalimis. Audito duomenims rinkti naudojami „syslog“ ir paprastojo tinklo valdymo protokolas SNMP. Agentai gali būti įdiegti į „Microsoft“ įrangą ar kitus produktus, nepalaikančius „syslog“ ir (arba) SNMP protokolo. Agentai skaito vietinius konfigūracinius failus ir perduoda informaciją pagrindiniam serveriui. Saugumo audito žurnalai taip pat gali būti perduoti tinklu į sistemą naudojant standartinį UDP protokolą, „syslog“ protokolą arba naujesnį perdavimo TCP protokolo ekvivalentą. Tokiu būdu sistema renka informaciją iš visų tipų klientų, serverių, ugniasienių ir tinklo įrangos. Be to, serveris gali aptikti prižiūrimo tinklo mazgų ir tinklo įrangos įjungimą ir išjungimą, t. y. tinklą, iš kurio renkama informacija. Sistema suprojektuota taip, kad ji galėtų veikti dviem režimais – tinklo ir saugumo. Tinkliniu režimu sistema veiktų kaip serveris, prijungtas prie tinklo. Be to, galima turėti ir alternatyvią konfigūraciją, t. y. savarankišką klientą ir vykdyti atskirą analizės klientą. Atskiros konfigūracijos pranašumas yra papildoma apsauga, kurią kliento sistema gauna, nebūdama prijungta prie tinklo. Autonominis klientas gali būti naudojamas analizuoti audito žurnalus iš daugiau nei vienos sistemos. Tačiau problema yra ta, kad visi saugumo audito įvykiai turi būti rankiniu būdu perkeliami į sistemą. Be to, aliarmo ir įspėjimo funkcijos neveiks taip, kaip numatyta, ir yra rekomenduojama jas išjungti.

Antrasis režimas, kuris yra saugos režimas, yra skirtas dviejų kategorijų vartotojams: super administratorius „root“ ir rankiniu būdu pridedamos paskyros, skirtos naudoti saugumo administratoriams. Šiems vartotojams suteikiamos privilegijos yra panašios į „root“ vartotojo, tačiau jie susieti su konkrečiais asmenimis. Saugumo požiūriu sistema veikia „aukšto lygio sistemos“ saugumo režimu, o tai reiškia, kad visiems vartotojams, naudojantiems sistemą, turi būti suteiktas saugumo patikimumas, kuris yra lygus ar didesnis už joje esančios informacijos saugumo klasifikaciją.

Serveris projektuojamas ir diegiamas su dviejų administravimo vartotojų abonementų tipų sistemos administratoriumi „sysadmin“ ir saugos administratoriumi „secadmin“, kaip priemonėmis atskirti vartotojams reikalingus dalykus. „Sysadmin“ administruoja sistemą, o „secadmin“ tvarko saugos žurnalus. Sistemai palaikyti kuriami keli kompiuterio/demono (*angl. daemon*) vartotojai, siekiant sumažinti pagrindinės paskyros poreikį. Tai apima duomenų bazės apibrėžimą, kur tam tikroms vartotojų grupėms suteikiama atskira prieiga atsižvelgiant į jų naudojimą.

Tokiu būdu suprojektuota sistema yra lanksti, ji turi galimybę išplėsti funkcionalumą, naudojant papildomą analizės programinę įrangą ir palaikyti skirtingo tipo vartotojus. Be to, tokia sistema leidžia integruoti siūlomą funkcionalumą su esamais įrankiais, atsižvelgiant į analitikų poreikį.

Atvirojo kodo programinės įrangos naudojimas leidžia įgyvendinti skaidrumą, paprastumą, užkirsti kelią daugybei saugumo spragų.

1.6. Darbo tikslas, uždaviniai, planas ir siekiami privalumai

Šio darbo tikslas – remiantis išanalizuotomis IT saugos audito problemomis ir jų sprendimo būdais, suprojektuoti IT saugos audito sistemą, kuri palengvintų saugos audito atlikimo procesą. Darbo uždaviniai:

- suprojektuoti sprendimą saugos politikos formalizavimui;
- suprojektuoti sprendimą audito mazgų duomenims surinkti;
- suprojektuoti sprendimą, kuris atliktu pačią audito procedūrą, t. y. palygintų saugos politikos dokumentą su surinktais mazgų duomenimis.

1.7. Siekiamo sprendimo apibrėžimas

Siekiama suprojektuoti tokią sistemą, kuri leistų auditoriui išspręsti audito atlikimo problemas, susijusias su IT infrastruktūros mazgų informacijos surinkimu bei jų palyginimu su įmonės saugos politikos dokumentu.

1.8. Analizės išvados

Tam, kad būtų užtikrinta informacinių technologijų infrastruktūros sauga, yra svarbu atlikti jos auditą. Jo vykdymui privalu turėti saugos politikos dokumentą, kuriuo yra remiamasi atliekant saugos vertinimą. Šis dokumentas padeda užtikrinti kokybišką įmonės procesų valdymą, kadangi informacija jame pateikiama taisyklių pavidalu. Saugos politikos dokumente apibrėžiami ne tik procesai, kaip turi būti vykdoma sauga, tačiau pateikiami ir saugos objektai. Rengiant saugos politikos taisykles yra svarbu apgalvoti ir aprašyti visas galimas saugumo spragas.

Saugos auditas, pagal atlikimo tipą, skirstomas į rankinį ir automatinį. Atliekant IT infrastruktūros auditą rankiniu būdu, procesas yra apsunkintas, kadangi šaltinių, iš kurių reikia surinkti informaciją, yra labai daug. Todėl dėl didelių duomenų kiekių, IT infrastruktūros saugos vertinimui rekomenduojama naudoti automatizuotus sprendimus.

Egzistuojantys rinkos sprendimai nėra tinkami automatizuotam saugos auditui atlikti dėl funkcionalumo trūkumo juose.

IT saugos politikos įgyvendinimo audito automatizuotas modelis susideda iš centralizuoto serverio, kuriame saugoma audito rezultatų informaciją. Audituojamuose mazguose įdiegiami specialūs agentai, kurie nuskaito vietinius konfigūracinius failus ir perduoda jų duomenis serveriui. Pagal šį modelį projektuojamos sistemos pasižymi lankstumu ir išplečiamumu: jos palaiko skirtingo tipo vartotojus ir leidžia integruoti papildomą funkcionalumą, atsižvelgiant į poreikį.

2. IT SAUGOS AUDITO SISTEMOS PROJEKTAS

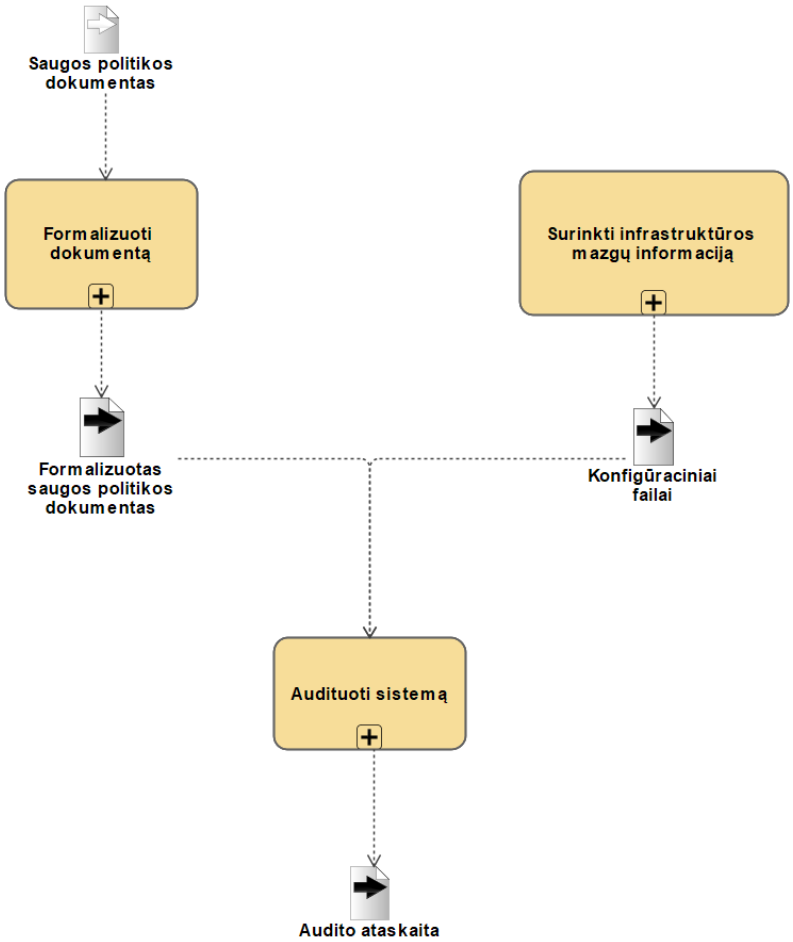
2.1. IT saugos audito sistemos projekto tikslas

Pagrindinis kuriamos sistemos tikslas – sumodeliuoti tokią informacinių technologijų saugos politikų įgyvendinimo audito paramos sistemą, kuri padėtų atlikti automatizuotą saugos auditą sąlyginai nedidelėse įmonėse.

Sistema, inicijavus audito procedūrą, turėtų surinkti informaciją iš įvairių informacinių technologijų infrastruktūros mazgų, kuri bus reikalinga saugos auditui, įgyvendinamu saugos politikomis, atlikti.

2.2. IT saugos audito sistemos projekto schema

IT saugos audito sistemos prototipo schema pavaizduota 2.1 pav. Joje matoma, kad turint įmonės patvirtintą saugos politikos dokumentą, reikia jį konvertuoti į formalizuotą politikos dokumentą – tokį, kurio informaciją galėtume lyginti su konfigūracinių failų informacija. Konfigūraciniai failai yra surenkami iš įvairių audituojamos infrastruktūros mazgų: tai gali būti operacinės sistema, užkarda ar kiti komponentai.

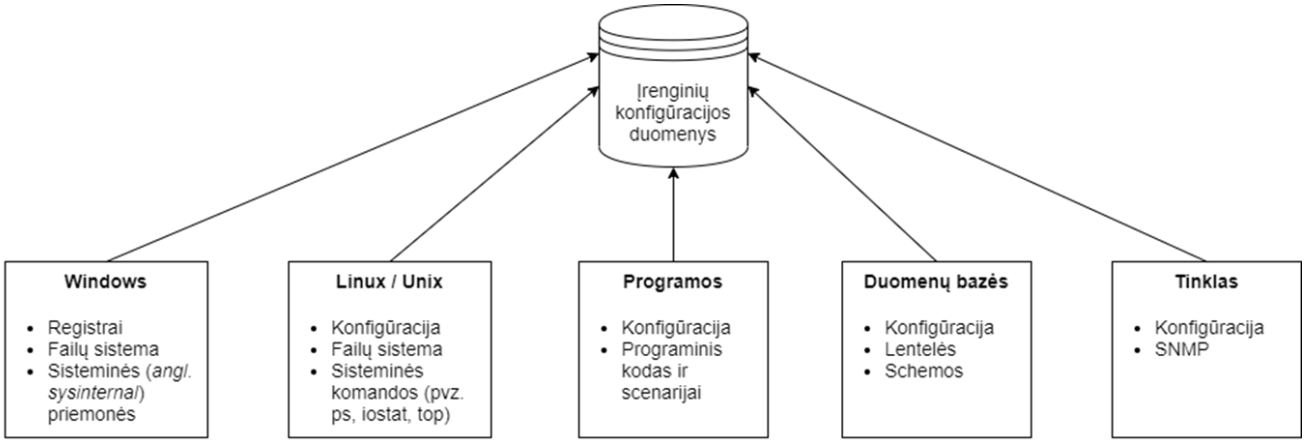


2.1 pav. Kuriamos sistemos projekto schema

Tada tų mazgų bei formalizuotos saugos politikos informacija yra lyginama tarpusavyje – atliekamas auditas. Jį atlikus yra suformuluojama audito ataskaita, kurioje pateikiama informacija apie turimos infrastruktūros mazgų ir saugos politikos dokumento atitiktį.

2.3. Konfigūraciniai failai

Norint atlikti saugos politika paremta auditą, reikia susirinkti konfigūracinių failų informaciją iš įvairių IT infrastruktūros mazgų. Tai gali būti įvairios užkardos, įsilaužimo aptikimo sistemos, maršrutizatoriai, operacinės sistemos ir kt., kaip pavaizduota 2.2 pav.



2.2 pav. Įrenginių konfigūracijos duomenų šaltiniai

Pateiktame paveiksle matoma, kad informacijos šaltinių yra daug ir įvairių: net imant vieną konkrečią sritį, šaltinių, iš kurių galima rinkti informaciją yra ne viena. Kalbant apie Windows OS įrenginius, iš jų registrų galima surinkti informaciją apie pačios sistemos konfigūraciją, įdiegtas programas ar turimą techninę įrangą, iš failų sistemos galima paimti prieigos kontrolės sąrašo informaciją, o naudojantis sisteminėmis priemonėmis, galima gauti informaciją apie vietinės saugos politikos konfigūraciją. Linux / Unix OS duomenų šaltiniai iš principo yra panašūs į Windows OS, tik prieiga prie duomenų yra kitokia – naudojamos specialios OS komandos.

Taip pat vienas iš galimų šaltinių – įvairios programos ir scenarijai, iš kurių, jei turi atvirai prieinamą vykdymo kodą, galima surinkti informaciją apie tai, kokias komandas jie vykdo ir ar juose nėra žalingo kodo.

Iš duomenų bazių konfigūracinių failų galima surinkti informaciją apie vartotojus, jų prieiga ir roles, o iš lentelių ir schemų gauti informaciją apie saugomis duomenis ir tuo duomenų tipus. Ši informacija gali pasitarnauti tikrinant, ar jautri informacija, tokia kaip slaptažodžiai, saugomi ne atviru tekstu ir ar naudojama maišos funkcija yra saugi.

Renkant informaciją iš tinklo įrenginių, vienas iš šaltinių gali būti konfigūraciniai failai, kuriuose yra saugoma informacija apie programinę ir aparatinę įrangas, slaptažodžius ir kt. Taip pat kaip duomenų šaltinį galima panaudoti SNMP, kurio pagalba galima surinkti informaciją apie tinkle veikiančius įrenginius.

Kadangi įrenginiai, iš kurių bus surenkama informacija gali grąžinti informaciją skirtingais formatais, prieš perduodant informaciją audito atlikimo mechanizmui, reikėtų gautą informaciją normalizuoti į vieną bendrą duomenų formatą. Toliau pateikiami keletas konkrečių šaltinių pavyzdžių.

Maršrutizatoriai

Maršrutizatoriaus konfigūracinio failo struktūra yra labai priklausoma nuo jo gamintojo ir programinės įrangos versijos. Pavyzdžiui *D-Link DIR-825* maršrutizatoriaus konfigūracinio failo turinys saugomas JSON formatu. Jo pavyzdys pateikiamas 2.3 pav.


```
{
    "add_sets": {
        "device_mode": "router"
    },
    "autoupdate": {
        "check_updates": false,
        "enable": true,
        "need_update": false,
        "server": "cpe.cgates.lt",
        "status": "latest_fw_version",
        "version": "1.0.1",
        "md5sum": "2878cffaf8cfae9229be0bed2c5bb68d",
        "path": "cpe.cgates.lt/Router/DIR_825E_RT8197F_CGATES/Firmware/2020.02.18-17.40_DIR_825E_RT8197F_CGATES_1.0.1_release.bin"
    },
    "default_pass": false,
    "httpaccess_hide": [
        {
            "dport": "443",
            "iface": "auto",
            "ips": "5.20.4.0",
            "source_mask": "255.255.255.0",
            "sport": "443"
        },
        {
            "dport": "443",
            "iface": "auto",
            "ips": "5.20.0.0",
            "source_mask": "255.255.255.0",
            "sport": "443"
        }
    ],

    ....
```


2.3 pav. D-Link DIR-825 maršrutizatoriaus konfigūracinio failo ištrauka

Šiame konfigūraciniame faile galima rasti pagrindinę informaciją apie maršrutizatorių: prisijungimo vardą, slaptažodžio maišos funkcijos rezultatą ir programinės įrangos versiją. Turint šiuos duomenis galima nustatyti, ar maršrutizatorius sukonfigūruotas saugiai. Turint maršrutizatoriaus gamintojo pavadinimą ir programinės įrangos versiją, galima patikrinti, ar įdiegti naujinimai bei rasti galimus pažeidžiamumus, o turint vartotojo vardą ir slaptažodį galima patikrinti, ar nepalikti standartiniai prisijungimo duomenys (pvz. admin – admin).

Operacinė sistema

Operacinės sistemos konfigūracinių failų šaltiniai gali būti keli. Kalbant apie Windows operacinės sistemos įrenginius, didelę dali informacijos galima pasiimti tiesiai iš registrų Ten galima rasti ir įdiegtų programų sąrašus, prieigos kontrolės sąrašus, prisijungimų informaciją, vartotojo profilį ir kt. Tačiau kitas gana naudingas Windows įrankis yra Vietinė saugos politika. Jos konfigūracinį failą galima išeksportuoti kaip tekstinį failą, kuriame duomenys atskiriami tabuliacijos ženklu, arba kaip CSV failą, kuriame duomenys atskiriami kabliataškiu. Failo pavyzdys pateikiamas 2.4 pav.

```
Policy  Security Setting
Enforce password history    0 passwords remembered
Maximum password age    10 days
Minimum password age    0 days
Minimum password length 10 characters
Password must meet complexity requirements  Enabled
Store passwords using reversible encryption Disabled
```

2.4 pav. Vietinės saugos politikos konfigūracinio failo ištrauka

Ten aprašoma slaptažodžių politika, vartotojų teisės pagal vartotojo lygį, paskyros blokavimo politika, ugniasienės taisyklės ir kt. Iš esmės – tai įrankis, leidžiantis administratoriams paprastai

nustatyti griežtas politikos taisykles kaip pavyzdžiui uždrausti išorinius atjungiamus prietaisus (tokius kaip USB atmintinė), limituoti nustatymus, kuriuos gali keisti vartotojas valdymo skyde (pavyzdžiui, leisti keisti ekrano rezoliuciją, tačiau neleisti keisti VPN nustatymų) ir kt.

