KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Dmitrijus Gurejevas

Organizacijos tinklo saugos politikos įgyvendinimo įvertinimas automatizuotomis priemonėmis

Magistro darbas

Darbo vadovas
doc. G. Činčikas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Dmitrijus Gurejevas

Organizacijos tinklo saugos politikos įgyvendinimo įvertinimas automatizuotomis priemonėmis

Magistro darbas

Recenzentas
dr. Audronė Janavičiūtė
2010-05-

Vadovas
doc. G. Činčikas
2010-05-

Konsultantas
lekt. A. Budnikas
2010-05-

Atliko
IFN-8/3 gr. stud.
Dmitrijus Gurejevas
2010-05-

Kaunas, 2010

Turinys

1. Summary

Assessment of enterprise network security policy implementation using automated means

Every organization process information in information systems and cannot manage without the protection of organization information systems. Due to reinforcing protection of organization and investments, a need to know the level of protection exists. In order to retain the same level of protection, security assessment works should be performed regularly. However, they are complicated, performed slowly, and the results are relevant only during the assessment.

The above mentioned problems can be solved constantly monitoring the network, registering the violations with the help of automated means, presenting the evaluation of the level of protection in numeric values, so that the changes in the level of security in time could be traced. Therefore, in the following work an automated mean, constantly monitoring the network and registering the violations according to the crated methodology, is created. Methodology relates organization security policy with the automated mean and provides it with the possibility to calculate the general evaluation of security considering the number and the level of risk of violations.

The „Snort“ tool, working in NIDS mode according to specially created rules, is chosen to register the violations. Information regarding the violations is saved in MySql data base. PHP language is applied to calculate and map the assessment of the level of security.

2. Įvadas

Kiekvienos organizacijos visos pastangos yra nukreipiamos į tikslų pasiekimą. Stengiamasi šių tikslų siekti efektyviai, minimaliomis išlaidomis pasiekiant maksimalią naudą. Šis siekis priverčia organizacijas apdoroti informaciją kompiuterinėse sistemose, dalintis ja su informacinių santykių subjektais panaudojant esamus tinklus, taikyti naujas technologijas. Su nuolatiniu naujų technologijų įdiegimu atsiranda skirtingų sričių problemų, kurios reikalauja sprendimo ir palaikymo. Viena iš tokių problemų yra duomenų apsauga. Organizacijos veikla ir organizacijos duomenų sauga yra neatskiriami dalykai. Nepajėgumas apdoroti informaciją dėl duomenų saugos incidento gali privesti prie organizacijos veiklos sustabdymo, kas yra neleistina, todėl tiriamojo darbo sritis – organizacijos duomenų sauga.

Organizacijos duomenų apsauga yra apibrėžiama, organizuojama, palaikoma, stiprinama. Jeigu saugos tikslai gali būti apibrėžti, tai turi atsispindėti organizacijos dokumentuose. Jeigu duomenų sauga gali stiprėti, tai ji gali turėti saugos lygį. Savo ruožtu, saugos lygis yra palaikomas, gali būti įvertinamas, gali svyruoti.

Yra svarbu žinoti: ar esama organizacijos tinklo vertybių saugos būsena atitinka užbrėžtą duomenų saugos lygį; ar duomenų saugos sistema pateisina savo lūkesčius; ar nepažeidžiamos saugos politikos taisyklės darbo, tinklo saugos priemonių kūrimo, įvertinimo, tobulinimo, pakeitimo metu; kokios saugos politikos taisyklės yra pažeidžiamos dažniausiai, kokiomis sąlygomis tai atsitinka. Taigi duomenų saugos lygio ir saugos tikslų įgyvendinimo įvertinimas duoda didelę naudą ir turi platų pritaikymą. Kadangi nauda yra didelė, duomenų saugos įvertinimas yra tiriamojo darbo objektas.

Norint išsiaiškinti ar įmanoma įvertinimo procesą automatizuoti organizacijos kompiuterių tinkle, ar galima saugos tikslų įgyvendinimo įvertinimą išreikšti skaitine reikšme, ar galima organizacijos tinkle duomenų saugos lygį stebėti nuolat darbe yra apžvelgiama: organizacijos duomenų sauga, ir jos gyvavimo ciklas, rizikos analizė, saugos politika, jos reikšmė, struktūra organizacijoje, tinklo saugos įvertinimo procesas, srauto analizės įrankiai.

Saugos įvertinimo procesas yra sudėtingas, o dėl kliūčių – lėtas. Siekiant palaikyti norimą saugos lygį, įvertinimo darbai yra nuolat kartojami. Saugos lygio palyginimui reikalingas kiekybinis rezultatas, o duomenų surinkimas iš skirtingų įvertinimo būdų nėra paprastas. Kadangi didelė darbo dalis yra atliekama rankiniu būdu, klaidos tikimybė yra aukšta. Svarbiausia, kad rezultatai yra aktualūs tik įvertinimo vykdymo metu. Koks yra saugos lygis kitu metu pasakyti nėra galimybės.

Šias problemas gali išspręsti automatizuotas įvertinimas skaitine reikšme. Taip pat reikalingas nuolatinis tinklo stebėjimas ir pažeidimų fiksavimas.

Aptartų sprendimų įgyvendinimui iškeltas darbo tikslas – sukurti organizacijos kompiuterių tinklo srities saugos politikos įgyvendinimo įvertinimo įrankį.

Šiam tikslui pasiekti reikalinga atlikti tokias užduotis:

1. išanalizuoti saugos organizavimo ir įvertinimo būdus;
2. sukurti saugos politikos įgyvendinimo įvertinimo skaičiavimo metodiką;
3. sukurti automatizuotą įrankį, kuris nuolat stebėtų tinklą ir fiksuotų pažeidimus.

Yra sukurta metodika, kurios pagalba galima apskaičiuoti organizacijos saugos politikos įgyvendinimo įvertinimą. Ši metodika yra pritaikyta sukurtam automatizuotam įrankiui. Metodikos komponentai atitinka saugos politiką, bendras įvertinimas atspindi pažeidimų kiekį ir rizikos analizės rezultatus. Automatizuotas įrankis atsako už techninę metodikos įgyvendinimo dalį.

Suderinus priemones tarpusavyje ir pritaikius įrankiui sukurtą metodiką, galima spręsti paminėtas problemas. Įrankis stebi tinklą, fiksuoja iš anksto aprašytus ir atitinkančius saugos politiką pažeidimus, apskaičiuoja bendrą įvertinimą pagal gautą informaciją. Įrankis stebi tinklą, fiksuoja pažeidimus nuolat, todėl išvengiamas pakartotinas įvertinimo darbų atlikimas.

3. Organizacijos duomenų saugos analizė

Organizacijos duomenų saugos sistemos vystymas yra organizacijos tikslo dalis. Todėl yra svarbu žinoti apie organizacijos duomenų saugą, įvertinimą, problemas, galimus jų sprendimus.

3.1. Aplinkos analizė

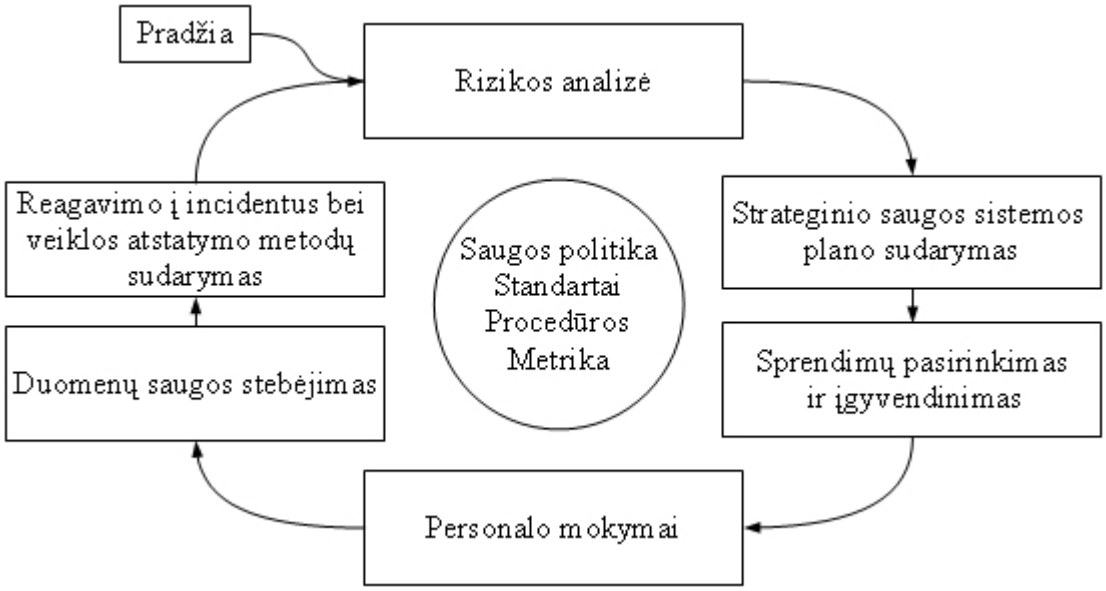
Analizuojama aplinka – tai organizacijos tinklo duomenų sauga, todėl reikia nustatyti, kokiais būdais yra organizuojama duomenų sauga, kaip yra palaikomas ir įvertinamas duomenų saugos lygis.

3.1.1. Saugos gyvavimo ciklas

Saugos gyvavimo ciklas parodo, kokius etapus reikia atlikti, norint pasiekti aukštą organizacijos tinklo saugumą [1]. Atliekant ciklo žingsnius, galima sistemingai spręsti uždavinius, susietus su duomenų sauga, gerinti saugos sistemą, apskaičiuoti išleistas lėšas, gautą naudą.

Toks požiūris yra priešingas „taškinių“ uždavinių sprendimo ideologijai, kur visos pastangos sutelkiamos atskiruose uždavinių sprendimuose, kaip užkardos taisyklių ar vartotojų prieigos tobulinimas. Be išankstinės analizės bei planavimo, dėl „taškinės“ taktikos naudojimo, gali atsirasti skirtingos sistemos organizacijos tinkle. Tokios sistemos gali būti nesuderinamos tarpusavyje ir neleistų ateityje efektyviai spręsti organizacijos uždavinių duomenų saugos srityje.

Reikalingas bendras sprendimas, leidžiantis sistemingai spręsti visos organizacijos saugos uždavinius. Saugos gyvavimo ciklas susidaro iš septynių pagrindinių komponentų, kuriuos galima traktuoti kaip duomenų saugos sistemos kūrimo etapus. Šie etapai pavaizduoti 1 paveiksle.



1 pav. Saugos gyvavimo ciklas

Saugos politikos, standartai, procedūros, metrika

Šis komponentas apibrėžia sritį, kur turėtų būti taikoma duomenų sauga, bei užduoda gautų rezultatų kriterijus. Suprojektuota duomenų saugos sistema atsispindi šiuose dokumentuose.

Saugos politika – tai bendras ketinimas ir kryptis kurie yra oficialiai nustatyti vadovybės [2]. Saugos politikos dokumentas organizacijos vadovybei suteikia galimybę valdyti ir turėti duomenų saugos palaikymą atsižvelgiant į verslo reikalavimus, įstatymus ir taisykles [3].

Kitaip tariant, saugos politika – tai vadovybės patvirtintų dokumentuotų sprendimų visuma, kuri yra orientuota į duomenų saugą ir jos išteklius [4].

Standartai yra suprantami ne tik kaip valstybiniai ar tarptautiniai standartai duomenų saugos srityje, bet ir organizacijos standartai, kurie gali stipriai įtakoti duomenų saugos sistemos kūrimą.

Kadangi saugos politika užbrėžia tik bendrą organizacijos duomenų saugos tikslą ir apibrėžia, tai bendrais terminais, reikalingi tikslesni dokumentai. Tai yra procedūros, instrukcijos, vadovai, techninės specifikacijos ir t. t. Priklausomai nuo organizacijos poreikių, yra sudaromi reikalingi šios kategorijos dokumentai, kurie, pavyzdžiui, nurodo tikslius procesus, tam tikro darbuotojo proceso žingsnius, aprašo konfigūraciją ar sistemos sudėtį.

Taip pat yra reikalinga metrika, kuri leidžia įvertinti duomenų saugos sistemos būseną prieš ir po įvykdytų sistemos pakeitimų. Metrika apibrėžia, kaip ir kuo yra išmatuojamas sistemos saugumas, kas įvertina išleistų lėšų ir gautos naudos santykį. Metrika priklauso nuo pasirinkto rizikos analizės metodo. Šie metodai leidžia įvertinti duomenų saugą lėšų atžvilgiu.

Rizikos analizė

Rizikos analizė – tai sistemingas informacijos naudojimas rizikos šaltinių nustatymui ir jos lygio įvertinimui [2]. Šio etapo rezultatai suteikia galimybę efektyviai sudaryti ir tobulinti duomenų saugumo sistemą. Rizikos analizė leidžia smulkiai aprašyti informacinės sistemos sudėtį ir struktūrą (jeigu tai nebuvo padaryta anksčiau) išdėlioti turimus išteklius pagal prioritetus atsižvelgiant į jų svarbumo lygį organizacijos darbui, įvertinti grėsmes ir nustatyti sistemos pažeidžiamumus.

Strateginio saugos sistemos plano sudarymas

Strateginio saugos sistemos plano sudarymui yra panaudojami rizikos analizės rezultatai. Toks planas leidžia paskirstyti lėšas, išteklius pagal prioritetus, todėl galima bus pasirinkti įrankius, priemones, sudaryti jų įgyvendinimo strategiją. Rizikos analizės rezultatai bei priimti sprendimai sudaro saugos politikos pagrindą.

Sprendimų pasirinkimas ir įgyvendinimas

Gerai struktūrizuoti sprendimų pasirinkimo kriterijai duomenų saugos srityje bei diegimo plano buvimas sumažina tikimybę, kad įgytos priemonės ar įrankiai taps kliūtimi organizacijos informacinės sistemos vystyme. Taip pat turi būti įvertintas pasirenkamas paslaugų tiekėjas, jo teikiamų paslaugų kokybė, tinkamumas, plėtros galimybės ir t. t. Be to, būtina aiškiai apibrėžti įgyvendinamo sprendimo vaidmenį sudaryto strateginio saugos sistemos plano vykdyme ir nustatytų duomenų saugos tikslų pasiekimą.

Personalo mokymai

Reikalingos pakankamos žinios ne tik informacinių skaičiavimo sistemų, bet ir duomenų saugos srityje. Žinių atnaujinimas ir tobulinimas yra būtinas norint sudaryti bei palaikyti saugią organizacijos kompiuterinę informacinę sistemą. Įdėtos pastangos, taip pat išleistos lėšos personalo mokymui, ženkliai padidina tinklo saugą, atsparumą nuo saugos incidentų bei leidžia geriau vykdyti tinklo saugos profilaktikos ir tobulinimo darbus.

Duomenų saugos stebėjimas

Duomenų saugos stebėjimas leidžia aptikti įsiskverbimus, įsilaužimus, anomalijas ir kitus įvykius, pažeidžiančius organizacijos saugą. Tai duomenų saugos sistemos bei jos programinių įrankių kontrolinė priemonė. Stebėjimo priemonės leidžia sekti saugos sistemų veikimo darbą, jų taisyklingumą, atitikimą užbrėžtiems duomenų saugos tikslams.

Reagavimo į incidentus bei veiklos atstatymo metodų sudarymas

Atsiradus saugos incidentui, turi būti atliktos efektyvios saugumo procedūros. Verslo sistemos darbingumas turi būti atstatytas. Tam tikslui pasiekti reikalingos iš anksto sudarytos procedūros žinomoms incidentų grupėms, kad verslo sistema būtų atstatyta kuo greičiau.

Visi šie komponentai yra susieti, o duomenų saugos sistemos tobulinimosi procesas vyksta nepertraukiamai.

3.1.2. Organizacijos lygiai duomenų saugos srityje

Siekiant užtikrinti duomenų saugą organizacijoje, ją reikia įdiegti ne tik techniniuose objektuose, bet visuose organizacijos hierarchijos lygiuose, pradedant nuo organizacijos valdžios ir užbaigiant darbų vykdytojais. Įdiegus suprojektuotus saugos mechanizmus, reikia palaikyti pasiektą saugos lygį, prižiūrėti atliekant audito darbus, sekti pakeitimus, lyginti skirtingas būsenas.

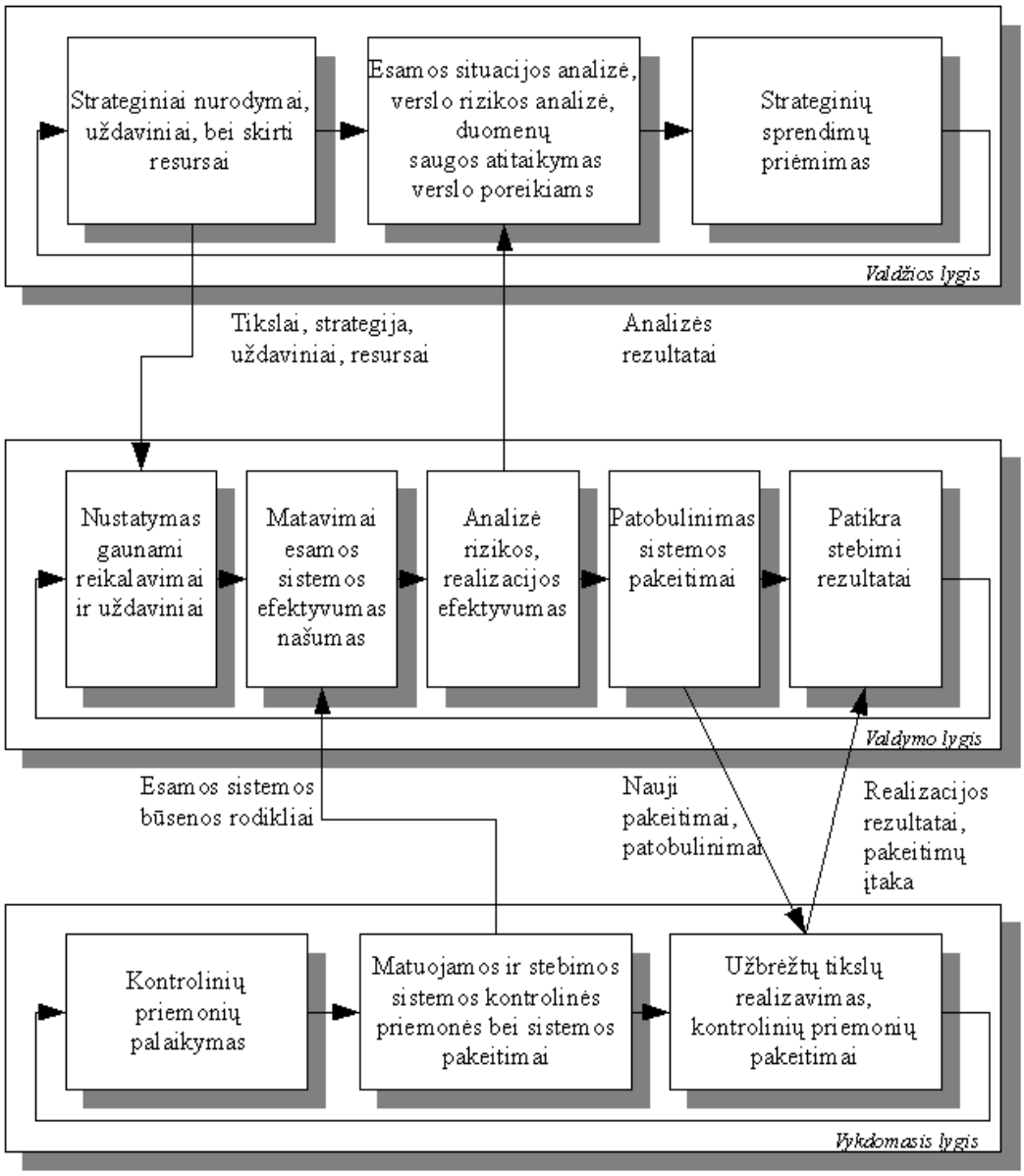
Duomenų sauga apima visas operacijas, vykdomas su informacija, fizinius ir techninius elementus, organizacijos tikslus, teisinius aspektus, visus informacijos gyvavimo ciklo žingsnius ir t. t. Todėl saugos sistema turi saugoti informaciją kur ji bebūtų, bet kokioje formoje. Remiantis šaltiniu [5], organizaciją galima suskirstyti į tris lygius, kur dirba saugos sistema. Tai valdžios lygis, valdymo lygis, ir vykdomasis lygis (2 pav.).

Valdžios lygis valdo verslo tikslus, uždavinius ir strategiją. Svarstoma, kaip saugos sistema turi elgtis atsižvelgiant į verslo poreikius, strategiją. Aukščiausiame lygyje valdo rizikas, priima strateginius sprendimus, svarsto lėšų paskirstymą. Už šio lygio korektišką veikimą yra atsakingi aukščiausi organizacijos vadovai.

Valdymo lygis atsako už organizacinių koordinacinių priemonių valdymą. Tai sistemų projektavimas, patobulinimo sprendimai, analizuojami esamos sistemos surinkti statistiniai duomenys, įvertinamos rizikos bei realizuotos sistemos efektyvumas, kontroliuojama, kaip yra vykdomi patobulinimai.

Vykdomasis lygis yra atsakingas už nurodytų pakeitimų sistemoje įvykdymą, sistemos kontrolės palaikymą, gedimų pašalinimą. Visos priemonės, kurios buvo diegtos rizikai sumažinti, susidaro iš fizinių, techninių, organizacinių priemonių kontrolės. Kontroliuojant ir stebint visų saugos sistemų elementus, yra renkama statistinė informacija ir perduodama valdymo lygiui, analizei atlikti bei sprendimui priimti.

Duomenų saugos sistemos funkcionavimo modelio su tarp lyginiais ryšiais bendra schema yra pavaizduota 2 paveiksle.



2 pav. Organizacijos lygiai duomenų saugos srityje

Valdžios lygis

Valdžia – tai santykių ir procesų struktūra, skirta nukreipti, valdyti organizaciją, siekti jos apibrėžtų tikslų ir uždavinių [6]. Šio lygio tikslas yra užduoti duomenų saugos sistemos strategiją, kuri palaikytų verslo strategiją ir kryptį. Taip pat nustatomi saugos vaidmuo ir paskirstomi prioritetai atsižvelgiant į visos organizacijos informacinius santykius [7]. Valdžia turi savo saugos viziją, kas yra leidžiama, o kas ne, kaip valdyti rizikas ir kaip turi būti valdoma aplinka. Visi reikalavimai saugai atsispindi aukšto lygio dokumentuose – saugos politikoje.

Valdžia nustato skirtingo laikotarpio duomenų saugos tikslus ir uždavinius

atsakingiems informacijos saugos skyriams pagal priimtus sprendimus. Taip pat apskaičiuojami ir išskiriami ištekliai tikslams realizuoti.

Pagrindiniai apdoroti esamos saugos sistemos efektyvumo rodikliai gaunami iš valdymo lygio. Šie duomenys yra analizuojami atsižvelgiant į visos organizacijos vystymo strategiją, nustatoma esama ir planuojama būklė.

Gauti rezultatai apie riziką, efektyvumą, finansus, suteikia galimybę suplanuoti naujus strateginius žingsnius, tikslus, patobulinimus.

Valdymo lygis

Valdymo lygmens užduotis yra organizacinių koordinacinių priemonių pritaikymas, vykdomojo lygio kontrolė, užsibrėžtų valdžios tikslų išpildymas, strateginių planų vystymas atsižvelgiant į organizacijos saugos politiką.

Šis lygmuo paremtas „Six Sigma“ patobulinimo metodu [8]. Šio metodo principo pagrindu galima sėkmingai kontroliuoti ir tobulinti vykdomojo lygio veiklą, atsižvelgiant į gautus nurodymus iš valdžios lygio. Šis metodas susidaro iš penkių saugos informacijos patobulinimo etapų, kurie yra įgyvendinti valdymo lygmenyje.

Valdymo lygmens etapai: nustatymas, matavimai, analizė, patobulinimas, patikra (2 pav.).

Nustatymo etape valdymo lygis iš valdžios lygmens gauna strateginius nurodymus, uždavinius bei resursus šiems uždaviniams įgyvendinti. Šiame etape gauti nurodymai suskirstomi į tikslius uždavinius, formuluojami reikalavimai, nustatomi rezultato kokybės kriterijai, pagal kuriuos bus tikrinamas vykdomojo lygio darbas.

Matavimo etape yra surenkami duomenys apie esamą saugos sistemą. Dažniausiai atkreipiamas dėmesys į sistemos efektyvumą, našumą, kontrolinių priemonių naudingumą. Sprendžiant, kada, kaip ir kokie statistiniai duomenys apie saugos sistemą bus surenkami, apgalvojami galimi sistemos patobulinimai.

