VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo taikymas informacijos saugos valdymo procese

2016-06-02
Vilnius

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas 621E14007

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

(Wolf)

GRĖSMĖ

(Wolf blows
the Weak House
of the Piggy)

PAŽEIDŽIAMUMAS

(Three Pigs
Securely and Happily
lives in the House)

SAUGUMAS

(Being eaten by Wolf)

RIZIKA

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Tikslas ir uždaviniai

Tikslas – pagerinti informacijos saugos valdymo grėsmių atvaizdavimo metodus ir grėsmių vertinimą.

Uždaviniai:

- išanalizuoti vizualizacija paremtų saugos sistemų projektus ir šiuolaikines vizualizacijos technologijas;
- atlikti grėsmių vizualizavimo panaudojimo probleminės srities analizę;
- pasiūlyti metodą grėsmių vizualizavimo taikymui informacijos saugos valdymo įgyvendinimui;
- įgyvendinti pasiūlytą metodą: sukurti prototipą ir jį išbandyti.

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

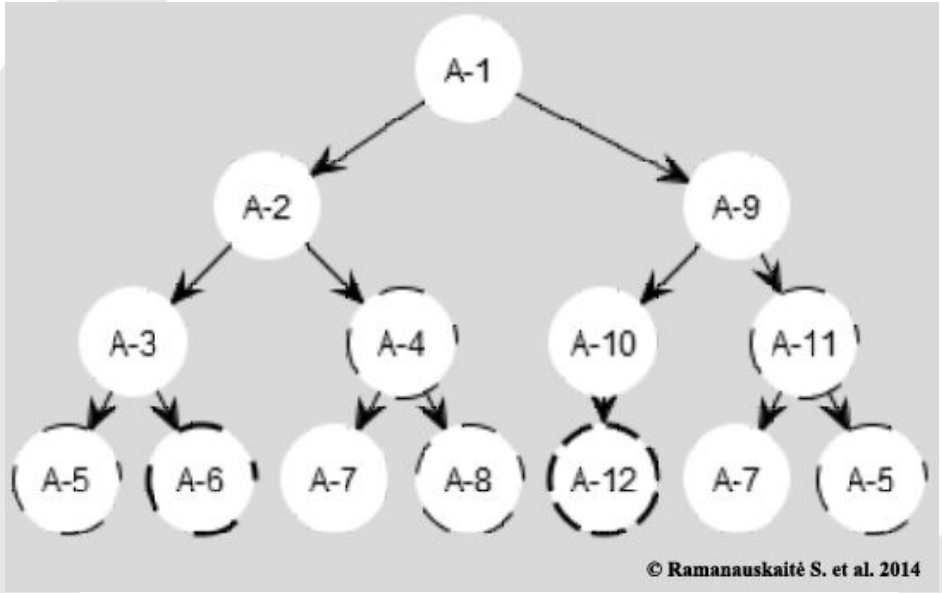
Problema

- Informacijos saugos rizikos valdymas yra didelės apimties ir daug laiko trunkantis procesas, kuris dažniausiai yra tik išsamiai aprašytas ir dažniausiai be grafinių elementų;
- Didėjant organizacijos dydžiui iš saugos dokumentacijos sunku greitai nustatyti kritinius taškus, kuriuose gali kilti grėsmės;
- Dažnai kintant organizacijos infrastruktūrai yra sudėtinga operatyviai ir tiksliai vykdyti rizikos vertinimą;
- Organizacijos neišnaudoja turimų informacinių išteklių integracijai su saugos valdymu.
- Žmogus – kritinis informacijos saugumo elementas.

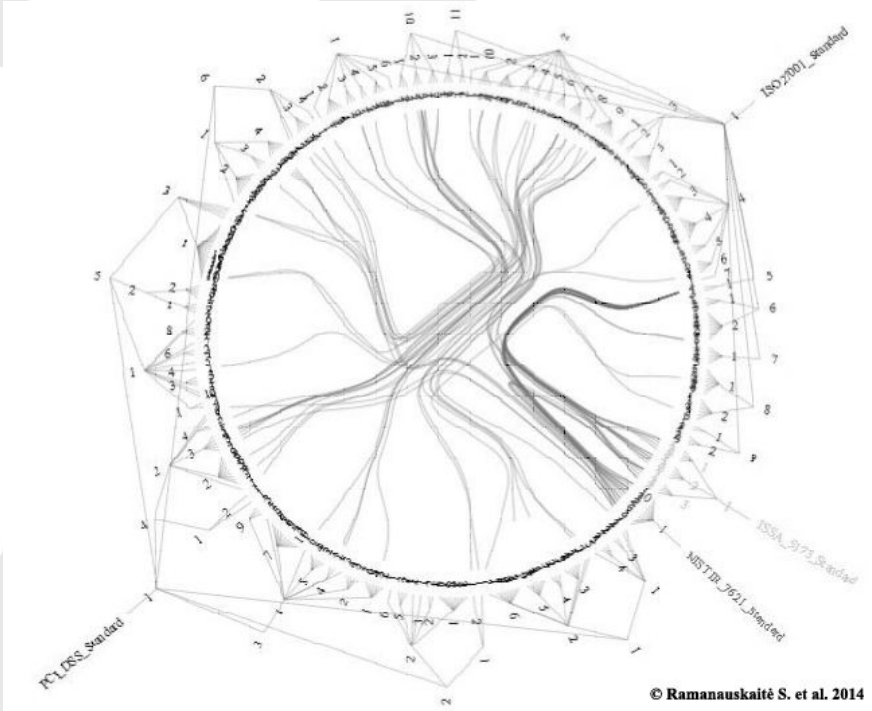
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Egzistuojantys vizualizavimo sprendimai (1/3)

- Saugumo standartų žymėjimas.