Pašto sistema

Pašto sistemos konfigūracinio failo pavyzdys pateiktas 2.5 pav. Turint tokė failą, galima gauti ir ištirti pagrindinius saugumo nustatymus, tokius kaip SMTP autentifikacija, kuri, jeigu yra išjungta, gali suteikti galimybę pasinaudoti pašto serveriu šlamšto siuntimui ar galimų prisijungimų kiekis, kuris jei ribojamas, padeda išvengti DoS atakų.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
    </startup>

  <!-- Below are the SMTP settings -->
  <system.net>
    <mailSettings>
      <smtp from="fromAddress@domain.com">
        <network host="smtpEmailServerAddress" port="25" enableSsl="true"
            userName="username" password="password"/>
      </smtp>
    </mailSettings>
  </system.net>

</configuration>
```

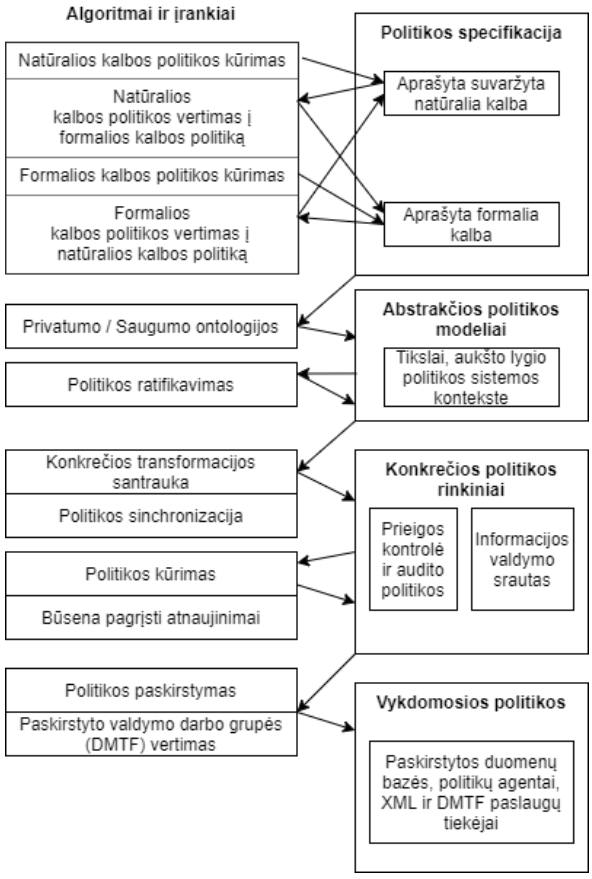
2.5 pav. Pašto sistemos konfigūracinio failo pavyzdys [19]

Taip pat galima patikrinti, ar naudojamas SPF, kuris užkerta kelią netikrų laiškų siuntimui, ar kuriami juodieji IP sąrašai bei ar šifruojami POP3 ir IMAP prisijungimai.

2.4. Saugos politikos formalizavimas

Tam, kad būtų galima atlikti automatizuotą infrastruktūros auditą, privalu turėti saugos politikos dokumentą, kurį gebėtų perskaityti kompiuteris. Todėl reikia rasti metodą, kaip natūralia kalba parašytą dokumentą paversti į kompiuteriui suprantamą dokumentą. Vienas iš tokių metodų – sluoksninis politikos modelis. Jis leidžia nuosekliai patikslinti, patvirtinti, paskirstyti ir atnaujinti politiką [20]. Šis modelis grafiškai pavaizduotas 2.6 pav., kuriame matome, jog pagrindiniai sluoksniai ir jų funkcijos yra:

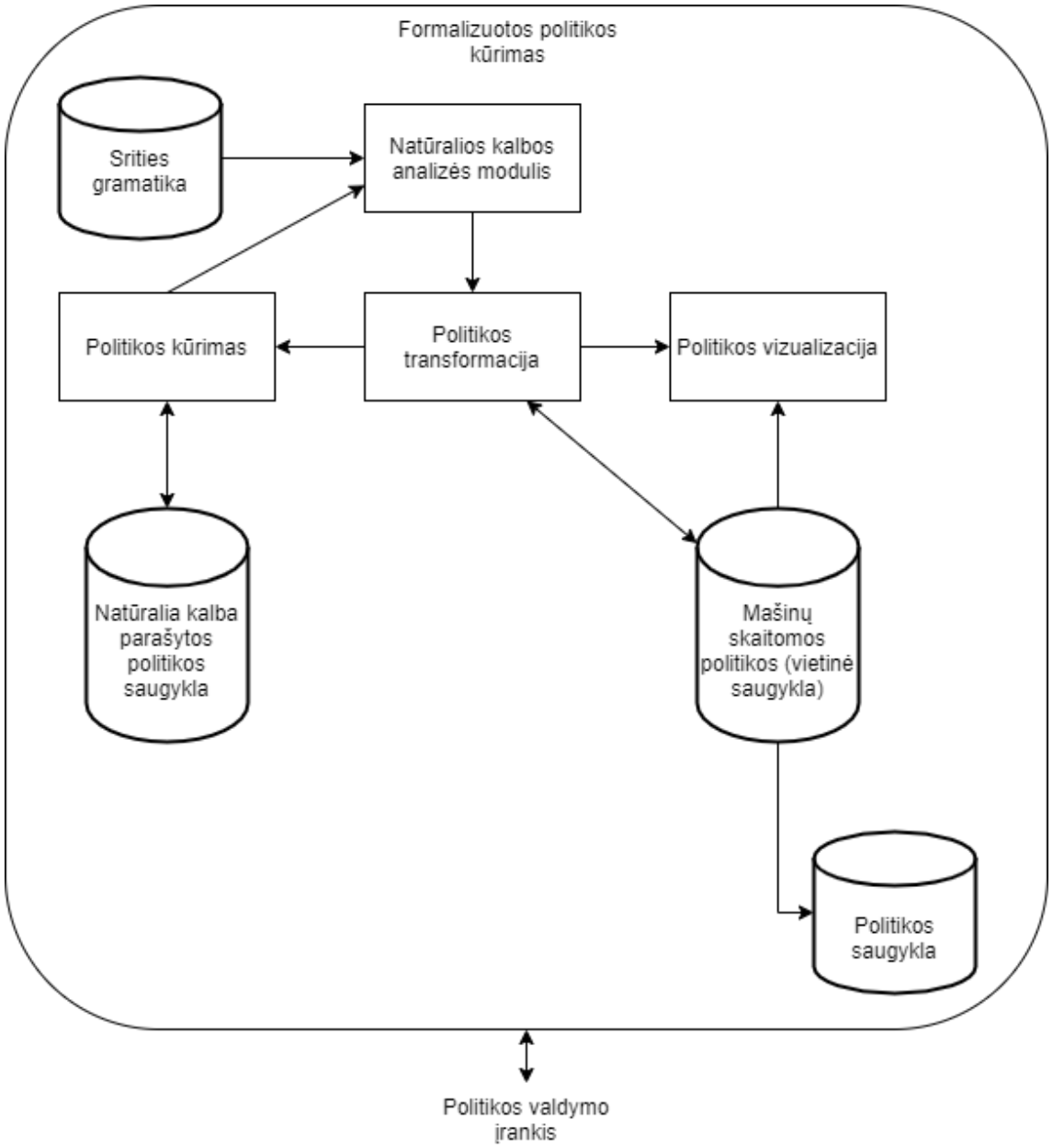
- politikos specifikacijos sluoksnis, kurį sudaro suvaržyta natūralios kalbos gramatika, padedanti apibrėžti saugumo politiką, įrankiai, kurie palaiko sintaksiškai teisingos politikos sudarymą ir ontologijos, leidžiančios natūralios kalbos politiką paversti abstrakčia politika;
- abstrakčios politikos sluoksnis, kuris automatiškai analizuoja abstrakčių semantinio teisingumo ir nuoseklumo strategijų rinkinius, naudodamas daugybę formalių metodų;
- konkrečios politikos sluoksnis, automatiškai paverčiantis teisingus ir nuoseklius abstrakčius politikos rinkinius į konkrečius politikos rinkinius, kuriuos turi palaikyti skirtingi paskirstytos sistemos komponentai, kad būtų pasiekti politikos tikslai;
- vykdomasis politikos sluoksnis, kuris remdamasis DMTF, transformuoja ir paskirsto konkrečius politikos rinkinius konkretiems įrenginiams prieš ir per diegimą, jo metu, bei teikia būsenos ataskaitas. Šiame sluoksnyje esanti politikos infrastruktūra lemia, kada įvykdytos politikos sąlygos.



2.6 pav. Sluoksninis politikos modelis [20]

Vienas iš saugos politikos aprašymo metodų yra jau minėtas suvaržytas natūralios kalbos naudojimas. Toks metodas yra skirtas kurti technines galimybes įmonėms apibrėžti suprantamas

saugos politikas ir susieti jas su politikų įgyvendinimu visoje IT infrastruktūroje. Politikos autoriai, naudodamiesi atitinkamais įrankiais, gali rašyti taisykles natūralia kalba, naudodamiesi taisyklių vadovu, arba gali importuoti esamas teksto taisykles ir pritaikyti jas naudodamiesi taisyklių vadovu. Tokio įrankio veikimo pavyzdys parodytas 2.7 pav. Tada įrankis natūraliąją kalbą paverčia struktūrizuotu formatu. Taip pat politikos autoriai gali naudoti struktūrizuotą formatą tiesiogiai, kad apibrėžtų elementus ir taisyklių ryšius. Įrankis sugeneruos atitinkamas natūralių kalbų versijas taisyklėms, sukurtoms naudojant šį metodą. Kūrėjai gali naudoti tik kurį nors metodą arba pereiti iš vieno metodo į kitą, o įrankis abu formatus sinchronizuos. Kai politika yra struktūrizuoto formato, jos vizualizacijos pateikiamos siekiant padėti politikos kūrėjams užtikrinti, kad politikos aprėptis būtų tokia, kokia buvo numatyta. Taip pat teikiamos analizės galimybės identifikuoti konfliktus ir dublikatus tarp politikos taisyklių. Galiausiai, kai politikos kūrėjas yra patenkintas sugeneruota saugos politika, įrankis sukuria politikos taisyklę norimu formatu, paremtą struktūrine natūralia kalba.



2.7 pav. Automatizuoto politikos kūrimo įrankio veikimo pavyzdys [20]

Standartizuotas metodas dokumento tipo apibrėžimams kurti yra naudojant žymėjimo deklaracijas. Tam reikalingas esamo duomenų tipo apibrėžimo (*angl. Data Type Definition*) rinkinio

papildymas papildomomis savybėmis, leidžiančiomis suprasti tikrąją informaciją. Vienas iš būdų pasiekti šį tikslą yra naudoti XML. XML schema suteikia galimybę naudoti XML egzempliorius papildytiems duomenų tipo apibrėžimams atvaizduoti.

XML dokumentas turi tiek loginę, tiek fizinę struktūrą. Loginę struktūrą sudaro deklaracijos, elementai, komentarai, ženklų nuorodos ir apdorojimo instrukcijos, kurios visos dokumente nurodomos aiškiu žymėjimu. Fizinę struktūrą sudaro saugyklos elementai, vadinami subjektais. Subjektas gali turėti nuorodą į kitą subjektą, kuris įtrauktas į tėvinį subjektą. Dokumentas prasideda „šaknimi“ arba dokumento subjektu, o visos loginės ir fizinės struktūros gali būti tinkamai įdėtos dokumento subjekto viduje. XML dokumentas taip pat gali būti gerai suformuotas ir (arba) galiojantis dokumentas [21]. Tinkamai suformuotas dokumentas turi atitikti pradinį dokumentą.

Loginė struktūra

Kiekviename XML dokumente yra vienas ar keli elementai, kurių ribas riboja pradžios ir pabaigos arba tuščių elementų žymos. Kiekvienas elementas turi tipą, identifikuojamą pagal pavadinimą, ir gali turėti atributų specifikacijų rinkinį. Kiekvieną atributo specifikaciją sudaro pavadinimo ir reikšmės pora. XML dokumento elementų struktūrą galima apriboti naudojant elementų tipo ir atributų sąrašo deklaracijas. Elemento tipo deklaracijos nurodo, kurie elementų tipai gali pasirodyti kaip elemento vaikai. Elementų deklaracijos yra logiškai sugrupuotos duomenų tipo apibrėžimo viduje.

Fizinė struktūra

XML dokumentą gali sudaryti viena ar daugiau saugyklų, vadinamų subjektais. Kiekvienas subjektas susideda iš turinio ir pavadinimo. Visuose XML dokumentuose yra dokumento subjektas, kuris naudojamas kaip atskaitos taškas XML analizatoriui. Nagrinėjamo subjekto turinys yra vadinamas jo pakeitimo tekstu ir laikomas neatsiejama dokumento dalimi. Subjektai dažniausiai naudojami fiziniam modeliavimui.

Formalizuota saugos politika

Atsižvelgiant į XML struktūros reikalavimus, galima aprašyti formalų saugos politikos dokumentą. XML struktūra yra dėkinga tuo, kad yra ganėtinai paprasta pridėti naujus elementus, nepažeidžiant jau esamos dokumento struktūros. Taigi, besikeičiant pradiniam saugos politikos dokumentui, iškyla mažiau nesuderinamumo problemų. Taip pat naudojant XML struktūrą, galima atskirai sugrupuoti saugos politikos punktus pagal kategorijas. Galimas XML saugos politikos dokumento pavyzdys pateikiamas 2.8 pav.