Analizės žingsnyje surinkti duomenys yra apdorojami atsižvelgiant į saugos sistemos įtaką verslui, bei analizuojamos rizikos. Nustatoma liekamoji rizika, ta, nuo kurios saugos sistema neapsaugo, bei apmąstomi būdai, kaip šią riziką galima sumažinti iki priimtino lygio. Diagnozuojama, kaip efektyviai dirba esama sistema. Nustatomi galimi sistemos pakeitimai. Analizės rezultatai bei siūlomi sistemos patobulinimai perduodami valdžios lygiui sprendimui priimti.

Patobulinimo etapo tikslas yra pateikti vykdomajam lygiui informaciją, kokie saugos elementai bus patobulinami ir kaip bus realizuojami pakeitimai. Taip suprojektuojamas rizikos

sumažinimas.

Patikros etapas, skirtas surinkti patobulinimo rezultatus, patikrinti, ar pavyko padarytais pakeitimais pasiekti tikslą. Tokias išvadas galima padaryti, kai vykdomasis lygmuo perduoda informaciją apie esamą bei pakeistą situaciją, praneša, kaip pakeitimai įtakoja kitus sistemos elementus.

Tokiu būdu valdymo lygmuo suteikia galimybę ne tik valdyti vykdomąjį lygį, bet ir užtikrinti įvykdymo kokybę. Tai padeda padaryti ciklinis žingsnių vykdymas.

Vykdomasis lygis

Vienas iš šio lygio svarbiausių tikslų yra nurodytų pakeitimų įdiegimas, realizacija. Taip pat atliekamas šių sistemų palaikymas, kontrolė, konfigūravimas, statistinių duomenų perdavimas valdymo lygiui tolimesnei analizei. Šis lygis taip pat yra suskirstytas į etapus atsižvelgiant į organizacijos poreikius. Siekiant suprasti, už ką yra atsakingas lygis, galima saugos užtikrinimo priemones suskirstyti į grupes.

Saugos užtikrinimo priemonės yra tokios: teisinės, moralinės-etinės, organizacinės, techninės, fizinės apsaugos priemonės [9].

Teisinės apsaugos priemonės – tai šalyje galiojantys įstatymai, įsakai, norminiai aktai, reglamentuojantys naudojimosi informacija taisykles. Šios priemonės užtikrina informacinių santykių subjektų teises ir nustato atsakomybę už šių teisių pažeidimą.

Moralinės-etinės apsaugos priemonės – tai elgesio normos, kurių nesilaikant menkinamas žmogaus, žmonių grupės ar organizacijos autoritetas. Šios normos gali būti tiek rašytinės, darbuotojų įsipareigojimai arba taisyklės organizacijoje, tiek nerašytinės, visos visuotinai pripažintos etinės elgesio normos.

Organizacinės apsaugos priemonės – tai taisyklės, reglamentuojančios duomenų apdorojimo sistemos funkcionavimo procesus, išteklių naudojimą, personalo veiklą ir vartotojų sąveikos su sistema tvarką.

Techninės apsaugos priemonės – tai priemonės, realizuotos techninėje arba programinėje įrangoje. Tai gali būti elektroniniai įtaisai, kaip piršto antspaudo nuskaitymo įtaisas, arba priemonė, realizuota programiniu būdu, tai duomenų šifravimas, užkardos, autentikacija, identifikacija ir kiti saugos mechanizmai.

Fizinės apsaugos priemonės, realizuojamos naudojant mechaninius, elektrinius prietaisus, kurių pagalba sukuriamos fizinės kliūtys. Šios priemonės apsaugo nuo pažeidėjų prasiskverbimo prie techninių įrenginių ar kompiuterinės įrangos. Tai specialiosios rakinamos patalpos, vaizdo stebėjimo sistemos, signalizacijos priemonės ir kita.

Vykdomasis lygis atlieka šių apsaugos priemonių kontrolę, palaikymą, patobulinimų įdiegimą, statistinių duomenų surinkimą.

3.1.3. Duomenų saugos rizika

Rizikos analizės dalis – tai viena iš svarbiausių dalių organizacijos hierarchijos lygiuose(2 pav.). Įvertinant organizacijos saugos lygį, yra svarbu atkreipti dėmesį į rizikos analizės rezultatus. Prieš analizuojant, kas yra rizika, turi būti apibrėžtos sąvokos.

Rizika – tai įvykio tikimybės ir jos pasekmių kombinacija [10]. Čia pasekmė dažniausiai yra suprantama kaip žala. Kitaip tariant tai galimybė prarasti dalį lėšų dėl duomenų saugos pažeidimo arba tai yra numatomos žalos dydis. Pažeidus tam tikrą duomenų saugos vertybę, yra nustatoma jos žala.

Žala – tai prarastų lėšų reikšmė.

Grėsmė – tai potencialiai galimas nepageidaujamas įvykis, kuriam įvykus gali būti padaryta žala vertybei, sistemai ar organizacijai.

Ataka – tai sėkmingai įvykdyta grėsmė.

Pažeidžiamumas – tai vertybės ar jų grupės silpna vieta, kuria gali pasinaudoti viena ar daugiau grėsmių.

Rizikos analizė – tai sistemingas informacijos naudojimas rizikos šaltinių nustatymui ir jos lygo įvertinimui.

Rizikos įvertinimas – tai pilnas rizikos analizės ir rizikos reikšmingumo įvertinimo procesas.

Rizikos reikšmingumo įvertinimas – tai palyginimo procesas skirtas nustatyti rizikos reikšmingumą, kur yra lyginami paskaičiuota rizika ir užsibrėžtos rizikos kriterijai. Rizikos reikšmingumo įvertinimo procesas skirtas identifikuoti pačias pavojingiausias rizikas.

Taip pat reikia atskirti sąvokas „rizika“ ir „grėsmė“. Rizika skiriasi nuo grėsmės tuo, kad grėsmė – tai galimas nepageidaujamas įvykis, o rizika apibrėžia galimos žalos kiekybinę reikšmę bei grėsmės realizacijos tikimybę.

Duomenų saugos sistemos incidentas – tai nepageidaujamas ar netikėtas įvykis duomenų saugos sistemoje, kuris su didele tikimybe gali sukelti grėsmes.

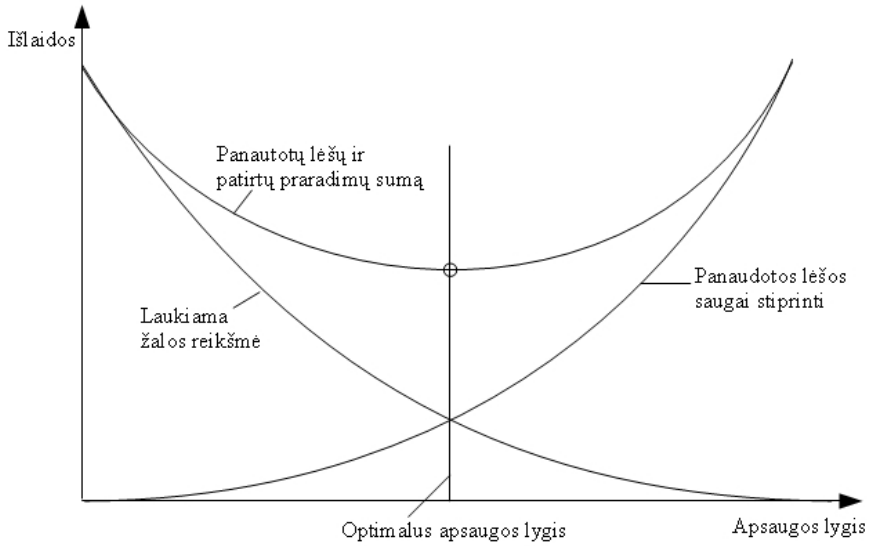
Rizikos valdymas atsirado tada, kai duomenų saugos sistemai pradėjo taikyti „protingo pakankamumo“ principą [11]. Šis principas gali būti apibrėžtas tokiais teiginiais:

- absoliučiai apsaugotos sistemos sudaryti neįmanomą,
- mažinant netektų lėšų reikšmę dėl saugos sistemos pažeidimų, tūri būti nustatyta

pusiausvyra tarp išleistų lėšų saugai gerinti ir gaunamo rezultato,

- saugos priemonių kaina neturi viršyti saugomų vertybių suminės kainos,
- nusikaltėlio panaudotų lėšų reikšmė turi gerokai viršyti siekto tikslo gautos naudos reikšmę.

Apytiksliai apskaičiavus esamai informacinei sistemai vidutinę laukiamą nuostolio reikšmę, tarkime per metus, priemonių kainą, kurios sumažina nuostolių riziką, galima rasti optimalų saugos sistemos lygį, suplanuoti išlaidas duomenų saugos priemonėms, tai ir yra rizikos valdymo tikslas. Šį tikslą gerai atvaizduoja 3 paveikslas.



3 pav. Rizikos valdymo tikslas

Deja, praktikoje tikslias išlaidų ir apsaugos lygio priklausomybių reikšmes apskaičiuoti neįmanoma, todėl aukščiau pateiktas analitinis būdas nepritaikomas, jis tik parodo rizikos įvertinimo esmę.

Rizikos aprašymui yra naudojamos skirtingos metodikos, standartai, vadovai ir rekomendacijos. Rizikos skaičiavimui naudojamos specifinės skalės, jos yra skirtingos ir priklauso nuo pasirinktos rizikos analizės metodikos. Rizikos įvertinamos pagal subjektyvius ar objektyvius kriterijus nurodant kiekybinės ar kokybinės reikšmes [12]. Dažniausiai pasirenkami subjektyvūs kriterijai nurodant kokybines reikšmes nes:

- rizikos įvertinimas turi atspindėti subjektyvią vertybės savininko nuomonę,
- turi būti įskaityti skirtingi aspektai, ne tik techniniai, bet ir organizaciniai, psichologiniai ir t. t.
- kokybinės skalės dažniausiai turi 3 – 7 gradacijas, kas yra patogu ir paprasta.

Dažniausiai yra naudojamas dviejų ar trijų faktorių rizikos įvertinimas. Paprasčiausiu atveju yra naudojami du faktoriai: įvykio tikimybė ir žalos dydis. Kuo didesnė rizikos

reikšmė, tuo didesnė tikimybė, kad nepageidautinas įvyks įvykis, ir tuo didesnė žala. Tai galima išreikšti formulė [12]:

$$riz = V \cdot P; \quad (1)$$

riz – rizikos skaitinė reikšmė

V – vertybės kaina, kuriai gresia pavojus arba žala

P – sėkmingos atakos, tai yra grėsmės įgyvendinimo tikimybė

Jeigu kintamieji yra kiekybiniai, rizikos reikšmė išreiškia laukiamą matematinę žalą. Jeigu kintamieji yra kokybiniai, daugybos ženklas yra neapibrėžtas. Todėl ši formulė yra nepritaikoma, o vietoj jos yra naudojama rizikos įvertinimo įvykių matrica. Iš pradžių turi būti apibrėžtos vertybės ir tikimybės kokybinės skalės [13].

Subjektyvi tikimybės kokybinė skalė:

A – įvykis beveik niekada neįvyksta.

B – įvykis pasirodo retai.

C – įvykio tikimybė už pasirinktą laikotarpį yra lygi apie 0,5.

D – greičiausiai įvykis atsitiks.

E – įvykis būtinai pasirodys.

Subjektyvi žalos kokybinė skalė:

N (Negligible) – žala labai maža, į ją nekreipiamas dėmesys.

Mi (Minor) – žala yra neženkli, pasekmės yra lengvai pašalinamos, išlaidos pasekmei likviduoti yra mažos, poveikis informacinėms technologijoms yra neženklus.

Mo (Moderate) – įvykis su vidutiniais rezultatais, išlaidos pasekmei likviduoti nėra didžiulės, poveikis informacinėms technologijoms nėra didelis ir neliečia kritiškai svarbių užduočių

S (Serious) – įvykis su rimtomis pasekmėmis, išlaidos pasekmei likviduoti yra ženklios, poveikis informacinėms technologijoms ženkliai trukdo vykdyti kritiškai svarbias užduotis

C (Critical) – žala yra labai didelė, kritiškai svarbias užduotis vykdyti yra neįmanoma

Rizika susijusi su tam tikru įvykiu priklauso nuo dviejų faktorių ir gali būti apibrėžtas kaip parodyta 1 lentelėje [12]:

1 lentelė. Dviejų faktorių rizikos įvertinimo įvykių matrica

	N (Negligible)	Mi (Minor)	Mo (Moderate)	S (Serious)	C (Critical)
A	1	1	1	2	2
B	1	1	2	2	3
C	1	2	2	2	3
D	2	2	2	2	3
E	2	3	3	3	3

Šis būdas yra paprasčiausias ir daugiausiai paplitęs. Šiuo atveju rizikos įvertinimui apibrėžti yra naudojama trijų reikšmių skalė: 1, 2, 3. Tai galima interpretuoti kaip žema rizika, vidutinė rizika ir aukšta rizika.

Taip pat galimos šio būdo modifikacijos, skirtingos skalės, faktoriai. Vienas iš jų – tai trijų faktorių rizikos įvertinimas, kur vietoje įvykio tikimybės naudojama grėsmės ir pažeidimo tikimybės sandauga (formulė 2) [12]:

$$riz = V \cdot P_{gresmes} \cdot P_{pažeidžiamumo}; \quad (2)$$

Jeigu kintamieji kokybiniai, turi būti naudojama rizikos įvertinimo įvykių matrica [12]:

2 lentelė. Trijų faktorių rizikos įvertinimo įvykių matrica

Žala	**Grėsmės lygis:**								
	Žemas			**Vidutinis**			**Aukštas**		
	Pažeidžiamumo lygiai:			**Pažeidžiamumo lygiai:**			**Pažeidžiamumo lygiai:**		
	Ž	**V**	**A**	**Ž**	**V**	**A**	**Ž**	**V**	**A**
N	0	1	2	1	2	3	2	3	4
Mi	1	2	3	2	3	4	3	4	5
Mo	2	3	4	3	4	5	4	5	6
S	3	4	5	4	5	6	5	6	7
C	4	5	6	5	6	7	6	7	8

Yra naudojama trijų grėsmės ir pažeidžiamumo lygių skalė: žemas, vidutinis, aukštas. Žalos skalė naudojama ta pati kaip ir 1 lentelėje. Rizikos įvertinimo skalė turi 0 – 8 gradacijas.

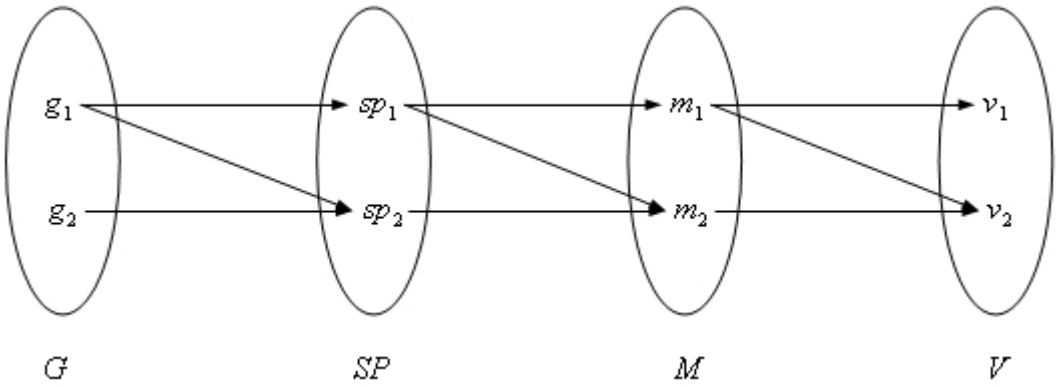
Nustačius riziką, gautas laukiamas žalos dydis yra palyginamas su apsaugos priemonių išlaidomis (3 pav.). Tada nutariama, ką reikia daryti su nustatyta rizika:

- sumažinti riziką, įdiegus apsaugos priemones mažinančias grėsmės tikimybę ar

naikinamojo poveikio koeficientą;

- pašalinti riziką, atsisakius vertybės, kuri turi tam tikrus pažeidžiamumus, naudojimo;
- pernešti riziką, apdraudžiant organizacijos vertybę;
- priimti riziką, susitaikant su galima žala;

Tarkime, yra priimtas sprendimas sumažinti riziką nuo tam tikrų grėsmių atitinkamomis saugos priemonėmis dokumentuojant šiuos veiksmus. Tai atvaizduota 4 paveiksle.



4 pav. Rizikos įvertinimo sudedamosios dalys

G – grėsmių aibė;

SP – saugos politikos taisyklių aibė;

M – apsaugos priemonių aibė;

V – saugomų vertybių aibė;

4 paveiksle parodyta, kad grėsmei pašalinti gali būti sudarytos keletą saugos politikos taisyklių, ir viena taisyklė gali pašalinti keletą grėsmių. Tą pačią savybę turi saugos priemonės ir vertybės.

Taigi turime pasirinktas rizikas, kurias reikia sumažinti, saugomų vertybių aibę. Galima išvardinti šių vertybių grėsmių aibę ir pasirinkti saugos priemones atsižvelgiant į jų kainą, kuri neviršija gaunamos naudos. Saugos politikoje yra užfiksuojami sprendimai, suformuluojamos taisyklės. Taip pat čia nurodomi procedūriniai dokumentai ir vadovai, kurių pagalba įgyvendinama ir palaikoma vertybių sauga.

3.1.4. Saugos politika

Kaip buvo išsiaiškinta 3.1.1 dalyje saugos politika – tai vadovybės patvirtintų dokumentuotų sprendimų visuma, kuri yra orientuota į duomenų saugą ir jos išteklius. Ši dokumentuota sprendimų visuma turi apibrėžti [3]:

1. duomenų saugos apibrėžimą, jos bendrų tikslų, galimybių ir veiklos sritį, taip pat

saugumo svarbą, kaip mechanizmą, leidžiantį informacijos naudojimą;

2. vadovybės ketinimus, susietus su tikslais, duomenų saugos valdymo principais;
3. infrastruktūrą, siekiant reguliuoti tikslus, kontrolines priemones, įskaitant riziką, jos įvertinimą ir valdymą;
4. trumpą duomenų saugos politikos, principų, standartų, reikalavimų, kurie yra ypatingai svarbūs organizacijai, paaiškinimą:
   a) įstatymų ir sutarčių reikalavimų atitikimas,
   b) reikalavimas išsilavinimui mokymams duomenų saugos srityje,
   c) veiklos nenutrūkstamumas,
   d) saugos politikos pažeidimo pasekmes,
5. bendras ir asmenines pareigas duomenų saugos valdyme įskaitant saugos incidentus;
6. saugos politikoje, nuorodos į dokumentaciją, kuri papildo ir detalizuoja politikos aspektus, į naudojamus įstatymus ir kitus dokumentus, pavyzdžiui, vartotojų saugos taisyklės atliekant konkrečias operacijas.

Tarptautinis standartas pagal minimalius reikalavimus rekomenduoja į saugos politiką įtraukti tokias dalis [10]:

1. įvadinė dalis, kuri išreiškia aukščiausios vadovybės rūpestį dėl organizacijos bei jos vystymo strategijos duomenų saugos problemų;
2. organizacinė dalis, aprašanti darbuotojų skyrius, komisijas, atsakingas grupes už pravedamus darbus duomenų saugos srityje;
3. vertybių valdymo dalis, aprašanti vertybes, jų priimtiną naudojimą, informacijos klasifikaciją bei jos naudojimą;
4. žmogiškųjų išteklių apsaugos dalis, apibūdinanti personalo pareigas, priėmimo, darbo ir atleidimo tvarką, taikomas personalui saugos priemones, tai pareigų aprašymas atsižvelgiant į duomenų saugą, mokymų ir kvalifikacijos pakeitimų organizavimas, reagavimo į saugos pažeidimus tvarka;
5. fizinės saugos dalis, aprašanti fiziškai apsaugotas sritis, vertybių fizinį saugojimo būdą;
6. dalis, aprašanti tinklų, ryšių naudojimo tvarką, eksploatacijos taisykles, trečių šalių ryšio paslaugų naudojimo taisykles;
7. dalis, aprašanti informacinių išteklių prieigos tvarką;
8. dalis, apibūdinanti sistemų palaikymo ir vystymo tvarką;
9. dalis, aprašanti saugos sistemos incidentų valdymą;
10. dalis, aprašanti verslo nepertraukiamumo veiklą;

11. teisinė dalis, patvirtinanti, kad saugos politika atitinka įstatymus, sutartis ir kitus teisinius dokumentus;

Saugos politika yra dažniausiai ne vienas dokumentas, o sudedamosios dalys, kurios aprašo tam tikrą saugos sistemos sritį. Tai gali būti nuotolinės prieigos saugos politika, rizikos analizės saugos politika, slaptažodžių naudojimo saugos politika, elektroninio pašto saugos politika ir taip toliau [14].

Todėl yra patogu saugos politikos dokumentus suskirstyti į hierarchijos lygius. Šie lygiai gali atitikti organizacijos struktūrą. Kaip buvo kalbėta aplinkos analizės dalyje, tai yra valdžios lygis, valdymo lygis, ir vykdomasis lygis.

Valdžios lygyje organizacijos tikslai yra formuojami atsižvelgiant į prieinamumo vientisumo ir konfidencialumo sąvokas. Visi šio lygio veiklos rezultatai, kurie yra aprašyti 3.1.2 dalyje, yra dokumentuojami aukšto lygio saugos politikoje. Pavyzdžiui, organizacijos saugos problemos, strateginiai saugos nurodymai atsižvelgiant į verslo strategiją, apsaugotų paslaugų poreikis. Remiantis [10] minimaliu saugos dalių sąrašu tai būtų įvadinė dalis kaip atskiras dokumentas.

Valdymo lygis (3.1.2 dalis) atsakingas už užbrėžtų tikslų organizavimą, koordinavimą. Todėl šiame hierarchijos lygyje saugos politikos dokumentai aprašo organizacinę veiklą, tokią kaip rizikos įvertinimo politika, sistemų tobulinimo politika ir taip toliau. Remiantis minimaliu saugos dalių sąrašu tai yra 2, 3, 4 punktai.

Vykdomajame lygyje (3.1.2 dalis) išvardintų sričių saugos politikos dokumentai aprašo saugos taisykles detaliau ir konkrečiau, bet neliečia realizacijos aspektų. Čia gali būti nurodoma pareiga, kuri yra apribota tam tikrai paslaugai, paslaugos teikimo sąlygos ir panašiai. Remiantis minimaliu saugos dalių sąrašu, tai yra 5 – 11 punktai. Paplitusios vykdomojo lygio saugos politikos [14]:

- pakankamo šifravimo – reikalavimai naudojamiems šifravimo algoritmams;
- tinkamo naudojimo – apibrėžia tinkamą įrangos bei paslaugų naudojimą;
- analoginių/ISDN tinklų naudojimo – nurodo šių linijų naudojimo standartus, fakso siuntimo ir priėmimo nuostatai, kompiuterių sujungimas;
- antivirusinės veiklos – apibrėžia vadovus ir procedūras, skirtas sumažinti virusų grėsmes;
- elektroninio pašto – pašto naudojimo, saugojimo, persiuntimo tvarka;
- interneto naudojimo – jautrios informacijos, žurnaliavimo, DMZ zonos sudarymo reikalavimai;

- nuotolinės prieigos, nešiojamų įrenginių naudojimo – nuotolinės prieigos tvarka, leidimai, nešiojamų įrenginių naudojimo tvarka, reikalavimai;
- ir kitos.

Saugos politikos dokumento galima sudėtis, jo reikalavimai:

- dokumento tikslas,
- dokumento galiojimo sritis,
- pačių politikos reikalavimų rinkinys:
  - draudžiamieji veiksmai,
  - naudojimo tvarka,
  - naudojimo stebėjimas,
  - politikos pažeidimo pasekmės,
  - naudojamų terminų saugos politikoje paaiškinimai.

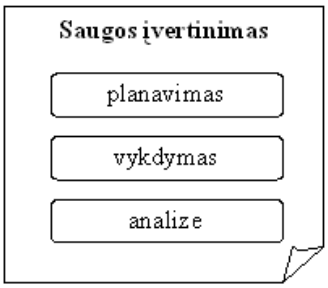
Priklausomai nuo saugos politikos tipo ir galiojimo srities dokumento turinys gali skirtis nuo šios aprašytos struktūros.

Taigi saugos politika – tai svarbiausias elementas organizacijos tinklo saugos įvertinime. Testuojant ir analizuojant saugos objektus yra būtina palyginti jų esamą būseną su norima.

3.1.5. Tinklo saugos įvertinimas

Atsižvelgiant į organizacijos lygius (3.1.2 dalis) techninis tinklo saugos įvertinimas vyksta vykdomojo lygio matavimo etape (2 pav.). Saugos įvertinimo procesas yra glaudžiai susijęs su organizacijos vertybe arba su saugos objektų testavimu bei jų analize. Analizuojant saugos objektą, galima nustatyti jo esamą saugos būseną ir palyginti su norima. Įvertinimo metu yra analizuojamos, tikrinamos, nustatomos objekto saugos savybės, kas leidžia pasiekti esamos situacijos tikslumą bei aiškumą. Šie rezultatai yra susisteminami valdomojo lygio matavimo etape, vyksta esamos sistemos būsenos analizė. Šio etapo rezultatai panaudojami rizikos analizei ir jos įvertinimui. Čia išskiriamos grėsmės, pažeidžiamumai, tikimybė, žala, rizika ir kita. Bendra išvada pateikiama valdžios lygiui strateginiam sprendimui priimti.

