MYKOLO ROMERIO UNIVERSITETAS

VERSLO IR MEDIJŲ MOKYKLA

(BUSINESS AND MEDIA SCHOOL (BMS))

ŽILVINAS ROPĖ

(Kibernetinio saugumo valdymas)

ORGANIZACIJOS X KIBERNETINĖS ERDVĖS GYNYBA

Magistro baigiamasis darbas

Darbo vadovas –

prof. dr. Darius Štitilis

Vilnius, 2015

TURINYS

SANTRUMPOS 5
ĮVADAS 6
1. KIBERNETINĖS ERDVĖS GYNYBOS TEORINIAI ASPEKTAI 9
1.1. MOKSLINĖS LITERATŪROS APŽVALGA 9
1.2. KIBERNETINĖS ERDVĖS GYNYBOS SAMPRATA 15
1.3. ORGANIZACIJŲ KIBERNETINĖS ERDVĖS GRĖSMIŲ VEKTORIAI 20
1.4. GRĖSMĖS ORGANIZACIJOMS KIBERNETINĖJE ERDVĖJE 25
1.5. PIRMOS DALIES APIBENDRINIMAS 33
2. MAŽŲ IR VIDUTINIŲ ORGANIZACIJŲ KIBERNETINĖS ERDVĖS GYNYBOS ORGANIZAVIMO PRINCIPAI 35
2.1. PAGRINDINIAI KIBERNETINĖS GYNYBOS ELEMENTAI 35
2.2. *HIPAA* SAUGUMO TAISYKLIŲ REIKALAVIMAI 40
2.3. *PCI DSS* DUOMENŲ SAUGUMO STANDARTAS 43
2.4. *20 CSC* KRITINIŲ SAUGUMO REIKALAVIMŲ 45
2.5. ANTROS DALIES APIBENDRINIMAS 48
3. ORGANIZACIJOS X KIBERNETINĖS ERDVĖS GYNYBOS TYRIMAS 50
3.1. ORGANIZACIJOS X TYRIMŲ METODOLOGIJA 50
3.2. ORGANIZACIJOS X ESAMOS KIBERNETINĖS ERDVĖS GYNYBOS PADĖTIES ANALIZĖ 55
3.3. KIBERNETINĖS ERDVĖS GYNYBOS STIPRINIMO REKOMENDACIJOS ORGANIZACIJAI X 60
3.4. KIBERNETINĖS GYNYBOS STIPRINIMO PRIEMONIŲ EFEKTYVUMO VERTINIMAS 62
IŠVADOS 67
REKOMENDACIJOS 69
LITERATŪROS SĄRAŠAS 70
SANTRAUKA 77
SUMMARY 78
PRIEDAI 79

PAVEIKSLĖLIŲ SĄRAŠAS

1 pav. Programinės įrangos pažeidžiamumų kainos.

2 pav. CIA triados modelis

3 pav. Suklastotas *Swedbank* laiškas

4 pav. Suklastota *Swedbank* svetainė

5 pav. CERT-LT 2014 m. gautų ir siųstų pranešimų tipai

6 pav. Botnet tinkluose aptiktų Lietuvos *IP* adresų kiekis

7 pav. Pranešimas apie *CBT-Locker* užšifruotus duomenis

8 pav. Microsoft kompanijos „gynybos į gylį“ modelis

9 pav. Keturi rizikų valdymo procesai

10 pav. Suklastotas laiškas, naudotas eksperimente Nr. 1

11 pav. Suklastotas laiškas, naudotas eksperimente Nr. 2

12 pav. EICAR AV PĮ testavimo kodas

13 pav. Organizacijos X saugumo naujinimų ataskaita

14 pav. Organizacijos X operacinės sistemos pažeidžiamumai

15 pav. Organizacijos X kiti sistemos pažeidžiamumai

16 pav. Ugniasienės vartotojo autentifikavimo langas

17 pav. AV PĮ ESET pranešimas apie pašalintą *EICAR* rinkmeną

18 pav. Pranešimas apie blokuojamą ***.exe** rinkmeną.