Grafų struktūra

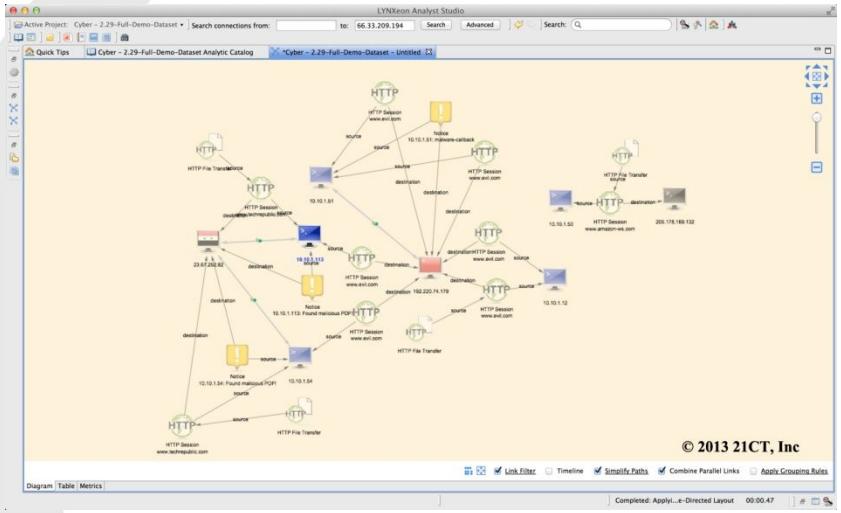


„Chord“ diagrama

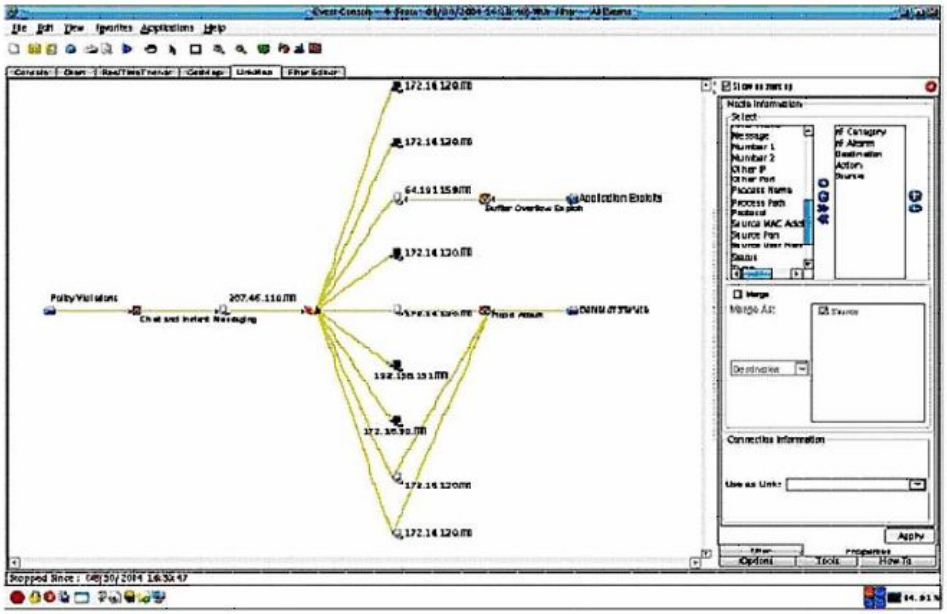
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Egzistuojantys vizualizavimo sprendimai (2/3)

- Tinklo srauto analizės ir vizualizavimo įrankiai.



LYNXeon™

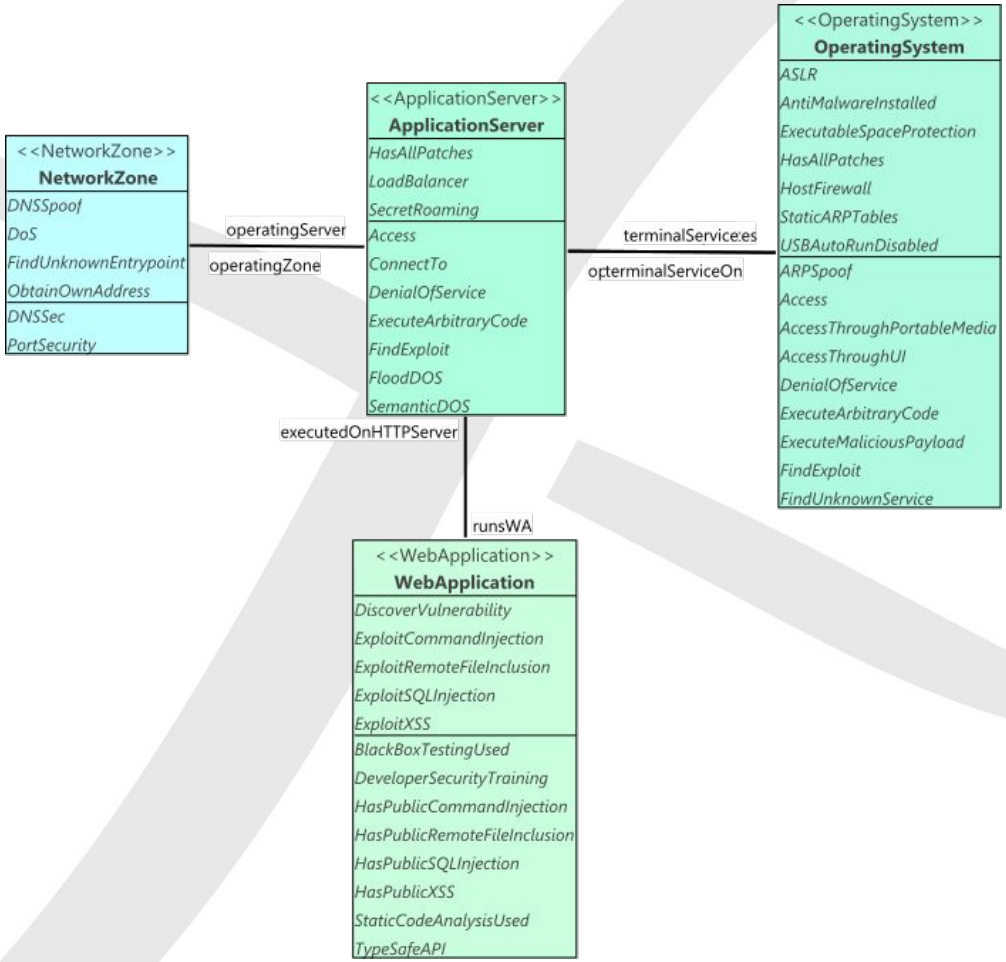


„CiscoWorks“ SIMS

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Egzistuojantys vizualizavimo sprendimai (3/3)

- SCADA sistemų architektūrų kibernetinio saugumo modeliavimas.