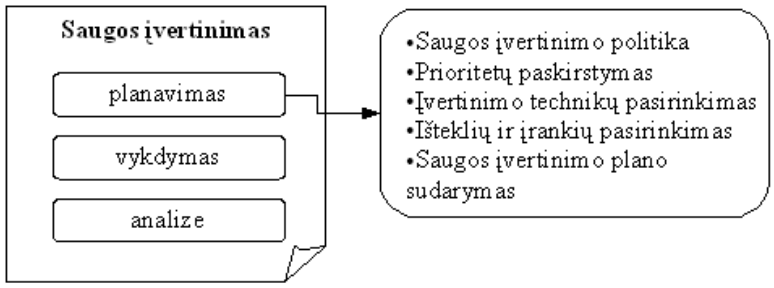
Testavimas ir analizė sudaro saugos įvertinimą. Šis įvertinimas turės tris etapus: planavimas, vykdymas, analizė [15]. Etapai pavaizduoti 5 paveiksle.



5 pav. Saugos įvertinimo etapai

3.1.5.1. Įvertinimo planavimas

Įvertinimo planavimo etapas – tai yra duomenų apie saugos situaciją surinkimas bei tinkamo saugos įvertinimo būdo pasirinkimas [16]. Dažniausiai yra surenkama informacija tokia, kaip įmonės vertybės, jų grėsmės, saugumo priemonės. Turint sukauptą informaciją, sprendžiama ir planuojama, kaip bus vykdomas saugos įvertinimas. Saugos įvertinimą reikia traktuoti kaip bet kokį kitą projektą, į kurį įeina projekto valdymo planas, tikslai, uždaviniai, įvertinimo sritis, saugos objektai, reikalavimai, testavimo tipų technikų pasirinkimas ir t. t. Saugos įvertinimo planavimo etapai pavaizduoti 6 paveiksle.



6 pav. Saugos įvertinimo planavimo etapai

Saugos įvertinimo politika

Įvertinimo vykdymui įmonės tinkle reikalinga duomenų saugos įvertinimo politika, kuri gali suteikti kryptį įvertinimo darbams. Šios politikos funkcija yra nustatyti įvertinimo darbų reikalavimus ir atsakingumą už šių reikalavimų išpildymą. Atsakingumas turi būti tolygiai paskirstytas visam vykdančiam įvertinimą personalui, įskaitant trečių šalių vykdytojus. Kadangi skirtingoms tinklų konfigūracijoms reikalingi skirtingi saugos įvertinimo metodai, įvertinimo politikoje turi būti paminėta, kokie įvertinimo testų ir tyrimų būdai yra pasirinkti ir kiek kartų darbai turi būti pakartoti. Be to, reikalingi reikalavimai dokumentacijai, tokiai kaip įvertinimo planui, darbuotojų rezultatų pateikimui prieinamu laiku, dažniu, forma.

Saugos įvertinimo politikos struktūra:

- reikalavimai, kurie įvertinimo metu turi būti išpildomi,

- atsakomybės paskirstymas,
- įvertinimo darbų vykdymas taikant pasirinktą įvertinimo metodiką,
- įvertinimo darbų dažnis,
- reikalavimai dokumentacijai, tokiems kaip įvertinimo planui ir rezultatams.

Prioritetų paskirstymas

Šiame darbų planavimo etape įmonės techninės vertybės, kurios bus vertinamos ir testuojamos yra skirstomos į kategorijas. Šis skirstymas reikalingas nes norima išdėlioti prioritetus testuojant saugos objektus. Kaip žinoma, ne visada techninės įmonės vertybės yra prieinamos testavimui, ir tam tikri testai turi būti atlikti ne vieną kartą. Todėl įvertinimo darbų planas bus efektyvus tuo atveju, jeigu bus atliktas techninių vertybių išskyrimas, prioritetų paskirstymas.

Įvertinimo technikų pasirinkimas

Yra daug faktorių, kurie lemia saugos įvertinimo technikų pasirinkimą, todėl yra patartina tiksliai apibrėžti saugos įvertinimo uždavinius, kad galima būtų tiksliai nusakyti įvertinimo sritį. Pasirinkus tikslius uždavinius ir atmetus nereikalingus įvertinimo darbus, reikia išvardinti saugos objektus, kurie bus vertinami.

Saugos uždavinių atlikimui galima naudoti ne vieną saugos įvertinimo techniką. Skirtingų technikų pritaikymas priklauso nuo apribojimų. Todėl reikia pasirinkti tinkamus resursus atsižvelgus į įvertinimo sritį. Kai kurių įvertinimo technikų pritaikymas gali kainuoti žymiai daugiau negu kiti, nes reikalauja brangių programinių ar techninių priemonių.

Taip pat yra laiko apribojimas. Įsiskverbimo testai gali pareikalauti daugiau resursų, laiko, negu pažeidžiamumų skenavimas. Nuo laiko priklauso išlaidos audito darbuotojams. Saugos objektai yra prieinami testui tik tam tikrais laiko tarpais.

Dar vienas apribojimas, kuris įtakoja įvertinimo technikos pasirinkimą, yra audito darbuotojų kvalifikacijos lygis. Žemą kvalifikaciją turintis auditorius nesugebės visapusiškai atlikti įsiskverbimo testus, tai paliks saugos spragas testuojamoje sistemoje.

Pasirinktos technikos nepasisekimo riziką irgi būtina įvertinti. Tokios technikos, kaip įsilaužimo testai, gali padaryti sistemą neveiksnia, atskleisti konfidencialią informaciją arba pažeisti jautrią informaciją. Tokiu atveju testo metu dažnai konfidencialią informaciją pakeičia klaidinga.

Pačios įvertinimo technikos yra suskirstytos į klases, tai palengvina jų pasirinkimą. Yra peržiūros įvertinimo technikos, kur peržiūrima įmonės dokumentacija, žurnalų failai ir t.

t. Saugos objektų identifikacijos ir analizės technikos, tokios kaip tinklo arba prievadų skenavimai, pažeidžiamumų nustatymai. Naudojamos saugos objekto pažeidžiamumų patvirtinimo technikos, tokios kaip bendrosios paslapties žinojimo - slaptažodžio nulaužimas.

Saugos įvertinimo technikos atliekamos iš dviejų pozicijų: išorinių ir vidinių. Kai testai atliekami iš išorės, yra testuojamas įmonės saugos perimetras. Kadangi saugos mechanizmai ir užkardos nepraleidžia daug srautų, dažniausiai yra ieškomi įmanomi pažeidžiamumai per populiariausius prieinamus servisus: HTTP, POP, IMAP, SMTP, FTP. Bandoma gauti prieigą per bevielį tinklą.

Vidiniai saugos testai yra ne taip apriboti kaip išoriniai. Vertintojas jau turi tam tikras prieigos teises, kas leidžia gauti tokią informaciją, kokią turi paprastas vartotojas. Be to, iš tokios pozicijos galima taikyti tokią techniką kaip tinklo šnipinėjimas. Dauguma testų yra orientuoti į tai, kad gautume daugiau prieigos teisių, pavyzdžiui, specialisto ar administratoriaus.

Išteklių ir įrankių pasirinkimas

Tų sistemų, kurios yra sudarytos saugumo įvertinimui, įrankių spektras priklauso nuo saugos testo tipo ir technikos reikalavimų. Planuojant saugumo įvertinimo procesą, reikia atsižvelgti į suplanuotas pasirinktas testavimo technikas ir atitinkamai nuspręsti, kokių išteklių prieiga bus reikalinga bei kokia techninė ir programinė įranga bus naudojama.

Pavyzdžiui, tikrinamos įmonės nuostatų, saugos politikų analizavimas skaitymas, dokumentacijos formavimas reikalauja įrankių, kuriuos panaudojant bus galima skaityti dokumentus ir formuoti ataskaitas. Sistemos, sukurtos vykdyti įsiskverbimo testus, pažeidžiamumo skenavimus, yra sudėtingos, turinčios tam tikrus minimalius reikalavimus techninei ir programinei įrangai.

Atsižvelgiant į išteklių prieinamumą, saugumo auditoriams gali prireikti fizinės prieigos prie serverių arba nuotolinės prieigos prie tinko naudojant virtualius privačius tinklus. Negalima pamiršti suteikti kiekvienam testuotojui prieigos teisės prie testuojamų išteklių. Tai leis apriboti testuotojus nuo konfidencialios informacijos bei registruoti jų veiklą.

Tokios testavimo technikos, kaip slaptažodžio nulaužimas, reikalauja dedikuoto serverio su galingomis techninėmis charakteristikomis. Testavimai vykdomi ilgais laiko tarpais sugeneruoja daug duomenų, kuriuos reikia kaupti. Tokiam tikslui pasiekti reikia didelės talpos kietųjų diskų.

Šiuo metu egzistuoja daug testavimo programinių įrankių, sukurtų atskirų programuotojų, valstybinių ar komercinių grupių. Tai gali būti atviro kodo programos,

apribotos nemokamos licencijos ar mokamos. Planuojant įvertinimo testus svarbu parinkti tinkamus programinius įrankius, nuolat sekti ir diegti atnaujinimus. Jeigu įrankis yra atviro kodo, būtina įsitikinti, ar gauta programinė įranga neturi žalingo kodo, ir yra parsiųsta iš patikimo šaltinio.

Programiniai įrankiai dažniausiai yra skirti konkrečiai operacinei sistemai. Tai priverčia vertintojus turėti skirtingas operacines sistemas skirtingų įrankių naudojimui, kas yra nepatogu. Žinoma, yra įrankiai, dirbantys keliose operacinėse sistemose, bet tai neišgelbėja auditoriaus nuo savo kompiuterio perkrovimo, darbų planavimo. Šiuos trūkumus išsprendžia virtualiosios mašinos. Į vieną auditoriaus kompiuterį galima įdiegti virtualias mašinas su skirtingomis operacinėmis sistemomis. Kiekvienos operacinės sistemos atvaizdo sukūrimas leidžia išsaugoti visus programinius įrankius su reikalingomis konfigūracijomis. Tai leidžia vykdyti užbrėžtus testus lygiagrečiai, vykdant darbų dokumentaciją, testus, duomenų analizę. Toks būdas leidžia automatizuotai registruoti testuotojo veiksmus. Be to, yra galimybė visą darbo aplinką perkelti į kitą darbinį kompiuterį perkeliant tik operacinių sistemų atvaizdus.

Saugos įvertinimo plano sudarymas

Šio etapo eigoje sudaromas pasirinktų įvertinimo veiksmų planavimas ir visos susijusios informacijos dokumentacija. Plano sudarymo pagrindiniai žingsniai yra tokie:

- saugos kontrolinių priemonių tipo nustatymas,
- saugumo kontrolinių priemonių nustatymas, bei jų saugos padidinimai, kurie turi būti įtraukti į saugos įvertinimo darbus,
- įvertinimo tipų ir technikų pasirinkimas atsižvelgiant į saugumo kontrolines priemones,
- dokumentacijos darbų po įvertinimo etapų ir atitikimo reikalavimams patikrinimų įtraukimas,
- laiko įvertinimas pasirinktų įvertinimo procedūrų pritaikymui prie organizacijos darbo aplinkos,
- papildomų įvertinimo darbų planavimas, jeigu reikia, naujų reikalingų saugos kontrolinių priemonių nustatymas,
- sudarytos įvertinimo procedūros pritaikymo strategijos konstravimas,
- įvertinimo procedūrų optimizavimas išvengiant pakartotinių darbų, bei perteklingo išteklių naudojimo.

3.1.5.2. Įvertinimo vykdymas

Pagrindiniai tikslai saugos įvertinimo vykdymo etape yra saugos objektų pažeidžiamumų ir saugos spragų nustatymas. Įvertinimo vykdymas turi griežtai atitikti sukurtą detalią įvertinimo politiką. Teisingas įvertinimo vykdymas priklauso nuo to, kaip tikslai testuotojas suprato iškeltus uždavinius. Todėl vykdant saugos įvertinimą būtina koordinuoti veiksmus su įvertinimo politika bei dokumentuoti etapų rezultatus. Saugos įvertinimo vykdymo etapai pavaizduoti 7 paveiksle. Be to, sėkmingą įvertinimo eigą gali sutrukdyti išorinės kliūtys [15].

7 pav. Saugos įvertinimo vykdymo etapai

Pasipriešinimas

Pasipriešinimo saugumo įvertinimo darbams šaltiniai gali būti įvairūs. Tai gali būti įmonės sistemų ar tinklo administratoriai, užfiksavę sistemos pakeitimus, arba paprasti vartotojai. Dažniausios pasipriešinimo priežastys būna tokios:

- Prieinamumo prie kompiuterinės sistemos, tinklo ar išteklių netekimas.
- Baimė atsidurti nepatogioje situacijoje arba gauti pastabą iš vadovybės dėl pareigybių vykdymo sutrikimų.
- Pasipriešinimas pasikeitimams arba organizacijos darbuotojų nenoras vykdyti savo darbą kitokiu būtu.

Gavus palaikymą ir pritarimą iš įmonės vadovybės tam tikrus pasipriešinimo faktorius galima pašalinti. Pats geriausias tokių kliūčių vengimas yra įvertinimo procesų įtraukimas į bendrą įstaigos saugumo politiką. Tokiu būdu įmonės administratoriai bei vartotojai bus informuoti ir pasiruošę visiems saugos įvertinimo darbams. Kaip įprasta, į įmonės saugos politiką įeina administracinė atsakomybė už nuostatų nesilaikymą.

Realistiškumo nepakankamumas

Dažnai prieš pradedant saugos įvertinimą įmonės vartotojai ar administratoriai sustiprina organizacijos saugos mechanizmus, atlieka pakeitimus sistemoje, siekiami priartinti ją prie įmonės saugos politikos ir nustatytų reikalavimų. Tai galima įvertinti pozityviai,

įvertinimo eigoje tokia sistema yra veikianti ir palaikoma administratorių. Bet įvertinimo pabaigoje visi padaryti nustatymai keičiami į pradinius. Tokių kliūčių padeda išvengti atsitiktiniai saugos įvertinimai, neinformuojant apie juos įmonės darbuotojų.

Staigus reagavimas į rastus silpnumus

Saugos įvertinimo eigoje yra surandami sistemos silpnumai. Kai tik įmonės administratoriai sužino apie tai, jie nori šiuos silpnumus pašalinti tikėdamiesi, kad auditoriai pakartos įvertinimą su ištaisyta sistema ir patvirtins, kad silpnumo nėra. Tai yra puiku, bet tokie papildomi įvertinimo darbai turi būti įtraukti į saugos įvertinimo planą, politiką. Be to, būtinas pakeistos sistemos įmonės saugos politikos bei reikalavimų atitikimo patikrinimas.

Laikas

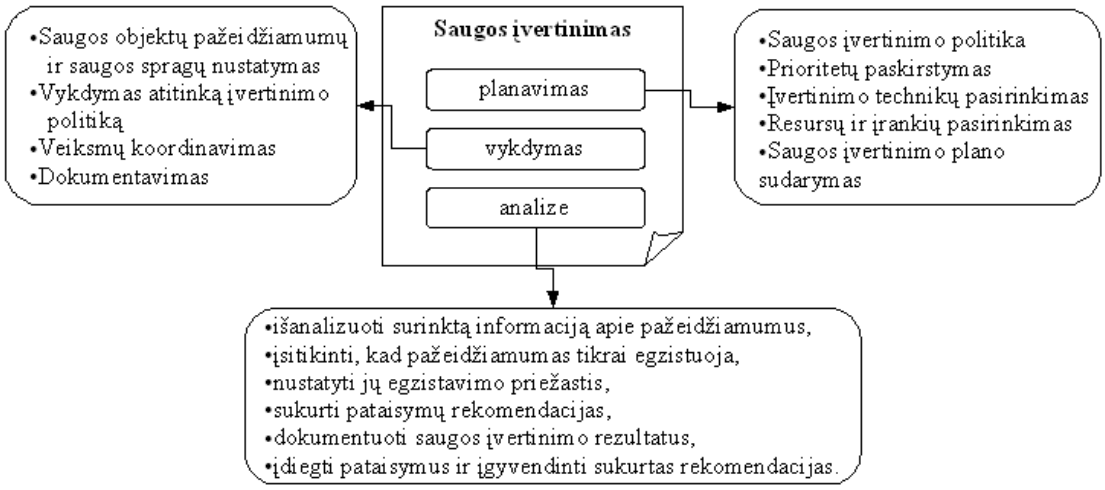
Dažnai saugos įvertinimas yra vykdomas įmonės sistemos vystymo arba diegimo metu su tam tikru laiko apribojimu. Nors saugos įvertinimo procesas turi būti sistemos vystymo ir diegimo gyvavimo ciklo dalis. Laikas yra rimtas apribojimas toms sistemoms, kurios yra kritinės informacijos gaminimo atžvilgiu. Įvertinimo procedūros gali nutraukti tokių sistemų prieinamumą, kas yra neleistina ir kas priverčia įvertinimo procedūras atlikti nedarbo laiku. Praktikoje sutinkama, kad įvertinimo darbai yra ribojami laiko atžvilgiu, kada tikri įsilaužėliai tokių apribojimų išvis neturi.

Įtaka naudojamos sistemos veikimui saugos įvertinimo metu

Nors plano sudarymo metu yra apgalvojama, kaip netrikdyti veikiančios sistemos veikimo ir kaip nenutraukti sistemos prieinamumo, vis tiek yra galimybė atsirasti netikėtai netyčinei situacijai. Todėl kiekvienas testas turi būti registruojamas. Į registraciją galima įtraukti tokius duomenis: laiko žymė, testo tipas, naudojamas testavimo įrankis, įrankio veiksmai, koks kompiuteris yra testuojamas ir t. t. Taip pat patartina turėti specialų įrankį, kuris registruoja testo metu auditoriaus veiksmus, komandas, klavišų paspaudimus. Šiam tikslui pasiekti yra daug programinių įrankių terminalo pavidalu ar su grafine sąsaja. Sukaupti duomenys gali padėti rasti sistemos prieinamumo nutraukimo priežastis ir priklausomai nuo situacijos gali įrodyti auditoriaus nekaltumą.

3.1.5.3. Įvertinimo analizė

Dažnai įvertinimo analizė vykdoma ne tik po įvertinimo užbaigimo, bet ir įvertinimo metu. Aptikus kritinius pažeidžiamumus, yra poreikis juos pašalinti. Bet daugiausia dėmesio analizei skiriama po įvertinimo darbų įvykdymo. 8 paveiksle pavaizduoti analizės metu atliekami žingsniai [15].



8 pav. Analizės metu atliekami žingsniai

Pirmi trys žingsniai skirti darbui su pažeidžiamumais. Norint įsitikinti, ar programiniai įrankiai nesuklydo, ir kad tikrai yra saugumo grėsmės, reikia panaudoti pažeidžiamumų patvirtinimo grupės technikas. Tai yra slaptažodžių nulaužimas, įsiskverbimo testai, socialinė inžinerija.

Turint patvirtintą informaciją apie saugumo pažeidžiamumus ir žinant pažeidžiamumų atsiradimo priežastis, nėra sunku sudaryti šių grėsmių pašalinimo planą. Šiam tikslui pasiekti yra keičiama įmonės saugos politika, nustatytos procedūros ar procesai, saugos architektūra, sistemų atnaujinimas.

Svarbu dokumentuoti saugos įvertinimo rezultatus. Į šią dokumentaciją įeina visi surasti saugos pažeidžiamumai, saugumo spragos, jų aprašai, bei šių spragų pašalinimo nurodymai.

Dokumentų, ataskaitų ar protokolų forma priklauso nuo to, kam ji yra skirta. Ataskaitoje, skirtoje išorinėms organizacijoms, turi būti įvertinimo metodikos aprašymas, įvertinimo rezultatai, analizės dalis ir rekomendacijos, ar kitos dalys atitinkančios tam tikrus reikalavimus. Dokumentai, kurie neišeis iš organizacijos ribų, gali būti aprašomojo pobūdžio.

3.1.5.4. Valdžios valdymo vykdymo lygių įvertinimo metodas

Pateiktas duomenų saugos įvertinimo metodas pagrįstas trijų valdžios, valdymo,

vykdymo lygių principu (VVVLĮM – Valdžios Valdymo Vykdymo Lygių Įvertinimo Metodas) [5]. Įvertinimo analizės metu galima paskaičiuoti saugos lygio skaitinį įvertinimą.

Pagrindinis šio metodo principas susidaro iš to, kad tikrinamas projektinis ir realizuotas patikimumas kiekviename VVVLĮM lygyje.

Projektinis patikimumas parodo, ar pakankamai gerai yra suprojektuoti sistemos elementai, procesai ar kontrolinės priemonės atsižvelgiant į organizacijos poreikius. Tai leidžia nustatyti, kaip turėtų veikti duomenų saugos sistema, jeigu visi diegimo ir konfigūravimo darbai būtų įvykdyti sėkmingai.

Realizuotas patikimumas parodo, kaip yra realizuotos apsaugos priemonės, ar yra vykdomi nurodymai, ar veikia saugos elementai taip, kaip buvo suplanuota, ar teisingai sukonfigūruotos techninės kontrolinės priemonės.

Be to, kiekvienas lygis turi savo kriterijų grupių kiekį. Šios kriterijų grupės atvaizduoja informacinės saugos sistemos funkcionavimo struktūrą.

Kriterijų grupės yra sudarytos atsižvelgiant į nagrinėtą aplinkos analizėje duomenų saugos sistemos struktūrą. Įvertinant valdžios lygmenį siūlomi tokie kriterijai:

1. Strateginis išlyginimas. Ši kriterijų grupė įvertina:

- apibrėžtą informacijos saugumo strategiją,
- apibrėžtus tikslus ir procesus sistemai tobulinti ir reorganizuoti,
- kaip vyksta pasiūlytų sprendimų priėmimas,
- kaip sudaromi patobulinimo planai, projektai,
- kaip planuojama saugos priemonių kontrolė, palaikymas.

Tai įvertinama siekiant patikrinti, ar projektuojamos priemonės atitinka organizacijos tikslus.

2. Saugos politika. Ši kriterijų grupė padeda patikrinti, ar teisingai sudaryta organizacijos saugos politika, ar teisingai pritaikyti standartai, vystymo procesai, realizacija, palaikymas. Tai leidžia įsitikinti, ar saugos veikla atitinka organizacijos poreikius, reguliavimą, reikalavimus.
3. Organizacinė struktūra. Ši kriterijų grupė įvertina organizacijos struktūrą, personalo atsakomybę už informacijos saugumą, tikrinama, ar nebus pažeisti informacinių santykių subjektų interesai.
4. Duomenų saugos kontrolė. Šie kriterijai suteikia galimybę įvertinti kaip valdžios lygis kontroliuoja priimamus sprendimus, nurodymus ir darbo našumą.

Valdymo lygmens siūlomas įvertinimo metodas leidžia nustatyti, kaip efektyviai

vyksta valdymo procesai. Įvertinimo kriterijai pagrįsti „Six Sigma“ patobulinimo metodu [8]:

1. Informacijos saugos tikslai.
2. Našumo parametrų nustatymas, formulavimas.
3. Našumo parametrų įvertinimas.
4. Būdo ar metodikos įvertinimas nustatant sausos sistemos įtakos verslui bei rizikos analizei.
5. Saugos sistemos kontrolinių priemonių vykdymas.
6. Patobulinimų realizacijos vystymas.
7. Patobulinimų realizacijos valdymas.

Vykdomojo lygmens įvertinimas siūlomas atsižvelgiant į saugumo priemonių kontrolę. Galimos tokios kriterijų grupės:

1. Techninės kontrolinės priemonės įdiegtos:
   a) perimetro lygyje,
   b) tinklo lygyje,
   c) tarnybinės stoties lygyje,
   d) programinės įrangos lygyje,
   e) duomenų lygyje.
2. Procedūrinės kontrolinės priemonės:
   a) pakeitimų valdymas,
   b) prieigos kontrolės valdymas,
   c) tarnybinių įsipareigojimų apribojimas,
   d) nenutrūkstamumo veiklos plano sudarymas,
   e) incidentų valdymas,
   f) mokymai.
3. Fizinės kontrolinės priemonės.

Kiekvieną šios grupės kriterijų siūloma vertinti keturiom būsenom: 0 – nepatikimas, 0,33 – dalinai patikimas, 0,66 – beveik patikimas, 1 - patikimas.

Taip vertinimas vyksta įvertinus kiekvienos grupės kriterijus iš projektinio ir realizuoto patikimumo pusės, suskaičiavus grupės kriterijų vidurkius, po to skaičiuojamas vieno lygio kriterijų grupių vidurkis, ir galiausiai visų lygių vidurkis.

Gautas įvertinimas yra subjektyvus. Vertintojas įvertina kiekvieną metodikos komponentą savo požiūrių. Čia gali suveikti žmogiškasis faktorius, klaidos tikimybė yra aukšta. Taip pat įvertinimas bus aktualus tik rezultatų gavimo metu. Po tam tikro laiko sistemoje gali įvykti pakeitimas. Rezultatai nenusako silpnų įvertinamųjų elementų rizikos.