```
<?xml version="1.0" encoding="UTF-8"?>
<saugosPolitika>
    <slaptazodziai>
        <stiprumoPolitika>
            <taisykliuRinkinys>
                <taisykle minSlaptIlgis="10"/>
                <taisykle minSkaitKiekis="1"/>
                <taisykle minSpecKieks="1"/>
            </taisykliuRinkinys>
        </stiprumoPolitika>
        <stiprumoPolitika>
            <taisykliuRinkinys>
                <taisykle minSlaptIlgis="10"/>
                <taisykle minSkaitKiekis="2"/>
            </taisykliuRinkinys>
        </stiprumoPolitika>
    </slaptazodziai>
    <leistinosProgramos>
        <leidziamiLeidejai>
            <leidejas>Intel</leidejas>
            <leidejas>Microsoft</leidejas>
            <leidejas>MSI</leidejas>
        </leidziamiLeidejai>
        <leidziamiPavadinimai>
            <programa>TeamViewer</programa>
            <programa>Jetbrains Toolbox</programa>
            <programa>XAMPP</programa>
        </leidziamiPavadinimai>
    </leistinosProgramos>
</saugosPolitika>
```

2.8 pav. XML saugos politikos dokumento pavyzdys

Pateiktame pavyzdyje saugos politikoje reikalaujama, kad slaptažodžiu stiprumas atitiktų vieną iš dviejų pateiktų taisyklių rinkinių: slaptažodis turi būti bent dešimties simbolių ilgio, kurį turi sudaryti bent vienas skaičius ir bent vienas specialus simbolis, arba slaptažodis turi būti bent dešimties simbolių ilgio, kurį turi sudaryti bent du skaičiai. Taip pat matoma, kad leidžiamų programų sąrašą sudaro dviejų tipų leidimai: kai leidžiamos visos nurodyto leidėjo programos (konkrečiai pavyzdyje *Intel, Microsoft, MSI*) ir papildomai leidžiamos atskiros programos (*TeamViewer, Jetbrains Toolbox, XAMPP*).

2.5. Saugos audito politikos atitikties skaičiavimo algoritmas

Saugos audito politikos atitiktis apskaičiuojama procentine išraiška skaičiuojant vidurkį: sudedamas kiekvieno audituojamo mazgo audito ataskaitos atitikusių saugos politikos punktų kiekis, padalinamas iš visų saugos politikos punktų kiekio ir gauta suma padauginama iš šimto.

2.6. IT saugos audito sistemos reikalavimai

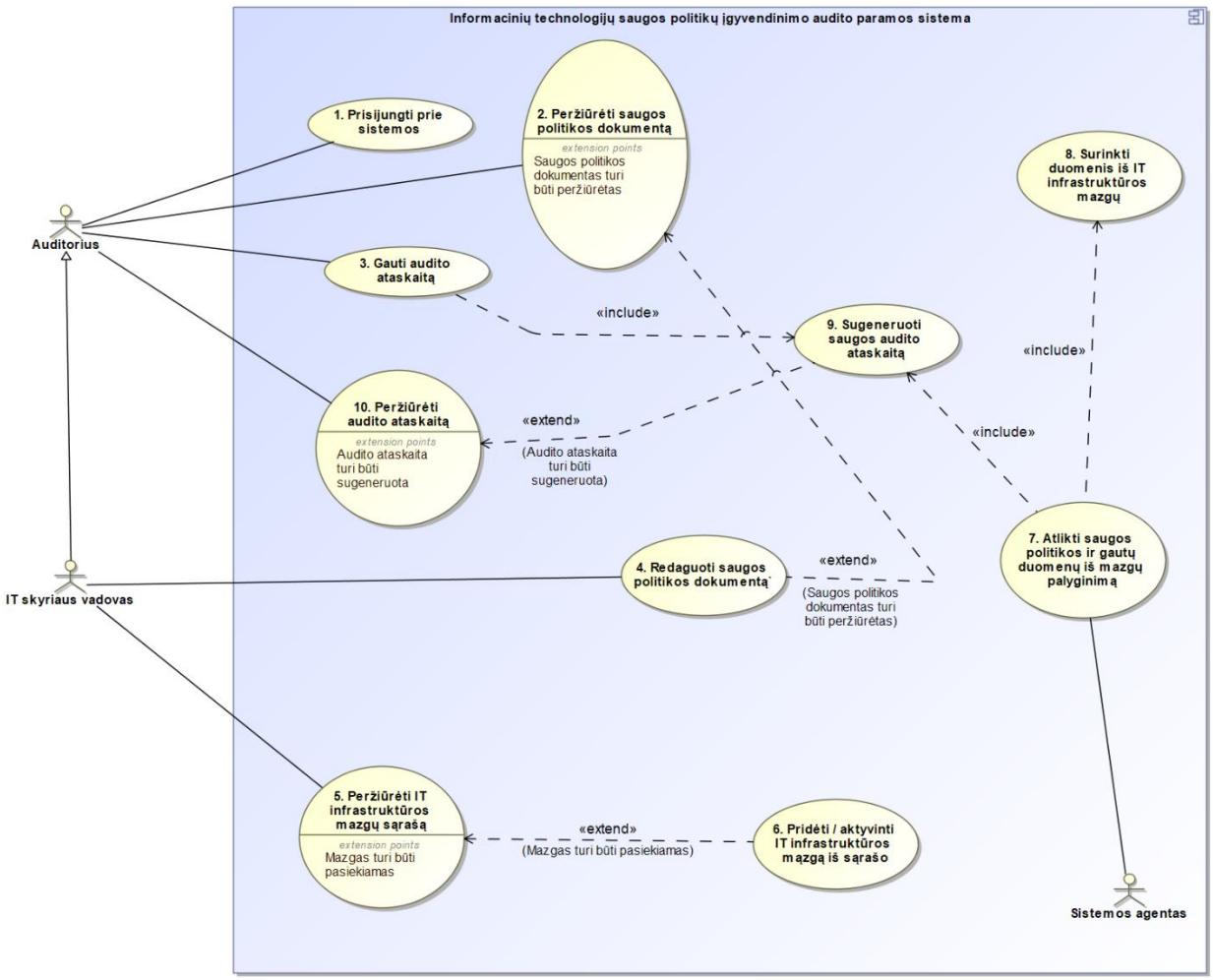
IT saugos audito sistemos vartotojų grupės

Išorinis saugos auditorius. IT saugos audito sistema galės naudotis iš išorės nusamdytas auditorius, kuris turės galimybę atlikti informacinių technologijų infrastruktūros auditą. Šiam vartotojui nereikės turėti specifinių žinių apie audituojamą sistemą: auditas bus inicijuojamas vieno mygtuko paspaudimu, o formalizuotas saugos politikos dokumentas bus atvaizduojamas taip, kad vartotojui neprireiktų specifinių IT žinių.

IT skyriaus vadovas. Kadangi saugumo reikalavimai įmonėje yra dinamiški, juos gali tekti atnaujinti, todėl šios vartotojų grupės asmuo privalo turėti techninių IT žinių: išmanyti IT sistemų saugą, tinklus.

IT saugos audito sistemos funkciniai reikalavimai

Automatizuoto saugos audito sistemos panaudos atvejų diagrama pavaizduota 2.9 pav. Kaip matoma minėtoje diagramoje, auditorius turi galimybę prisijungti prie sistemos, peržiūrėti įmonės turimą saugos politikos dokumentą bei gauti sistemos agento suformuotą audito ataskaitą.



2.9 pav. Automatizuoto saugos audito sistemos panaudos atvejų diagrama

IT skyriaus vadovas paveldi visus auditoriaus galimus veiksmus bei papildomai gali redaguoti turimą saugos politikos dokumentą, peržiūrėti IT infrastruktūros mazgų sąrašą bei pridėti arba pašalinti mazgus iš sąrašo. Tiesa, kad galėtų vykdyti pastarąjį veiksmą, mazgas turi būti pasiekiamas. Sistemoje

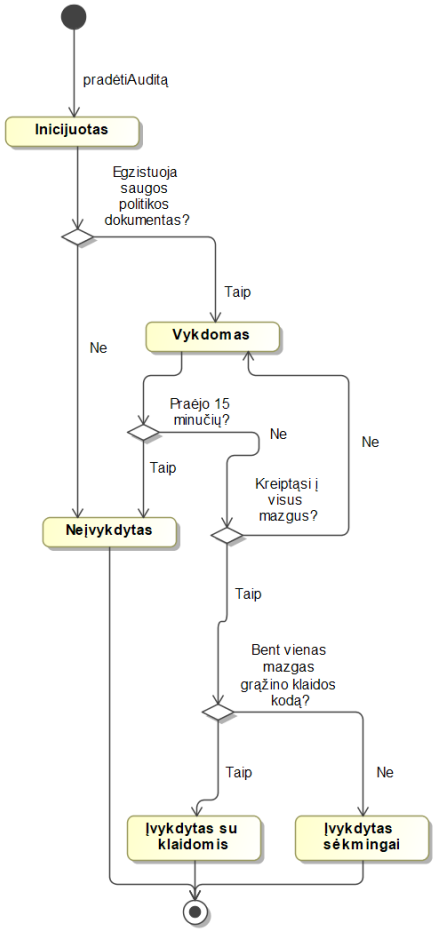
taip pat egzistuoja sistemos agentas, kuris surenka duomenis iš IT infrastruktūros mazgų, palygina gautus duomenis su turimu saugos politikos dokumentu ir sugeneruoja saugos audito ataskaitą.

IT saugos audito sistemos nefunkciniai reikalavimai

- paprasta vartotojo sąsaja;
- informaciniai vartotojo pranešimai turi būti aiškūs ir suprantami, kuriems suprasti nėra reikalingos specifinės informacinių technologijų žinios;
- sistemos vartotojo sąsaja turi atitikti HTML5 standartą;
- sistema prieinama tik prisijungus prie vidinio įmonės tinklo;
- sistemos sąsaja turi atsiverti ne lėčiau nei per 5 sekundes;
- audito procedūra turi būti inicijuojama asinchroniškai.

Reikalavimai IT saugos audito sistemos sprendimui

IT saugos audito sistema turi surinkti visų infrastruktūroje žinomų mazgų informaciją, palyginti ją su turima formalizuota saugos politika bei grąžinti auditoriui audito ataskaitą, su išsamiais atitikties / neatitikties punktais. Atliktų auditų istorija turi būti prieinama nepriklausomai nuo to, kada auditas buvo atliktas. Audito ataskaitos turi būti kategorizuojamos pagal jų būsenas, kurių kitimas pavaizduotas 2.10 pav.

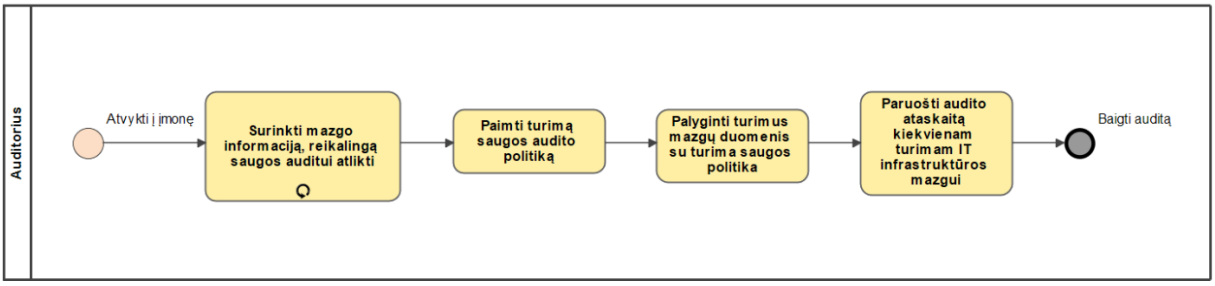


2.10 pav. Audito ataskaitos duomenų esybės būsenų diagrama

Formalizuotą saugos politikos dokumentą redaguoti gali tik IT skyriaus vadovas. Visi saugos politikos punktai turi saugoti informaciją apie jų atnaujinimo laiką. Pačių punktų ištrinti negalima, juos galima tik įgalinti / išjungti.

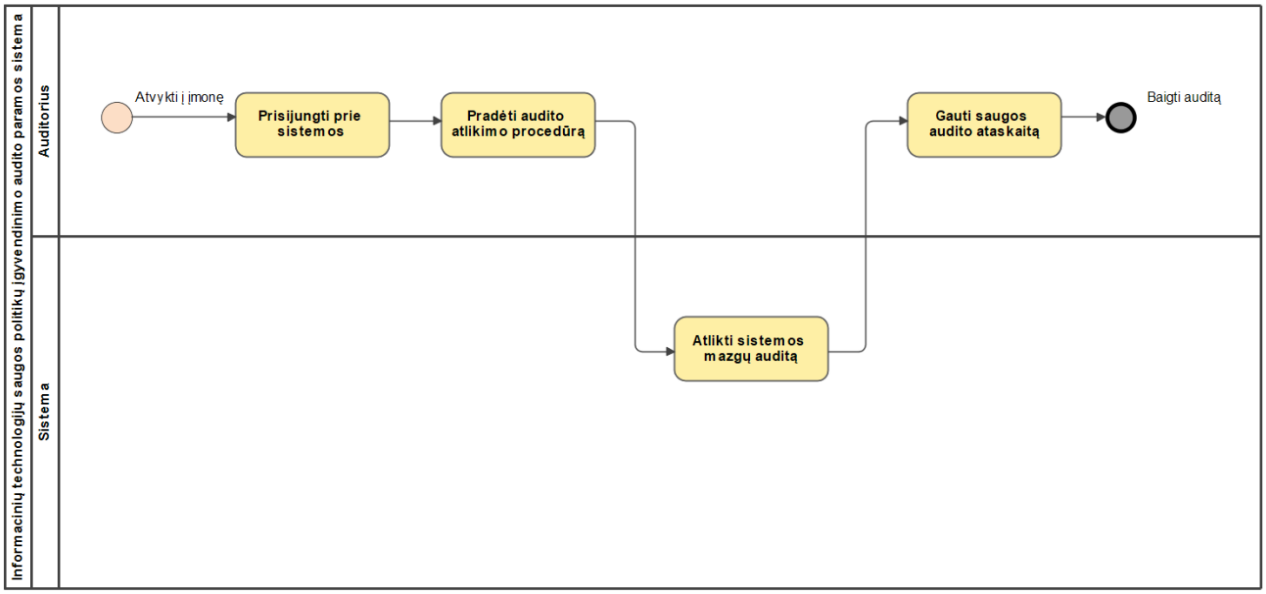
2.7. Audito veiklos procesai

Neturint įdiegto automatizuoto saugos audito atlikimo sistemos, saugos audito atlikimo veiklos modelis atrodytų šitaip: auditorius, atvykęs į įmonę, eina prie kiekvieno įmonės infrastuktūros mazgo. Priklausomai nuo mazgo tipo, nusprendžia, kaip surinkti reikiamą informaciją saugos auditui atlikti. Šį veiksmą kartoja su visais įmonėje esančiais mazgais. Turėdamas reikiamą mazgų informaciją, auditorius paima įmonės turimą saugos politikos dokumentą ir lygina iš mazgų gautą informaciją su turima saugos politika. Atlikęs analizę, auditorius kiekvienam įrenginiui parašo atitikties ataskaitą, kurias vėliau susistemina į vieną bendrą ataskaitą. Esamos veiklos procesų modelis pavaizduotas 2.11 pav.



2.11 pav. Audito atlikimo esamos veiklos procesų modelis

Įdiegus siūlomą sprendimą, auditoriui nebereikės fiziškai nuvykti prie kiekvieno iš mazgų ir galvoti, kaip gauti iš jo reikiamą informaciją: atvykęs į įmonę auditorius prisijungs prie įdiegtos automatizuotos audito sistemos ir joje, inicijavęs audito atlikimo procedūra, gaus jau suformuotą ataskaitą apie saugos politikos dokumento atitiktį. Būsimos veiklos procesų modelis pavaizduotas 2.12 pav.



2.12 pav. Audito atlikimo būsimos veiklos procesų modelis

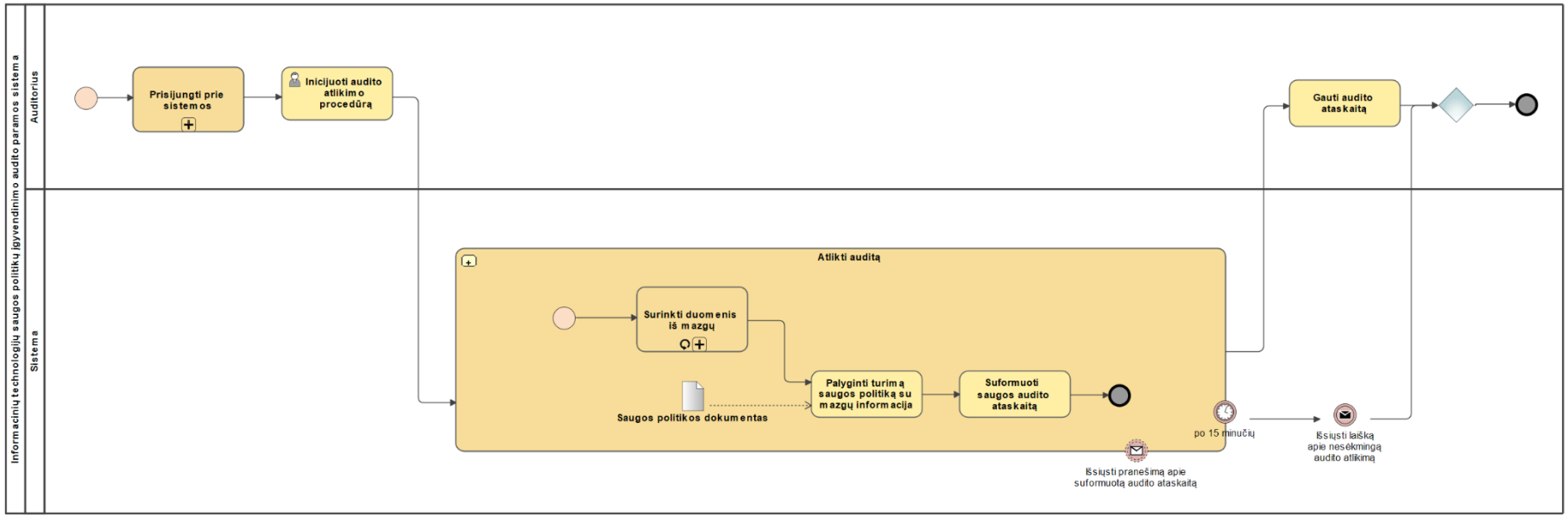
Taigi, kaip matoma iš pateiktų veiklos modelių, įdiegus automatizuotą saugos audito sprendimą procesai vyks daug paprasčiau: auditorius gebės auditą atlikti greičiau ir efektyviau, kadangi jam nereikės atlikti duomenų surinkimo ir jų analizės pačiam.

Audito atlikimo proceso modelis pavaizduotas 2.13 pav. Jame matoma, kad auditorius, norėdamas atlikti auditą, privalo būti prisijungęs prie sistemos. Tai atlikęs, jis inicijuoja audito atlikimo procedūrą: pradedami rinkti duomenys iš turimų IT infrastruktūros mazgų, jie lyginami su saugos politika. Tada suformuojama saugos audito ataskaita ir ji pateikiama auditoriui. Nesuformavus

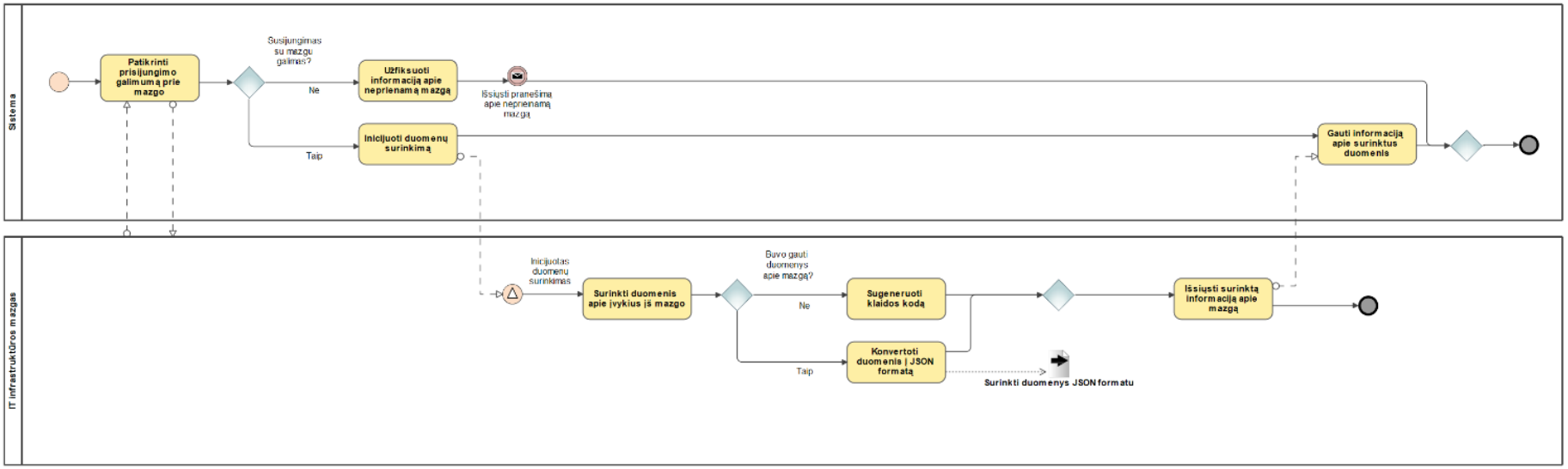
ataskaitos per 15 minčių, ataskaitos generavimas yra nutraukiamas ir vartotojui išsiunčiamas elektroninis laiškas apie nesėkmingą audito atlikimo procedūrą.

Duomenų surinkimo proceso modelis pavaizduotas 2.14 pav. Jame matoma, kad inicijavus duomenų surinkimą iš mazgų yra kreipiamasi į IT infrastuktūros mazgą ir patikrinama, ar galima su juo susijungti. Jei susijungimas galimas, jame inicijuojama duomenų surinkimo procedūra. Nepavykus surinkti duomenų, sistemai grąžinamas klaidos kodas. Jei duomenų surinkimas pavyko sėkmingai, mazgas pateikia informaciją apie save JSON formatu ir juos išsiunčia sistemai.

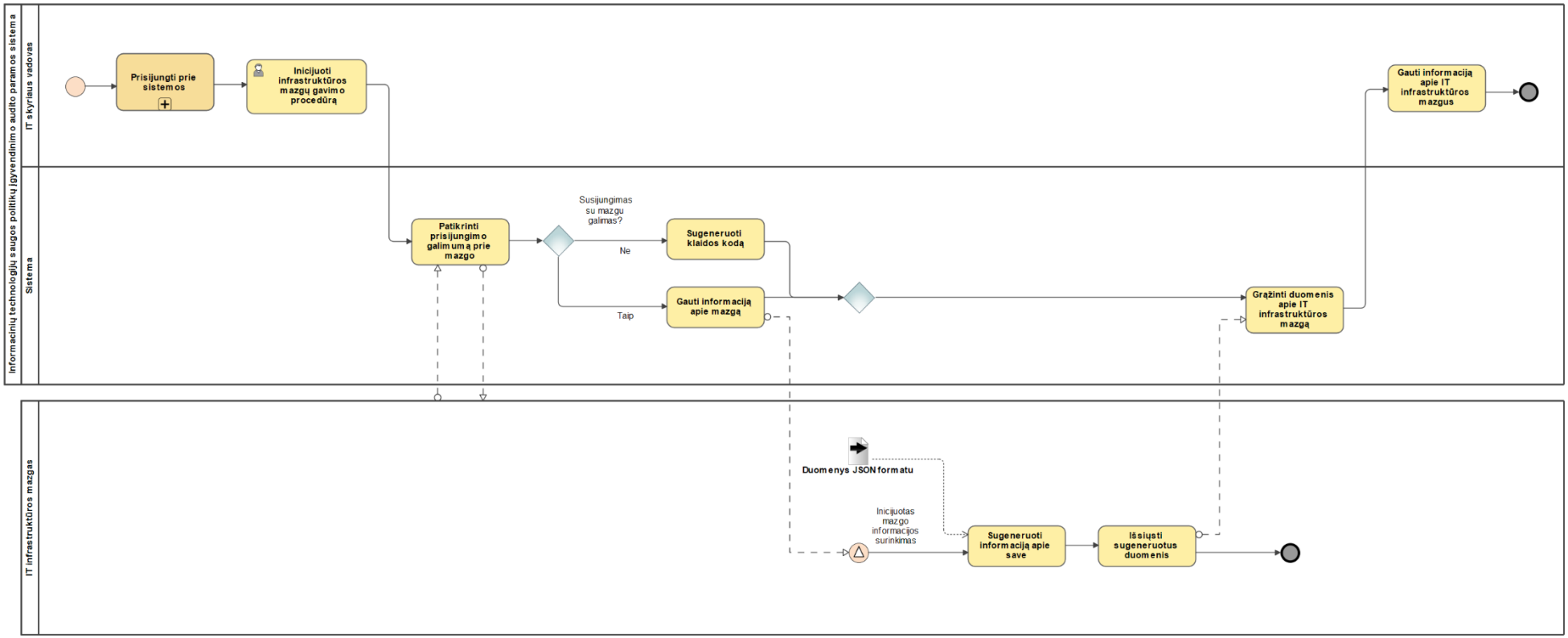
IT infrastruktūros mazgų informacijos peržiūros proceso modelis pavaizduotas 2.15 pav. Jame matoma, kad IT skyriaus vadovas, prisijungęs prie sistemos gali peržiūrėti IT infrastruktūros mazgų informaciją: jam išsiuntus užklausą tikrinamas kiekvieno sistemos mazgo prieinamumas. Jei susijungimas nepavyko, vartotojui grąžinamas klaidos kodas. Priešingu atveju mazgas sugeneruoja informaciją apie save ir tą informaciją JSON formatu išsiunčia sistemai, kuri apdoroja gautus duomenis ir vartotojui grąžina informaciją apie kiekvieną sistemos mazgą.



2.13 pav. Audito atlikimo proceso modelis



2.14 pav. Duomenų surinkimo proceso modelis



2.15 pav. IT infrastruktūros mazgų informacijos peržiūros proceso modelis

2.8. IT saugos audito sistemos projektavimo išvados

Saugos audito sistema susideda iš trijų pagrindinių dalių: saugos politikos dokumento formalizavimo, audito mazgų konfigūracinių failų informacijos surinkimo ir paties audito atlikimo. Tam, kad sistemą būtų vadinama automatizuota, visų šių trijų dalių procesai turi vykti automatizuotai.

Vienas iš saugos politikos formalizavimo metodų yra suvaržytos kalbos naudojimas – sudaromas skaitmeninis saugos politikos dokumentas, kuris yra kuriamas remiantis natūralia kalba aprašytu saugos politikos dokumentu ir naudojantis turima sakinių duomenų baze. Tokiu būdu sukurtas politikos dokumentas gali būti konvertuojamas į sistemoms perskaitomą formatą, pavyzdžiui XML, kuris vėliau panaudojamas automatizuotam saugos auditui atlikti.