CySeMoL modelio dalis

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

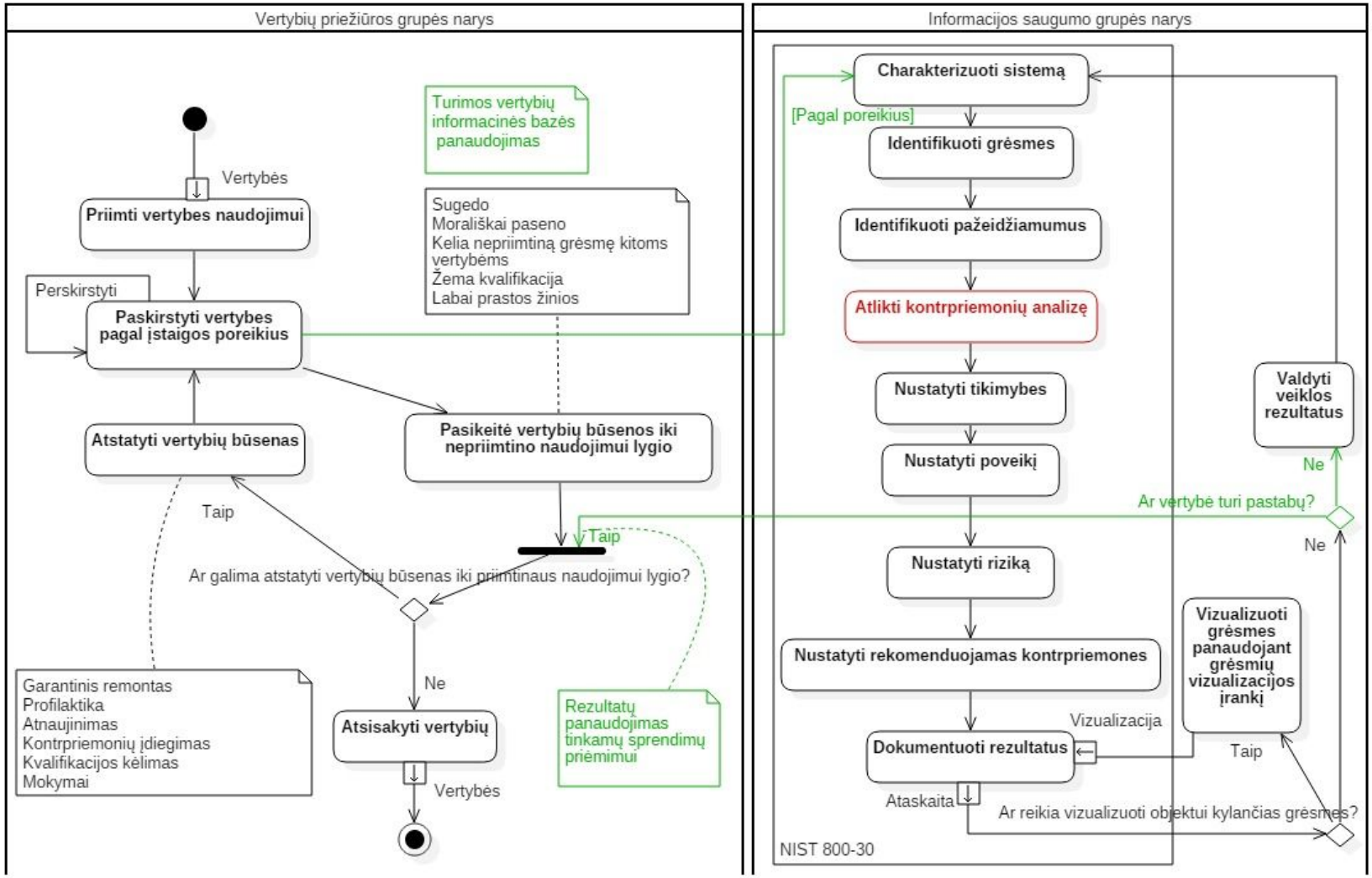
Vertybių priežiūra ir rizikos valdymas

Pagal NIST 800-30 parengtas rizikos valdymo gaires yra skiriami 9 rizikos vertinimo etapai:

1. Charakteristikų nustatymas;
2. Grėsmių identifikavimas;
3. Pažeidžiamumų identifikavimas;
4. Apsaugos priemonių analizė;
5. Tikimybių nustatymas;
6. Poveikių analizė;
7. Rizikos nustatymas;
8. Rekomenduojamos apsaugos priemonės;
9. Apibendrinanti dokumentacija.