3.1.6. Saugos testų tipai

Saugos testai reikalingi saugos objektų analizei, grėsmių ir pažeidžiamumų nustatymui.

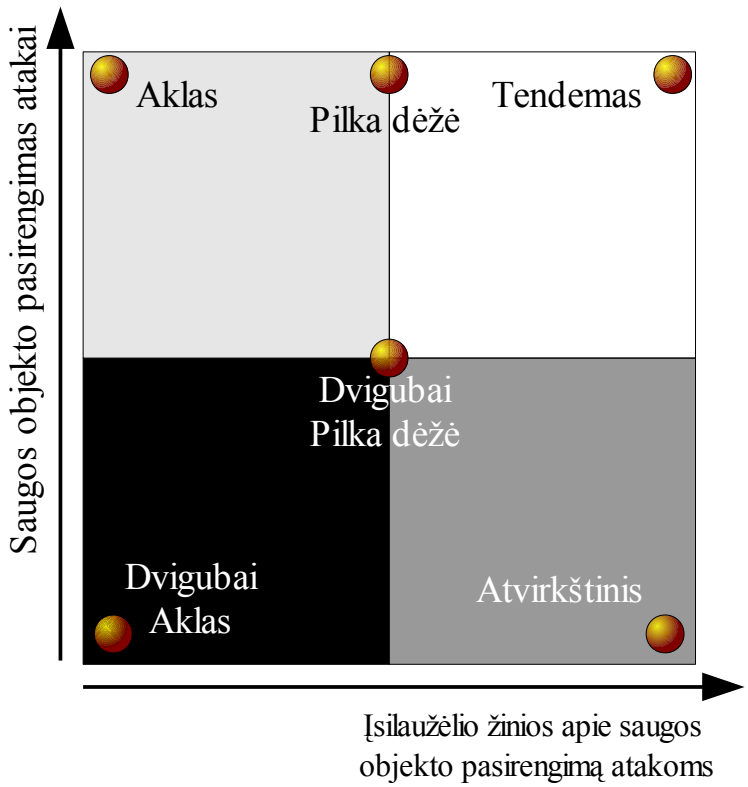
Saugos testų metu išskiriamos dvi sąvokos:

- saugos objekto pasirengimas atakai,
- įsilaužėlio žinios apie saugos objekto pasirengimą atakoms.

Pirmoji sąvoka nusako saugomo objekto atsparumo lygį nuo atakų [17]. Kuo daugiau saugos priemonių yra susieta su šiuo objektu, tuo didesnis atsparumo lygis nuo įsilaužėlio atakų. Tai gali būti visi saugos mechanizmai bei kontrolinės priemonės: užkarda, kriptografiniai metodai, autentifikacijos priemonės, žurnaliavimas ir t. t.

Antroji sąvoka nusako įsilaužėlio žinių lygį apie saugos objektus ar jų saugos priemones. Pavyzdžiui, žinant vidinę įmonės tinklo adresaciją, įsilaužėlis gali aptikti kompiuterius ir skenuoti jų prievadus.

Saugos testo tipas priklauso nuo šių dviejų sąvokų. 9 paveiksle parodytos galimos kombinacijos.



9 pav. Saugos testų tipai

Testo tipas „Aklas“

Auditorius bando atakuoti saugos objektą be žinių apie objekto saugos priemones,

vertybes, prieigos galimybes. Saugos objektas yra apsaugotas saugos priemonėmis, kurios apsaugo nuo iš anksto žinomų auditoriaus veiksmų. Toks testas patikrina auditoriaus praktinius įgūdžius. Šio testo sritis priklauso nuo auditoriaus galimybių ir patirties.

Testo tipas „Dvigubai aklas“

Auditorius bando atakuoti saugos objektą be žinių apie objekto saugos priemones, vertybes, prieigą. Saugos objektas iš anksto „nežino“ apie auditoriaus ketinimus, testo priemones, prieigos būdus. Toks testo tipas leidžia patikrinti auditoriaus praktinius įgūdžius bei saugos objekto elgseną esant „nežinomoms“ objektui atakoms. Tokio tipo testus dažniausiai atlieka nepriklausomi auditoriai, siekdami išbandyti įdiegtus saugos mechanizmus, rasti naujas spragas ar pažeidžiamumus.

Testo tipas „Pilka dėžė“

Auditorius bando atakuoti saugos objektą su ribotomis žiniomis apie objekto saugos priemones, vertybes ir žiniomis apie prieigos kanalus. Saugos objektas yra apsaugotas saugos priemonėmis, kurios apsaugo nuo iš anksto žinomų auditoriaus veiksmų. Toks testo tipas leidžia patikrinti auditoriaus praktinius įgūdžius, bei saugos objekto elgseną esant „nežinomoms“ objektui atakoms. Testo sritis priklauso nuo auditoriaus pradinių žinių kiekio apie testuojamą objektą. Taip pat rezultatai priklauso nuo auditoriaus galimybių ir patirties. Tokio testo tipo metu dažniausiai pasirenkama pažeidžiamumų skenavimo technika.

Testo tipas „Dvigubai Pilka dėžė“

Auditorius bando atakuoti saugos objektą su ribotomis žiniomis apie objekto saugos priemones, vertybes ir pilnomis žiniomis apie prieigos kanalus. Saugos objektas apsaugos priemonių diegimo metu buvo žinoma apie audito sritį ir laiko tarpus, bet ne apie prieigos kanalus arba testavimo kryptis. Toks testo tipas leidžia patikrinti auditoriaus praktinius įgūdžius bei saugos objekto elgseną esant „nežinomoms“ objektui atakoms. Testo sritis priklauso nuo auditoriaus pradinių žinių kiekio apie testuojamą objektą. Taip pat rezultatai priklauso nuo auditoriaus galimybių ir patirties. Toks testo tipas dar žinomas kaip „Baltos dėžės“ auditas.

Testo tipas „Tendemas“

Ir saugos objektas, ir auditorius iš anksto pasiruošę auditui ir žino apie saugos įvertinimo detales. Šis testo tipas leidžia patikrinti įdiegtas objekto saugumo priemones ir nustatyti saugos klaidas. Bet šio testo metu negalima sužinoti objekto pasiruošimą nežinomoms situacijoms, aplinkos būsenoms, skirtingiems veiksniams. Testo rezultatai

priklauso nuo auditoriaus išankstinių žinių kokybės apie saugos objektą, kaip ir nuo jo patirties. Toks tipas dažnai yra vadinamas „Kristalinė dėžė“.

Testo tipas „Atvirkštinis“

Auditorius atakuoja saugos objektą turėdamas visas žinias apie saugos procesus ir saugos priemones. Tuo tarpu objekto saugos priemonių kūrimo metu nebuvo žinoma apie tai, kas kada ir kaip auditorius vykdys testavimus. Pagrindinis šio testo tikslas yra sužinoti objekto pasiruošimo lygį nežinomoms situacijoms, aplinkos būsenoms, skirtingiems veiksniams. Testo rezultatai priklauso nuo auditoriaus išankstinių žinių kokybės apie saugos objektą ir ypač nuo auditoriaus sumanumo, patirties, gebėjimų sugalvoti naujas pažeidžiamumo kryptis. Toks testo tipas dar yra vadinamas „Raudonos komandos pratybos“.

Kai kurie testų tipai naudojami atitinkamose testavimo technikose.

3.1.7. Testavimo technikos

Šiuo metu yra sukurta daug testavimo ir tikrinimo technikų, kurios leidžia įvertinti sistemų ir tinklų saugos situaciją. Kaip jau buvo minėta, tai yra peržiūros įvertinimo technikos, kur peržiūrima įmonės dokumentacija, saugos objektų identifikacijos ir analizės technikos, tokios kaip tinklo arba prievadų skenavimai, saugos objekto pažeidžiamumų patvirtinimo technikos saugos spragų egzistavimo įsitikinimui [15].

Peržiūros technikos

Peržiūros technikos yra traktuojamos kaip pasyvūs testai. Šiais testais galima nustatyti sistemos, programinės įrangos, įmonės saugos politikos, procedūrų, tinklo saugos spragas. Be šių technikų negali apsieiti ir kitos kategorijos testai, tokie kaip įsiskverbimo testai. Šios technikos yra pasyvios, todėl turi mažiausią įtaką ir pakeitimo riziką sistemoms. Tokia charakteristika skaitoma kaip privalumas. Peržiūros technikos:

- Dokumentacijos peržiūra.
- Žurnalinių failų peržiūra.
- Saugos taisyklių rinkinių peržiūra.
- Sistemos konfigūracijos peržiūra.
- Tinklo šnipinėjimas.
- Failų vientisumo patikrinimas.

Objektų identifikacijos ir analizės technikos

Šių technikų pagrindinis tikslas yra techninė išteklių, sistemų, įmonės techninių vertybių, saugos objektų identifikacija ir pažeidžiamumų nustatymas. Dauguma priemonių dirba skenavimo pagrindu, nors yra naudojami ir netechniniai būdai, tokie kaip įmonės inventorizacijos sąrašai ar paprasčiausias fizinis patikrinimas, jeigu tam tikra naudojama technika nėra prijungta prie tinklo. Objektų identifikacijos ir analizės technikos:

- Tinklo įrenginių nustatymas.
- Tinklo įrenginių prievadų ir jų servisų identifikacija.
- Pažeidžiamumų skenavimas.
- Bevielio tinklo skenavimai.

Objektų pažeidžiamumų patvirtinimo technikos

Šios technikos naudoja peržiūros ir objektų identifikacijos ir analizės technikų sukauptus duomenis, rastų pažeidžiamumų patvirtinimui, tyrimui. Tokie testai parodo saugos spragas ir šių spragų panaudojimo rezultatus. Objektų pažeidžiamumų patvirtinimo technikos:

- Slaptažodžių nulaužimas.
- Įsiskverbimo testai.

3.2. Darbo problema tikslas ir uždaviniai

Analizuojant saugos gyvavimo ciklą 3.1.1 dalyje 1 paveiksle, saugos politika arba dokumentuotų sprendimų visuma yra centre. Visų kitų etapų rezultatai yra fiksuojami dokumentuose, kurie apibrėžia visos organizacijos duomenų saugą. 3.1.4 dalis „Saugos politika“ parodo, kaip saugos politika aprašo organizacijos duomenų saugą, kaip išsidėsto saugos politikos hierarchijos lygiai, kas įtikina, kad dokumentuotų sprendimų visuma atvaizduoja siekiamą organizacijos duomenų saugą.

Šiuolaikinėje organizacijoje duomenų sauga, apibrėžta saugos politikoje yra užtikrinama saugos mechanizmų, apsaugos automatinių priemonių. Visa ši priemonių visuma vadinama saugos sistema. Duomenų saugos sistemos apriboja veiklą ir draudžia neleistinus veiksmus, atsižvelgiant į saugos politikos reikalavimus.

Įvykus saugos politikos taisyklės pažeidimui, organizacijos duomenų saugos lygis krenta, pažeidžiamas saugos politikos vientisumas ir atsakingas saugos sistemos komponentas. Iš to seka, kad galima apibrėžti saugos lygį, jį galima įvertinti.

Atsižvelgiant į 3.1.1 skyrius „Saugos gyvavimo ciklas“, 3.1.2 „Organizacijos lygiai

duomenų saugos srityje“ galima teigti, kad yra atliekami nuolatiniai saugos sistemos stebėjimo įvertinimo ir palaikymo darbai. Šie darbai vyksta pagal organizacijos lygių etapų seką (2 pav.). Etapai valdymo lygmenyje: matavimai, patikra; vykdomajame etape: matuojamos ir stebimos sistemos kontrolinės priemonės. Analizuojant saugos objektą, galima nustatyti, ar jis atitinka saugos reikalavimus apibrėžtus saugos politikoje, ar ne. Saugos lygis priklauso nuo vykdomų saugos reikalavimų skaičiaus. Siekiant nustatyti saugos politikos atitikimą esamai būsenai, yra aprašyti skirtingi įvertinimo metodai 3.1.5, 3.1.6, 3.1.7 dalyse. Taip pat duomenų saugos lygį galima išreikšti kiekybine skaitine reikšme. Tai gali padaryti VVVLĮM metodas pateiktas 3.1.5.4 dalyje.

Peržvelgus visą išanalizuotą medžiagą galima išskirti tokias problemas:

1. norint gauti įvertinimą, reikia atlikti daug sudėtingų veiksmų:
   1.1. įvertinimo metodika yra sudėtinga,
   1.2. įvertinimo plano sudarymo sudėtingumas,
   1.3. kliūtys, skirtingi įvertinimo būdai ir jų valdymas, kas padaro įvertinimą sudėtingą,
   1.4. rezultatų iš skirtingų įvertinimo būdų surinkimas ir bendro įvertinimo skaičiavimas yra sudėtingas,
   1.5. žmogiškasis faktorius, klaidos;
2. rezultatai yra aktualūs tik įvertinimo vykdymo metu.

Analizuoti įvertinimo būdai leis įvertinti duomenų saugą, bet jie yra sudėtingi. Norint atlikti įvertinimą, reikia įvykdyti labai daug sudėtingų veiksmų, priklausomai nuo pasirinkto įvertinimo būdo. Atsižvelgiant į organizacijos lygių etapų seką (2 pav.) įvertinimo darbai vyksta kiekvieno valdomojo ciklo metu, o ciklas yra kartojamas dažnai, kas priverčia nuolat kartoti sudėtingą darbą.

Įvertinimo plane turi būti atskirai specialiai sudaryta įvertinimo saugos politika (3.1.5.1 dalis). Taigi sudėtinga yra ne tik įvertinimo metodika, bet ir pasiruošimo darbai yra atliekami rimtai ir atsakingai. Būtina išskirstyti prioritetus, pasirinkti įvertinimo technikas atsižvelgiant į jų apribojimus ir tinkamumą organizacijos tinklui, įvertinti turimus išteklius ir įrankių spektrą. Pasiruošimo darbų klaidos lemia įvertinimo darbų rezultatus.

Įvertinimo vykdymo metu yra susiduriama su daugeliu kliūčių (3.1.5.2 dalis). Nepaisant to, įvertinimo saugos politika turi būti vykdoma, įvertinimo technikų, būdų ir atitinkamas įrankių spektras turi būti efektyviai valdomas, kas yra sudėtinga.

Norint suskaičiuoti bendrą saugos įvertinimą, reikia surinkti įvertinimo rezultatus. Kaip jau buvo minėta, įvertinimo technikų ir būdų yra daug, jų rezultatai yra specifiniai, skirtingų formatų, kas apsunkina rezultatų surinkimą, susisteminimą, organizacijos duomenų

saugos įvertinimo skaitinės reikšmės skaičiavimo procesą.

Kadangi įvertinimo procesas yra sudėtingas, o šie darbai nuolat kartojami, yra atliekamas didelis rankinis darbas, dėl to didelė klaidos tikimybė.

Svarbiausia, kad po visų įvertinimo etapų bus paskaičiuotas vienkartinis įvertinimas. Rezultatai yra aktualūs tik įvertinimo vykdymo metu. Kitą dieną saugos sistemos būsena gali pasikeisti. Dėl didelio darbų ir kliūčių kiekio įvertinimas negali būti kartojamas dažnai.

Šių problemų sprendimas yra toks:

1. automatizuotas įvertinimas skaitine reikšme,
2. nuolatinis automatizuotas tinklo stebėjimas ir pažeidimų fiksavimas.

Šiais laikais mechanizacija ir automatizacija padeda spręsti problemas. Šis atvejis nėra išimtis. Automatizuoti būdai padės išvengti klaidų, sudėtingų įvertinimo darbų kartojimo. Taip pat šios priemonės leidžia nuolat stebėti tinklą.

Šiuos sprendimus gali realizuoti automatizuotas įrankis kuris:

- nuolat fiksuotų saugos politikos pažeidimus,
- skaičiuotų saugos politikos įgyvendinimo įvertinimą.

Pirmą kartą nustatant automatizuoto įrankio parametrus, sudėtingumas yra panašus į įprastą įvertinimo procesą. Bet automatizuotas įrankis įvertina esama saugą nuolat, nesikeičiant įvertinimo aplinkai atlikinėti įvertinimo darbų nebereikės. Tokiu būdu, yra išvengiami pakartotini įvertinimo veiksmai. Todėl yra mažiau tikėtina, kad automatizuoto įrankio vartotojas padarys klaidą.

Kadangi įrankis yra vienas, jį valdyti nebus sudėtinga, tai galės atlikti IT srities specialistas. O įvertinimo rezultatų surinkimo ir skaičiavimo veiksmų daryti nebereikės. Šie veiksmai yra atliekami automatizuotai. Rezultatai yra pateikiami vienoje aplinkoje.

Kaip buvo minėta, automatizuotas įrankis veikia nuolat, todėl rezultatai yra aktualūs nuolat ir pasiekiami visada.

Vienas iš darbo siekių – tai duomenų sauga tinkle, todėl

Taigi darbo tikslas – sukurti organizacijos kompiuterių tinklo srities saugos politikos įgyvendinimo įvertinimo įrankį.

Šiam tikslui pasiekti reikalinga atlikti tokias užduotis:

1. išanalizuoti saugos organizavimo ir įvertinimo būdus;
2. sukurti saugos politikos įgyvendinimo įvertinimo skaičiavimo metodiką;
3. sukurti automatizuotą įrankį, kuris nuolat stebėtų tinklą ir fiksuotų pažeidimus.

Kadangi darbo tikslas yra susietas su duomenų sauga tinkle, automatizuotas įrankis apsiribos tinklo sritimi. Įrankis galės įvertinti ne tik tinklo saugos politiką, o visų saugos

politikos dokumentų taisykles atsižvelgiant į tinklo srities galimybes.

Saugos organizavimo ir įvertinimo būdai jau buvo išanalizuoti 3.1 dalyje.

3.3. Reikalavimai metodikai ir įrankiui

Norint pasiekti suformuluotą tikslą bei uždavinius, reikės sukurti metodiką ir įrankį. Reikalavimai metodikai ir įrankiui yra tokie:

Reikalavimai metodikai

1. Kadangi organizacijos sauga atsispindi saugos politikoje, metodika turi atitikti saugos politikos taisykles. Todėl reikalingas atskiras metodikos saugos politikos reikalavimų (MSPR) rinkinys:
   1.1. MSPR rinkinys apibrėžia pažeidimus, kuriuos stebės įrankis;
   1.2. MSPR-ai turi būti draudžiamojo pobūdžio;
   1.3. MSPR-ai turi atitikti automatizuoto įrankio galimybes.
2. Reikalinga galimybė sugrupuoti metodikos saugos politikos reikalavimus, kad metodika atitiktų organizacijos saugos politikos dokumentų struktūrą.
3. Metodikos komponentai turi atitikti metodikos saugos politikos reikalavimų rinkinį.
4. Metodikos bendras įvertinimas turi išreikšti pažeidimų kiekį ir šių pažeidimų žalos riziką:
   4.1. kiekiui išreikšti naudojamas kintamasis – yra/nėra pažeidimo;
   4.2. metodika turi remtis rizikos analizės rezultatais.

Reikalavimai įrankiui

1. Nuolatinis tinklo stebėjimas.
2. Automatinis pažeidimų fiksavimas pagal metodikos saugos politikos reikalavimų rinkinį.
3. Informacijos apie pažeidimus saugojimas.
4. Įvertinimo skaičiavimas pagal sukurtą metodiką ir rezultato atvaizdavimas.
5. Pažeistų saugos politikos reikalavimų sąrašo atvaizdavimas.

3.4. Automatizuotų priemonių pasirinkimas

Automatizuotas įrankis pagal nustatytus reikalavimus gali būti sudarytas iš tokių priemonių (12 pav.):

- TSP – tinklo stebėjimo priemonė,

- ĮRP – Įrašų registravimo priemonė,
- ĮSP – Įvertinimo skaičiavimo priemonė,
- RAP – Rezultatų atvaizdavimo priemonė.

Šios dalies tikslas nustatyti konkrečias priemones, kurios tenkina reikalavimus.

Tinklo stebėjimo priemonė (TSP)

Tinklo paketams stebėti ir kaupti yra tokie populiariausi įrankiai: „Wireshark", „TcpDump", „Snort".

„TcpDump" – tai tinklo srauto analizatorius [18]. Pagrindinė jo funkcija yra saugoti tinklo srautą. Šį srautą galima perimti visiškai, arba dalinai, nurodant tam tikrus paketo filtro parametrus [19]. Srautas yra filtruojamas pagal paketų antraščių laukus. Valdymas vyksta komandinės eilutės pagalba nurodant parametrus.

„Wireshark" – tai vienas iš populiariausių tinklo protokolų analizatorių [20]. Veikimo principas yra toks pat kaip ir įrankio „TcpDump" – saugoti tinklo srautą ir jį analizuoti. Šis įrankis turi daug kitų papildomų galimybių, kaip vartotojo sąsaja, nuolat atnaujinamas protokolų spektras, platus srauto saugojimo bei importavimo formatų pasirinkimas ir kitos.

Pradinis „Snort" [21] įrankio kūrimo tikslas buvo toks pat kaip „TcpDump" ir „Wireshark" – stebėti tinklo srautą, jį saugoti, analizuoti, išvesti į ekraną paketų dominančius laukus. Bet kūrėjai ties šia vietą nesustojo, ir įrankis buvo vystomas toliau. Vystymo rezultatas – įsilaužimo aptikimo sistema (IDS – intrusion detection system). Dabar šis įrankis gali dirbti tokiais režimais:

- šnipinėjimo režimas – paprasčiausias tinklo srauto nuskaitymas ir paketų atvaizdavimas ekrane;
- saugojimo režimas – paketai yra nuskaitomi saugojami;
- tinklo įsilaužimo aptikimo sistemos režimas (NIDS) – automatinis srauto analizavimas ir sutikrinimas pagal tam tikras sukurtas taisykles;
- „Inline" režimas – panaudojant „Snort" sintaksę, galima atlikti veiksmus, reaguoti į įvykius, dar vadinamas (IPS – intrusion prevention system).

Nustatytus darbo reikalavimus gali tenkinti įrankis „Snort", dirbantis „NIDS" režimu. Toliau yra išvardintos pagrindinės šio režimo funkcijos:

- tinklo srauto stebėjimas,
- automatizuota srauto paketų turinio analizė atsižvelgiant į vartotojo sukurtas taisykles,
- pranešimo apie paketo atitikimą taisyklei generavimas,

- atitikusių taisyklėms srauto paketų saugojimas.

Įrankio „Snort“ įsilaužimo aptikimo sistemos branduolys yra sukurtos įrankio taisyklės, signatūros. Šios signatūros yra nuolat palaikomos ir atnaujinamos. Panaudojant signatūras yra aprašomi paketo fragmentai, kurie yra palyginami su stebimu srautu. Kai fiksuojamas srauto paketo atitikimas signatūrai, yra atliekamas apibrėžtas veiksmas.

Įrankis „Snort“ turi savo signatūrų kūrimo sintaksę. Tai leidžia kurti savo signatūras ir fiksuoti norimus paketus. Panaudojus šią galimybę, tinklo sraute galima fiksuoti metodikos saugos politikos reikalavimo rinkinio pažeidimus.

Įrankio „Snort“ kiekviena taisyklė turi tokią struktūrą [21] (3 lentelė):

3 lentelė. Įrankio „Snort“ taisyklės struktūra

Veiksmas	Protokolas	Šaltinio IP adresas	Šaltinio prievadas	Srauto kryptis	Tikslo IP adresas	Tikslo prievadas	Taisyklės kūnas

Galimi tokie veiksmai: alert, log, pass, activate, dynamic, drop, sdrop, reject. Dažniausiai yra naudojamas veiksmas alert. Jeigu aprašyta taisyklė atitinka pagautą paketą, „Snort“ padarys įrašą apie pažeidimą.