Konfigūracinių failų surinkimo procese susiduriama su problema, kad yra daug šaltinių, iš kurių reikia surinkti informaciją. Taigi egzistuoja dideli duomenų kiekiai, kurie gali būti gaunami skirtingais duomenų formatais, todėl svarbi šio proceso dalis – gautų duomenų normalizavimas prieš perduodant juos audito atlikimo procedūrai.

Sistemos projekte aprašytos dvi vartotojų rolės, kurioms aprašytas sistemos funkcionalumas. Taip pat sistemoje egzistuoja duomenų surinkimo agentas, kuris surenka duomenis iš IT infrastruktūros mazgų bei atlieka pačią audito procedūrą.

Sistema suprojektuota taip, kad pati audito atlikimo procedūra būtų atliekama fiziškai nebūnant prie kiekvieno iš audituojamų įrenginių: audito iniciatorius naudojantis interneto naršykle sistemoje pradeda audito procedūrą, kurią atlikus, sistema informuoja jį apie audito rezultatus: pranešamas audito statusas, suteikiama galimybė peržiūrėti išsamią audito ataskaitą.

3. IT SAUGOS AUDITO SISTEMOS PROTOTIPO REALIZAVIMAS

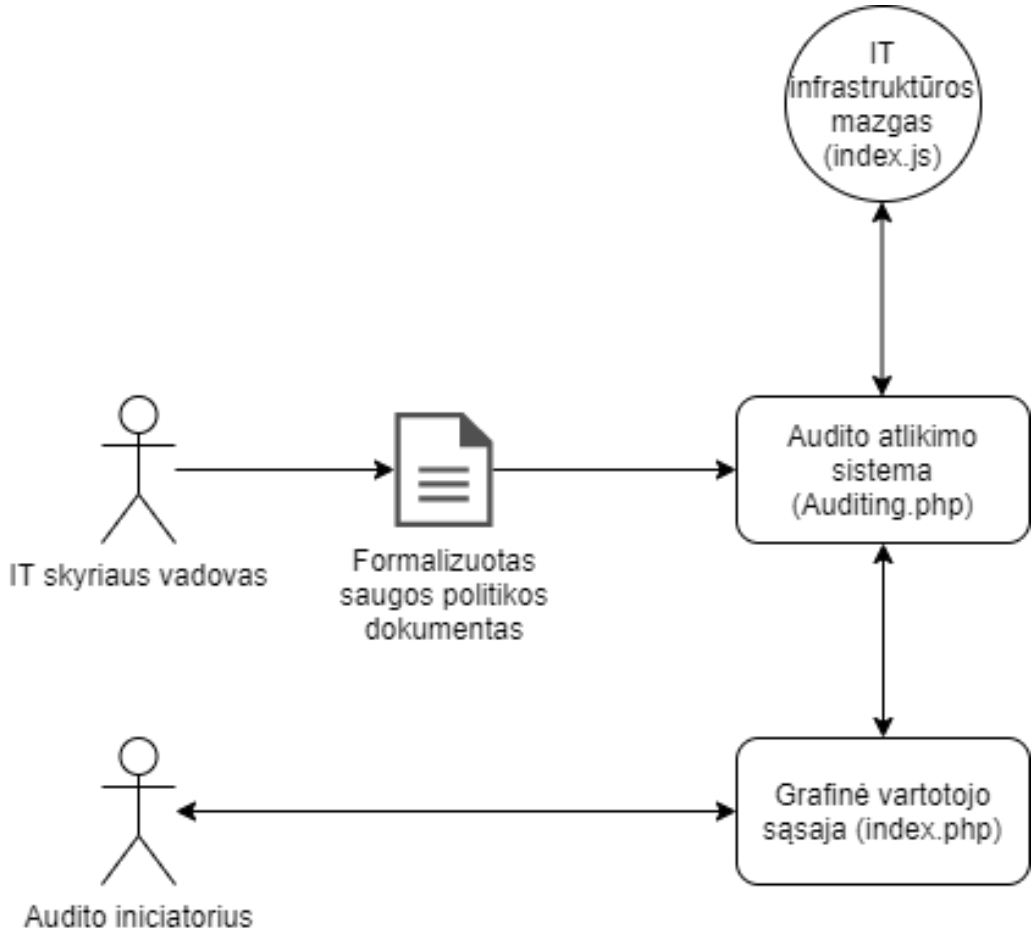
3.1. IT saugos audito sistemos prototipo realizavimo technologijos

Sistemos vartotojo sąsają ir logika realizuota naudojant PHP bei JavaScript programavimo kalbas. Duomenų surinkimui sukurtas Batch scenarijus bei du PowerShell scenarijai, kurie paleidžiami vartotojo per vartotojo sąsają. Visi turimi duomenys saugomi MariaDB duomenų bazėje.

3.2. IT saugos audito sistemos prototipo architektūra

Informacinių technologijų saugos politikų įgyvendinimo audito paramos sistemos prototipą, kurio architektūra grafiškai pavaizduota 3.1 pav. sudaro:

- audito ataskaitų generavimo posistemė (*Auditing.php*);
- mazguose veikiantys mikroservisai (*index.js*);
- formalizuotas saugos politikos dokumentas, saugomas duomenų bazėje;
- grafinė vartotojo sąsaja (*index.php*).



3.1 pav. IT saugos audito sistemos prototipo architektūra

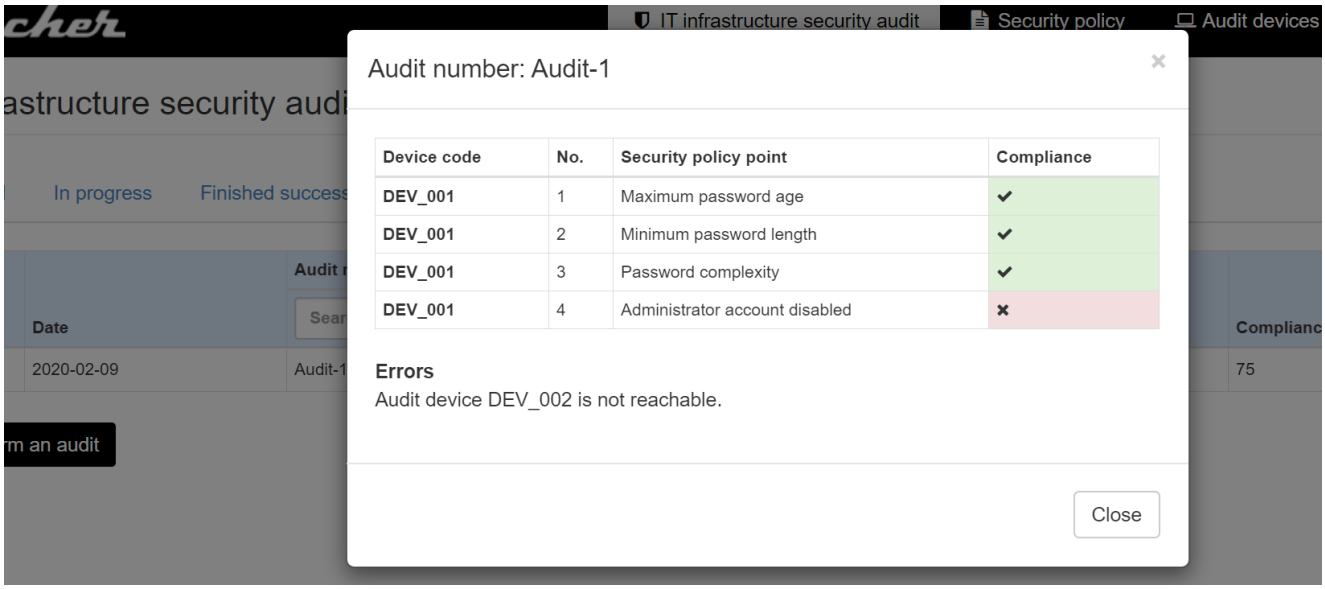
Prieigą prie formalizuoto saugos politikos dokumento turi tik IT skyriaus vadovas, kuris gali jį redaguoti. Audito iniciatorius (tai gali būti tiek IT vadovo rolės vartotojas, tiek išorinio auditoriaus rolės vartotojas) naudodamasis grafine vartotojo sąsaja gali inicijuoti audito atlikimo procedūrą.

3.3. IT infrastruktūros mazgo paruošimas auditui

Kad infrastruktūros mazgas grąžintų reikiamą informaciją saugos auditui atlikti, reikia jį paruošti. Tam yra reikalingi du failai: *node.js* technologija aprašytas ir į *.exe* failą sukompiliuotas mikroservisas ir tekstinis failas, kuriame aprašytas kelias į konfigūracinius failus. Automatiniam mikroserviso paleidimui panaudotas užduočių planavimo įrankis (*angl. Task scheduler*), kuriame nurodoma, kad mikroservisas visada įsijungtų ir pasileistų įjungus kompiuterį.

3.4. Informacijos rinkimas iš skirtingų IT infrastruktūros mazgų

Informacija iš IT infrastruktūros mazgų surenkama pagal turimą jų sąrašą, kuriame pateikiamas mazgo IP adresas ir pavadinimas. Inicijavus audito atlikimo procedūrą, tai užfiksuojama duomenų bazėje. Fone kas minutę periodinė užduotis (*angl. cronjob*) tikrina, ar yra inicijuotų auditų. Jei taip, pradedama audito procedūra: iš eilės einama per mazgų sąrašą ir kreipiamasi į kiekvieną iš jų cURL bibliotekos pagalba.



3.2 pav. Audito su klaidomis ataskaitos pavyzdys

Tuo tarpu kiekviename iš mazgų yra paleistas mikroservisas, kuris laukia užklausos iš žiniatinklio aplinkos per 8081 prievadą. Mikroserviso turinys pateikiamas 7.1 priede. Gavus užklausą, iš nurodytos numatytosios konfigūracinių failų direktorijos yra nukopijuojami failai, kurie reikalingi auditui atlikti. Failai kopijuojami kiekvienos užklausos metu tam, kad pasikeitus kofigūraciniams failams nereikėtų iš naujo paleisti mikroserviso. Nukopijavus visus reikiamus failus, pirmiausia nuskaitomas leidžiamų IP adresų sąrašas. Jei besikreipiantysis IP adresas yra sąraše, jam leidžiama duomenų gavimo procedūra: paleidžiamas *.bat* scenarijus, kuris inicijuoja duomenų iš mazgo surinkimą ir grąžinimą. Šio scenarijaus turinys pateikiamas 7.4 priede. Scenarijaus viduje paleidžiami abu *.ps1* scenarijai, kurie surenka informaciją apie įdiegtas programas ir prieigos kontrolės sąrašus. Pastaroji informacija reikalinga tik iš serverio, kuriame saugomi bendri failai. Taigi tam panaudojamas *.txt* failas, kuriame saugomas serverio IP adresas ir taip prieigos kontrolės sąrašo informacija grąžinama tik iš šio mazgo. Sėkmingai įvykdžius duomenų surinkimą, jie išsiunčiami. Jei informacijos gavimas buvo nesėkmingas, tai taip pat atsispindi gautoje audito ataskaitoje. Tokios ataskaitos pavyzdys parodytas 3.2 pav.

3.5. Informacijos rinkimas mazgo viduje ir jos grąžinimas iniciatoriui

Kaip jau minėta anksčiau, mikroserviso veikimui reikalingi du failai: pats mikroserviso *.exe* failas ir tekstinis failas, kuriame nurodytas kelias į konfigūracinius failus. Šie failai reikalingi pačiam audito atlikimui. Vykdomieji, arba scenarijų failai, vykdymo metu patys sugeneruoja papildomus tekstinius failus. Visų jų sąrašas, funkcionalumas ir struktūra aprašyti 3.1 ir 3.2 lent.

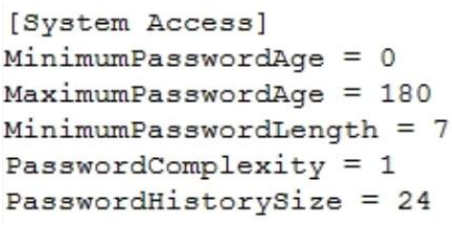
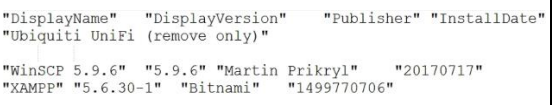
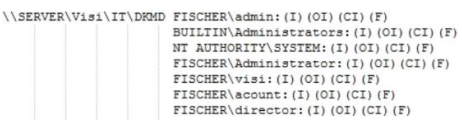
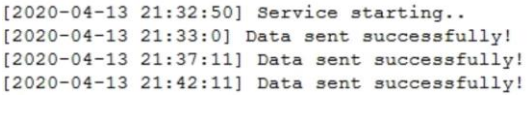
3.1 lent. Konfigūracinių failų sąrašas

Pavadinimas	**Paskirtis**	**Sandara**	**Pavyzdys**
files_path.txt	Nurodo, kur saugomi konfigūraciniai failai.	Tekstinė eilutė be skyriklio.	`\\SERVER\\Visi\\IT\\DKMD\\`
org_allowed_ips.txt	IP adresų sąrašas, kuriems leidžiama gauti informaciją iš mikroserviso.	Tekstinė eilutė su kablelio ir tarpo skyrikliu.	`192.168.137.1, 192.168.91.128`
org_export_acl.ps1	Scenarijus, skirtas surinkti prieigos kontrolės sąrašo informacijai.	*cmdlet* komandos su individualiais parametrais.	`icacls \\SERVER\Visi\IT\DKMD /t > ACL.txt`
org_export_apps_list.ps1	Scenarijus, skirtas surinkti įdiegtų programų sąrašui.	*cmdlet* komandos su individualiais parametrais.	`Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate | Where-Object {$_.Publisher -ne 'Microsoft Corporation' -and $_.Publisher -ne 'Intel Corporation'} | Export-Csv -Encoding "Unicode" -Delimiter "`t" -path InstalledPrograms.txt -notype`

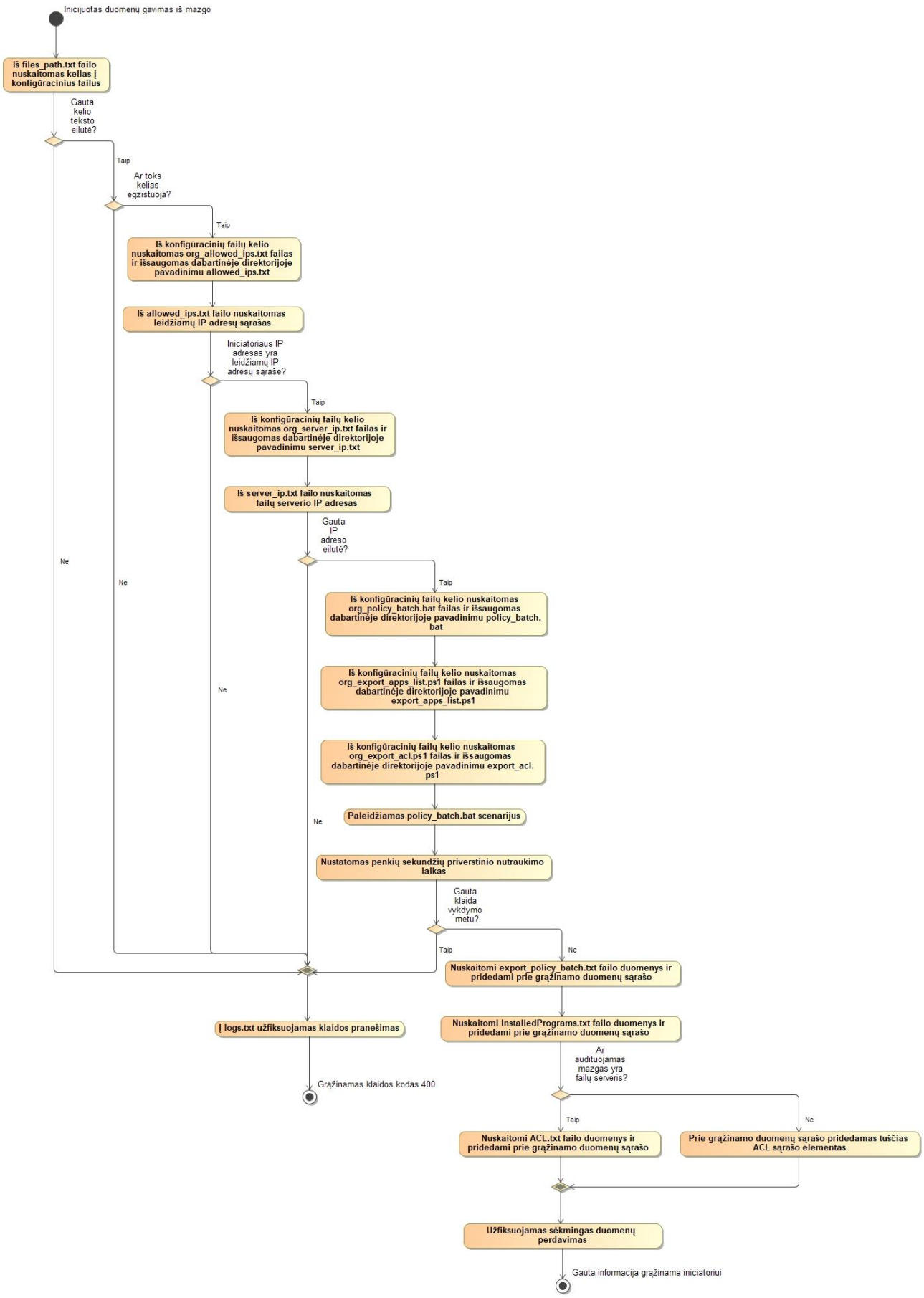
org_policy_batch.bat	Scenarijus, skirtas surinkti vietinės saugos politikos informacijai.	„Microsoft“ komandos su individualiais parametrais.	`@ECHO off`
			`set "params=%*"`
			`secedit.exe /export /cfg ./export_policy_batch.txt`
			`powershell.exe "& './export_apps_list.ps1'"`
			`powershell.exe "& './export_acl.ps1'"`
			`exit`

org_server_ip.txt	Serverio, kuriame saugomi bendri failai, IP adresas.	Tekstinė eilutė be skyriklio.	`192.168.3.151`

3.2 lent. Mikroserviso sugeneruotų failų sąrašas

Pavadinimas	**Paskirtis**	**Sandara**	**Pavyzdys**
export_policy_batch.txt	Saugomi gauti vietinės saugos politikos duomenys	Tekstinis, kelių eilučių UTF-16LE koduotės failas	
InstalledPrograms.txt	Saugomas gautas įdiegtos programinės įrangos sąrašas	Tekstinis, kelių eilučių ir kelių stulpelių UTF-16LE koduotės failas. Stulpeliai skiriami tabuliacijos simboliu.	
ACL.txt	Saugomi gauti prieigos kontrolės sąrašai	Tekstinis, kelių eilučių UTF-16LE koduotės failas.	
logs.txt	Saugomi klaidų ir informaciniai pranešimai	Tekstinis kelių eilučių UTF-8 koduotės failas	

Pats duomenų surinkimas vykdomas tokia tvarka: inicijavus surinkimą, iš tekstinio failo yra nuskaitomas kelias, iš kurio bus kopijuojami konfigūraciniai failai. Jei kelias nuskaitytas sėkmingai, iš tos direktorijos nuskaitomas leistinų IP adresų sąrašas. Jei besikreipiančiojo IP adresas yra tame sąraše, iš konfigūracinių failų direktorijos nukopijuojamas tekstinis failas, kuriame įrašytas failų serverio IP adresas. Tada bandoma nuskaityti tą failą: jei IP adresas gautas, iš konfigūracinių failų direktorijos nukopijuojami scenarijų failai, kuriuos vykdant, gaunama reikiama informacija. Nukopijavus failus paleidžiamas *.bat* scenarijus (jo viduje paleidžiami *.ps1* scenarijai) ir taip yra sugeneruojami vietinės saugos politikos, įdiegtų programų ir prieigos kontrolės sąrašo tekstiniai failai. Po to nuskaitomi tų failų duomenys, jie sudedami į JSON masyvą ir toks masyvas grąžinamas iniciatoriui. Jei kažkuriame iš minėtų žingsnių įvyksta klaida, ji užfiksuojama klaidų žurnale ir iniciatoriui grąžinamas klaidos kodas 400. Viso proceso veiklos diagrama pavaizduota 3.3 pav.



3.3 pav. Mikroserviso veiklos diagrama

3.6. Informacijos šaltiniai

Informacija auditui atlikti surenkama iš trijų vietų:

- secedit.sdb duomenų bazės failo, kuriame saugoma vietinės saugos politikos informacija. Šis failas imamas ne tiesiogiai iš jo buvimo vietos (Windows\security\database), o naudojantis „Windows Security Configuration Editor Tool“ įrankiu secedit.exe. Taip daroma todėl, nes duomenų bazės failas užšifruotas ir iš išorės neperskaitomas;
- HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall* registro, kuriame saugoma įdiegtos programinės įrangos informacija;
- NTFS particijoje esančios MFT lentelės, iš kurios duomenys paimami icacls.exe įrankio pagalba.

3.7. Surinktos informacijos iš IT infrastruktūros mazgų informacija

Informacijos rinkimas iš vietinės saugos politikos konfigūracijos

Naudojant Batch scenarijų, gaunama informacija iš pradžių yra išsaugoma *.txt* faile. Ištrauka iš failo pateikiama 3.4 pav.