19 pav. PĮ naujinimo ataskaita

20 pav. Pranešimas apie blokuotą prieigą prie **facebook.com** portalo.

LENTELIŲ SĄRAŠAS

1 lentelė. Pažeidžiami protokolai, naudojami DDOS atakoms vykdyti.

2 lentelė. PCI DSS, HIPAA ir *20 CSC* metodikų palyginimas

3 lentelė. Organizacijai X rekomenduojamos kibernetinės gynybos priemonės

SANTRUMPOS

RRT – Ryšių reguliavimo tarnyba;

CERT – reagavimo į kompiuterių incidentus tarnyba;

CERT-LT – Lietuvos RRT reagavimo į kompiuterių incidentus padalinys;

SANS – (angl. The SysAdmin, Audit, Network, and Security Institute) Sistemų administratorių, audito, tinklų ir saugumo institutas;

PCI DSS – (angl. Payment Card Industry Data Security Standard) Mokėjimo kortelių pramonės duomenų saugumo standartas;

HIPAA – (angl. Health Insurance Portability and Accountability Act) Sveikatos draudimo mobilumo ir apskaitos įstatymas;

EICAR – (angl. The European Institute for Computer Anti-Virus Research) Europos kompiuterių antivirusų tyrimų institutas;

IT – informacinės technologijos;

PĮ – programinė įranga;

AV PĮ – antivirusinė programinė įranga;

APT – (angl. Advanced Persistent Threat) pažangi patvari grėsmė;

DDOS – (angl Distributed Denial of Service) paskirstytoji paslaugos trikdymo paslauga;

IP adresas – (angl. Internet Protocol Address) Interneto protokolo adresas;

MAC adresas – (angl. Media Access Control Address) fizinis tinklo plokštės adresas;

IoT – (angl. Internet of Things) daiktų Internetas;

USB – (angl. Universial Serial Bus) universalioji nuoseklioji jungtis;

CIA – (angl. Confidentiality, Integrity, Availability) Konfidencialumas, vientisumas, pasiekiamumas;

PIN – (angl. Personal Identification Number) Asmeninis identifikavimo numeris;

SIM – (angl. Subscriber Identification Module) Abonento identifikavimo modulis;

WSUS – (angl. Windows Server Update Services) Windows serverio naujinimų tarnyba;

EMET – (angl. The Enhanced Mitigation Experience Toolkit) Papildomos *PĮ* apsaugos priemonių rinkinys;

MBSA – (angl. Microsoft Baseline Security Analyzer) *Microsoft* bazinis saugumo analizavimo įrankis.

ĮVADAS

XXI amžiaus pradžioje stebimas nuolatinis įtampos augimas kibernetinėje erdvėje. 2007 m. pasaulinio masto kibernetinės atakos buvo nukreiptos prieš Estijos vyriausybinius ir žiniasklaidos tinklalapius, taip pat buvo sutrikdytas elektroninės bankininkystės bei interneto paslaugų teikimas. Tai paskatino Estiją parodyti iniciatyvą 2008-05-14 įsteigiant NATO Kibernetinio saugumo kompetencijų centrą Taline. Tų pačių metų rugpjūtį vykusio Rusijos ir Gruzijos ginkluoto konflikto metu lygiagrečiai buvo puolama Gruzijos kibernetinė erdvė. Abiem atvejais buvo vykdomos paskirstytos paslaugos trikdymo DDOS atakos, kuriose buvo naudojami užkrėsti ir įtraukti į *botnet* tinklus kompiuteriai iš viso pasaulio. Toks atakos maskavimo būdas puolėjui suteikia galimybę išlaikyti anonimiškumą, o gynyba apsunkinama, nes nėra tikslaus atakos šaltinio.