Galimi tokie protokolai: TCP, UDP, IP, ICMP

Nurodomas šaltinio ir tikslo IP adresas, prievado numeris ir srauto kryptis, skliaustuose įdedamas taisyklės kūnas. Pavyzdys gali būti toks:

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "external mountd access";)
```

Toliau yra išvardinti pagrindiniai taisyklės kūne naudojami parametrai: msg:"<pranešimas>"; sid:<sveikas skaičius>; content:[!] "<eilute>"; ttl:[<sveikas skaičius-><=]<sveikas skaičius>; ir daug kitų.

- msg – vartotojo pažeidimo apibūdinimas,
- sid – pažeidimo unikalus numeris,
- content – svarbiausias parametras, simbolių ar bitų eilutė, kuri yra ieškoma srauto paketuose,
- ttl – IP paketo antraštės lauko reikšmė.

Taip pat šis įrankis saugo užfiksuotą srautą ir turi jau integruotas tokias galimybes:

- paketų saugojimas failuose,
- paketų ir papildomos informacijos saugojimas duomenų bazėje,
- pranešimų išsiuntimas į el. pašto dėžutę apie užfiksuotą srautą,
- kitos galimybės.

TSP-ei reikalavimai yra tokie:

1. Nuolatinis tinklo stebėjimas.
2. Automatinis pažeidimų fiksavimas pagal metodikos saugos politikos reikalavimų rinkinį.
3. Informacijos apie pažeidimus saugojimas.

„TcpDump“ ir „Wireshark“ įrankiai gali tik surinkti ir atvaizduoti paketus, o automatizuotai reaguoti į stebimo srauto turinį jie negali.

Iš reikalavimų sąrašo ir įrankio „Snort“ funkcijų rinkinio galima padaryti išvadą, kad įrankis „Snort“ pildo TSP reikalavimus. Šis įrankis yra atviro kodo, nuolat palaikomas, turi daug sąsajų su kitomis technologijomis, tai priduoda įrankiui didelį lankstumą, universalumą ir suteikia platų pritaikymą ateityje. Pagrindinis jo privalumas yra tai, kad „Snort“ reaguoja į stebimą srautą pagal iš anksto aprašytas taisykles, išsaugo tik reikiamus paketus, gali nuolat veikti.

Įrankis „Snort“ turi vieną iš technologinių trūkumų. Dirbant NIDS režimu įrankis negali filtruoti paketus pagal OSI modelio kanalinio lygio informaciją. Norint apibrėžti darbo vietą, reikalinga žinoti IP Mac adresus ir komutatoriaus tinklinės sąsajos vardą. Šią problemą gali išspręsti jau įdiegtas į „Snort“ įrankį – preprocesorius „arpspoof preprocessor“. Jį panaudojant sraute yra lyginamos IP ir Mac adresų poros. Esant pažeidimui, ĮRP bus padarytas atitinkamas įrašas.

Įrašų registravimo priemonė (ĮRP)

Pagal nutylėjimą, įrankis „Snort“ turi galimybę saugoti informaciją apie užfiksuotus paketus pasirinktoje duomenų bazėje. Išsaugotų įrašų atvaizdavimui yra jau sukurtas įrankis ACID (Analysis Console for Intrusion Databases) [22]. ACID skirtingais būdais gali atvaizduoti įrankio „Snort“ pranešimus, saugomus duomenų bazėje MySql.

ACID yra sukurtas PHP kalba, todėl rezultatai yra išvedami panaudojant žiniatinklio serverį „Apache“, tai leidžia prisijungti nutolusiems vartotojams. Prisijungimas prie ACID sistemos gali būti apsaugotas slaptažodžiu arba užšifruotu kanalu panaudojant TLS protokolą.

Dažniausiai įrankio „Snort“ vartotojai naudoja ACID atvaizdavimo įrankį, tai yra patogu ir paprasta. Norint pasinaudoti šiuo privalumu, „Snort“ įrankis gali būti nustatytas taip, kad fiksuojami pranešimai būtų saugomi MySql duomenų bazėje. Tai gi ĮRP – tai MySql duomenų bazė.

Įvertinimo skaičiavimo priemonė (ĮSP)

Kadangi ACID įrankis yra naudojamas darbui su užfiksuotais pranešimais, būtų

patogu, jeigu čia pat būtų išvedami metodikos skaičiavimo rezultatai. Panaudojant tą pačią PHP kalbą, galima sukurti PHP skriptą, kuris kreipiasi į duomenų bazę, ir suskaičiuoja bendrą metodikos įvertinimą. Kreiptis į MySql duomenų bazę, PHP kalba turi visas galimybes. Taigi bendro įvertinimo skaičiavimui bus naudojama PHP kalba.

Rezultatų atvaizdavimo priemonė (RAP)

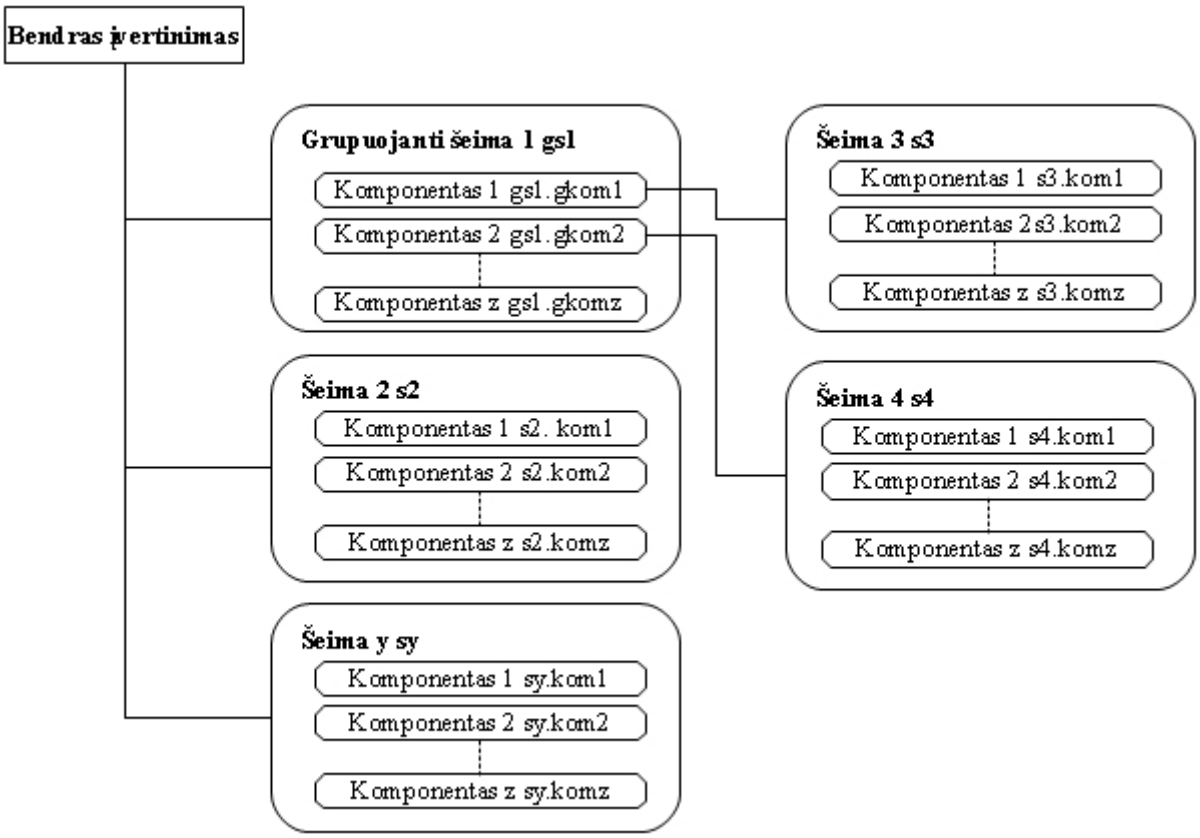
Suskaičiavus bendrą metodikos įvertinimą PHP kalba, yra patogu atvaizduoti rezultatus tinklapyje ar net ACID įrankyje. Šią funkciją galima atlikti PHP kalbos skriptu, integravus gautus rezultatus į HTML kodą. Taip rezultatai bus prieinami nuotoliniu būdu, kas yra labai patogu. RAP – tai PHP skriptas, atvaizduojantis rezultatus tinklapyje.

4. Įvertinimo metodikos ir automatizuoto įrankio projektas

Šioje dalyje pateikiama saugos politikos įgyvendinimo įvertinimo skaičiavimo metodika bei automatizuotų priemonių projektas, kuris atitinka suprojektuotą metodiką. Panaudojant šiuos komponentus bus galima pasiekti darbo tikslą.

4.1. Saugos politikos įgyvendinimo įvertinimo skaičiavimo metodika

Tinklo saugos politikos įgyvendinimo įvertinimo skaičiavimui reikalinga bendra metodika. Ši metodika turi atspindėti saugos politikos reikalavimų rinkinį. Kadangi ne visus organizacijos saugos politikos reikalavimus galima patikrinti automatizuotomis priemonėmis, reikalavimų rinkinys turi atitikti šių priemonių galimybes.



10 pav. Saugos politikos įgyvendinimo įvertinimo metodikos bendra schema

10 paveiksle yra pavaizduota saugos politikos įgyvendinimo įvertinimo skaičiavimo metodikos bendra schema. Ši metodika susidaro iš šeimų bei komponentų aibės. Jeigu komponentai atitiks saugos reikalavimo rinkinio komponentus, o šeimos specifines saugos politikas arba saugos politikų taisyklių grupę, galima bus sudaryti metodiką, kuri atitinka saugos reikalavimų rinkinį ir apskaičiuoja įvertinimą.

Šeima – tai metodikos dalis, kuri atitinka specifinę saugos politiką arba saugos

politikos taisyklių grupę. Į šią grupę įeina tos pačios tematikos saugos politikų taisyklės, dažniausiai tai atskira saugos politika, pavyzdžiui darbo stočių saugumo politika ar slaptažodžių politika. Šeima skirta palengvinti komponentų valdymą, juos sugrupuoti.

Komponentas – tai metodikos dalis, kuri atitinka saugos politikos reikalavimą. Šis komponentas gali nurodyti ar reikalavimas yra pažeidžiamas įgyjant reikšme „R“ 1 arba ne įgyjant reikšmę 0. Kadangi komponentų grupė priklauso vienai šeimai, o šeimos sudaro bendrą įvertinimą, komponentų koeficientai „K“ turi būti paskirstyti taip, kad bendras įvertinimas nebūtų didesnis už vienetą. Koeficiento skaičiavimas bus aptartas vėliau. Komponentas žymimas nurodant šeimą ir komponentą, pavyzdžiui $s_2.kom_1$. Be to būtina nurodyti komponento koeficientą $K.s_2.kom_1$.

Taip pat komponentas gali atstovauti kitą šeimą. 10 schemoje tai komponentai $gs_1.gkom_1$ ir $gs_1.gkom_2$ su papildomu „g“ žymėjimu. Šie komponentai neturi reikšmių ir koeficientų ir į bendro įvertinimo skaičiavimą neįtraukiami. Tai skirta tam, kad galima būtų sudaryti šeimų hierarchiją, suteikti metodikai lankstumą ir pritaikyti esamai organizacijos saugos politikai.

4.1.1. Saugos politikos taisyklių pritaikymas metodikos komponentams

Kaip buvo apžvelgta 3.1.4 dalyje „Saugos politika“, saugos politikos dokumentų visuma skirstoma į tris organizacijos lygius. Kiekvienas saugos politikos dokumentas turi savo taisyklių aibę. Siekiant pritaikyti saugos politikos taisykles kuriamai metodikai, kiekviena taisyklė turi būti susieta su vienu metodikos komponentu. Sudarytos taisyklės vadinsis – saugos politikos reikalavimų rinkiniu.

Šios taisyklės turi būti draudžiamojo pobūdžio, nes tinklo stebėjimo priemonės turi specifinį apribojimą. Jos analizuoja praeinantį tinklo srautą ir gali fiksuoti tik tam tikrus įvykius – pažeidimus. Esant galimybei, saugos politikos taisyklę reikia perdaryti, kitaip sudarant įrankio saugos politikos reikalavimų rinkinį sukurti teisingą reikalavimą, kuris atitiks nepakeičiamą taisyklę. Turi būti pažymėta, kad sukurtas reikalavimas atitinka tam tikrą saugos politikos taisyklę.

Patogumui metodikos komponentus galima jungti į šeimą, tai atitiktų taisyklių jungimą į saugos politikos dokumentą. Kai kurių šeimų komponentai atstovauja kitoms šeimoms, šis ryšys gali atitikti vienos saugos politikos priklausomybę kitai. Šias savybes galima pamatyti 10 paveiksle.

Tokiu būdu kuriamą metodiką galima pritaikyti organizacijos saugos politikos dokumentų visumai. Taip pat galima lanksčiai grupuoti metodikos komponentus, tai labai palengvina specialisto darbą, esant sudėtingai saugos politikai.

4.1.2. Koeficiento reikšmės nustatymas

Jeigu metodika neturėtų koeficientų, bendras įvertinimas atvaizduotų nepažeistų taisyklių kiekį. Suprantama, tokia reikšmė nebus vertinga. Kiekviena saugos politikos taisyklė yra sukurta siekiant užkirsti kelią grėsmės įgyvendinimui. Atsižvelgiant į punktą (3.1.3 Duomenų saugos rizika), grėsmė, žala, ir kiti elementai yra įvertinami kiekybiškai arba kokybiškai. Taigi šie įvertinimų rezultatai gaunami rizikos analizės etape, o rezultatų forma priklauso nuo pasirinktos įvertinimo skalės, rizikos analizės metodo.

Kadangi metodikos komponentas yra susijęs su saugos politikos taisykle, grėsme, žala arba su rizikos analizės rezultatais, metodikos komponentui galima priskirti koeficientą, kuris nurodytų komponento svorį. Tokiu būdu metodikos bendras skaitinis įvertinimas tiksliau atspindės užfiksuotų pažeidimų svarbą.

Siekiant, kad rizikos analizės rezultatai atspindėtų metodikos bendrą įvertinimą, reikia grėsmes susieti su saugos politikos taisyklėmis, kas pavaizduota 4 paveiksle. Tai leidžia vienai saugos politikos taisyklei spręsti keletą grėsmių, kas verčia turėti keletą rizikos reikšmių, nes kiekviena grėsmė turi savo rizikos reikšmę.

Šio darbo kuriama metodika nepriklauso nuo rizikos analizės vykdymo metodikos. Nesvarbu kokia skalė ar būdas būtų pasirinktas rizikos įvertinimo metu, rizikos reikšmė yra daugiau ar mažiau tikslesnė. Kuo sudėtingesnė rizikos analizės metodika ir skalė, tuo tikslesnė rizikos reikšmė.

Turi būti pasirinkta viena rizikos analizės metrika, kuri pritaikoma visai metodikai. Kiekviena saugos politikos taisyklė arba metodikos komponentas turės vieną rizikos reikšmę. Visos šios reikšmės turi sudaryti bendrą įvertinimą. Kadangi bendras metodikos įvertinimas neviršija vieneto, reikia kiekvienam komponento koeficientui paskaičiuoti proporciją.

Taigi koeficientas turi būti apskaičiuojamas taip (formulė 3):

$$K_i = \frac{riz_i \cdot Bmax}{\sum_{i=1}^{t} riz_i}; i = (\overline{1,t}); \qquad (3)$$

K_i – komponento koeficientas,

riz_i – rizikos reikšmė, susieta su komponentu ir K_i ,

$Bmax$ – metodikos bendro įvertinimo maksimali reikšmė, šioje metodikoje tai

vienetas,

$\sum_{i=1}^{t} riz_i$ – visų komponentų rizikos reikšmių suma.

Gali atsitikti taip, kad komponentas ir jo saugos politikos taisyklė sprendžia keletą grėsmių, tuo pačiu turi keletą rizikos reikšmių. Tokiu atveju, riz_i tai šių rizikos reikšmių suma.

Jeigu pažeidimų nėra užfiksuota, bendras metodikos įvertinimas bus lygus savo maksimaliai reikšmei – vienetui, nes visi komponentai turi reikšmes lygias nuliui ir iš bendro įvertinimo nėra ką atimti. Atsiradus pažeidimui, jo komponentas įgyja vieneto reikšmę, ir bendro įvertinimo reikšmė sumažėja tiek, kiek yra lygus pažeidimo komponento koeficientas.

4.1.3. Bendro įvertinimo skaičiavimas

Kuriama metodika suteikia galimybę išreikšti esamą saugos situaciją skaitine reikšme. Šis bendras įvertinimas atspindi pažeidimų kiekį ir jų pavojingumą.

Tam, kad bendras įvertinimas būtų tikslus, grupuojančių šeimų ir komponentų su žymėjimu „g“ rezultatai skaičiuojami nebus. Į bendro įvertinimo skaičiavimą įeis visi galiniai metodikos komponentai, kurie neturi atstovaujamų šeimų. Bendro organizacijos tinklo saugos politikos įgyvendinimo įvertinimo skaitines reikšmės skaičiavimas pavaizduotas 4 formulėje.

$$R = Bmax - \sum_{i=1}^{y} \sum_{j=1}^{s_i.z} (R.s_i.kom_j \cdot K.s_i.kom_j); \qquad (4)$$

R – metodikos bendras įvertinimas,

$Bmax$ – metodikos bendro įvertinimo maksimali reikšmė, šioje metodikoje tai vienetas,

$R.s_i.kom_j$ – komponento kom_j skaitinė reikšmė, kuris priklauso šeimai s_i ,

$K.s_i.kom_j$ – komponento kom_j kuris priklauso šeimai s_i koeficientas,

y – visų galinių šeimų kiekis, be „g“ žymėjimo,

$s_i.z$ – visų komponentų kiekis priklausančių šeimai s_i ,

i ir j – šeimos ir komponento indeksai.

Suma susumuoja visų užfiksuotų pažeidimų reikšmes ir atima iš vieneto. Tokiu būdu yra gaunamas organizacijos tinklo saugos politikos įgyvendinimo bendras įvertinimas.

4.2. Automatizuoto įrankio projektas

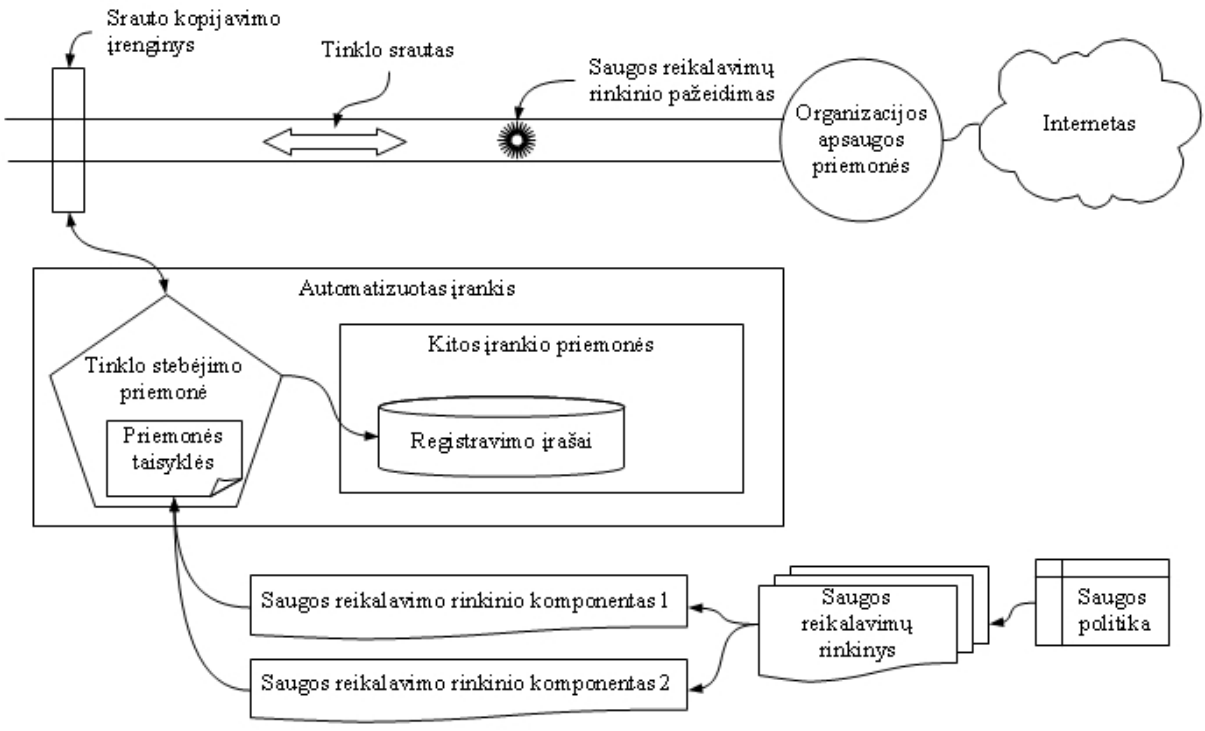
Norint apibrėžti automatizuotą įrankį, reikia nurodyti jo funkcijas, architektūrą, duomenų tarp automatizuoto įrankio priemonių srautus.

4.2.1. Automatizuoto įrankio funkcijos

Automatizuotas įrankis turi atlikti tokias funkcijas:

1. nuolatinis pažeidimų stebėjimas
2. įvertinimo paskaičiavimas pagal sukurtą metodiką ir rezultato atvaizdavimas
3. pažeistų saugos politikos reikalavimų sąrašo atvaizdavimas

Automatizuotas įrankis turi fiksuoti saugos politikos pažeidimus. Šis fiksavimas pavaizduotas 11 paveiksle.



11 pav. Saugos politikos pažeidimų fiksavimas

Pirmam tikslui pasiekti reikalinga tinklo stebėjimo priemonė (TSP), įrašų registravimo priemonė (ĮRP) ir saugos reikalavimų rinkinys. Į šio rinkinio sudėtį yra įtraukiamos tokios saugos politikos taisyklės, kurias galima stebėti tinklo sraute naudojant automatizuotą įrankį. Reikia pasirinkti automatizuota priemonę, kuri gali nuolat stebėti tinklo srautą. Ši priemonė turi turėti galimybę įvesti taisykles, pagal kurias bus atpažinti tinklo srauto fragmentai, ir galimybę padaryti registravimo įrašus. Saugos politikos viena taisyklė atitinka saugos reikalavimų rinkinio komponentą (11 pav.). Šį komponentą aprašo automatizuoto įrankio

pasirinktos priemonės taisyklių grupė.

Automatizuoto įrankio antra funkcija yra įvertinimo paskaičiavimas pagal sukurtą metodiką ir rezultato atvaizdavimas. Pagal metodikoje surinktas formules, kita įrankio priemonė, vadinama įvertinimo skaičiavimo priemonė (ĮSP), turi paskaičiuoti saugos lygio įvertinimą. Norint gauti tokius rezultatus, ši priemonė turi integruoti sukurtą įvertinimo skaičiavimo metodiką. Metodikos komponentų reikšmės bus nuskaitomos iš įrašų registravimo priemonės. Vartotojui prireikus turi būti atliekamas bendras saugos politikos įvertinimas, rezultato išvedimas.

Automatizuoto įrankio trečia funkcija yra pažeistų saugos politikos reikalavimų sąrašo atvaizdavimas. Ši funkcija atliekama vartotojui inicijuojant skaičiavimą ir pasirinkus įvertinimo laikotarpį. Atvaizduotame sąraše turi būti tokia informacija:

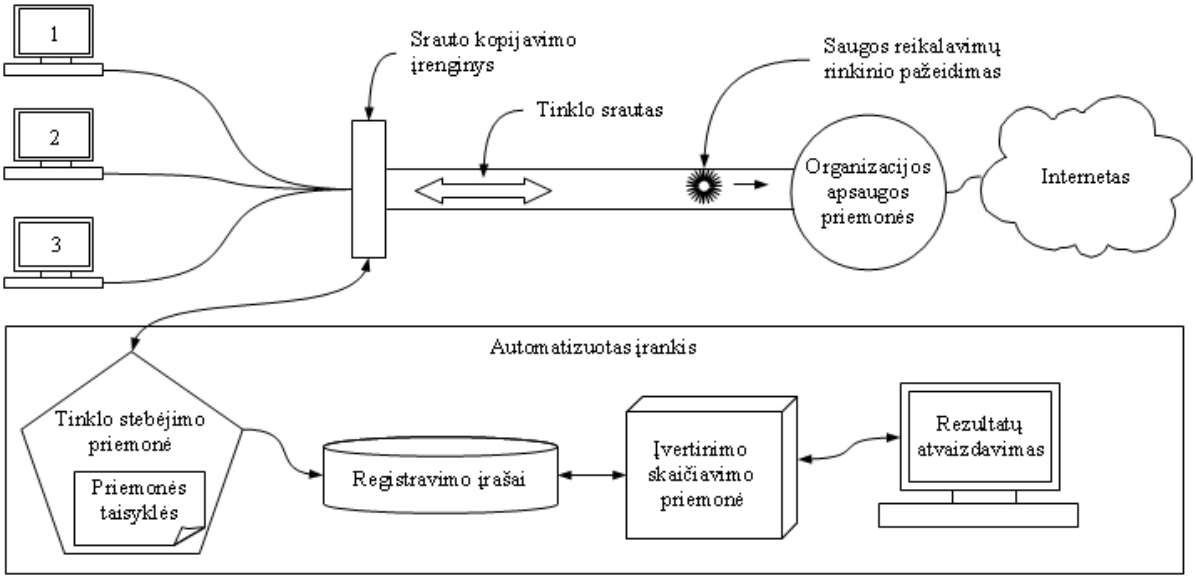
- pažeidimo unikalus numeris tinklo stebėjimo priemonės (TSP) sistemoje,
- pirmas komponento pažeidimo laikas,
- kiek kartų per pasirinktą laikotarpį buvo užfiksuotas pažeidimas,
- saugos reikalavimo rinkinio komponento pavadinimas.

4.2.2. Automatizuoto įrankio architektūra

Automatizuotas įrankis susidaro iš tokių priemonių:

1. Srauto kopijavimo įrenginys;
2. Tinklo stebėjimo priemonė (TSP);
3. IDS sintakse sukurtas taisyklių rinkinys, atitinkantis saugos politikos reikalavimų rinkinį;
4. Įrašų registravimo priemonė (ĮRP), sauganti įrašus apie pažeidimus;
5. Įvertinimo skaičiavimo priemonė (ĮSP);
6. Rezultatų atvaizdavimo priemonė (RAP);

Automatizuotų priemonių schema pavaizduota 12 paveiksle.



12 pav. Automatizuoto įrankio priemonės

Srauto kopijavimo įrenginys gali būti kartotuvas „Hub“, sujungiantis visus tinklo kompiuterius ir automatizuotą įrankį. Taip pat gali būti panaudotas maršrutizatorius su srauto kopijavimo galimybe. Jeigu tinklas yra didelis, turi atskirus potinklius, galima naudoti keletą srauto kopijavimo įrenginių reikiamose vietose. Šie įrenginiai turi būti prijungti prie TSP.

TSP – įsilaužimo aptikimo sistema. Ji yra naudojama tik kaip priemonė tinklo srautui stebėti, reaguoti į saugos politikos reikalavimų pažeidimus, saugoti užfiksuotų pažeidimų informaciją įrašų registravimo priemonėje (ĮRP). Ji neaptinka įsilaužimų ir anomalijų tinkle. Toks sprendimas yra priimtas tik todėl, kad ši priemonė:

- turi galimybę sukurti taisykles, kurios atitinka saugos politikos reikalavimų rinkinį,
- leidžia stebėti tinklą realiame laike ir nuolat,
- jau turi automatinio pranešimų išsaugojimo funkciją,
- jau turi duomenų srauto fragmentų išsaugojimo funkciją,
- turi kitas, jau veikiančias funkcijas.

TSP-ei tinkamos yra tik tokios saugos politikos taisyklės, kurių įgyvendinimą galima stebėti tik tinklo sraute. TSP negali stebėti vykstančių veiksmų vartotojų kompiuteriuose ar kituose įrenginiuose. Taip pat, pagal OSI lygmenis, tinklo srauto paketus, TSP naudojant, TSP taisyklės gali analizuoti nuo tinklinio lygio iki taikomojo. Kanalinio lygio duomenys yra prieinami kitais TSP-ės ne automatiniais būdais.

ĮRP duomenų bazė priima įsilaužimo aptikimo sistemos pranešimus. IDS priemonė jau turi tokią funkciją. Be to, nėra sudėtinga ĮSP-ei atlikti reikiamos informacijos paieškos operacijas. Tai gi kaip universali priemonė „MySql“ duomenų bazė puikiai tinka

automatizuotam įrankiui.

Darbui su duomenų baze prireiks MySql bei Php skriptų. Duomenų apdorojimą, bendro tinklo saugos įvertinimo apskaičiavimą puikiai atliks Php kalba parašytas skriptas bei jo vykdymo priemonė. Tai ir bus ĮSP.