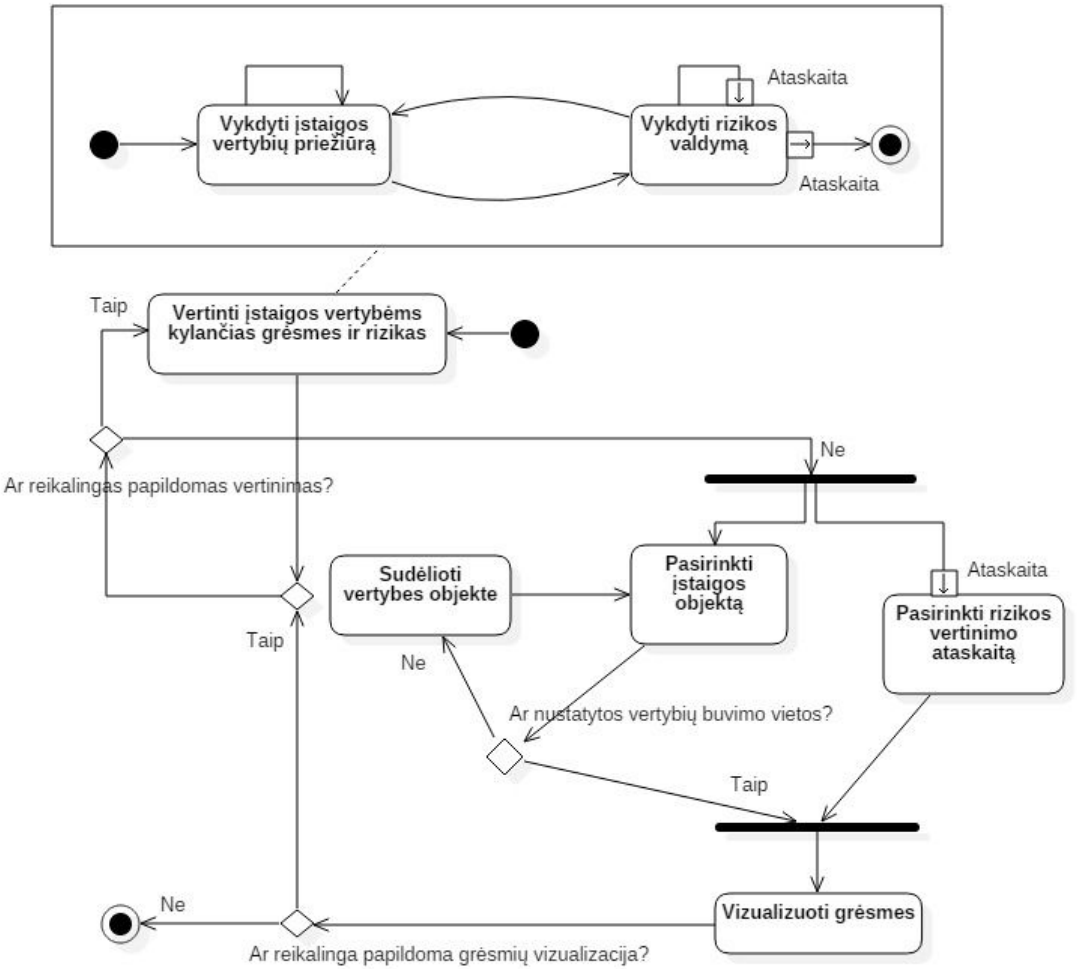
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo schema



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo grėsmių vizualizavimo eksplikacijos schema



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (1/8)

- Rizikos valdymo sistema, kurioje galima apibrėžti įstaigos ar kito struktūrinio padalinio vertybes, jas susieti, apibrėžti vertybėms kylančias grėsmes, pažeidžiamumus ir trimatėje erdvėje atvaizduoti visus probleminius taškus.

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (2/8)

Administratoriai | Įstaigos | Inventorius | Vertybės | Veiksmai | Rizikos valdymas | Saugos vizualizacija

Rizikos valdymas | Grėsmių sąrašas | Pažeidžiamumų sąrašas | Priskyrimas | Nustatymai

Rizikos valdymas

Rizikos vertinimas - pagal vertybes (inventorinė)

Rizikos vertinimas pagal 2016-01-01 planą Nr. 6 (Paulius Narkevičius/2016-01-01)

Viso: 8 | 100 | Įrašų puslapyje | 1 | Atnaujinti

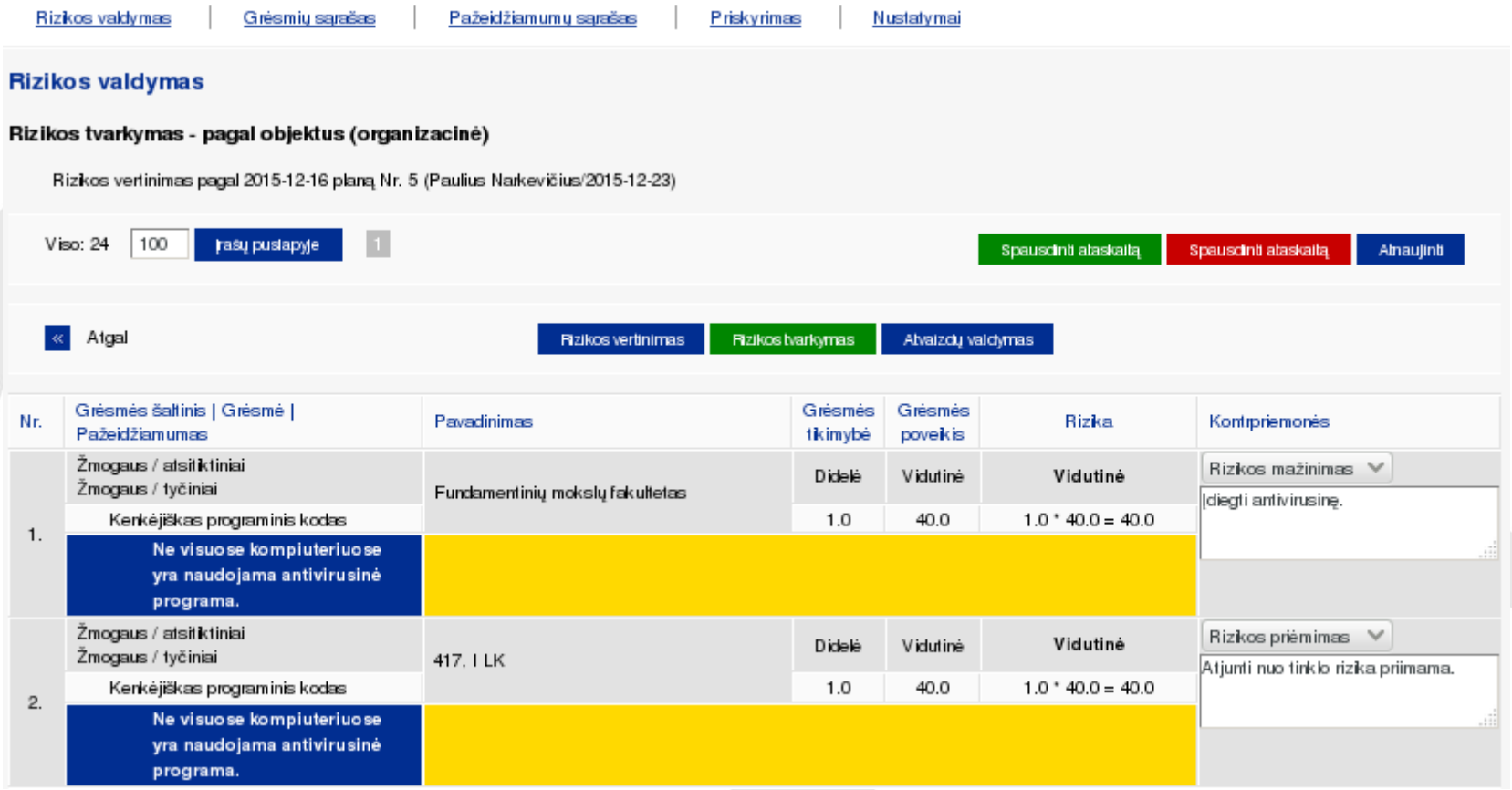
« Atgal | Rizikos vertinimas (skaitmenys) | Rizikos tvarkymas | Atvaizdų valdymas