```
[System Access]
MinimumPasswordAge = 0
MaximumPasswordAge = 10
MinimumPasswordLength = 0
PasswordComplexity = 0
PasswordHistorySize = 0
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
NewAdministratorName = "Administrator"
NewGuestName = "Guest"
```

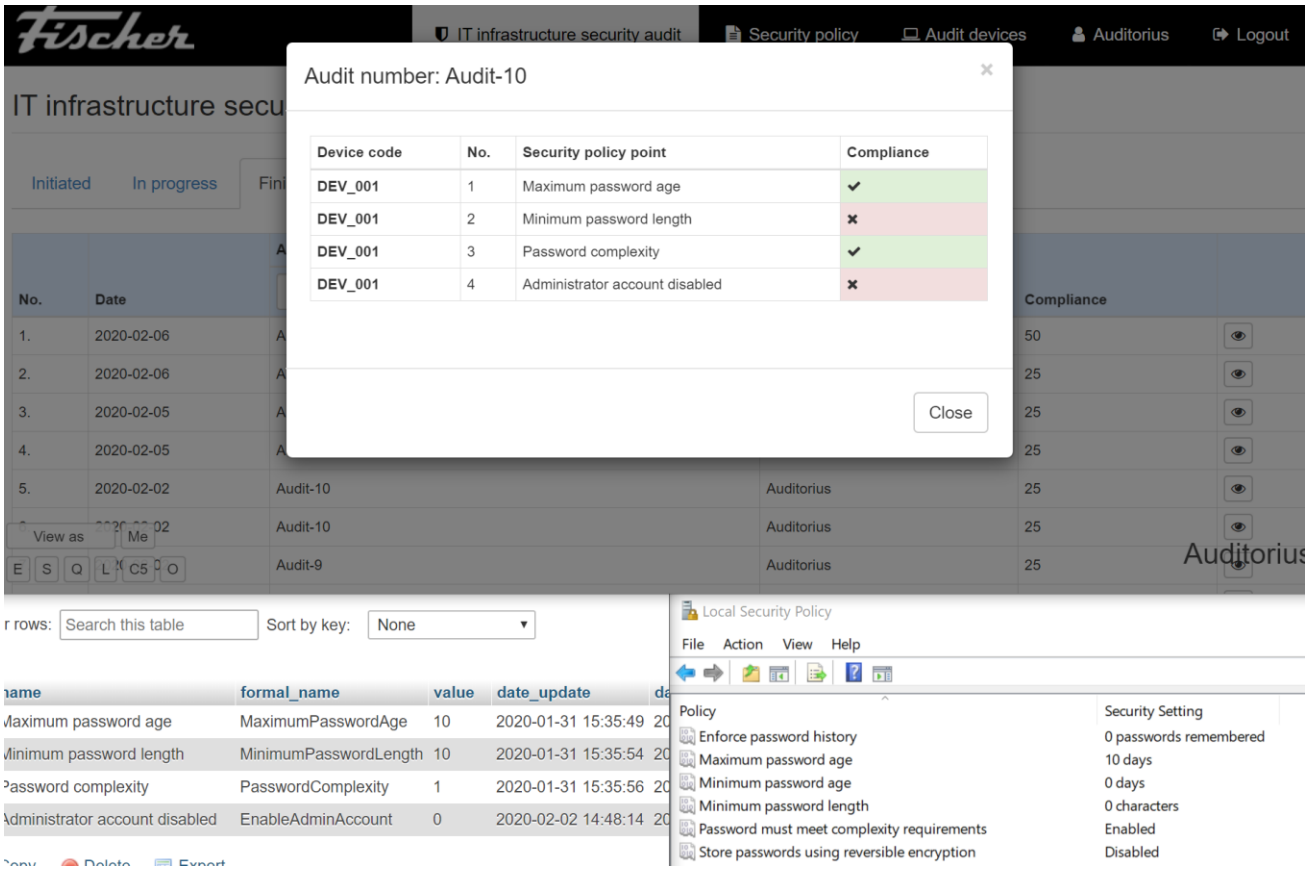
3.4 pav. Gautos vietinės saugos politikos, tekstinio failo formatu, ištrauka

Tuo tarpu duomenų bazėje, prie saugos politikos punkto, yra saugomas formalus punkto pavadinimas ir galima to punkto reikšmė. Pavyzdys pateikiamas toliau, 3.5 pav.:

name	formal_name	value
Maximum password age	MaximumPasswordAge	10
Minimum password length	MinimumPasswordLength	10
Password complexity	PasswordComplexity	1
Administrator account disabled	EnableAdminAccount	0

3.5 pav. Duomenų bazės ištrauka, aprašanti formalią saugos politiką

Turint formalų politikos punkto pavadinimą ir surinktus duomenis, galima juos lyginti tarpusavyje. Tai daroma paėmus visą turimą formalią saugos politiką, einant per kiekvieną jos punktą ir ieškant tokio punkto turimuose duomenyse. Jei nerandamas toks punktas – atlikus auditą jo būsena bus pažymėta kaip „Atlikta su klaidomis“ bei audito ataskaitoje bus matomas punktas, kuris nebuvo patikrintas. Radus tokį punktą turimuose duomenyse, yra tikrinama jo reikšmė. Atlikus visų punktų patikrinimą, apskaičiuojamas atlikto audito atitikties procentas. Atlikto audito ataskaitos pavyzdys parodytas 3.6 pav.

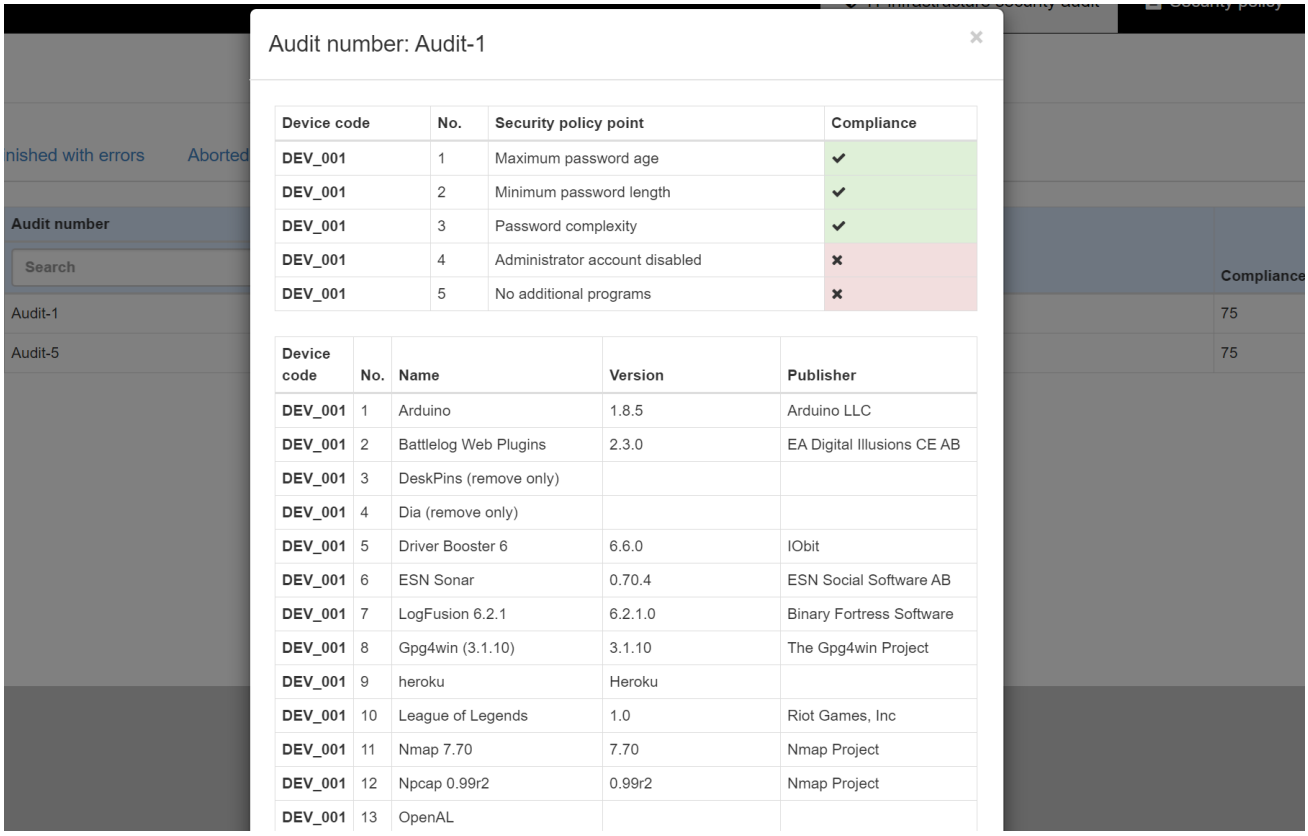


3.6 pav. Atliktos audito ataskaitos pavyzdys

Viršutiniame paveikslo lange matome audito informacijos ataskaitą. Žemiau kairėje pateikiami saugos punktai su galimomis reikšmėmis, o kairėje pusėje – Windows konfigūracinio failo ištrauka, iš kurios yra surinkinėjami duomenys. Kaip matome, audito sistema duomenis surinko ir palygino teisingai.

Informacijos rinkimas iš Powershell konfigūracijos valdymo sistemos

Informacijai apie įrenginyje įdiegtas programas panaudotas Powershell karkasas ir scenarijus, kuris padeda vartotojams greitai automatizuoti užduotis, kurias valdo operacinė sistema [22]. Scenarijaus pavyzdys, skirtas surinkti įdiegtų programų sąrašui pateiktas 7.2 priede.



3.7 pav. Įdiegtų programų įrenginyje sąrašo pavyzdys

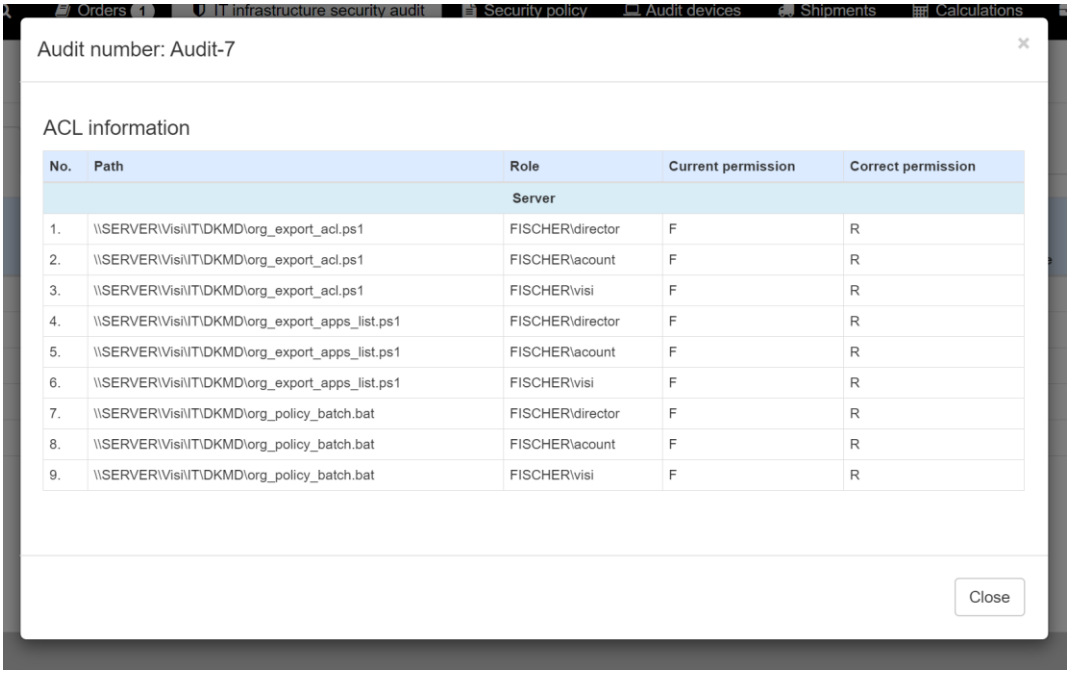
Scenarijus aprašytas taip, kad praleistų sistemines programas tokias kaip Microsoft Redistributable, Intel Graphics ir kt. Būtina pabrėžti, kad kiekvienam mazgui šis scenarijus gali skirtis priklausomai nuo paties įrenginio aparatinės ir programinės įrangos sudėties.

Gavus įdiegtų programų sąrašą, jis yra lyginamas su leidžiamos programinės įrangos sąrašu, ir programos, kurios yra neleistinos įdiegti, atspausdinamos išsamios audito ataskaitos lange.

To paties karkaso pagalba surenkama prieigos kontrolės sąrašo (*angl. Access Control List - ACL*) informacija. Šio scenarijaus pavyzdys pateikiamas 7.3 priede. Informacijos surinkimui naudojama sisteminė Windows icacls komanda, kuri grąžina prieigos informaciją nurodytai direktorijai ir visiems joje esantiems failams. Prieigos leidimai žymimi šiais simboliais [23]:

- F (angl. full access) – pilna prieiga,
- M (angl. modify access) – redagavimo prieiga,
- RX (angl. read and execute access) – skaitymo ir paleidimo prieiga,
- R (angl. read-only access) – tik skaitymo prieiga,
- W (angl. write-only access) – tik rašymo prieiga.

Prieigos leidimų sąrašo pavyzdys pateikiamas 3.8 pav.



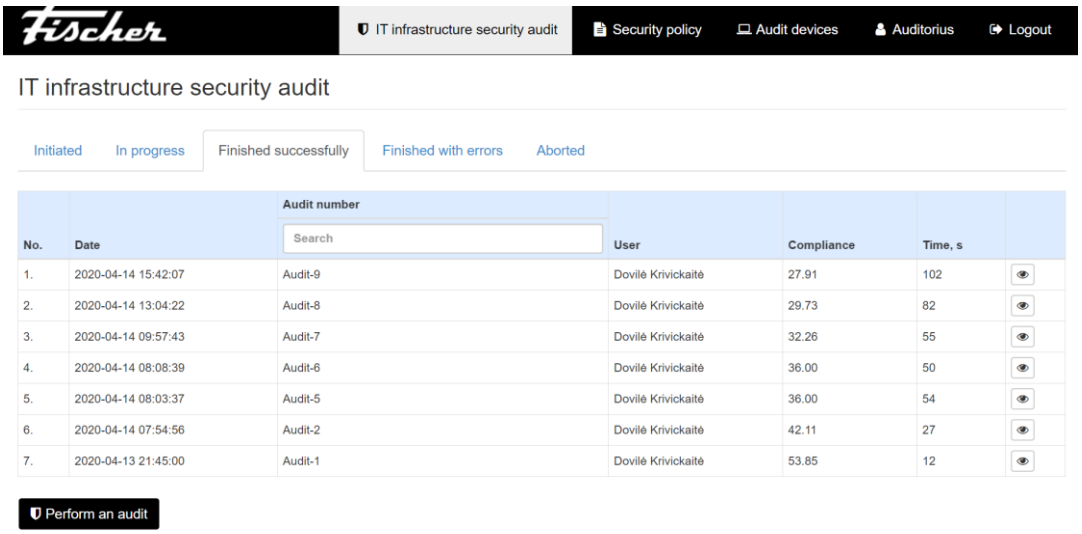
No.	Path	Role	Current permission	Correct permission
		Server		
1.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\director	F	R
2.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\acount	F	R
3.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\visi	F	R
4.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\director	F	R
5.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\acount	F	R
6.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\visi	F	R
7.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\director	F	R
8.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\acount	F	R
9.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\visi	F	R

3.8 pav. Prieigos kontrolės sąrašo informacija

Iš pateikto paveikslo matome, kad nurodytiems failams (*org_export_acl.ps1*, *org_export_apps_list.ps1* ir *org_policy_bath.bat*) yra suteiktos pilnos prieigos teisės (vartotojams, kurių rolė *director*, *account* arba *visi*), nors pagal aprašytą saugos politikos dokumentą, šioms vartotojų rolėms turėtų būti nustatyta tik skaitymo prieiga.

3.8. IT saugos audito sistemos prototipo vartotojo sąsaja

IT saugos audito sistemos vartotojo sąsaja realizuota kaip žiniatinklio programa, todėl yra pasiekiama per vartotojo norimą naršyklę. Sistemos meniu juostoje matomi trys pagrindiniai punktai: IT infrastruktūros saugos auditas, Saugos politika ir Audito įrenginiai.



No.	Date	Audit number	User	Compliance	Time, s
1.	2020-04-14 15:42:07	Audit-9	Dovilė Krivickaitė	27.91	102
2.	2020-04-14 13:04:22	Audit-8	Dovilė Krivickaitė	29.73	82
3.	2020-04-14 09:57:43	Audit-7	Dovilė Krivickaitė	32.26	55
4.	2020-04-14 08:08:39	Audit-6	Dovilė Krivickaitė	36.00	50
5.	2020-04-14 08:03:37	Audit-5	Dovilė Krivickaitė	36.00	54
6.	2020-04-14 07:54:56	Audit-2	Dovilė Krivickaitė	42.11	27
7.	2020-04-13 21:45:00	Audit-1	Dovilė Krivickaitė	53.85	12

3.9 pav. IT saugos auditų informacijos langas

IT infrastruktūros saugos audito lange matoma pagrindinė įvykdytų auditų informacija, kuri išskirstyta pagal audito būsenas: inicijuotas, vykdomas, sėkmingai įvykdytas, užbaigtas su klaidomis ir atšauktas. Taip pat šiame lange yra galimybė inicijuoti auditą – tam veiksmui atlikti reikia paspausti audito inicijavimo mygtuką, esantį apačioje. Šis langas pavaizduotas 3.9 pav.

Išsamesnė kiekvieno audito informacija pasiekiama spustelėjus peržiūros mygtuką dešinėje pusėje. Naujai atsidariusiame lange matoma audituotų įrenginių atitiktis saugos politikos dokumentui. Tai pat ten pateikiama papildomai įdiegtų programų bei prieigos kontrolės sąrašo informacija. Pastaroji informacija sutrauka pagal kiekvieną įrenginį, tad norint peržiūrėti kiekvieno įrenginio informaciją, reikia spustelėti ant norimo įrenginio pavadinimo. Lango apačioje pateikiama informacija apie audito metu gautas klaidas, jei tokių buvo. Šis langas pavaizduotas 3.10 pav.

Audit number: Audit-9

Security policy

Device code	Administrator account disabled	Auto turn off after 17:00	Correct Access Control List (ACL)	Maximum password age	Minimum password length	No additional programs	Password complexity
IT_Dovile	✔	–	Not aplicable	✔	✔	✖	✔
Server	✔	–	✖	✖	✖	✔	✔
IT_Alvydas	✔	–	Not aplicable	✖	✖	✖	✖
IT_Laurynas	✔	–	Not aplicable	✖	✖	✖	✖
IT_Gustas	✔	–	Not aplicable	✖	✖	✖	✖
Aušra_PC	✔	–	Not aplicable	✖	✖	✖	✖
Diana_PC	✔	–	Not aplicable	✖	✖	✖	✖

Additional programs

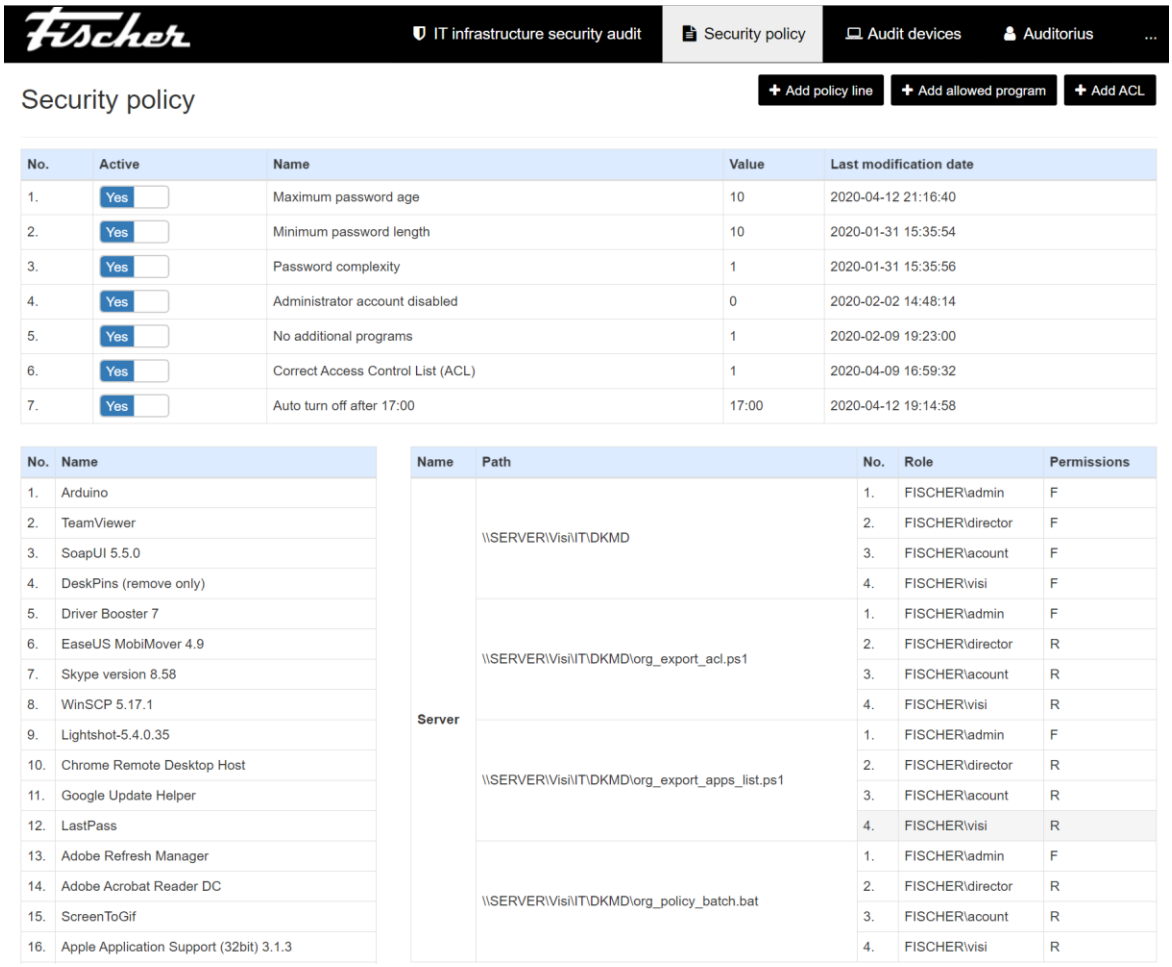
No.	Name	Version	Publisher
		IT_Dovile	
1.	Quake III Gold	2.0.0.2	GOG.com
2.	Adobe Flash Player 32 PPAPI	32.0.0.344	Adobe
3.	Brave	80.1.5.123	Brave Software Inc
4.	glogg	v1.1.4-x86_64	
5.	McAfee WebAdvisor	4.1.1.90	McAfee, LLC.
		IT_Alvydas	
		IT_Laurynas	
		IT_Gustas	
		Aušra_PC	
		Diana_PC	

ACL information

No.	Path	Role	Current permission	Correct permission
		Server		
1.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\director	F	R
2.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\acount	F	R
3.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\visi	F	R
4.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\director	F	R
5.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\acount	F	R
6.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\visi	F	R
7.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\director	F	R
8.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\acount	F	R

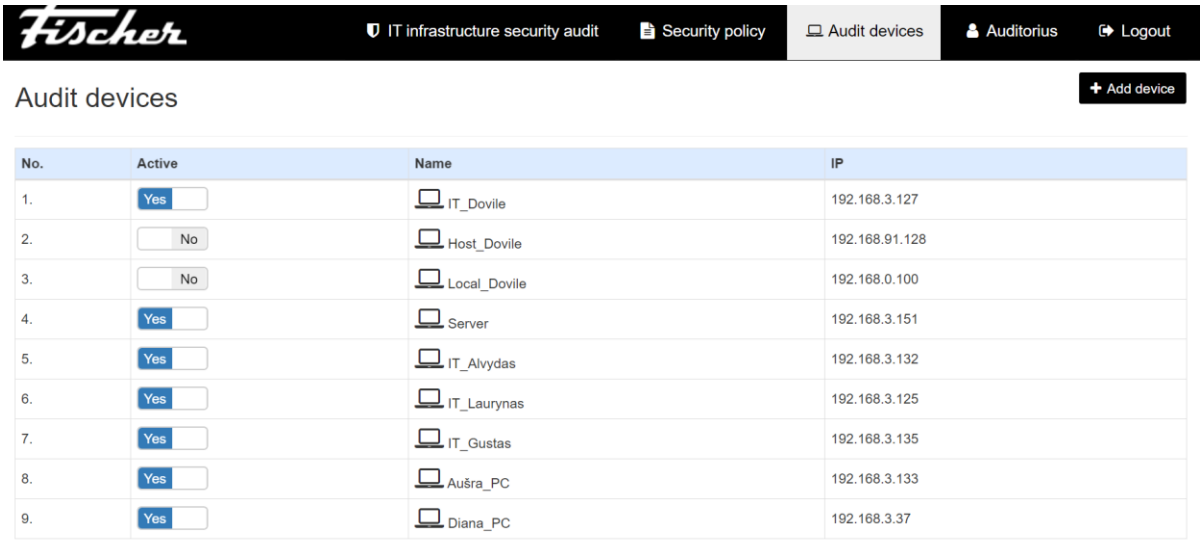
3.10 pav. Išsamesnės konkrečios audito ataskaitos langas

Saugos politikos lange galima peržiūrėti ir redaguoti formalizuotą saugos politiką: pridėti leistiną programą, naują politikos dokumento eilutę ar prieigos kontrolės sąrašo eilutę bei keisti saugos politikos eilutės aktyvumą. Šis langas pavaizduotas 3.11 pav.



3.11 pav. Saugos politikos langas

Audito įrenginių lange galima peržiūrėti audituojamų įrenginių informaciją, pridėti naują įrenginį ar keisti įrenginio aktyvumą. Šis langas pavaizduotas 3.12 pav.



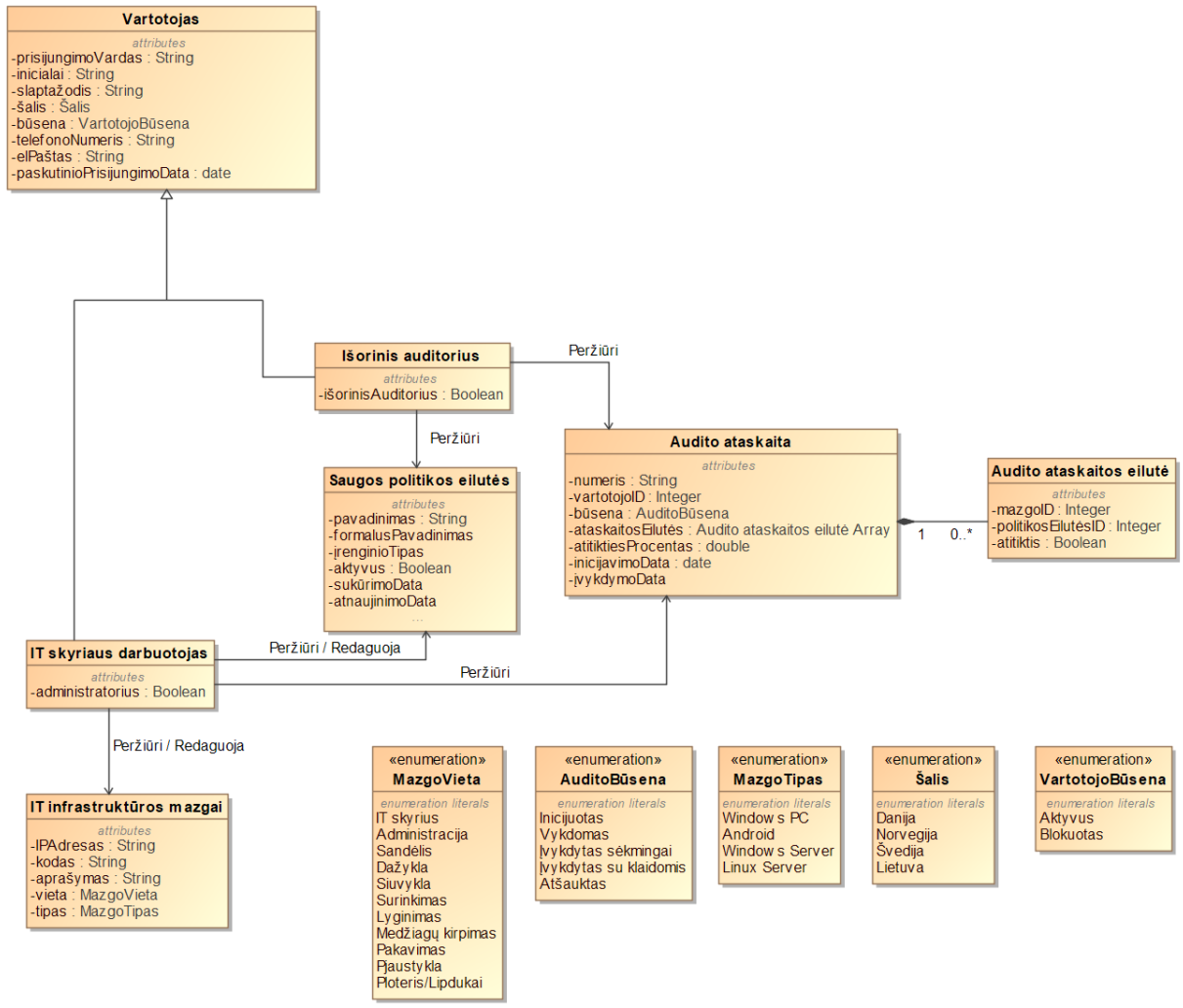
3.12 pav. Audito įrenginių informacijos langas

3.9. IT saugos audito atitikties skaičiavimo metodika

IT saugos audito atitikties procentas yra skaičiuojamas vidurkio principu: atitinkamai kiekvienam įrenginiui paimamas visų saugos politikos punktų kiekis ir padalinamas iš atitinkančių punktų kiekio. Kai kurie saugos politikos punktai galioja ne visiems įrenginiams, todėl skaičiuojant atitikties procentą į tai yra atsižvelgiama – į galutinį kiekį tokie punktai neįtraukiami. Nerasti saugos politikos punktai yra traktuojami kaip neatitinkantys, taigi, jie įtraukiami į galutinį skaičių.

3.10. IT saugos audito sistemos prototipo duomenų modelis

Toliau pateiktame 3.13 pav. prototipo duomenų modelyje matoma, kad sistemoje saugoma informacija apie vartotojus, kurie skirstomi pagal tipus: išorinis auditorius ir IT skyriaus darbuotojas. Abiejų tipų vartotojai gali peržiūrėti audito ataskaitos duomenis, kuriuos sudaro informacija apie pačią audito ataskaitą ir audito ataskaitos eilučių informacija. Taip pat yra galimybė peržiūrėti saugos politikos dokumentą, kurį sudaro informacija apie patį saugos politikos dokumentą bei saugos politikos eilučių informacija. IT skyriaus darbuotojas papildomai gali redaguoti saugos politikos dokumentą bei peržiūrėti ir redaguoti IT infrastruktūros mazgų sąrašą.



3.13 pav. IT saugos audito sistemos prototipo duomenų modelis

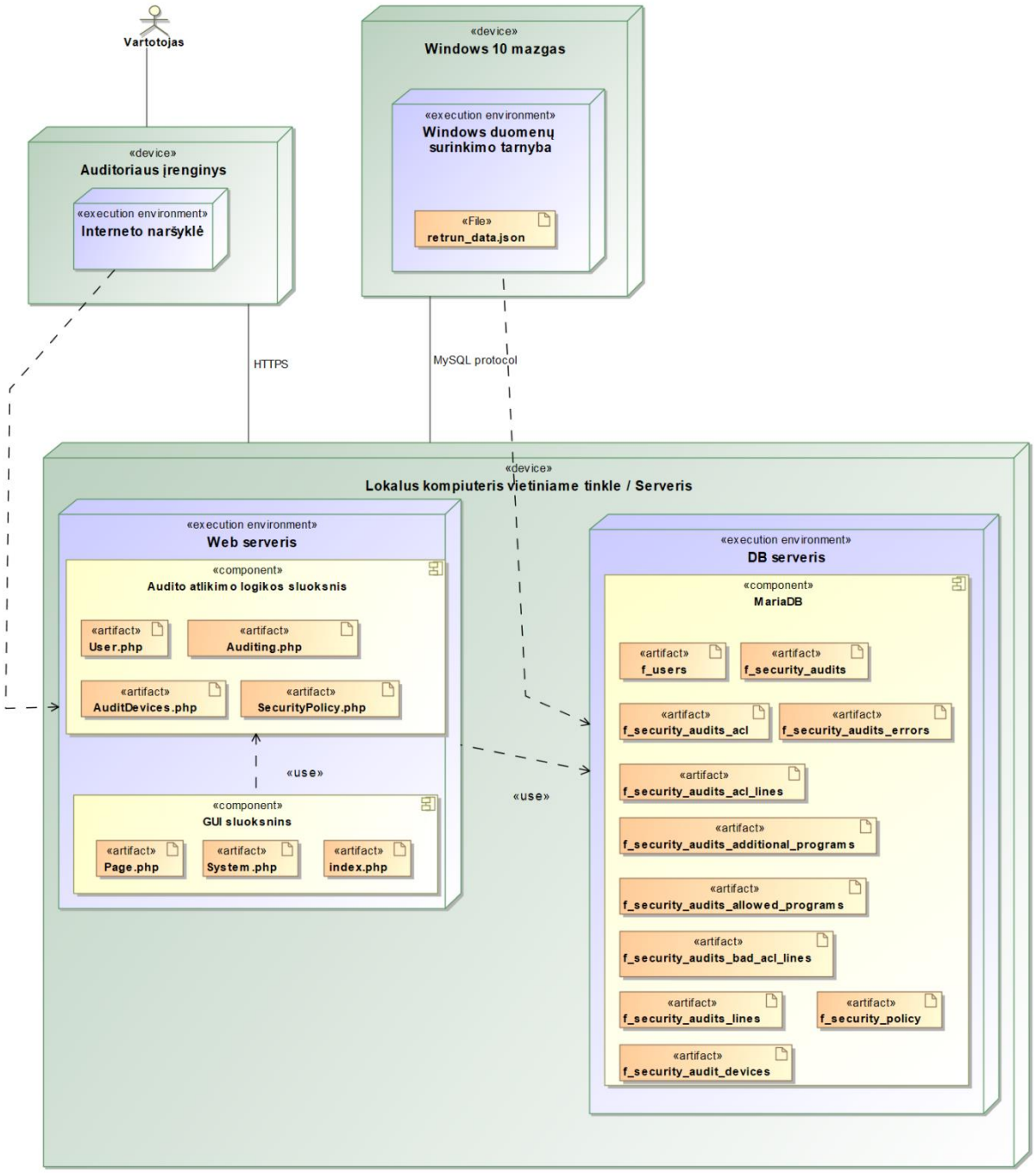
Saugos politikos dokumentą sudaro eilutės, apie kurias saugoma tokia informacija: pavadinimas, formalus pavadinimas (šis pavadinimas naudojimas politikos lyginimui su gauta mazgų

informacija), įrenginio, kuriam taikomas šis politikos punktas, tipas, aktyvumo žymą bei sukūrimo bei eilutės atnaujinimo datos.

Taip pat sistemoje saugoma audito ataskaitos informacija: audito inicijavimo ir vykdymo pabaigos datos, vartotojo, kuris inicijavo auditą, ID, audito būsena, audito atitikties procentas bei pačios audito eilutės. Jas sudaro mazgo ID, politikos eilutės, kuri buvo tikrinama, ID bei atitiktis tai eilutei.

3.11. IT saugos audito sistemos prototipo diegimo modelis

Žemiau pateiktame 3.14 pav. matomas saugos audito sistemos prototipo diegimo modelis. Jį sudaro auditoriaus įrenginys, turintis interneto naršyklę, IT infrastruktūros mazgas bei serveris.



3.14 pav. IT infrastruktūros automatizuoto saugos audito sistemos diegimo modelis

Mazguose įdiegtos duomenų surinkimo tarnybos, kurios perduoda surinktus duomenis į duomenų bazės serverį, esantį fiziniame serverio įrenginyje JSON formatu. Fiziniame serveryje yra