Įvertinimo bei pažeistų saugos politikos reikalavimų sąrašo atvaizdavimui tiks Html kalba. Php skriptas puikiai gali kintamuosius ir atvaizdavimo duomenis transformuoti į Html kodą. Tam tikslui pasiekti reikės Apache serverio su Php palaikymu. Tai yra rezultatų atvaizdavimo priemonė (RAP).

Tokių priemonių panaudojimas bei suderinimas tarpusavyje suteiks galimybę įvertinti saugos reikalavimų rinkinio įgyvendinimą automatizuotai.

4.2.3. Duomenų srautai

Šis skyrius skirtas apibrėžti duomenų srautų judėjimą kiekvienai įrankio priemonei.

4.2.3.1. Srauto kopijavimo įrenginys (SKĮ)

SKĮ skirtas analizuojamame tinklo taške atvaizduoti srautą tinklo stebėjimo priemonei. Srauto kopijavimo įrenginys gali būti trijų tipų:

1. Tinklo kartotuvas „Hub“. Šis įrenginys sujungia kompiuterius, vienas iš lizdų yra sujungiamas su tinklo stebėjimo priemone.
2. Tinklo maršrutizatorius, turintis srauto kopijavimo galimybę.
3. Specialus, šiam tikslui skirtas įrenginys. Šie įrenginiai įeina į komercinę IDS komplektaciją.

Šie įrenginiai gali būti diegiami kompiuterių sujungimo mazge, tarp potinklių, tarp potinklio ir užkardos. Duomenų srautai pavaizduoti 4 lentelėje.

4 lentelė. SKĮ duomenų srautai

	Įeinantys duomenys	Vidiniai veiksmai	Išeinantys duomenys
1.	bendras matomas tinklo srautas	visų įrenginio lizdų srautų kopijavimas į vieną, kuris yra sujungtas su TSP	bendras matomas tinklo srautas

4.2.3.2. Tinklo stebėjimo priemonė (TSP)

TSP skirta saugos politikos pažeidimams fiksuoti. Duomenų srautai pavaizduoti 5 lentelėje.

5 lentelė. TSP duomenų srautai

	Įeinantys duomenys	Vidiniai veiksmai	Išeinantys duomenys
1.	bendras matomas tinklo srautas, kurį suteikia SKĮ	srauto stebėjimas realiame laike	įrašas apie saugos politikos pažeidimą
2.		taisyklių atitikimo srauto fragmentui vykdymas	pažeidimo srauto fragmento išsaugojimas

4.2.3.3. Įrašų registravimo priemonė (ĮRP)

Įrašų registravimo priemonė skirta pažeidimų duomenims saugoti. Duomenų srautai pavaizduoti 6 lentelėje.

6 lentelė. ĮRP duomenų srautai

	Įeinantys duomenys	Vidiniai veiksmai	Išeinantys duomenys
1.	saugojami įrašai apie pažeidimus iš TSP	pažeidimo įrašo paieška	pažeidimo įrašo duomenų suteikimas
2.	užklausos apie pažeidimus iš ĮSP		pažeidimo papildomų duomenų suteikimas

4.2.3.4. Įvertinimo skaičiavimo priemonė (ĮSP)

ĮSP skirta saugos politikos įvertinimo skaičiavimui. Duomenų srautai pavaizduoti 7 lentelėje.

7 lentelė. ĮSP duomenų srautai

	Įeinantys duomenys	Vidiniai veiksmai	Išeinantys duomenys
1.	užklausa apie rezultatų atvaizdavimą su nurodytu laikotarpiu	saugos politikos pažeidimų paieška	reikiamo saugos reikalavimo rinkinio komponento paieškos užklausa
2.	pažeidimo įrašo duomenų gavimas iš registravimo įrašų priemones	bendro saugos įvertinimo skaičiavimas	rezultatų perdavimas į RAP

4.2.3.5. Rezultatų atvaizdavimo priemonė (RAP)

Rezultatų atvaizdavimo priemonė skirta rezultatams suformuoti ir atvaizduoti. Duomenų srautai pavaizduoti 8 lentelėje.

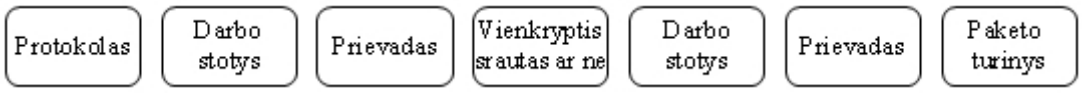
8 lentelė. RAP duomenų srautai

	Įeinantys duomenys	Vidiniai veiksmai	Išeinantys duomenys
1.	įvertinimo laikotarpio įvedimas	rezultatų suformavimas, atvaizdavimas	rezultatų į ekraną išvedimas
2.	vartotojo užklausa į duomenų atvaizdavimą		

4.2.4. Priemonių projektas

4.2.4.1. TSP projektas

11 paveiksle pavaizduota saugos politika, saugos reikalavimų rinkinys, komponentai ir priemonės taisyklės. Kuriant TSP taisykles reikia pritaikyti saugos politikos taisykles priemonės sintaksei. Tuo tikslu reikia apibrėžti metodikos saugos politikos reikalavimo (MSPR) būtinus laukus, kuriuos atitiks TSP sintaksę. MSPR turi apibrėžti tokią informaciją (13 pav.):



13 pav. MSPR sudedamosios dalys

Tai laukai, be kurių negalima bus sukurti TSP taisyklių. Paketo turinys gali būti tuščias, nes užtenka nurodyti kitus laukus. Vienam MSPR gali būti sukurtos daug TSP taisyklių. Kitaip tariant, MSPR tiksliau aprašo saugos politikos taisykle, tai įgalina stebėti pažeidimus tinklo sraute. MSPR rinkinio pavyzdys yra pateiktas 5.1.1 dalyje.

4.2.4.2. ĮRP projektas

Įrankis „Snort“ yra sukurtas taip, kad automatiškai saugo informaciją apie pažeidimus. Taigi viskas bus naudojama pagal nutylėjimą. Taisyklės parametru „msg“ į duomenų bazę turi būti įrašomas pažeidimą apibūdinantis pranešimas. Be to, MSPR gali turėti daug susietų taisyklių, todėl prie kiekvienos taisyklės turi būti nurodomas parametras „sid“, kuris lygus MSPR numeriui. Taip pat reikia sukurti papildomą lentelę, kur bus saugomos metodikos komponentų rizikos reikšmės. Tai bus lentelė su pavadinimu „riz_reik“, su laukais:

id – automatinis eilės numeris

sid – TSP taisyklės, pažeidimo numeris

reikalavimo_nr – MSPR numeris

riz – rizikos reikšmė

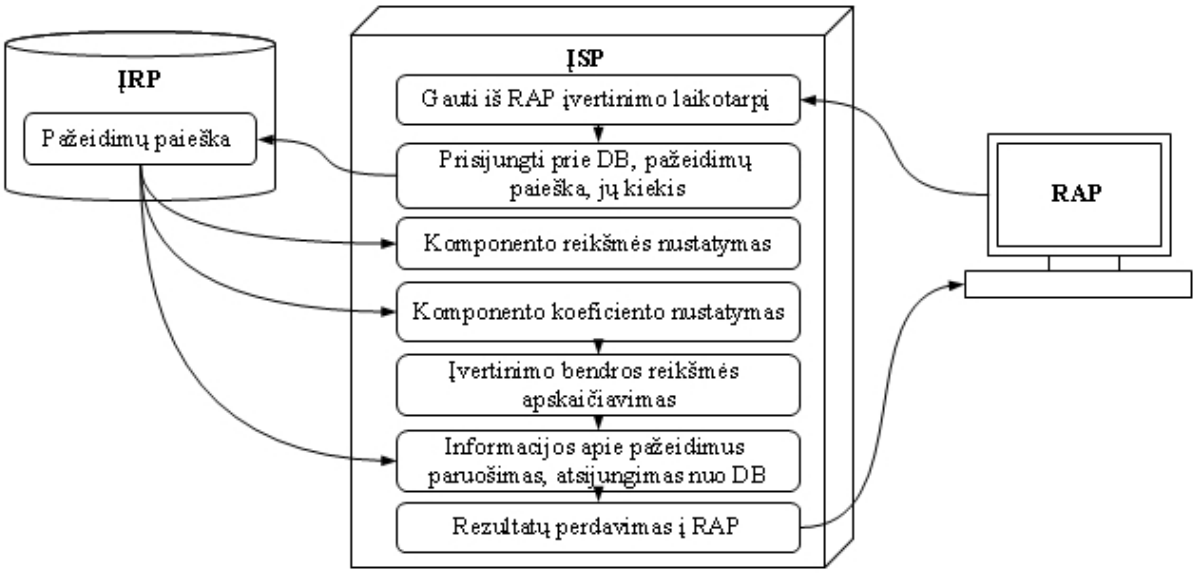
Sukaupus informaciją apie pažeidimus ir įrašius pažeidimų rizikos reikšmes galima skaičiuoti bendrą įvertinimą.

4.2.4.3. ĮSP projektas

Įvertinimo skaičiavimo priemonė turi atlikti tokias funkcijas:

- priimti iš RAP pradžios ir pabaigos datą, laiką;
- prisijungti prie MySql duomenų bazės;
- rasti pažeidimų tipus pagal nurodytą taisyklėse parametrą „sid“ atitinkamu laikotarpiu ir nustatyti, kiek yra pažeidimų tipų ir koks yra jų kiekis;
- suskaičiuoti bendrą įvertinimą;
- paruošti duomenis RAP-ei.

ĮSP ir RAP veiksmų seka pavaizduota 14 paveiksle.



14 pav. Įvertinimo skaičiavimo priemonės veiksmų seka

1. Vartotojas inicijuoja skaičiavimą, nurodo įvertinimo laikotarpį.
2. ĮSP skenuoja duomenų bazę:
   2.1 prisijungia prie duomenų bazės,
   2.2 pagal įvertinimo metodikos sukurtą skriptą ieško įrašų apie kiekvieną komponentą.
3. DB gražina rezultatus apie pažeidimus.
4. Komponentų reikšmių nustatymas:
   4.1 jeigu pažeidimas yra, komponentas įgyja reikšmę 1,

4.2 jeigu tokio komponento įrašas nerandamas, reikšmė lygi nuliui.

5. Komponentų koeficientų nustatymas: iš duomenų bazės gautos rizikos reikšmės, jos yra perskaičiuojamos į koeficientus pagal 3 formulę.
6. Surinkus rezultatus skriptas pagal įvertinimo metodikos 4 formulę apskaičiuoja bendro įvertinimo reikšmę;
7. Informacijos apie pažeidimus paruošimas, atsijungimas nuo DB.
8. Rezultatai yra perduodami RAP-ei norint atvaizduoti rezultatus vartotojui.

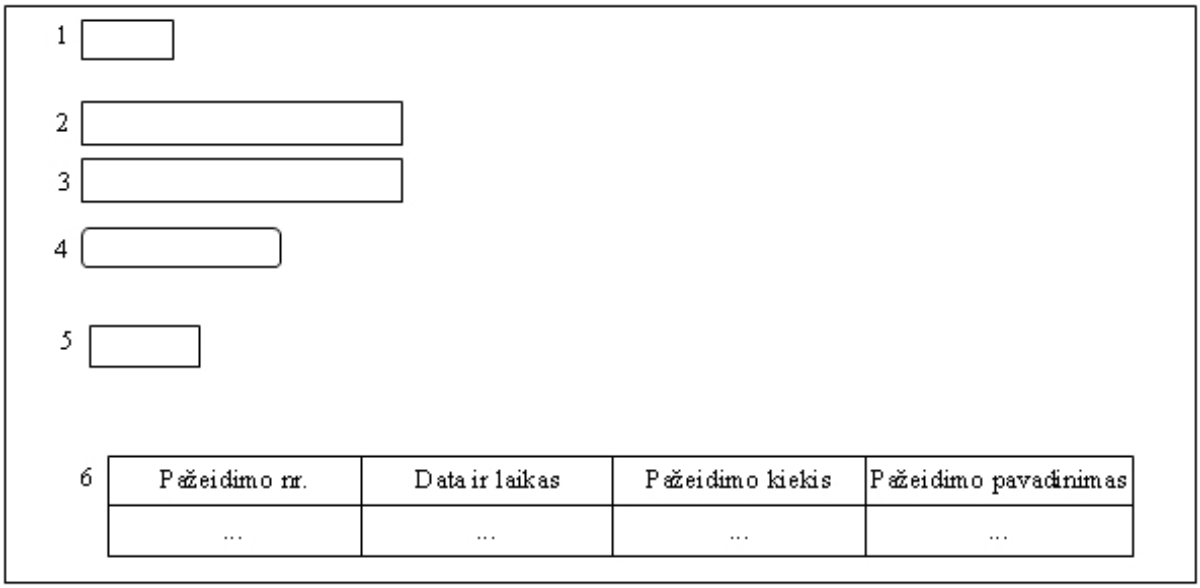
Taip turi būti atliekamas ĮSP darbas.

4.2.4.4. RAP projektas

RAP turi suteikti galimybę vartotojui:

- pasirinkti įvertinimo laikotarpį;
- inicijuoti bendro įvertinimo skaičiavimą;
- pamatyti bendro įvertinimo reikšmę;
- pamatyti informaciją apie pažeidimus, čia įeina tokie laukai:
  - pažeidimo numeris,
  - pirmo pažeidimo pasirodymo data ir laikas,
  - pažeidimo užfiksavimo kiekis,
  - pažeidimo apibūdinimas.

Kaip išvedama informacija vartotojui pavaizduota 15 paveiksle.



15 pav. Schematinis rezultatų lango vaizdas

Jeigu vartotojui yra patogu dirbti su ACID įrankiu, stebėti daromus pažeidimus, kurti

naujus, gauti platesnę informaciją, galima į ACID valdymo langą įdėti nuorodą į RAP. Suskaičiavus bendrą įvertinimą, galima pagal pažeidimo numerį gauti platesnę informaciją, sugrįžtant į ACID įrankį. Sugrįžimui yra skirtas mygtukas ar nuoroda 1.

Antras ir trečias schemos elementas skirtas įvertinimo laikotarpio pradžios ir pabaigos datos ir laiko nurodymui. Pagal šį nurodytą laikotarpį, ĮSP iš ĮRP išrinks atitinkamus pažeidimus. Kiti pažeidimai nebus įtraukti į bendro įvertinimo skaičiavimą.

Ketvirtas elementas tai bendro įvertinimo inicijavimo skaičiavimo mygtukas. Nurodžius laikotarpį ir nuspaudus šį mygtuką, ĮSP pradeda savo darbą.

Penktas laukas skirtas bendro įvertinimo skaitinės reikšmės atvaizdavimui.

Šeštas elementas skirtas informuoti vartotoją apie užfiksuotus pažeidimus ir suteikti pradinę informaciją.

5. Metodikos pritaikymas ir įrankio prototipas

5.1. Metodikos pritaikymas

Pasiūlytą metodiką reikia ne tik teoriškai aprašyti, bet ir pritaikyti priemonėms, kurios automatizuotai vertins organizacijos tinklo saugos politikos įgyvendinimo įvertinimą.

5.1.1. Metodikos saugos politikos reikalavimų rinkinys

Parinkime iš organizacijos saugos politikos keletą tinkamų organizacijos tinklui ir įrankiui taisyklių [14].

1. Tinklas susidaro tik iš griežtai apibrėžtų įrenginių skaičiaus.
2. Galiniai tinklo mazgai negali suteikti prieigos prie tinklo kitiems įrenginiams.
3. Vartotojas el. laiškus gali siųsti tik iš darbo vietos.
4. Draudžiama naudoti, pateikti ir registruoti savo el. pašto adresą internetinėse sistemose.
5. Vartotojas prie FTP paslaugos gali prisijungti prie savo paskyros tik iš savo darbo vietos.
6. Draudžiama naudoti įmonės tinką tokiai informacijai persiųsti: pornografija, grasinimai, elektroninės vagystės, autorinių teisių pažeidimai ir kita.
7. Kiekvienas vartotojas turi siunčiamų bylų tipų apribojimą.

Sudarykime atitinkamą saugos politikai MSPR rinkinį atsižvelgdami į 4.2.4.1 dalies nurodymus.

1. Tinkle yra tokie draudžiami įrenginiai: IP – 192.168.1.60 Mac – 00-50-56-C0-00-01; (draudžiamų įrenginių sąrašas); prievadas yra bet koks; kryptis bet kokia; paketų turinys bet koks.
2. Turi būti aprašytas kiekvienas tinklo įrenginys, kurių siunčiamame sraute kiekvienoje paketo antraštėje yra tam tikra TTL reikšmė, būdinga tinklo įrenginiui: protokolas IP; įrenginiai IP – 192.168.1.60 TTL=128; kiti įrenginiai su TTL reikšmėmis.
3. Kiekvienos tinklo darbo stoties iš organizacijos siunčiamas srautas yra tikrinamas; tikslo šaltinis yra bet koks; tikslo paketo prievado numeris yra 25; paketo turinys yra toks: „MAIL FROM:“ ir ne „<vartotojas%40įmonė.lt>“. Pažeidimo pranešime turi būti nurodytas darbo stoties adresas.
4. Iš kiekvienos organizacijos darbo stoties turi būti tikrinamas išsiunčiamas srautas į 80

prievadą; paketo turinyje užfiksuotas nors vienas organizacijos darbuotojo el. pašto adresas laikomas pažeidimu. Protokolas TCP; įrenginys IP – 192.168.1.60; išsiunčiamas srautas; tikslo įrenginys bet koks; prievado numeris 80; paketo turinys: „vartotojas%40organizacija.lt". Taip aprašoma kiekviena darbo stotis. Pažeidimo pranešime turi būti nurodytas darbo stoties adresas.

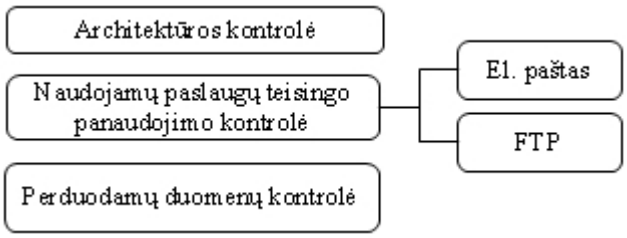
5. Iš kiekvienos organizacijos darbo stoties turi būti tikrinamas išsiunčiamas srautas iš organizacijos į 21 prievadą; tokiame sraute priklausomai nuo darbo stoties, užfiksavus paketo turinyje eilute „USER|20|" ir sekančius simbolius nelygius vartotojo vardui, bus fiksuojamas pažeidimas. Protokolas TCP; įrenginys IP – 192.168.1.60; išsiunčiamas srautas; tikslo įrenginys bet koks; tikslo prievado numeris 21; paketo turinys: „USER|20|" ir ne „gurejevas". Taip aprašoma kiekviena darbo stotis. Pažeidimo pranešime turi būti nurodytas darbo stoties adresas.
6. Stebimas kiekvieno organizacijos įrenginiu įeinantis ir išeinantis srautas. Sraute vyksta draudžiamų žodžių ir jų junginių paieška. Radus draudžiamą turinį, yra fiksuojamas pažeidimas. Protokolas: TCP, įrenginys 192.168.1.60; prievadas bet koks, srauto kryptis bet kokia, paketo turinys: sex, porn, reklama ir t. t. Pažeidimo pranešime turi būti nurodytas darbo stoties adresas.
7. Stebimas kiekvieno organizacijos įrenginio įeinantis ir išeinantis srautas. Sraute vyksta draudžiamų bylų plėtinių paieška. Radus draudžiamą turinį, yra fiksuojamas pažeidimas. Protokolas: TCP, įrenginys 192.168.1.60; prievadas bet koks, srauto kryptis bet kokia, paketo turinys: .exe .mpeg ir t. t. Pažeidimo pranešime turi būti nurodytas darbo stoties adresas.

Šis rinkinys atitinka automatizuoto įrankio apribojimus:

- reikalavimai yra draudžiamojo pobūdžio;
- šiu taisyklių nepageidaujamus įvykius galima stebėti ir fiksuoti tinklo sraute.

5.1.2. Metodikos šeimų nustatymas

Iš metodikos saugos politikos reikalavimų rinkinio galime sudaryti metodikos šeimas, kurias vertins automatizuotas įrankis. Į šeimą galima apjungti tos pačios tematikos reikalavimus. Jeigu reikalavimai yra iš atskiro dokumento, tada šeima – to dokumento pavadinimas.



16 pav. Saugos politikos šeimų bendra schema

Iš pateiktų saugos politikos reikalavimų sudarytos šeimos yra pavaizduotos 16-ame paveiksle.

Architektūros kontrolė

Į šią šeimą įeina pirmi du reikalavimai: tinklas susidaro tik iš griežtai apibrėžtų įrenginių skaičiaus ir tinklo leisti įrenginiai negali suteikti prieigą prie tinklo kitiems įrenginiams. Šie reikalavimai yra susieti su įrenginių kiekio ribojimu įmonės tinkle, todėl jie yra jungiami.

Naudojamų paslaugų tinkamo panaudojimo kontrolė.

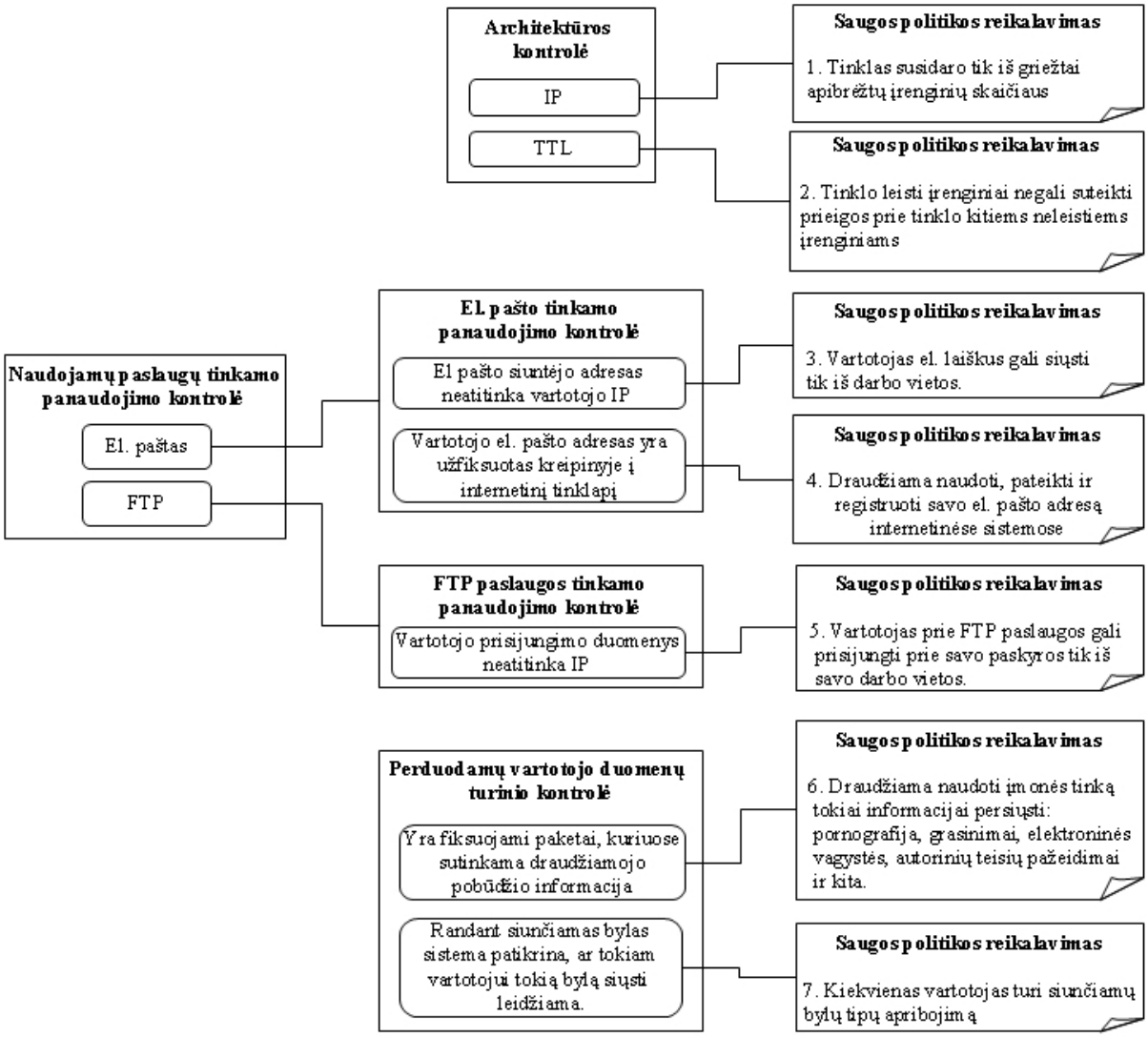
Ši šeima susidaro iš 3 – 5 reikalavimų. Kadangi trečias ir ketvirtas reikalavimas priklauso el. pašto sričiai, o penktas FTP sričiai, yra sudaromos papildomos šių sričių šeimos. Jas jungia viena naudojamų paslaugų teisingo panaudojimo kontrolės šeima, kuri yra kaip grupuojanti. Jos grupuojantys komponentai atstovauja el. pašto ir FTP šeimoms.

Perduodamų duomenų kontrolė

Šeštas ir septintas reikalavimai yra jungiami į perduodamų duomenų kontrolės šeimą.

5.1.3. Saugos politikos komponentų nustatymas

Kai yra sukurtos metodikos šeimos, turi būti apibrėžti jų komponentai. Trumpas komponentų apibūdinimas su saugos politikos reikalavimų rinkinio susiejimu yra pavaizduotas 17 paveiksle.

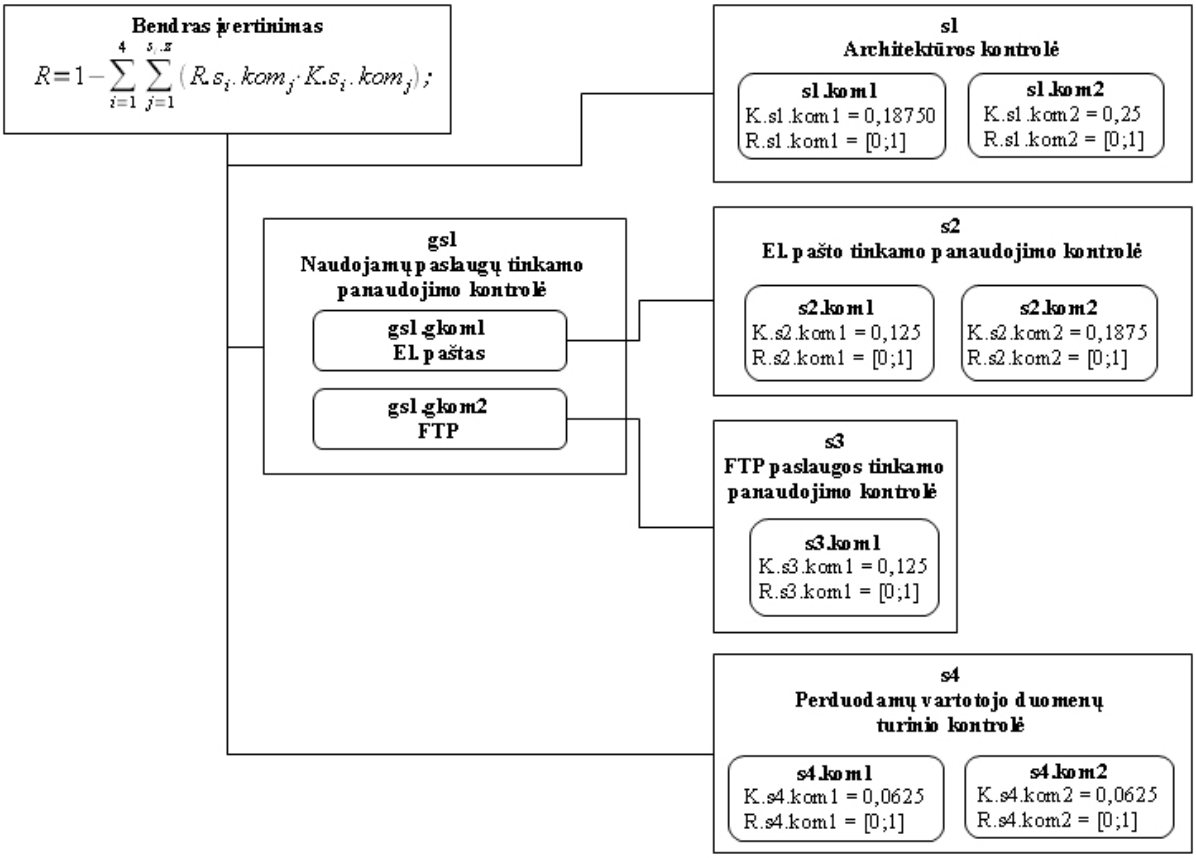


17 pav. Metodikos šeimos ir jų komponentai

Metodikos komponentai atitinka metodikos saugos politikos reikalavimų rinkinį ir priklauso nustatytoms šeimoms (5.1.2 dalis).

5.1.4. Saugos politikos įgyvendinimo įvertinimo skaičiavimo metodikos pritaikymo pavyzdys

18 paveiksle yra pavaizduota saugos politikos įgyvendinimo įvertinimo metodikos pritaikymo pavyzdžio schema. Saugos politikos sritys virto šeimomis, o konkretūs reikalavimai – komponentais. Šio darbo 4.1 dalyje yra pateikti 18 paveikslo kintamųjų paaiškinimai.



18 pav. Metodikos pritaikymo schema

Kai bus užfiksuotas pažeidimas, komponento $R.s_i.kom_j$ reikšmė taps lygi vienetui (4 formulė) ir komponento koeficientas įtakos bendrą įvertinimą. Tarkime, rizikos analizė buvo įvykdyta ir kiekvienai saugos politikos taisyklei yra priskirta tam tikra rizikos reikšmė. Šios reikšmės pavaizduotos 9 lentelėje.

9 lentelė. Saugos politikos reikalavimų rinkinio rizikos reikšmės

	Saugos politikos reikalavimai:						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Rizikos reikšmės:	3	4	2	3	2	1	1

Kai rizikos reikšmės yra nustatytos, galima pagal 3 formulę suskaičiuoti metodikos komponentų koeficientus. Koeficientų reikšmės yra nurodytos 10 lentelėje.

10 lentelė. Saugos politikos reikalavimų rinkinio rizikos reikšmės

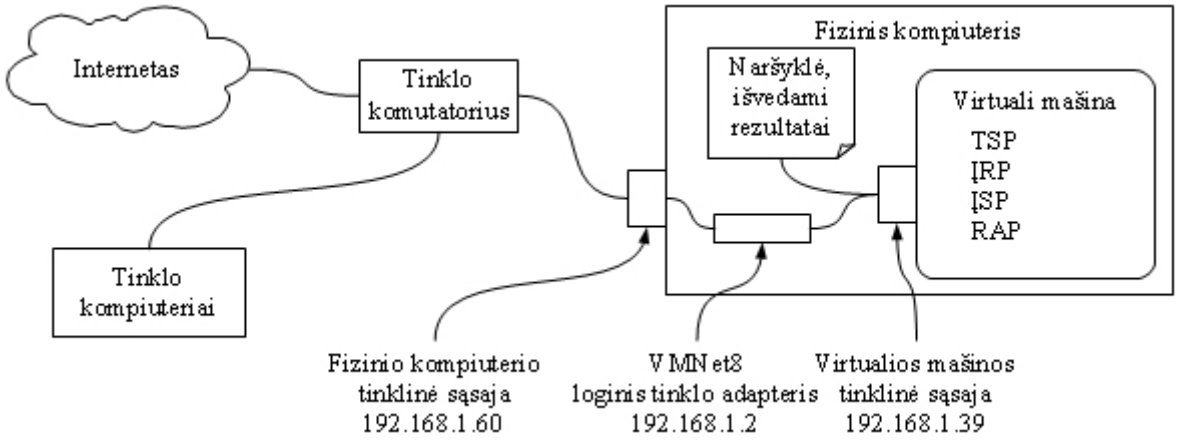
	Metodikos komponentai:						
	K.s1.kom1	**K.s1.kom2**	**K.s2.kom1**	**K.s2.kom2**	**K.s3.kom1**	**K.s4.kom1**	**K.s4.kom2**
Koeficientų reikšmės:	0,18750	0,25000	0,12500	0,18750	0,12500	0,06250	0,06250

Komponentų reikšmės bus nustatytos TSP ir įrašytos į ĮRP. Susumavus visas

pažeidimų reikšmes ir atėmus rezultatą iš maksimalaus bendro įvertinimo – vieneto, gausime bendro įvertinimo reikšmę. Konkrečiu atveju, jeigu suveiktų tik vienas pažeidimas, $s_1.kom_1$ rezultatas būtų lygus: 0,81250. Užfiksavus visus pažeidimus, bendras įvertinimas bus lygus nuliui.

5.2. Įrankio prototipas

Automatizuotas įrankis yra įdiegtas į virtualios mašinos „VMWare“, „Windows XP Pro“ operacinę sistemą. Per „VMWare“ įrankio virtualią sąsają „VMNet8“ darbo automatizuotas įrankis gali stebėti siunčiamą ir gaunamą srautą iš fizinio kompiuterio.



19 pav. Įrankio prototipas

Tokio sujungimo pakaks sumodeliuoti sudarytus MSPR.

5.2.1. TSP prototipas

Norint realizuoti MSPR, reikia sudaryti tokias taisykles:

1. `alert ip $DRAUDZIAMI_IP any -> any any (msg: "[spt] naudojama draudziama adresacija"; sid:1000001;)`
2. `alert ip $LEIDZIAMI_IP any -> any any (msg: "[spt] TTL reiksme kita!"; ttl: !128; sid:1000002;)`
3. `alert tcp 192.168.1.60 any > any 25 (content:"MAIL FROM:"; content: !"<gurejevas %40greitojipagalba.lt>"; msg: "[spt] is darbo vietos 60 siunciamo laisko el. adresas yra ne gurejevas@greitojipagalba.lt";sid:1000003;)`
4. `alert tcp 192.168.1.60 any -> any 80 (msg:"[spt]vartotojas (gurejevas) iš darbo stoties 60 issiunte savo el.pasto adresa i web serveri"; content:"gurejevas %40greitojipagalba.lt";sid:1000004;)`
5. `alert tcp !192.168.1.60 any > any 21 (content:"USER|20|"; content:!"gurejevas"; msg: "[spt] Is stoties 60 prisijungimas prie FTP su kitu vardu";sid:1000005;)`
6. `alert tcp 192.168.1.60 any > any any (content:"sex"; msg: "[spt] darbo stotis: 60, uzfiksuota draudziama informacija";sid:1000006;)`
7. `alert tcp 192.168.1.60 any > any any (content:".exe" content:".mpeg"; msg: "[spt] darbo stotis: 60, uzfiksuotas draudziamas bylos siuntimas";sid:1000007;)`

Šios taisyklės turi būti įrašytos į bet kokį failą, o šis failas turi būti nurodytas „Snort“ įrankiui konfigūracijos „snort.conf“ faile. Taisyklių įtraukimo eilutės atrodo taip:

```
var RULE_PATH /etc/rules
include $RULE_PATH/taisykles.rules
```

„Snort“ įrankio paleidimas atliekamas tokia komanda:

```
C:\Snort\bin\snort.exe -c "C:\Snort\etc\snort.conf" -l "C:\Snort\logs" -i 1 -d -e -X
```

5.2.2. ĮRP prototipas

„Snort“ užfiksavęs pažeidimą siunčia pranešimą į MySql duomenų bazę. Norint sukurti duomenų bazės lenteles, kur bus saugoma pažeidimo informacija, reikia įdiegti MySql, sukurti duomenų bazę „Snort“ ir įvykdyti lentelių sukūrimo skriptą, kuris jau yra „Snort“ įrankio kataloge „contrib/create_mysql“. Skirpto vykdymo metu sukuriamos tokios lentelės: schema, event, signature, sig_reference, reference, reference_system, sig_class, sensor, iphdr, tcphdr, udphdr, icmphdr, opt, data, encoding, detail.

Taip pat reikia sukurti papildomą lentelę, kur bus saugomos metodikos komponentų rizikos reikšmės. Apie tai yra rašoma 4.2.4.2 dalyje. Norint padaryti naują įrašą, reikia pasinaudoti įrankiu „phpMyAdmin“ arba sql skriptu:

```
INSERT INTO riz_reik (sid, reikalavimo_nr, riz) VALUES ('1000001', '1','3');
```

Duomenų bazė panaudojant TSP bus automatiškai užpildoma duomenimis apie pažeidimus.

Pranešimų atvaizdavimui yra įrankis ACID. Jį panaudojus galima stebėti, kokie įrašai buvo padaryti, taip testuoti „Snort“ įrankio veikimą.

5.2.3. ĮSP prototipas

Bendro įvertinimo skaičiavimas yra realizuojamas PHP kalba. Sukurtas skriptas atlieka nurodytas 4.2.4.3 dalyje funkcijas ir veiksmus.

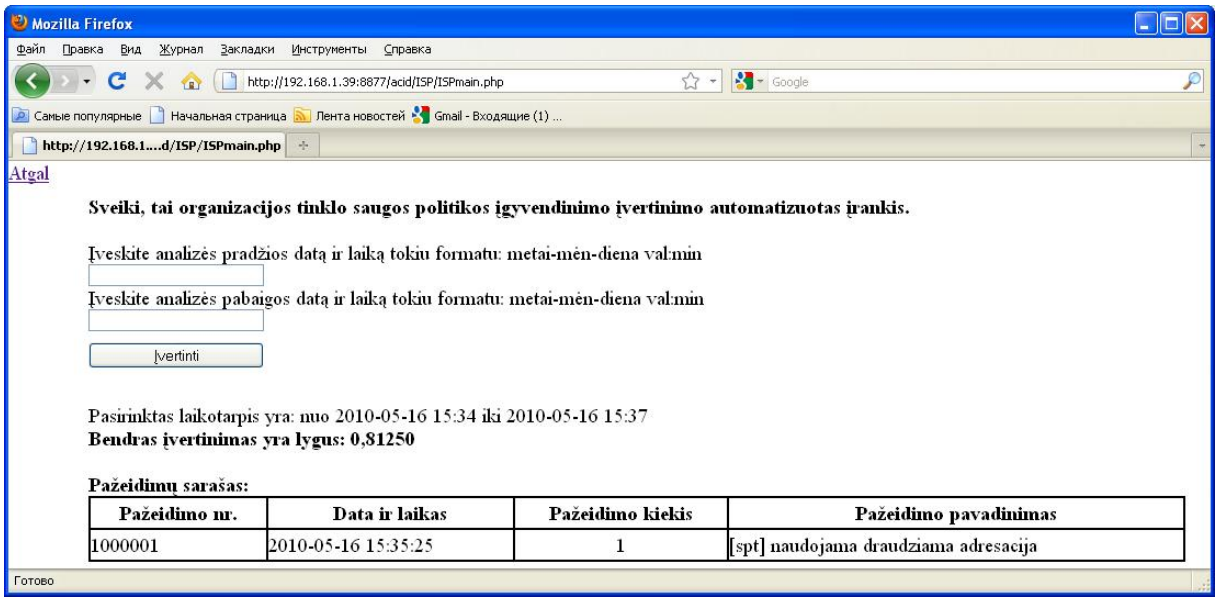
Šis pavyzdys nustato, kiek kartų buvo užfiksuotas tam tikras pažeidimas.

```
for (i=1; i<=y; i++){
  for (j=1; j<=R_s_kom[i][0]; j++;){
  $Query =     '
        SELECT  Count event.cid
        FROM event,signature
        WHERE sig_sid = ? and event.signature=signature.sig_id and ? < event.timestamp
and ? > event.timestamp
        ';
  $Stmt = $DB->prepare($Query);
  $Stmt->bind_param('iss',$sid_s_kom[i][j],t1,t2); //parametrizuoti kintamieji
  $Stmt->execute();
  Stmt->bind_result($pz_s_kom);
```

```
    }
}
```

5.2.4. RAP prototipas

RAP priemonė taip pat kaip ir ĮSP naudoja PHP kodą, todėl rezultatų atvaizdavimas galimas iš laikinų kintamųjų. RAP-ės išvaizda pavaizduota 20 paveiksle.



20 pav. RAP-ės išvedamų duomenų langas

Data ir laikas yra įvedami tokiu formatu: metai-mėnuo-diena valandos:minutės. Pavyzdžiui 2010-05-20 15:16. Po to spaudžiamas mygtukas „įvertinti“. ISP atlieka savo darbą, ir RAP išveda rezultatus.

5.2.5. Pažeidimo užfiksavimo scenarijus

Tarkime, automatizuotas įrankis stebi vieną iš tinklo potinklių. Automatizuotas įrankis užfiksuos saugos politikos pažeidimą, tai pavaizduota 12 paveiksle.

Įvyko pažeidimas – 2 kompiuteris išsiuntė neleidžiamą bylą „juokelis.exe“. Tinklas tęsia savo darbą kaip įprasta. Jeigu yra saugumo priemonė, kuri to padaryti neleidžia, tolimesnė sesija bus nutraukta. Bet kokiu atveju pažeidimas yra fiksuojamas. Srauto kopijavimo įrenginys šiuo metu ir sujungia 1 2 3 kompiuterius ir kopijuoja visą srautą į TSP. Pažymėtina, kad TSP neturi savo IP adreso, todėl nėra galimybės į ją kreiptis.

Kadangi TSP nuolat stebi tinklo srautą, kiekviena bitų seka yra palyginama su iš anksto apibrėžtomis taisyklėmis. Šiose taisyklėse buvo nurodyta, kad reikia padaryti registravimo įrašą į duomenų bazę, jeigu tinklo sraute pasitaikys bitų seka „.exe“.

Taisyklė atrodo taip:

```
alert tcp 192.168.1.60 any > any any (content:".exe" content:".mpeg"; msg: "[spt] darbo stotis: 60, uzfiksuotas draudziamas bylos siuntimas";sid:1000007;)
```

Registravimo įrašas į duomenų bazę yra automatiškai įvykdomas, nes TSP jau turi tokią funkciją. Taisyklės parametras „content“ pagauna nepageidaujamą srauto fragmentą. Į lentelę „signature“ į lauką „sig_name“ yra įrašomas „msg“ pranešimas, kiti laukai taip pat yra užpildomi automatiškai. Daugiau veiksmų nevyksta. TSP toliau stebi srautą.

Kai vartotojas įvedęs įvertinimo laikotarpį, paspaudžia skaičiavimo mygtuką automatizuoto įrankio RAP-ėje, ĮSP atlieka tokius veiksmus:

- priima įvestą įvertinimo laikotarpį;
- kreipiasi į duomenų bazę, kur yra sukaupti TSP registravimo įrašai, rizikos reikšmės;
- apskaičiuoja bendrą įvertinimą;
- nustato pažeidimų tipus;
- nustato pažeidimų kiekį;
- perduoda duomenis RAP išvedimui į ekraną.

Įvertinimo skaičiavimo priemonės veiksmų seka pavaizduota 14 paveiksle.

Taip rezultatai išvedami į ekraną. Jeigu reikia, atsakingas specialistas pagal išvestą informaciją gali gauti papildomą informaciją apie pažeidimą prisijungęs prie ĮRP, arba išanalizavęs TSP „log“ failus, kurie yra kuriami automatiškai.

6. Eksperimentinė dalis

Eksperimentas leidžia įsitikinti, ar problemos sprendimas pasirinktas tinkamai. Bus išbandyti metodikos saugos politikos reikalavimai, pažeidimų rezultatai, įrankio trūkumai.

6.1. Metodikos saugos politikos reikalavimų tyrimas

Tyrimui tiks panaudotas metodikos pavyzdyje saugos politikos reikalavimų rinkinys. Šiuos reikalavimus galima įvertinti analizės dalyje aprašytais būdais ir sukurtu šiame darbe automatizuotu įrankiu.

6.1.1. Tinklas susidaro tik iš griežtai apibrėžtų įrenginių skaičiaus

Saugos reikalavimo patikrinimas nenaudojant sukurto įrankio

Panaudojame saugos objektų identifikacijos techniką. Tai yra įrenginių paieška tinklu. Vienas iš daugelio įrankių kuris gali atlikti tokią funkciją, yra „Nmap“ [23]. „Nmap“ turi daug įrenginių nustatymo būdų: TCP connect(), SYN, Ping, UDP, IP protocol, ACK scan ir kiti. Pasirinkus vieną iš tinkamų skenavimo būdų, įrenginiams yra siunčiami signalai. Pagal įrenginių atsakymą sprendžiama, ar įrenginys yra tinkle, kokie jo IP ir Mac adresai, ir nustatoma, ar tai tinklo legalus įrenginys, ar tai pažeidėjo įrenginys.

Saugos reikalavimo patikrinimas panaudojant sukurtą įrankį

Į automatizuoto įrankio tinklo stebėjimo priemonę (TSP) įvedama tokia taisyklė:

```
alert ip $DRAUDZIAMI_IP any -> any any (msg: "[spt] naudojama draudziama adresacija"; sid:1000001;)
```

TSP leidžia pagauti paketą išeinančiame sraute iš vidinio organizacijos tinklo. Ši taisyklė remiasi tik IP adresu ir suveikia, kai randamas išeinantis iš tinklo paketas su draudžiamu IP. IP adresu galima pasitikėti, nes TSP seka tinklo IP ir Mac adresų porų pasikeitimus. Tai atliekama TSP komponento dėka vadinamo „arpspoof preprocessor“. „Snort“ TSP-ės „snort.conf“ faile reikia įrašyti tokias elutes:

```
preprocessor arpspoof
arpspoof_detect_host: 10.10.10.10 29:a2:9a:29:a2:9a
arpspoof_detect_host: 10.10.10.11 29:a2:9a:29:a2:9b (ir taip toliau)
```

Atsiradus nenumatytai IP ir Mac adresų porai, TSP į įrašų registravimo priemonę (ĮRP) įrašys pranešimą apie pažeidimą:

```
[ 05/15-16:20:00.939243 ] [112:2:1] <eth1> (spp_arpspoof) Ethernet/ARP Mismatch request for Source.
```

Įvertinimo skaičiavimo priemonė (ĮSP), radusi nors vieną iš šių pranešimų, ĮRP-ėje žymės, kad yra pažeidimas, ir bendras įvertinimas bus sumažintas. Bendro įvertinimo skaitinė reikšmė priklauso nuo rizikos pažeidimo santykinės reikšmės – koeficiento. Rizikos pažeidimo santykinė reikšmė yra 0,18750, o jeigu kitų pažeidimų už nustatytą laikotarpį nebuvo, bendro įvertinimo reikšmė lygi 0,81250.

Kaip rezultatų atvaizdavimo priemonė išveda rezultatus apie pažeidimą pavaizduota 20 paveiksle.

6.1.2. Tinklo leisti įrenginiai negali suteikti prieigą prie tinklo kitiems įrenginiams

Saugos reikalavimo patikrinimas nenaudojant sukurto įrankio

Šiam tikslui pasiekti galima panaudoti bet kokį tinklo protokolų analizatorių, tarkim „TcpDump“ arba „Wireshark“. Išsaugojęs keletą paketų visiems IP adresams tinkle, galime analizuoti juos rankiniu būdu. Reikia patikrinti ar „ttl“ reikšmė yra tokia, kokia turi būti kiekvienam kompiuteriui.

Saugos reikalavimo patikrinimas panaudojant sukurtą įrankį

Į automatizuoto įrankio TSP įvedama tokia taisyklė:

```
alert ip $LEIDZIAMI_IP any -> any any (msg: "[spt] TTL reiksme kita!"; ttl: !128; sid:1000002;)
```

TSP stebėdama išeinantį iš kompiuterių srautą, tikrina TTL reikšmę. Jeigu bus rastas nors vienas paketas su skirtinga nei nustatyta TTL reikšme, į ĮRP bus padarytas įrašas. ĮSP tokį įrašą ras ir sumažins bendrą įvertinimą.

6.1.3. Vartotojas el. laiškus gali siųsti tik iš darbo vietos

Saugos reikalavimo patikrinimas nenaudojant sukurto įrankio

Šiuo atveju reikia atlikti testą. Siunčiame iš darbo vietos laišką iš kito el pašto adreso paskyros. Už apsaugos priemonės sukauptą srautą analizuojame tinklo protokolų analizatoriumi. Ieškome SMTP protokolo siuntimo pradžios paketą „235 go ahead“. Jeigu po šio paketo nėra nurodymo, iš ko yra siunčiamas laiškas, vadinasi apsaugos priemonė suveikė ir užblokavo sujungimą.

Jeigu apsaugos priemonės nėra, tenka pasitikėti darbuotojų sąžiningumu.

Saugos reikalavimo patikrinimas panaudojant sukurtą įrankį

Į automatizuoto įrankio TSP įvedama tokia taisyklė:

```
alert tcp 192.168.1.60 any > any 25 (content:"MAIL FROM:"; content: !"<gurejevas %40greitojipagalba.lt>"; msg: "[spt] is darbo vietos 60 siunciamo laisko el. adresas yra ne gurejevas@greitojipagalba.lt";sid:1000003;)
```

Šiuo būdu yra stebimi paketai siunčiami iš 60-tos darbo stoties 25 prievadu ir fiksuojamas pažeidimas, kai siuntėjo el. pašto adresas yra ne toks, koks turi būti. Kadangi TSP turi veikiantį preprocesorių, kuris stebi IP ir Mac adresų pasikeitimus, užtenka pasitikėti IP adresu. Jeigu tinklo fragmente bus IP Mac pažeidimas, suveiks taisyklė sid – 1000001, kur rizika jau yra įskaičiuota.

6.1.4. Draudžiama naudoti, pateikti ir registruoti savo el. pašto adresą internetinėse sistemose

Saugos reikalavimo patikrinimas nenaudojant sukurto įrankio

Kaip ir anksčiau, vienas iš būdų, tai tinklo srauto surinkimas ir paketų analizė. Reikia kaupti ir saugoti kompiuterio išeinantį tinklo srautą, o vėliau surinktuose paketuose ieškoti kreipinių į serverius (80 prievadas) ir el. pašto adresų.

Saugos reikalavimo patikrinimas panaudojant sukurtą įrankį

Į automatizuoto įrankio TSP įvedama tokia taisyklė:

```
alert tcp 192.168.1.60 any -> any 80 (msg:"[spt]vartotojas (gurejevas) iš darbo stoties 60 issiunte savo el.pasto adresa i web serveri"; content:"gurejevas %40greitojipagalba.lt";sid:1000004;)
```

Taip bus užfiksuotas pažeidimas, kai darbo stotis kreipsis 80 prievadu ir pakete bus aptiktas šios stoties darbuotojo el. pašto adresas. IP adresu galime pasitikėti, nes už IP Mac vientisumą atsakinga pirma taisyklė sid – 1000001.

6.1.5. Vartotojas prie FTP paslaugos gali prisijungti prie savo paskyros tik iš savo darbo vietos

Saugos reikalavimo patikrinimas nenaudojant sukurto įrankio

Naudojamas rankinis paketų analizavimo būdas.

Saugos reikalavimo patikrinimas panaudojant sukurtą įrankį

TSP panaudojant šią taisyklę užfiksuos pažeidimą:

```
alert tcp !192.168.1.60 any > any 21 (content:"USER|20|"; content:!"gurejevas"; msg:
```

```
"[spt] Is stoties 60 prisijungimas prie FTP su kitu vardu";sid:1000005;)
```

6.2. Automatizuoto įrankio rezultatas

Atlikus saugos politikos reikalavimų patikrinimą nenaudojant ir panaudojant sukurtą įrankį, rezultatus galima apibendrinti 11 lentelėje.

11 lentelė. Kokias problemas išsprendžia sukurtas įrankis

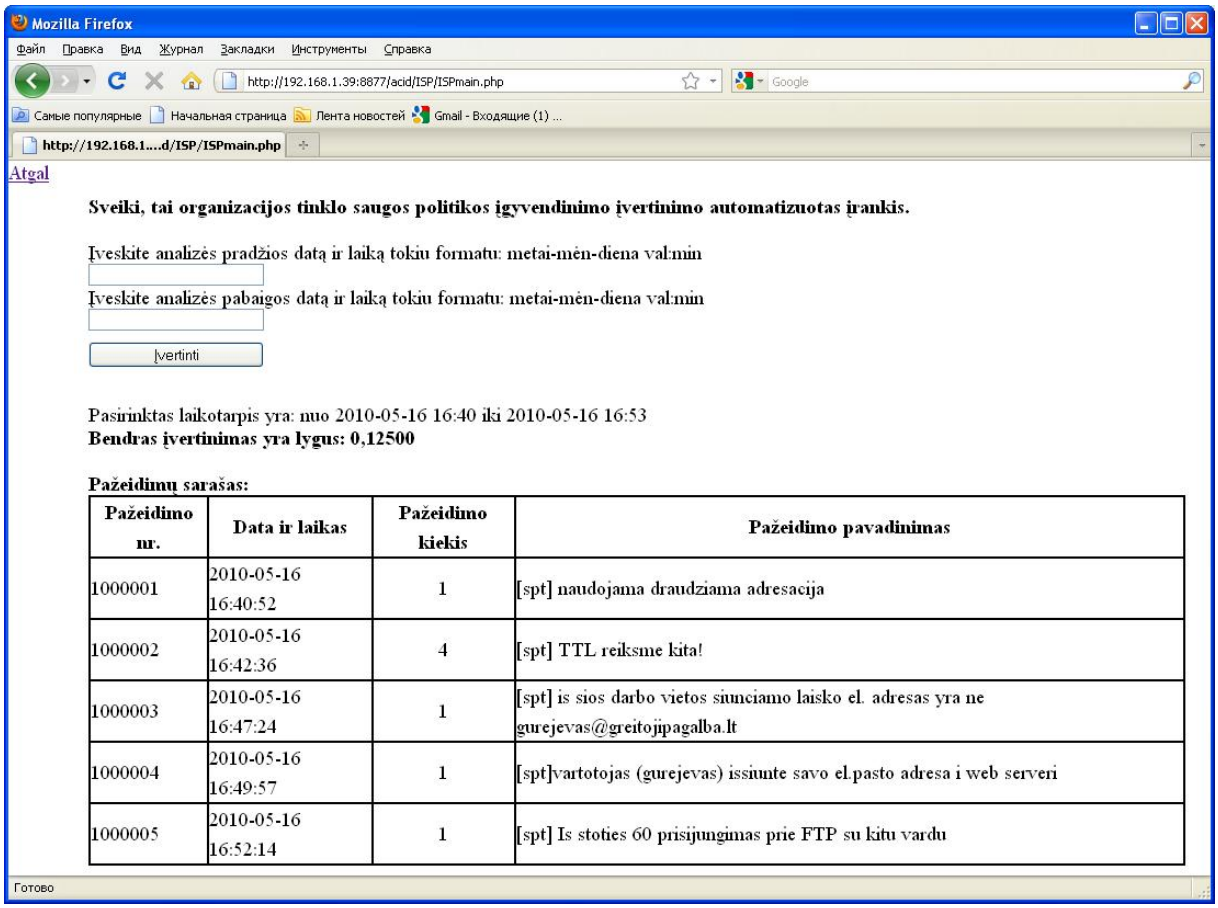
Problema	**Ar be įrankio išlieka problema?**	**Ar su įrankiu išlieka problema?**
norint gauti įvertinimą, reikia atlikti daug sudėtingų veiksmų	taip	ne
žmogiškasis faktorius, klaidos	taip	ne
rezultatų iš skirtingų įvertinimo būdų surinkimas ir bendro įvertinimo skaičiavimas yra sudėtingas	taip	ne
rezultatai yra aktualūs tik įvertinimo vykdymo metu	taip	ne

Jeigu yra sudarytas didelis saugos politikos reikalavimų rinkinys, patikrinti kiekvieną reikalavimą be sukurto automatizuoto įrankio išties yra sudėtinga. Pateiktų saugos politikos reikalavimų rinkinio patikrinimui be įrankio tektų skirti daug laiko paketų analizei. Dėl monotoniško darbo gali suveikti žmogiškasis faktorius, gali būti padaryta klaida. Taip pat reiktų surinkti rezultatus ir panaudojant atskirą priemonę paskaičiuoti bendrą įvertinimą. Didžiausia problema yra ta, kad įvertinimą mes gauname įvertinimo vykdymo metu, kuris vėliau praranda aktualumą dėl galimų pasikeitimų sistemoje.

Visas šias problemas leidžia išspręsti sukurtas automatizuotas įrankis. Vieną kartą tiksliai sukonfigūravus įrankį, pažeidimai yra fiksuojami įrankio veikimo metu ir pagal tai suskaičiuojamas bendras saugos politikos reikalavimo rinkinio įvertinimas. Viskas yra atliekama automatizuotai ir papildomų veiksmų atlikti nereikia.

Bendro įvertinimo reikšmės kitimas laike

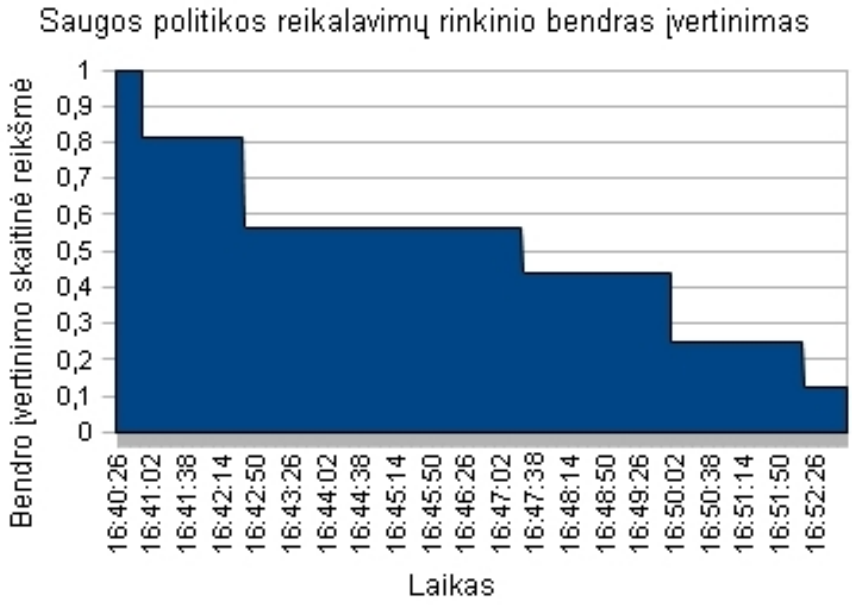
Pagal pažeidimų užfiksavimo laiką galima pavaizduoti, kaip bendras įvertinimas kinta laike. Sudarykime įrankiui tokias sąlygas, kad būtų užfiksuoti 1000001 – 1000005 (sid – pažeidimo identifikacijos numeris) pažeidimai iš eilės. Pasirinktas laiko tarpas yra nuo 16:40 iki 16:53. Kaip RAP išves duomenis apie pažeidimus ir bendrą įvertinimą pavaizduota 21 paveiksle.



Pažeidimo nr.	Data ir laikas	Pažeidimo kiekis	Pažeidimo pavadinimas
1000001	2010-05-16 16:40:52	1	[spt] naudojama draudziama adresacija
1000002	2010-05-16 16:42:36	4	[spt] TTL reiksme kita!
1000003	2010-05-16 16:47:24	1	[spt] is sios darbo vietos siunciamo laisko el. adresas yra ne gurejevas@greitojipagalba.lt
1000004	2010-05-16 16:49:57	1	[spt]vartotojas (gurejevas) issiunte savo el.pasto adresa i web serveri
1000005	2010-05-16 16:52:14	1	[spt] Is stoties 60 prisijungimas prie FTP su kitu vardu

21 pav. RAP išveda penkis pažeidimus ir paskaičiuotą bendrą įvertinimą

Bendro įvertinimo reikšmės kitimas laike pavaizduotas 22 grafike.



22 pav. Bendro įvertinimo reikšmės kitimas laike

Bendro įvertinimo reikšmė priklauso nuo pasirinkto laiko tarpo ir per tą laiko tarpą užfiksuotų pažeidimų tipų kiekio. Grafike pavaizduotas penkių pažeidimų fiksavimas. Jeigu

būtų užfiksuoti visi metodikos saugos politikos rinkinio reikalavimai, bendras įvertinimas taptų lygus nuliui. Jeigu per pasirinktą laikotarpį pažeidimų nebuvo užfiksuota, bendras įvertinimas bus lygus vienetui.

Norint palyginti bendro įvertinimo reikšmes tarp tam tikrų laiko momentų, reikia nurodyti pradžios ir pabaigos laiką tokį patį. Po to procedūrą pakartoti su kitu laiku, o reikšmes palyginti.

6.3. Sukurto įrankio trūkumai

Kadangi saugos politikos taisyklės yra atrenkamos atsižvelgiant į automatizuoto įrankio galimybes ir tinklo srities apribojimą, įrankio rezultatai apibrėžia tik organizacijos tinklo saugos dalį.

Įrankis negali stebėti šifruoto srauto.

TSP-ės taisyklių sukūrimas turi būti tikslus, teisingas ir visapusiškai apgalvotas. Kitaip galimas taisyklės suveikimas neesant pažeidimui. Jeigu saugos politikos reikalavimų rinkinys yra didelis, taisyklių kūrimas gali būti sudėtingas. Tai reikia atlikti tik vieną kartą, sistemos diegimo metu.

Jeigu organizacijos tinklas nesikeičia, darbuotojai lieka savo vietose ir t. t., sukurtas įrankis gali būti ilgai naudojamas be pakeitimų. Jeigu įvykdomas pakeitimas organizacijos tinkle, pavyzdžiui, sukuriama nauja darbo vieta, reikalingas viso saugos politikos reikalavimų rinkinio peržvelgimas, koregavimas. Esant organizacijos tinklo pakeitimams taip pat yra keičiamos tinklo saugos priemonių taisyklės, saugos politikos reikalavimai, rizikos analizės rezultatai ir t. t.

7. Išvados

1. Analizės metu buvo nustatyta, kad organizacijos sauga yra organizuojama ciklu. Tai parodo saugos gyvavimo ciklas, valdžios valdymo ir vykdymo lygių koncepcija. Siekiama sauga apibrėžiama saugos politikoje, todėl būtina nuolat stebėti ir vertinti saugos lygį.
2. Panaudojant pasiūlytą metodiką galima apskaičiuoti organizacijos kompiuterių tinklo saugos politikos įgyvendinimo įvertinimą skaitine reikšme, kuri parodo kaip nukrito saugos lygis per analizuojamą laiko tarpą.
3. Pasiūlyta metodika atitinka saugos politikos dokumentų hierarchiją, leidžia sukurti metodikos saugos politikos reikalavimų rinkinį, kuris susieja saugos politikos taisykles su tinklo stebėjimo priemonės sintakse. Bendra įvertinimo skaitinė reikšmė išreiškia užfiksuotų pažeidimų kiekį ir rizikos įtaką į organizacijos saugą, kas leidžia tiksliau nustatyti saugos lygį.
4. Eksperimentas parodė, kad įrankis automatizuoja įvertinimo procesą pagal iš anksto aprašytas taisykles, kas padeda išvengti sudėtingų kartojamų įvertinimo darbų.
5. Eksperimento metu buvo įsitikinta, kad rezultatai aktualūs tiek, kiek dirbo įrankis, o šis gali stebėti tinklą ir fiksuoti pažeidimus nuolat. Organizacijos tinklo saugos politikos įgyvendinimo įvertinimo skaitinė reikšmė priklauso nuo skirtingų užfiksuotų pažeidimų kiekio, pasirinkto laikotarpio, kurio metu buvo fiksuojami pažeidimai, metodikos saugos politikos reikalavimų rizikos reikšmių.

8. Literatūra

[1] Группа разработки решений Майкрософт по безопасности и соответствию регулятивным нормам, „Руководство по управлению рисками в области безопасности“, // internetinė prieiga http://technet.microsoft.com/ru-ru/library/cc163143.aspx [interaktyvus]

[2] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements [interaktyvus]

[3] ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management [interaktyvus]

[4] В.А. Галатенко „Основы информационной безопасности“, // internetinė prieiga http://www.intuit.ru/department/security/secbasics/6/ [interaktyvus]

[5] Kryukov D., Eleonora L., „CONCEPT OF INFORMATION SECURITY SYSTEM EVALUATION MODEL“ // internetinė prieiga http://web.ebscohost.com/ehost/detail?vid=4&bk=1&hid=108&sid=b7408cdb-6e8f-4b8b-81f6-7bbda1c8e45%40sessionmgr108&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=iih&AN=35471865 [interaktyvus]

[6] Informacinių technologijų valdžios institucija. IT Governance institute „CobiT 4.1” [interaktyvus]

[7] Informacinių sistemų audito ir kontrolės asociacija. Information Systems Audit and Control Association // internetinė prieiga http://www.isaca.org/ [interaktyvus]

[8] Peter Peterka „The DMAIC Method in Six Sigma“ //prieiga per interneta: http://www.buzzle.com/editorials/10-24-2005-79640.asp [interaktyvus]

[9] Kazanavičius E., Venčkauskas A., Liutkevičius A., Vrubliauskas A. Informacijos saugos vadyba. Kaunas 2008 [interaktyvus]

[10] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management [interaktyvus]

[11] Герасименко В.А., Малюк А.А, „Основы защиты информации“, М.: Инкомбук, 1997 [interaktyvus]

[12] С. Симонов „Технологии и инструментарий для управления рисками“ //informacinis biuletenis Jet Info Nr2 (117)2003 [interaktyvus]

[13] Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30 [interaktyvus]

[14] SANS (SysAdmin, Audit, Network, Security) Institute, „SANS Security Policy Project“ // internetinė prieiga http://www.sans.org/security-resources/policies/#template [interaktyvus]

[15] Scarfone K., Souppaya M., Cody A., Orebaugh A., „Technical Guide to Information Security Testing and Assessment“ SP 800-115 „NIST“ 2008 [interaktyvus]

[16] Susan Snedaker, „IT Security Project Management“ Styngress Handbook. [interaktyvus]

[17] Pete Herzog, „Open-Source Security Testing Methodology Manual“ „OSSTMM 3.0 Lite.“ 2008 [interaktyvus]

[18] „TCPDUMP“ //prieiga per interneta: http://www.tcpdump.org/tcpdump_man.html [interaktyvus]

[19] „Man pcap-filter - packet filter syntax“ //prieiga per interneta: http://www.manpagez.com/man/7/pcap-filter/ [interaktyvus]

[20] „Wireshark“ //prieiga per interneta: http://www.wireshark.org/ [interaktyvus]

[21] SNORT Users Manual 2.8.5 //prieiga per interneta: http://www.snort.org/assets/125/snort_manual-2_8_5_1.pdf [interaktyvus]

[22] ACID – Analysis Console for Intrusion Databases //prieiga per interneta: http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html [interaktyvus]

[23] Andrew J. Bennieston „NMAP - A Stealth Port Scanner“ //prieiga per interneta: http://nmap.org/bennieston-tutorial/ [interaktyvus]

9. Santrumpų ir terminų žodynas

Informacija – informacija suprantama kaip žinios apie faktus, įvykius, procesus, reiškinius, objektų padėtį (jų savybes, charakteristikas) konkrečioje srityje, naudojamo (būtino) priimamiems sprendimams optimizuoti tų objektų valdymo procese Ошибка: источник перекрестной ссылки не найден.

Subjektas – valstybė (visą ar atskirus jos organus ir organizacijas), visuomenines arba komercinės organizacijos (susivienijimas) ir įmonė (juridinis asmuo), pavienis pilietis (fizinis asmuo) Ошибка: источник перекрестной ссылки не найден.

Informaciniai santykiai – savo veiklos procese subjektai gali būti tarpusavyje susiję įvairiais santykiais, liečiančiais tam tikros informacijos gavimo, saugojimo, apdorojimo, platinimo ir naudojimo klausimus. Tokius subjektų santykius vadinsime informaciniais santykiais, o juose dalyvaujančius subjektus – informacinių santykių subjektais Ошибка: источник перекрестной ссылки не найден.

Informacinių santykių subjektai – tai subjektai dalyvaujantys informaciniuose santykiuose Ошибка: источник перекрестной ссылки не найден.

VVVLĮM – Valdžios Valdymo Vykdymo Lygių Įvertinimo Metodas

Saugos politikos įgyvendinimas – ši sąvoka yra naudojama apibrėžti įmonės saugos politikos įgyvendinimo būseną. Tai ne pačių saugos politikos reikalavimų įgyvendinimo procesas, o būsena, kuri nusako ar visi reikalavimai yra pildomi.

Saugos politikos realizacijos įvertinimas – ši sąvoka apibrėžia saugos politikos realizacijos įvertinimą skaitine reikšme. Ši reikšmė yra skaičiuojama pagal sukurtą metodika, kuri atspindi pasirinktą saugos politikos reikalavimų rinkinį.

Automatizuotos priemonės – Tai įsilaužimų aptikimo sistemos „Snort“ kaip priemonė stebėti tinklu perduodamą srautą panaudojimas. „MySql“ duomenų bazė kaip priemonė priimti ir saugoti iš įsilaužimų aptikimo sistemos pranešimus. „PHP“ kalbos pagalba galima atrinkti sukauptus pranešimus iš duomenų bazės, juos apdoroti sukurtu skriptu pagal sukurtą metodiką ir paskaičiuoti bendrą įvertinimą.

Automatizuotas įrankis – tai aukščiau minėtų automatizuotų priemonių visuma, kuri leidžia įvertinti tinklo saugos politikos reikalavimų rinkinio vykdymą, tuo pačiu tinklo saugą.

Rizika – tai įvykio tikimybės ir jos pasekmių kombinacija [10]. Čia pasekmė, dažniausiai yra suprantama kaip žala. Kitaip tariant tai galimybė prarasti dalį lėšų dėl duomenų saugos pažeidimo, arba numatomos žalos dydis. Pažeidus tam tikrą duomenų saugos

vertybę, yra nustatoma jos žala.

Žala – tai prarastų lėšų reikšmė.

Grėsmė – tai potencialiai galimas nepageidaujamas įvykis, kuriam įvykus gali būti padaryta žalą vertybei, sistemai ar organizacijai [10].

Ataka – tai sėkmingai įvykdyta grėsmė.

Pažeidžiamumas – tai vertybės ar jų grupės silpna vieta, kuria gali pasinaudoti viena ar daugiau grėsmių [10].

Rizikos analizė – tai sistemingas informacijos naudojimas rizikos šaltinių nustatymui ir jos lygo įvertinimui [10].

Rizikos įvertinimas – tai pilnas rizikos analizės ir rizikos reikšmingumo įvertinimo procesas [10].

Rizikos reikšmingumo įvertinimas – tai palyginimo procesas skirtas nustatyti rizikos reikšmingumą, kur yra lyginami paskaičiuota rizika ir užsibrėžtos rizikos kriterijai [10]. Rizikos reikšmingumo įvertinimo procesas skirtas tam, kad identifikuoti pačias pavojingiausias rizikas.

Duomenų saugos sistemos incidentas – tai nepageidaujamas ar netikėtas įvykis duomenų saugos sistemoje, kuris su didele tikimybe gali sukelti grėsmes [10].

SKĮ – srauto kopijavimo įrenginys

TSP – tinklo stebėjimo priemonė

ĮSP – įvertinimo skaičiavimo priemonė

RAP – rezultatų atvaizdavimo priemonė

MSPR – metodikos saugos politikos reikalavimas (-ai)

IDS – įsilaužimo aptikimo sistema

NIDS – tinklo įsilaužimų aptikimo sistema

ACID (Analysis Console for Intrusion Databases) – įrankis, skirtas peržūrai su įrankio „Snort“ išsaugotais pranešimais.

TLS – (Transport Layer Security) – kriptografinis protokolas, užšifruojantis duomenų perdavimo kanalą tarp tinklo mazgų

MySql – atviro kodo MySql duomenų bazė

PHP – žiniatinklio programavimo kalba

HTML – hiperteksto ruošimo kalbos standartas

Apache – žiniatinklio serveris

10. Paveikslų sąrašas

11. Lentelių sąrašas