Nr.	Grėsmės šaltinis | Grėsmė | Pažeidžiamumas	Grupės	Grėsmės tikimybė	Grėsmės poveikis	Rizika	Rūšys	Grėsmės tikimybė	Grėsmės poveikis	Rizika	Vertybė	Grėsmės tikimybė	Grėsmės poveikis	Rizika
1.	Žmogaus / tyčiniai Atsisakymo aptarnauti ataka Paskirstyta atsisakymo aptarnauti ataka **Bus užkištas tinklo mazgas ir neprieinamos paslaugos internetu.**	Kompiuterinė įranga	Maža	Vidutinė	Maža	Kompiuteris	Maža	Vidutinė	Maža	LENOVO ThinkCentre M58e	Didelė	Didelė	Didelė
		Ryšio įranga	Maža	Vidutinė	Maža	Nešiojamas kompiuteris	Maža	Vidutinė	Maža	LENOVO mouse	Maža	Maža	Maža
						Serveris	Maža	Vidutinė	Maža	LENOVO keyboard	Maža	Maža	Maža
						Monitorius	Maža	Vidutinė	Maža	LENOVO ThinkCentre M73	Didelė	Vidutinė	Vidutinė
						Klaviatūra	Maža	Vidutinė	Maža	DELL Inspiron 15.6" Touch-Screen Laptop	Vidutinė	Vidutinė	Vidutinė
						Pelė	Maža	Vidutinė	Maža	DELL monitorius	Maža	Maža	Maža
						Spausdintuvas	Maža	Vidutinė	Maža	HP Scanjet 200	Maža	Maža	Maža
						Skaitytuvas	Maža	Vidutinė	Maža				
2.	Žmogaus / tyčiniai Duomenų vagystė Sugadinti duomenys **Dėl naudojamos pasenusios technologijos neužtikrinamas naudotojų prieigos teisių valdymas įstaigos tinkle**					Serveris	Vidutinė	Didelė	Vidutinė	LENOVO ThinkCentre M73	Vidutinė	Didelė	Vidutinė

Atlikti įstaigos vertybėms kylančių grėsmių ir rizikos vertinimą

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (3/8)



Rizikos valdymas | Grėsmių sąrašas | Pažeidžiamumų sąrašas | Priskyrimas | Nustatymai

Rizikos valdymas

Rizikos tvarkymas - pagal objektus (organizacinė)

Rizikos vertinimas pagal 2015-12-16 planą Nr. 5 (Paulius Narkevičius/2015-12-23)

Viso: 24 | 100 | Įrašų puslapyje | 1 | Spausdinti ataskaitą | Spausdinti ataskaitą | Atnaujinti

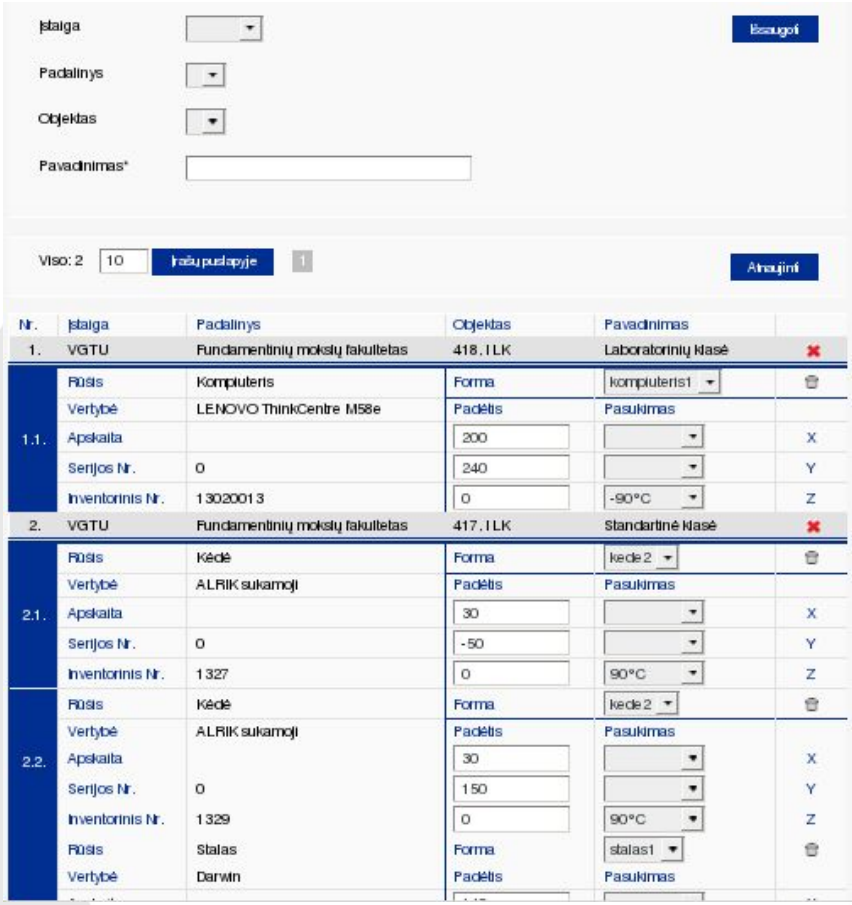
Atgal | Rizikos vertinimas | Rizikos tvarkymas | Atvaizdų valdymas