duomenų bazės serveris, kuriame įdiegta MariaDB duomenų bazės valdymo sistema, bei žiniatinklio serveris, kuriame įdiegta audito atlikimo sistema. GUI sluoksnio komponente parodyti kokie failai sudaro šį sluoksnį: *Page.php* faile aprašyta GUI aplinka, meniu juostos ir kiti su atvaizdavimu susiję dalykai. *System.php* failas atsakingas už puslapių nukreipimą. Audito atlikimo logikos sluoksnyje patalpinti failai, kurie atsakingi už visą audito atlikimo logiką: pradedant saugos politikos peržiūra ir baigiant audito ataskaitos generavimu.

3.12. Saugos audito sistemos prototipo realizacijos išvados

Prototipe realizuoti du iš trijų pagrindinių automatizuoto audito atlikimo veiksmų: informacijos surinkimas iš mazgų konfigūracinių failų ir audito politikos lyginimas su turimų konfigūracinių failų informacija. Saugos politikos formalizavimas nebuvo realizuotas, tad formalus saugos politikos dokumentas buvo aprašytas rankiniu būdu.

Informacija iš mazgų surenkama naudojantis Batch ir PowerShell scenarijais, kuriuose aprašytos specialios komandos duomenų surinkimui iš vietinės saugos politikos konfigūracijos, registrų ir NTFS particijoje esančios MFT lentelės. Scenarijų vykdymo metu, jie gautus rezultatus išsaugo tekstiniame faile, kurie vėliau nuskaitomi, sugrupuojami ir grąžinami sistemai JSON formatu.

Saugos audito ataskaitai paruošti yra lyginama turima formali saugos politika ir duomenys, gauti iš konfigūracinių failų. Kiekvienas politikos punktas yra žymimas kaip atitinkantis, neatitinkantis ir nerastas. Palyginus visus saugos politikos punktus yra apskaičiuojamas atitikties procentas visai IT infrastruktūrai. Taip pat užbaigus audito atlikimo procedūrą, vartotojui pateikiama galimybė peržiūrėti išsamesnę audito ataskaitos informaciją apie neatitinkančius saugos politikos punktus kiekvienam įrenginiui.

Saugos audito sistemos prototipe realizuota vartotojo sąsaja, kurioje galima peržiūrėti ir redaguoti saugos politikos dokumentą, įjungti / išjungti audituojamus įrenginius bei peržiūrėti anksčiau atliktų saugos auditų ataskaitas. Ataskaitose pateikiama informacija apie saugos politikos atitiktį kiekvienam įrenginiui, įdiegtų programų sąrašas, prieigos kontrolės sąrašas bei klaidos, jei tokių buvo. Audito procedūra inicijuojama asinchroniškai, kad netrikdytų vartotojo darbo su sistema, o kreipimasis į IT infrastruktūros mazgus realizuotas sinchroniškai, taikant priverstinio nutraukimo laiko žymą.

4. IT SAUGOS AUDITO SISTEMOS PROTOTIPO TYRIMAS

4.1. IT saugos audito sistemos prototipo tyrimo tikslas ir uždaviniai

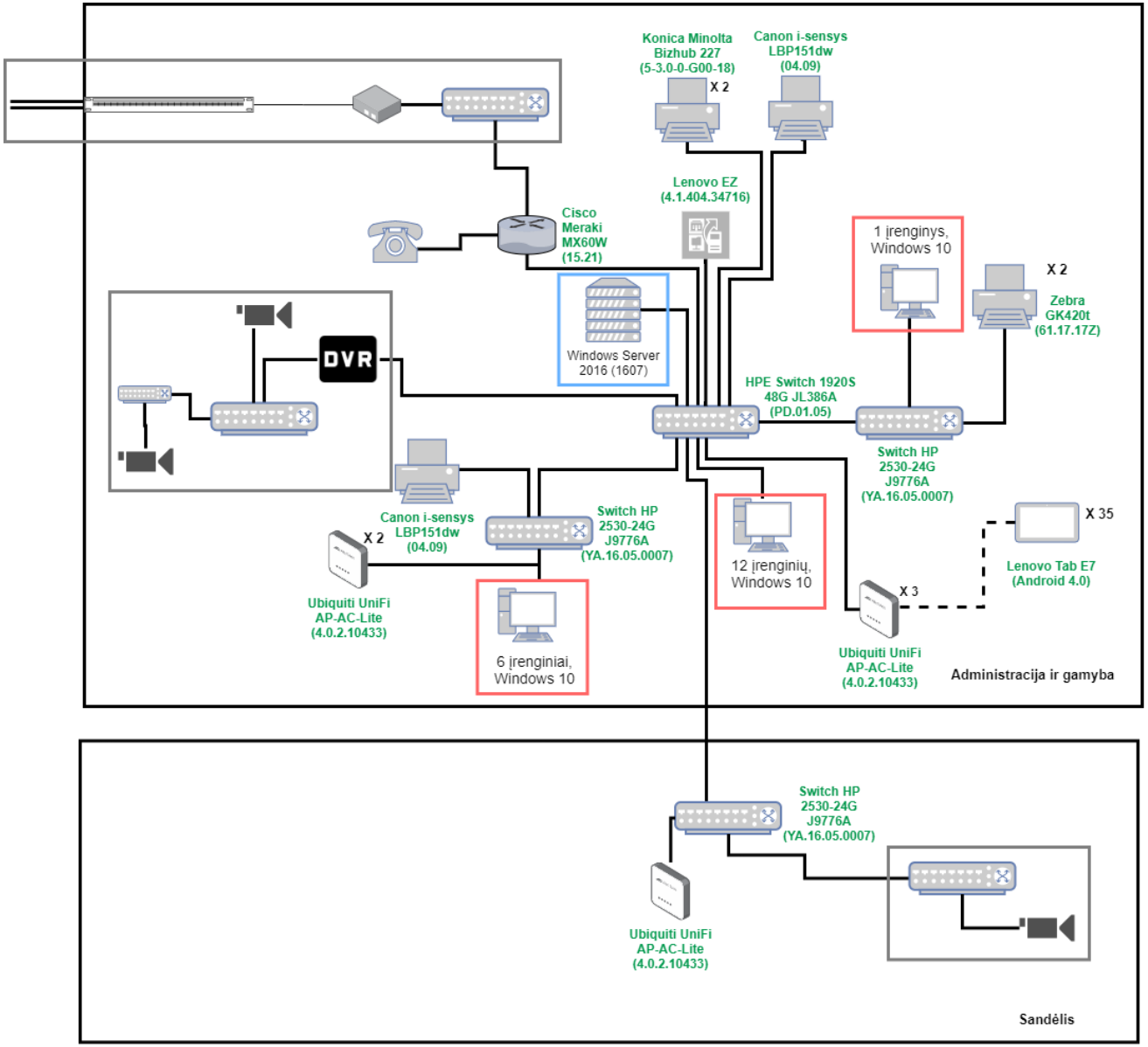
Tikslas – ištirti prototipo veikimą funkcionalumo, kokybiniu ir kiekybiniu matais bei įvertinti įmonės IT infrastruktūros saugumą, naudojantis sukurtu prototipu. Tyrimo uždaviniai:

- palyginti prototipo funkcionalumą su egzistuojančiais sprendimais;
- ištirti gaunamų duomenų kokybę saugos auditui atlikti;
- ištirti prototipo veikimą didėjant duomenų kiekiui;
- įvertinti įmonės IT infrastruktūros saugumą naudojantis realizuotu prototipu.

4.2. IT saugos audito sistemos prototipo tyrimo aplinka

Turimos infrastruktūros schema pavaizduota 4.1 pav. Mazgai, iš kurių renkama informaciją saugos auditui – Windows 10 OS kompiuteriai, kurie schemoje pažymėti raudonai. Įvairūs failai bei įmonės duomenys saugomi serveryje, kuris pažymėtas mėlyna spalva. Iš šio įrenginio papildomai surenkama prieigos kontrolės sąrašo informacija. Pilnam infrastruktūros saugumo ištyrimui papildomai reikėtų surinkti informaciją iš Android OS planšečių, maršrutizatorių, spausdintuvų bei ugniasienių (visų tokių tipų įrenginių informacija schemoje pažymėta žaliai, kur skliaustuose nurodoma programinės įrangos versija), tačiau prototipe šios dalys nerealizuotos. Pilkai apibraukti įrenginiai yra konfigūruojami ir prižiūrimi išorinių įmonių, todėl jų pavadinimai ir programinės įrangos versijos informacija yra nepateikiami. Surinkta informacija iš mazgų lyginama su aprašyta formalizuota saugos politika ir auditoriui pateikiama ataskaita apie tai, kiek ir kokių mazgų atitinka aprašytą saugos politiką. Saugos politikos formalizavimo metodas prototipe nebuvo realizuotas, todėl formalizuota saugos politika buvo aprašyta rankiniu būdu.

Tyrimas atliktas nuotoliniu būdu, prisijungus prie įmonės tinklo per VPN. Prieš pradedant tyrimą, mazguose buvo įdiegtas mikroprocesas, kuris surenka ir grąžina duomenis cURL bibliotekos pagalba. Vartotojo sąsajos programinis kodas ir duomenų bazė patalpinta lokaliame kompiuteryje, su kurio prisijungta prie įmonės vidinio tinklo.



Žymėjimas	Reikšmė
	Optinė panelė (ODF)
	Keitiklis
	Komutatorius
	Maršrutizatorius
	Telefonas
	Tinklinė duomenų saugykla (NAS)
	Serveris
	Spausdintuvas
DVR	Vaizdo įrašymo įrenginys (DVR)
	Kamera
	Prieigos taškas
	Kompiuteris
	Planšetė

4.1 pav. Turimos infrastruktūros schema

4.3. IT saugos audito sistemos prototipo palyginimas su egzistuojančiomis sistemomis funkcionalumo požiūriu

Lyginant sistemas buvo išskirti pagrindiniai punktai, kurie yra svarbūs pilnam automatizuoto sistemos audito atlikimui. Žemiau esančioje 4.1 lent. pateikiama lyginamoji sukurto prototipo ir egzistuojančių sistemų analizės rezultatai.

4.1 lent. Prototipo ir egzistuojančių sistemų lyginamoji analizė

	Kuriama sistema	*„Risk Watch“*	*„PC system audit“*	*„CRAMM“*	*„Solarwinds Access Rights Manager“*	*„audits.io“*
Saugos audito atitikties skaičiavimas	Taip	Taip	Ne	Ne	Ne	Taip
Išsami audito ataskaita	Taip	Taip	Taip	Taip	Taip	Taip
Audituojamų įrenginių valdymas	Taip	Ne	Ne	Ne	Taip	Ne
Automatizuotas auditas atliekamas remiantis saugos politikos dokumentu	Taip	Taip	Ne	Taip	Ne	Ne
Prieigos kontrolės sąrašo auditavimas	Taip	Ne	Ne	Ne	Taip	Ne
Įdiegtos programinės įrangos auditavimas	Taip	Ne	Taip	Ne	Ne	Ne

Kaip matome iš pateiktos lentelės, analizės metu nebuvo rasta tokia sistema, kuri atitiktų visus išsikeltus funkcionalumo punktus. Taigi, norint rinktis jau egzistuojančius rinkos produktus tam, kad būtų galima atlikti pilną sistemos auditą, reikėtų derinti kelis skirtingus programinės įrangos sprendimus.

4.4. IT saugos audito sistemos prototipo duomenų kokybinis tyrimas

Norint gauti kuo teisingesnius audito ataskaitos, saugos politika buvo kuriama dviem etapas: iš pradžių buvo sudarytas bendras, iš anksto žinomas formalus saugos politikos dokumentas. Tada inicijuotas auditas ir analizuotas jo gautas turinys: peržiūrimas gautų įdiegtų programų įrenginiuose sąrašas ir, esant poreikiui, papildomas saugos politikos dokumentas. Ypač tai aktualu sudarant leidžiamų programų sąrašą, kadangi sudėtinga iš anksto sudaryti programų sąrašą dėl vartotojų ir jų darbo specifikos įvairovės.

Gaunant vietinės saugos politikos ar prieigos kontrolės sąrašo informaciją nesusidurta su jokiais sunkumais, tačiau pastebima problema su programų sąrašu. Tai programinės įrangos versijos spausdinimas prie programinės įrangos pavadinimo. Tokiais atvejais sudėtinga užtikrinti sklandų programinės įrangos įtraukimą į leidžiamų programų sąrašą, kadangi kiekvieną kartą atsinaujinus programinę įrangą ji iš naujo turėtų būti įtraukta į sąrašą. Taip pat tyrimo metu nustatyta, kad kartais gaunama tik programinės įrangos versija – be jos pavadinimo ar kūrėjo, tad tam, kad pagerinti gaunamų duomenų kokybę, reikėtų nuodugniau ištirti šį atvejį.

Taip pat tyrimo metu siekta rasti optimaliausia priverstinio nutraukimo (*angl. timeout*) laiką negavus duomenų iš įrenginio. Bandymų metu pastebėta, kad pradžioje nustatytas 5 sekundžių laiko tarpas yra per trumpas kai kuriems įrenginiams, todėl laikas buvo padidintas iki 10 sekundžių.

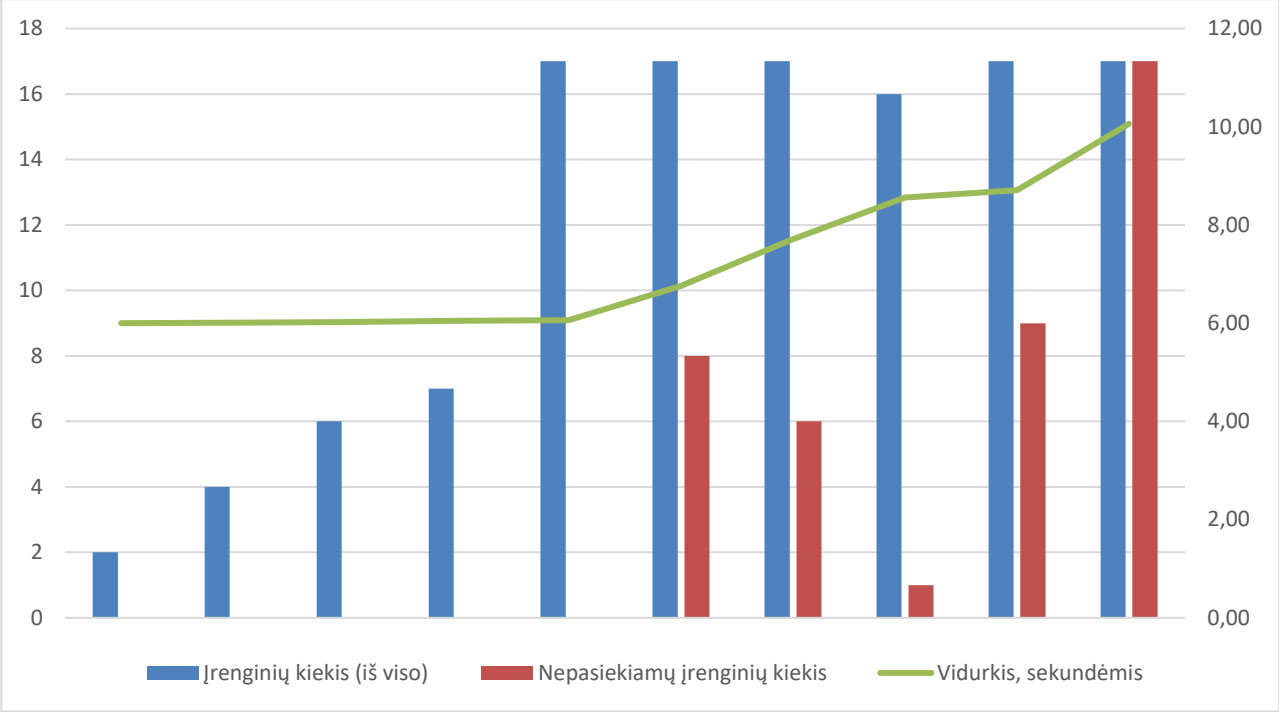
4.5. IT saugos audito sistemos prototipo duomenų kiekybinis tyrimas

IT saugos audito kiekybinis tyrimas atliktas apskaičiuojant vidutinį audito atlikimo greitį kintant audito įrenginių kiekiui. Skaičiuojant vidurkį svarbu atsižvelgti į tai, kad pati audito procedūra galėjo būti pradėta vykdyti iki 60 sekundžių vėliau nei buvo inicijuota, kadangi periodinė užduotis, vykdanti audito procedūrą, paleidžiama kas minutę. Dėl šios priežasties, prieš skaičiuojant vidurkį, audito pradžios data yra suapvalinama iki artimiausios minutės reikšmės. Pavyzdžiui, jei audito procedūra buvo inicijuota 15:42:07, skaičiuojant vidurkį imama 15:43:00 reikšmė. Toliau 4.2 lentelėje pateikiami kiekybinio tyrimo rezultatai.

4.2 lent. Kiekybinio tyrimo rezultatai

Vykdymo laikas, sekundėmis	Įrenginių kiekis	Nepasiekiamų įrenginių kiekis	Vidurkis, sekundėmis
12	2	0	6
24	4	0	6,01
37	6	0	6,02
49	7	0	6,05
103	17	0	6,06
115	17	8	6,76
131	17	6	7,71
137	16	1	8,56
148	17	9	8,71
171	17	17	10,06

Iš aukščiau pateiktos lentelės matome, kad audito atlikimo laikas yra tiesiogiai priklausomas nuo įrenginių kiekio: kuo daugiau audituojamų įrenginių, tuo ilgiau užtrunka pats auditas. Tačiau svarbu paminėti, jog didėjant įrenginių kiekiui, vidutinis vieno įrenginio audito laikas nedidėja, o išlieka panašus – apie 6,7 sekundės. Taigi iš pateiktų duomenų matome, kad algoritmo atlikimo laiko funkcinė išraiška idealiu atveju (kai atsako visi įrenginiai) yra *6n,* o blogiausiu atveju (kai neatsako nei vienas įrenginys) – *10,06n,* kur n – įrenginių kiekis, todėl galima teigti, kad audito atlikimo algoritmo laiko sudėtingumas yra tiesinis (žymimas *O(n)*). Gautų duomenų diagrama pateikiama 4.2 pav.



4.2 pav. Kiekybinio tyrimo rezultatų diagrama

Audito atlikimo laikas yra priklausomas nuo įrenginių kiekio todėl, kad į kiekvieną įrenginį yra kreipiamasi sinchroniškai (tik sulaukus atsakymo arba nesulaukus atsakymo iš įrenginio per 10 sekundžių, kreipiamasi į kitą įrenginį), tad norint pagerinti audito atlikimo algoritmo laiko sudėtingumą, reikėtų į kiekvieną iš įrenginių kreiptis asinchroniškai.

4.6. Konkrečios įmonės IT saugos vertinimas, remiantis realizuotu prototipu

Atlikto IT saugos audito ataskaita pateikiama 4.3 pav. Iš ten pateiktų duomenų matoma, kad atitiktis saugos politikos dokumentui yra tik 37,21%: tik vienas iš tirtų įrenginių atitinka slaptažodžio keitimo laiko bei minimalaus jo ilgio punktus, vos du įrenginiai atitinka slaptažodžio sudėtingumo punktą. Šešiuose iš septyniolikos kompiuterių rasta įdiegtų programų, kurios nėra leidžiamos aprašytame formaliame saugos politikos dokumente. Taip pat pastebima, kad įrenginyje, kuriam taikomas prieigos kontrolės sąrašo vertinimas, netinkamai sukonfigūruoti leidimai nurodytiems failams ar aplankalams: šiuo metu jie turi pilną prieigą, nors pagal saugos formalų saugos politikos dokumento aprašą, jiems turėtų būti nustatyta tik skaitymo prieiga. Taigi, galima teigti, jog įmonės IT infrastruktūra nėra saugi apibrėžtos saugos politikos aprėptyje.

Audit number: Audit-29 (37.21%)

Security policy

Device code	Administrator account disabled	Correct Access Control List (ACL)	Maximum password age	Minimum password length	No additional programs	Password complexity