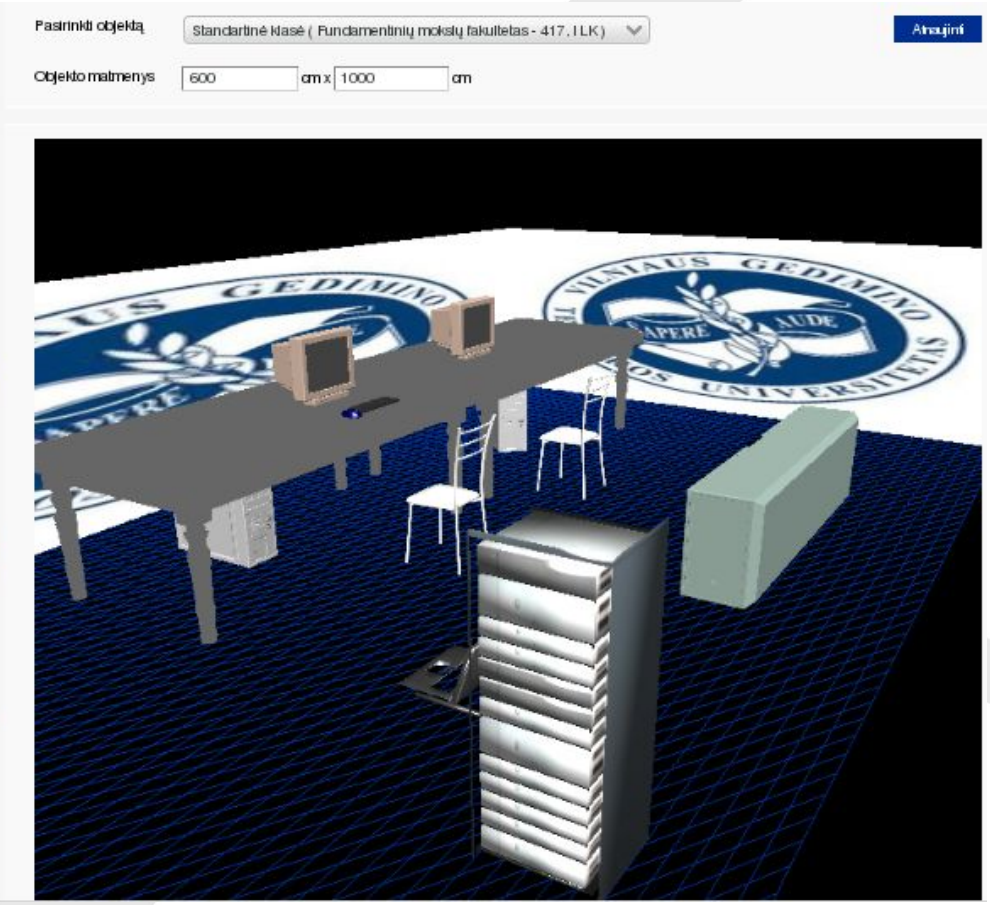
Nr.	Grėsmės šaltinis | Grėsmė | Pažeidžiamumas	Pavadinimas	Grėsmės tikimybė	Grėsmės poveikis	Rizika	Kontrpriemonės
1.	Žmogaus / atsitiktiniai Žmogaus / tyčiniai	Fundamentinių mokslų fakultetas	Didelė	Vidutinė	Vidutinė	Rizikos mažinimas Įdiegti antivirusinę.
	Kenkėjiškas programinis kodas		1.0	40.0	1.0 * 40.0 = 40.0	
	Ne visuose kompiuteriuose yra naudojama antivirusinė programa.					
2.	Žmogaus / atsitiktiniai Žmogaus / tyčiniai	417. I LK	Didelė	Vidutinė	Vidutinė	Rizikos priėmimas Atjunti nuo tinklo rizika priimama.
	Kenkėjiškas programinis kodas		1.0	40.0	1.0 * 40.0 = 40.0	
	Ne visuose kompiuteriuose yra naudojama antivirusinė programa.					

Atlikti rizikos tvarkymą

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (4/8)