IT_Dovile	✔	Not aplicable	✔	✔	✔	✔
Server	✔	✖	✖	✖	✔	✔
IT_Alvydas	✔	Not aplicable	✖	✖	✔	✖
IT_Laurynas	✔	Not aplicable	✖	✖	✖	✖
IT_Gustas	✔	Not aplicable	✖	✖	✖	✖
Ausra_PC	✔	Not aplicable	✖	✖	✔	✖
Diana_PC	✔	Not aplicable	✖	✖	✔	✖
Jovita_PC	✔	Not aplicable	✖	✖	✔	✖
Lipdukai_UPS_PC	✔	Not aplicable	✖	✖	✔	✖
Sigute_PC	✔	Not aplicable	✖	✖	✔	✖
Milda_PC	✔	Not aplicable	✖	✖	✖	✖
Vytautas_PC	✔	Not aplicable	✖	✖	✖	✖
Mindaugas_PC	✔	Not aplicable	✖	✖	✖	✖
Tomas_PC	✔	Not aplicable	✖	✖	✔	✖
Audrius_PC	✔	Not aplicable	✖	✖	✖	✖
Lipdukai_PC	✔	Not aplicable	✖	✖	✔	✖
Ploteris_PC	✔	Not aplicable	✖	✖	✔	✖

Additional programs

No.	Name	Version	Publisher
		IT_Laurynas	
1.	LinkChecker 9.3	20180423	
2.	mp3splt		
3.	mp3splt-gtk		
		IT_Gustas	
1.	Brave	81.1.7.98	Brave Software Inc
2.	ApowerPDF V5.1.0.0716	5.1.0.0716	Apowersoft LIMITED
		Milda_PC	
1.	ESET Online Scanner v3		
2.	PDFCreator	1.7.2	pdfforge
		Vytautas_PC	
1.	AIMP	v4.51.2084, 01.12.2018	AIMP DevTeam
2.	Brave	81.1.7.98	Brave Software Inc
		Mindaugas_PC	
1.	HiSuite	9.1.0.305	
2.	IronPython 2.7.3	2.7.31000.0	IronPython Team
		Audrius_PC	
1.	Bundled software uninstaller		
2.	EGR-ShellExtension	1.2.1.100	EasternGraphics
3.	FilesFrog Update Checker		
4.	UmmyVideoDownloader	1.7.0.2	20160825

ACL information

No.	Path	Role	Current permission	Correct permission
		Server		
1.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\director	F	R
2.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\acount	F	R
3.	\\SERVER\Visi\IT\DKMD\org_export_acl.ps1	FISCHER\visi	F	R
4.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\director	F	R
5.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\acount	F	R
6.	\\SERVER\Visi\IT\DKMD\org_export_apps_list.ps1	FISCHER\visi	F	R
7.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\director	F	R
8.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\acount	F	R
9.	\\SERVER\Visi\IT\DKMD\org_policy_batch.bat	FISCHER\visi	F	R

4.3 pav. Konkrečios įmonės IT infrastruktūros saugos audito ataskaita

4.7. IT saugos audito sistemos prototipo tyrimo išvados

Palyginus realizuotą sistemos prototipą su rinkoje egzistuojančiais sprendimais pastebėta, kad nei vienas iš analizuotų sprendimų netenkina visų automatizuotai audito sistemai reikalingų funkcinių reikalavimų, taigi, realizuotas prototipas funkcionalumo požiūriu, yra pranašesnis.

Tiriant gaunamus konfigūracinių failų duomenis nustatyta, kad kai kuriuose programinės įrangos pavadinimuose įrašoma ir programos versija, kas sukelia tam tikrų nepatogumų, kadangi kiekvieną kartą atsinaujinus programinei įrangai ji iš naujo turėtų būti įtraukta į leidžiamų programų sąrašą, tačiau visumoje, gaunami duomenys yra kokybiški.

Tyrimo metu pastebėta, kad audito atlikimo laikas tiesiogiai priklauso nuo įrenginių kiekio ir galimybės prie jų prisijungti. Taip yra todėl, kad kreipimasis į mazgus atliekamas sinchroniškai. Atliekant tyrimą buvo rastas optimalus priverstinio nutraukimo laikas, kai mazgas nepasiekiamas, tam, kad audito procedūra neužsitęstų. Tačiau nepaisant didelio įrenginių kiekio, vidutinis vieno įrenginio atsakomumo greitis išlieka panašus, tad realizuoto algoritmo laiko sudėtingumas yra tiesinis.

Naudojantis sukurtu sistemos prototipu, atliktas konkrečios įmonės IT infrastruktūros auditas, kurio metu nustatyta, kad kai kuriuose įrenginiuose netinkamai sukonfigūruoti slaptažodžių reikalavimų punktai, taip pat rasta įdiegtų programų, kurios nėra aprašytos leistinų programų sąraše bei netinkamai nustatyta prieigos kontrolė saugos politikos dokumente aprašytiems aplankalams ir failams, taigi įmonės IT infrastruktūra nėra saugi apibrėžtos saugos politikos aprėptyje.

5. IT SAUGOS AUDITO SISTEMOS ANALIZĖS, PROJEKTAVIMO IR REALIZAVIMO IŠVADOS

Tam, kad būtų galima atlikti saugos auditą, reikia sukurti saugos politikos dokumentą, kuriame taisyklių pavidalu aprašomos galimos saugumo spragos, procesai, kaip turi būti vykdoma sauga bei objektai, kuriuos reikia apsaugoti. Efektyvesniam audito atlikimui rekomenduojama naudoti automatizuotus sprendimus, kadangi egzistuoja dideli duomenų kiekiai, ir rankiniu būdų juos surinkti ir išanalizuoti yra problematiška. Automatizuoto IT saugos audito sistemai projektuoti naudojamas modelis, kuris susideda iš centralizuoto serverio ir agentų, diegiamų audituojamuose įrenginiuose, kadangi tokiu būdu suprojektuotos sistemos pasižymi lankstumu ir išplečiamumu. Egzistuojantys rinkos sprendimai nėra tinkami automatizuotam saugos auditui atlikti dėl funkcionalumo trūkumo juose.

Dėl šios priežasties buvo suprojektuota automatizuoto saugos audito sistema, susidedanti iš trijų dalių: saugos politikos formalizavimo, audito mazgų konfigūracinių failų informacijos surinkimo ir paties audito atlikimo. Saugos politikos formalizavimui naudojamas suvaržytos kalbos metodas, kurio pagalba sukuriamas skaitmeninis saugos politikos dokumentas, kuris gali būti konvertuojamas į kompiuteriui perskaitomą duomenų formatą. Duomenų surinkimui suprojektuotas agentas, kuris surenka informaciją iš audituojamų įrenginių bei atlieka formalaus saugos politikos dokumento palyginimą su gautais įrenginių duomenimis. Sistema suprojektuota taip, kad audito procedūra būtų atliekama fiziškai nebūnant prie audituojamų įrenginių – auditas inicijuojamas naudojantis interneto naršykle.

Prototipe realizuotos dvi suprojektuotos sistemos dalys – informacijos surinkimas iš konfigūracinių įrenginių failų bei pačios audito procedūros atlikimas, o formalus saugos politikos dokumentas aprašytas rankiniu būdu. Įrenginiuose įdiegtas mikroprocesas, kuris surenka duomenis iš vietinės saugos politikos konfigūracijos, registrų ir NTFS particijoje esančios MFT lentelės, bei grąžina surinktą informaciją sistemai, kuri atlieka saugos audito procedūrą.

Atlikus realizuoto prototipo tyrimą, nustatyta, kad realizuotas prototipas funkcionalumo požiūriu yra pranašesnis už rinkoje esančius egzistuojančius sprendimus. Taip pat patikrinta gaunamų duomenų kokybė: nustatyta, kad kai kurios programos prie savo pavadinimo įrašo programinės įrangos versiją, kas sukelia tam tikrų nepatogumų, kadangi kiekvieną kartą atsinaujinus programinei įrangai, toks programos pavadinimas turėtų būti įtrauktas į leidžiamų programų sąrašą saugos politikos dokumente.

Eksperimento metu ištirtas prototipo veikimas didėjant duomenų kiekiui: saugos audito atlikimo laikas tiesiogiai priklauso nuo įrenginių kiekio ir galimybės jų prisijungti. Tačiau didėjant įrenginių kiekiui, vidutinis audito atlikimo laikas vienam įrenginiui nesikeičia, todėl nustatyta, kad realizuoto algoritmo laiko sudėtingumas yra tiesinis.

Naudojantis realizuotu prototipu buvo atliktas konkrečios įmonės IT infrastruktūros auditas, kuris parodė, kad įrenginiuose netinkamai sukonfigūruoti slaptažodžių reikalavimai, įdiegtos papildomos programos bei nustatyta netinkama prieigos kontrolė nurodytiems failams ir direktorijoms, taigi įmonės IT infrastruktūra nėra saugi apibrėžtos saugos politikos aprėptyje.

6. LITERATŪRA

[1] Egidijus Kazanavičius, Algimantas Venčkauskas, Agnius Liutkevičius, Arūnas Vrubliauskas, „Informacijos saugos politika,“ įtraukta *Informacijos saugos vadyba*, Kaunas, 2008, pp. 49-80.

[2] „ISSAI 3200 – Veiklos audito procesas,“ [Tinkle]. Available: https://www.vkontrole.lt/INTOSAI_standartai/ISSAI_3200_20016_LT.pdf. [Kreiptasi 20 sausis 2020].

[3] „Lietuvos Respublikos Seimas,“ 4 rugsėjis 1997. [Tinkle]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.42817. [Kreiptasi 4 gruodis 2019].

[4] „Lietuvos Respublikos Seimas,“ 24 liepa 2013. [Tinkle]. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399?jfwid=-bgd9ay3ie. [Kreiptasi 4 gruodis 2019].

[5] „ISACA Lithuania Chapter,“ [Tinkle]. Available: http://www.isaca.org/chapters1/Lithuania/COBIT/Pages/default.aspx?utm_referrer=direct%2Fnot%20provided. [Kreiptasi 4 gruodis 2019].

[6] D. L. Cannon, CISA Certified Information Systems Auditor Study Guide, 2011.

[7] L. M. N. G. Andrius Januta, „Informacinės saugos audito vykdymas remiantis ISO/IEC 27000 šeimos standartų reikalavimais,“ *Jaunųjų mokslininkų darbai,* pp. 110-117, 25 gegužė 2011.

[8] „European Union Agency For Cybersecurity,“ [Tinkle]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_riskwatch.html. [Kreiptasi 1 gruodis 2019].

[9] „Software Advice,“ [Tinkle]. Available: https://www.softwareadvice.com/risk-management/riskwatch-profile/. [Kreiptasi 1 gruodis 2019].

[10] „Softinventive Lab,“ [Tinkle]. Available: https://www.softinventive.com/pc-audit/. [Kreiptasi 24 balandis 2020].

[11] „European Union Agency For Cybersecurity,“ [Tinkle]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. [Kreiptasi 1 gruodis 2019].

[12] Mohamed Ghazouani, Sophia Faris, Hicham MedromiAdil Sayouti, „Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk,“ *International Journal of Computer Applications,* t. 103, nr. 8, pp. 36-42, 2014.

[13] „Solarwinds,“ [Tinkle]. Available: https://www.solarwinds.com/access-rights-manager/use-cases/role-based-access-control. [Kreiptasi 24 balandis 2020].

[14] Plan Brothers, [Tinkle]. Available: https://www.planbrothers.io/products/audits. [Kreiptasi 24 balandis 2020].

[15] Rafael Accorsi, Adolf Hohl, Delegating Security Logging in Pervasive Computing Systems, 2006.

[16] „National Institute of Standards and Technology,“ rugsėjis 2006. [Tinkle]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf. [Kreiptasi 26 sausi 2020].

[17] Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, 4th Ed, 2007.

[18] Olof Söderström, Esmiralda Moradian , „Secure Audit Log Management,“ 2013. [Tinkle]. Available: https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050913X00079/1-s2.0-S1877050913010053/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEPP%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIF63ekbnjUamN9Muj0%2F2tv89mvQ3GJz13tXZogv1bR7qAiEAmjgW6Pgwj5. [Kreiptasi 26 sausis 2020].

[19] „Knight Codes,“ 11 rugpjūtis 2016. [Tinkle]. Available: https://knightcodes.com/.net/2016/08/11/configure-SMTP-from-config-file.html. [Kreiptasi 19 balandis 2020].

[20] Kirk Schloegel, Tom Markham, Walt Heimerdinger, Alberto Egon Schaeffer-Filho, Morris Sloman, Emil C. Lupu, Seraphin B. Calo, Jorge M. Lobo, „Security Policy Automation from Specification to Device Configuration,“ įtraukta *26th Army Science Conference*, Orlando, 2008.

[21] Nathan N. Vuong, Geoffrey S. Smith, Yi Deng, „anaging Security Policies in a Distributed Environment Using eXtensible Markup Language,“ *Advancing Computing as a Science & Profession,* pp. 405-411, 2001.

[22] „Microsoft,“ 27 rugpjūtis 2018. [Tinkle]. Available: https://docs.microsoft.com/lt-lt/powershell/scripting/overview?view=powershell-7. [Kreiptasi 10 vasaris 2020].

[23] „Microsoft,“ [Tinkle]. Available: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/icacls. [Kreiptasi 14 balandis 2020].

7. PRIEDAI

7.1. priedas. Mikroserviso, surenkančio duomenis iš mazgo turinys

```
const express = require('express');
const path = require('path');
const bodyParser = require('body-parser');
const fs = require('fs');
const IpDeniedError = require('express-ipfilter').IpDeniedError;

const os = require('os');
var ifaces = os.networkInterfaces();
var this_ip_address = '';

Object.keys(ifaces).forEach(function (ifname) {
    ifaces[ifname].forEach(function (iface) {
        if ('IPv4' !== iface.family || iface.internal !== false) {
            // skip over internal (i.e. 127.0.0.1) and non-ipv4 addresses
            return;
        }
        if (ifname.startsWith("NIC1")) {
            this_ip_address = iface.address;
        } else if (ifname.startsWith("Wi-Fi")) {
            this_ip_address = iface.address;
        }
    });
});

const child_process = require('child_process');

const port = 8081;
const app = express();
app.use(bodyParser.json());

var current_directory = path.dirname(process.execPath);

function addLogs(error_message) {
    var date_ob = new Date();
    var date = ("0" + date_ob.getDate()).slice(-2);
    var month = ("0" + (date_ob.getMonth() + 1)).slice(-2);
    var year = date_ob.getFullYear();
    var hours = date_ob.getHours();
    var minutes = date_ob.getMinutes();
    var seconds = date_ob.getSeconds();

    var datetime = "[" + year + "-" + month + "-" + date + " " + hours + ":" +
minutes + ":" + seconds + "] ";

    console.log(error_message);
    fs.appendFile(path.join(current_directory, 'logs.txt'), "\n" + datetime +
error_message, (err) => {});
}

app.get('/', (req, res) => {
    var client_ip = req.connection.remoteAddress;
```

```
    var from_path_name =
String.raw`${fs.readFileSync(path.join(current_directory,
'files_path.txt')).toString('UTF-8')}`
    if (from_path_name === '') {
        addLogs('No from path!');
        res.send('400');
    } else {
        try {
            if (fs.existsSync(from_path_name)) {
                fs.copyFileSync(from_path_name + 'org_allowed_ips.txt',
path.join(current_directory, 'allowed_ips.txt'));

                var ips = fs.readFileSync(path.join(current_directory,
'allowed_ips.txt')).toString('UTF-8');
                var ips = ips.split(", ");
                if (ips !== '' && ips.includes(client_ip)) {
                    fs.copyFileSync(from_path_name + 'org_server_ip.txt',
path.join(current_directory, 'server_ip.txt'));

                    var server_ip = fs.readFileSync(path.join(current_directory,
'server_ip.txt')).toString('UTF-8');

                    if (server_ip !== '') {
                        // Copy files from original files directory
                        fs.copyFileSync(from_path_name + 'org_policy_batch.bat',
path.join(current_directory, 'policy_batch.bat'));

                        fs.copyFileSync(from_path_name +
'org_export_apps_list.ps1', path.join(current_directory,
'export_apps_list.ps1'));

                        fs.copyFileSync(from_path_name + 'org_export_acl.ps1',
path.join(current_directory, 'export_acl.ps1'));
                        // Start data collecting
                        child_process.exec(path.join(current_directory,
'policy_batch.bat'), function(error, stdout, stderr) {
                            setTimeout(function () {
                                if (error) {
                                    res.send('400');
                                    addLogs(error);
                                } else {
                                    var policy_value =
fs.readFileSync(path.join(current_directory,
'export_policy_batch.txt')).toString('UTF-16LE');
                                    var programs_value =
fs.readFileSync(path.join(current_directory,
'InstalledPrograms.txt')).toString('UTF-16LE');
                                    if (this_ip_address == server_ip) {
                                        var ACL_value =
fs.readFileSync(path.join(current_directory, 'ACL.txt')).toString('UTF-16LE');
                                    } else {
                                        var ACL_value = '';
                                    }
                                    addLogs('Data sent successfully!');
                                    res.send({'policy_value': policy_value,
'programs_value': programs_value, 'ACL_value': ACL_value});
```

```
                                }
                            }, 5000);
                        });
                    } else {
                        res.send('No Server IP!')
                        addLogs('No Server IP!');
                    }
                } else {
                    res.send('Access denied!')
                    addLogs('Access denied!');
                }
            } else {
                addLogs('Path ' + from_path_name + ' does not exists!');
                res.send('400');
            }
        } catch(err) {
            addLogs(err);
            res.send('400');
        }
    }
});

app.use((err, req, res, _next) => {
    if (err instanceof IpDeniedError) {
        res.status(401)
    } else {
        res.status(err.status || 500)
    }
    addLogs(err);
    res.send(err)
});

addLogs('Service starting..');
app.listen(port, '0.0.0.0');
```

7.2. priedas. Powershell scenarijaus, gaunančio įdiegtų programų sąrašą, turinys

```
Get-ItemProperty
HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-
Object DisplayName, DisplayVersion, Publisher, InstallDate | Where-Object
{$_.Publisher -ne 'Microsoft Corporation' -and $_.Publisher -ne 'Intel
Corporation' -and $_.Publisher -ne 'Intel' -and $_.Publisher -ne 'Samsung' -and
$_.Publisher -ne 'Samsung Electronics Co., Ltd.' -and $_.Publisher -ne 'MSI Co.,
LTD' -and $_.Publisher -ne 'Micro-Star International Co., Ltd.' -and $_.Publisher
-ne 'Cisco Systems, Inc.' -and $_.Publisher -ne 'The GnuPG Project' -and
$_.Publisher -ne 'Google LLC' -and $_.Publisher -ne 'Intel(R)' -and $_.Publisher
-ne 'Oracle Corporation' -and $_.Publisher -ne 'Mozilla' -and $_.Publisher -ne
'Notepad++ Team' -and $_.Publisher -ne 'JetBrains s.r.o.' -and $_.Publisher -ne
'Dropbox, Inc.' -and $_.Publisher -ne 'CyberLink Corp.' -and $_.Publisher -ne
'Apple Inc.' -and $_.Publisher -ne 'Intel(R) Corporation' -and $_.Publisher -ne
'Realtek Semiconductor Corp.' -and $_.Publisher -ne 'Opera Software' -and
$_.Publisher -ne 'Lenovo Group Ltd.' -and $_.Publisher -ne 'Roger' -and
$_.Publisher -ne 'ROGER' -and $_.Publisher -ne 'Lenovo' -and $_.Publisher -ne
'Schneider Electric' -and $_.Publisher -ne 'Skype Technologies S.A.' -and
$_.Publisher -ne 'Zebra Technologies' -and $_.Publisher -ne 'TDC' -and
```

```
$_.Publisher -ne 'UPS' -and $_.Publisher -ne 'United Parcel Service, Inc.' -and
$_.Publisher -ne 'Lenovo Group Limited' -and $_.Publisher -ne 'Realtek' -and
$_.Publisher -ne 'Adobe Systems Incorporated' -and $_.Publisher -ne 'CANON INC.'
-and $_.Publisher -ne 'KONICA MINOLTA' -and $_.Publisher -ne 'Adobe Systems, Inc'
-and $_.Publisher -ne 'Zebra Technologies Corporation' -and $_.Publisher -ne
'TeamViewer' -and $_.Publisher -ne 'NVIDIA Corporation' -and $_.Publisher -ne
'SolidWorks Corporation' -and $_.Publisher -ne 'Plantronics, Inc.' -and
$_.Publisher -ne 'Autodesk' -and $_.Publisher -ne 'Oracle' -and $_.Publisher -ne
'Oracle, Inc.' -and $_.Publisher -ne 'Google, Inc.' -and $_.Publisher -ne 'Dolby
Laboratories Inc' -and $_.Publisher -ne 'AMD' -and $_.Publisher -ne 'Advanced
Micro Devices, Inc.' -and $_.Publisher -ne 'Google Inc.' -and $_.Publisher -ne
'CANON INC.' -and $_.Publisher -ne 'Vimicro Corporation' -and $_.Publisher -ne
'Dassault Systemes SolidWorks Corp' -and $_.Publisher -ne 'Summa' -and
$_.Publisher -ne 'Microsoft' -and $_.Publisher -ne 'MicrosoftH' -and $_.Publisher
-ne 'Protexis Inc.' -and $_.Publisher -ne 'Avilda' -and $_.Publisher -ne 'Your
Company Name' -and $_.Publisher -ne 'Adobe Systems, Inc.' -and $_.Publisher -ne
'Adobe' -and $_.Publisher -ne 'Sun Microsystems, Inc.'  -and $_.Publisher -ne
'Summa bvba' -and $_.Publisher -ne 'Enter Srl'} | Export-Csv -Encoding "Unicode"
-Delimiter "`t" -path InstalledPrograms.txt -notype
```

7.3. priedas. Powershell scenarijaus, gaunančio prieigos kontrolės sąrašą, turinys

```
icacls \\SERVER\Visi\IT\DKMD /t > ACL.txt
```

7.4. priedas. Batch scenarijaus, gaunančio vietinės saugos politikos duomenis ir paleidžiančio Powershell scenarijus, turinys

```
@ECHO off
set "params=%*"
cd /d "%~dp0" && ( if exist "%temp%\getadmin.vbs" del "%temp%\getadmin.vbs" ) &&
fsutil dirty query %systemdrive% 1>nul 2>nul || (  echo Set UAC =
CreateObject^("Shell.Application"^) : UAC.ShellExecute "cmd.exe", "/k cd
""%~sdp0"" && %~s0 %params%", "", "runas", 1 >> "%temp%\getadmin.vbs" &&
"%temp%\getadmin.vbs" && exit /B )
secedit.exe /export /cfg ./export_policy_batch.txt
powershell.exe "& './export_apps_list.ps1'"
powershell.exe "& './export_acl.ps1'"
exit
```