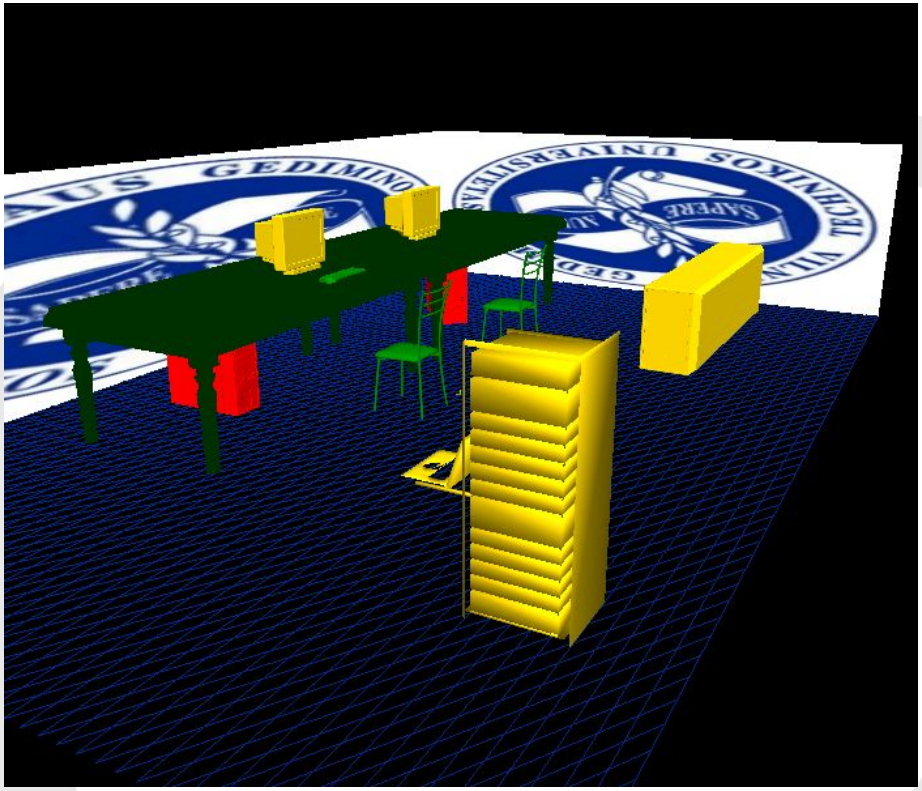




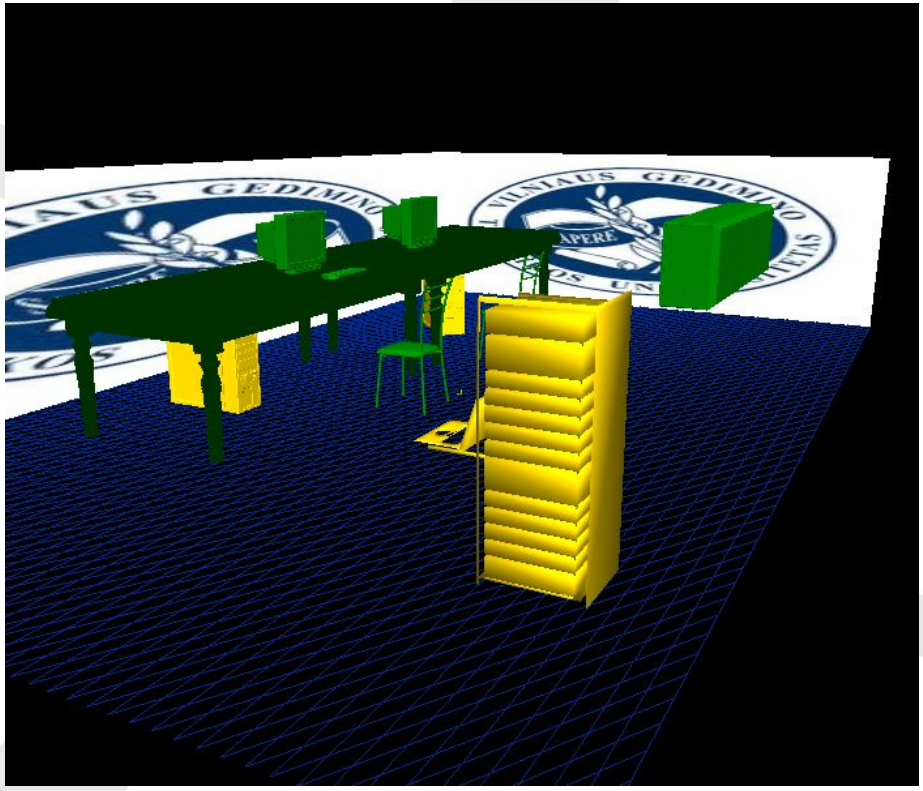
Nustatyti vertybių buvimo vietą įstaigoje

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (5/8)



Prieš kontrpriemonių įgyvendinimą



Po kontrpriemonių įgyvendinimo

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (6/8)

RODYKLĖ

▶ Atskaitos taškas | ⊕ Nauja rizika | ⊖ Rizikos nenustatyta | ↓ Rizika sumažėjo | ▮▮ Rizika išliko tokia pati | ↑ Rizika padidėjo

Nr.	Grėsmės šaltinis | Grėsmė | Pažeidžiamumas	Rizikos vertinimas pagal 2015-12-13 planą Nr. 1			Rizikos vertinimas pagal 2016-01-01 planą Nr. 2			Rizikos vertinimas pagal 2016-05-27 planą Nr. 3			
		Pokytis	Rizika		Pokytis	Rizika		Pokytis	Rizika		
1.	Žmogaus / tyčiniai Atsisakymo aptarnauti ataka Paskirstyta atsisakymo aptarnauti ataka **Bus užkištas tinklo mazgas ir neprieinamos paslaugos internetu.**	▶	Maža (1.0)		↑	Didelė (100.0)		↓	Maža (5.0)		▲
2.	Žmogaus / tyčiniai Duomenų vagystė Sugadinti duomenys **Dėl naudojamos pasenusios technologijos neužtikrinamas naudotojų prieigos teisių valdymas įstaigos tinkle**				⊕	Vidutinė (50.0)		▮▮	Vidutinė (50.0)		▲
3.	Aplinkos / žmogaus sukelti Gaisras **Gaisras, kurį sukėlė aplinkiniai pastatai ar objektai.**				⊕	Vidutinė (50.0)		↓	Maža (5.0)		▲
4.	Žmogaus / atsitiktiniai Žmogaus / tyčiniai Kenkėjiškas programinis kodas **Ne visuose kompiuteriuose yra naudojama antivirusinė programa.**				⊕	Didelė (100.0)		↓	Vidutinė (50.0)		▲

Stebėti kylančių grėsmių ir rizikos pokyčius laiko ašyje

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (7/8)

RODYKLĖ

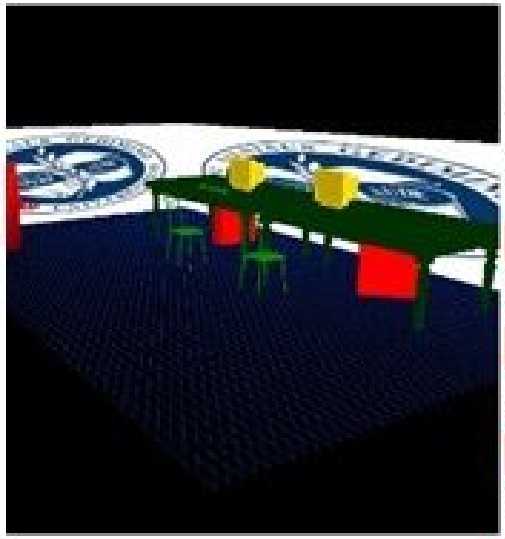
Atskaitos taškas | Nauja rizika | Rizikos nenustatyta | Rizika sumažėjo | Rizika išliko tokia pati | Rizika padidėjo

Nr.	Grėsmės šaltinis | Grėsmė | Pažeidžiamumas	Rizikos vertinimas pagal 2015-12-13 planą Nr. 1		Rizikos vertinimas pagal 2016-01-01 planą Nr. 2		Rizikos vertinimas pagal 2016-05-27 planą Nr. 3	
		Pokytis	Rizika	Pokytis	Rizika	Pokytis	Rizika
1.	Žmogaus / tyčiniai Atsisakymo aptarnauti ataka Paskirstyta atsisakymo aptarnauti ataka **Bus užkištas tinklo mazgas ir neprieinamos paslaugos internetu.**	▶	Maža (1.0)	↑	Didelė (100.0)	↓	Maža (5.0)
		Kompiuterinė įranga (1.0), Ryšio įranga (1.0), Kompiuteris (1.0), Spausdintuvas (1.0), Serveris (1.0), Monitorius (1.0), Nešiojamas kompiuteris (1.0), Klaviatūra (1.0), Pelė (1.0), LENOVO ThinkCentre M58e (1.0), LENOVO mouse (1.0), LENOVO keyboard (1.0), LENOVO ThinkCentre M73 (1.0), DELL Inspiron 15.6" Touch-Screen Laptop (1.0),		Kompiuterinė įranga (5.0), Ryšio įranga (5.0), Kompiuteris (5.0), Spausdintuvas (5.0), Serveris (5.0), Monitorius (5.0), Nešiojamas kompiuteris (5.0), Klaviatūra (5.0), Pelė (5.0), Skaitytuvas (5.0), LENOVO ThinkCentre M58e (100.0), LENOVO mouse (1.0), LENOVO keyboard (1.0), LENOVO ThinkCentre M73 (50.0), DELL Inspiron 15.6" Touch-Screen Laptop (5.0),		Kompiuterinė įranga (5.0), Kompiuteris (5.0), Spausdintuvas (5.0), Serveris (5.0), Monitorius (5.0), Nešiojamas kompiuteris (5.0), Klaviatūra (5.0), Pelė (5.0), Skaitytuvas (5.0), LENOVO ThinkCentre M58e (5.0), LENOVO mouse (5.0), LENOVO keyboard (5.0), LENOVO ThinkCentre M73 (5.0), DELL Inspiron 15.6" Touch-Screen Laptop (5.0),	

Detalūs kylančių grėsmių ir rizikos pokyčių duomenys

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Grėsmių vizualizavimo metodo įgyvendinimas (8/8)



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETO

INVENTORINĖ RIZIKOS VALDYMO

ATASKAITA

Atliko: Paulius Narkevičius

Data: 2016-01-01

Lapai: 29

Grėsmės tikimybė	Grėsmės žala	Rizika
Didelė	Didelė	Didelė
1.0	100.0	1.0 * 100.0 = 100.0
Didelė	Didelė	Didelė
1.0	100.0	1.0 * 100.0 = 100.0
Didelė	Didelė	Didelė
1.0	100.0	1.0 * 100.0 = 100.0
Didelė	Didelė	Didelė
1.0	100.0	1.0 * 100.0 = 100.0
Didelė	Didelė	Didelė
1.0	100.0	1.0 * 100.0 = 100.0
Didelė	Vidutinė	Vidutinė
1.0	50.0	1.0 * 50.0 = 50.0
Didelė	Vidutinė	Vidutinė

Rizikos valdymo ataskaitų formavimas PDF formatu

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Naujumas ir aktualumas

- Vizualizacija dar nėra plačiai naudojama saugos sprendimuose siekiant apibrėžti turimų vertybių geolokaciją ir joms kylančių grėsmių ir rizikos laipsnį;
- Automatizuojamas įstaigos vertybių administravimas ir joms kylančių grėsmių ir rizikos valdymo procesas;
- Galimybė su informacijos saugumu susijusią informaciją pateikti grafine forma;
- Galimybė trimatę grafiką naudoti internete ar intraneto tinkle, o prieigai naudoti tik interneto naršyklę be jokių papildomų įskiepių ar papildinių;
- Greitai nustatyti organizacijos kritinius taškus.

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Išvados

- Grėsmių vizualizacijos sprendimai dažniausiai naudoja spalvų skalę siekiant išskirti grėsmės kritiškumo dydį ir atkreipti dėmesį į pačias pavojingiausias grėsmes, kurias privaloma mažinti siekiant apsaugoti savo vertybes;
- Grėsmių vizualizacija sprendžia informacijos saugos suvaldymo problemą ir apsaugoti turimas vertybes nuo kylančių išorinių ir vidinių grėsmių, ir atitinkamai padėti išsirinkti tinkamas kontrpriemones;
- Grėsmių vizualizacijos prototipas pagerina informacijos saugos grėsmių vertinimą ir leidžia kritiškiau vertinti ir atskirti vertybes;
- Grėsmių vizualizacijos taikymui ir įstaigos vertybių rodiklių valdymui geriausiai tinka panaudoti vaidmenimis grindžiamą prieigos kontrolę siekiant atskirti naudotojų vaidmenis ir NIST rizikos valdymo metodologiją siekiant užtikrinti informacijos saugos valdymą.

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Tezių aprobavimas

- Svarbiausieji darbo rezultatai pagal tezių tematiką pateikti 2015 m. balandžio 16 dienos pranešime, skaitytame Vilniaus Gedimino technikos universitete vykusioje 18-osios Lietuvos jaunųjų mokslininkų konferencijoje „Mokslas – Lietuvos ateitis“.

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Klausimai

Ačiū už dėmesį.

(Wolf making his dinner out of Shoes)