Stuxnet ataka, aptikta 2010 metais, taip pat prisidėjo prie įtampos eskalavimo kibernetinėje erdvėje. *Stuxnet* buvo sukurtas Irano branduolinės programos vystymo stabdymui ir įvardinamas kaip neprecedentinis kibernetinis ginklas, sukurtas fiziniam įrangos sunaikinimui – atakos metu buvo sugadintas penktadalis Irano branduolinių centrifugų.

Įtampa neslūgsta ir pastaraisiais metais, 2014-ieji pažymėti kibernetinėmis atakomis nukreiptomis prieš kompaniją *Sony*, JAV banką *JPMorgan Chase & Co*, Estijos URM, NATO svetaines, 2015 metų pradžioje po teroristų išpuolio Paryžiuje kibernetinės atakos taikiniais tapo JAV kariuomenės paskyras socialiniuose tinkluose *Twitter* ir *YouTube* (Lamothe, 2015).

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio *CERT-LT* duomenimis, nuo 2006 m. (registruoti 93) iki 2014 m. (registruoti 36 136) incidentų skaičius išaugo daugiau kaip 388 kartus. *CERT-LT* išskiria keletą incidentų tipų: virusai, užvaldymas, klastojimas, manipuliacija, paslaugos trikdymai ir kt. Atakų taikiniais tampa tiek pavieniai fiziniai asmenys, tiek privataus sektoriaus organizacijos ir valstybės institucijos. Žymesnėmis atakomis Lietuvos kibernetinėje erdvėje galime įvardinti 2012 m. įvykusią paslaugos trikdymo ataką prieš Lietuvos banko sistemas bei 2013 m. DDOS ataką prieš *Delfi.lt* portalą.

Temos aktualumas. Kibernetinių incidentų dinamika rodo, kad kibernetinės erdvės patrauklumas neteisėtai veiklai vykdyti nuolat didėja. Kibernetinių atakų taikiniais tampa ne tik pavieniai asmenys, bet ir organizacijos ar net valstybės. 2007 m. vykdytoje kibernetinėje atakoje prieš Estiją buvo panaudotas *botnet* tinklas, kurį sudarė apytikriai 85 tūkst. užkrėstų kompiuterių iš 178 valstybių (Tsagourias, 2014). Tai parodo problemos mąstą bei leidžia daryti prielaidą, kad tiek viešojo, tiek privataus sektoriaus organizacijos yra patrauklus taikinys kibernetiniams nusikaltėliams, suteikiantis galimybę vykdyti nusikalstamas veikas maksimaliai išnaudojant anonimiškumo faktorių.

Pateikti faktai suponuoja idėją, kad organizacijoms kibernetinėje erdvėje kyla realios grėsmės, tuo pačiu aktuali tampa organizacijos kibernetinės gynybos problematika, kurią sąlygoja tiek išorinė aplinka (teisinė bazė, tarptautiniai standartai, paslaugų tiekėjai ir kt.), tiek vidinė organizacijos aplinka (IT vadybos metodikų taikymas, IT personalo kvalifikacija bei kaita, riboti finansiniai ištekliai ir kt.). Kibernetiniai incidentai organizacijoms kelia daug įvairių pavojų, tokių kaip finansiniai nuostoliai, intelektinės nuosavybės vagystės, veiklos tęstinumo praradimas, žala reputacijai, partnerių ir klientų pasitikėjimo praradimas.

Kibernetinės gynybos priemonių įdiegimas reikalauja iš organizacijų papildomų išteklių: žmogiškųjų, finansinių, žinių ir pan. Ribotų kibernetinės gynybos išteklių problematika ypač aktuali mažoms ir vidutinėms organizacijoms, kurių veikla nėra tiesiogiai susijusi su informacinėmis technologijomis. Organizacijos, kurių veikla tiesiogiai susijusi su IT turi daugiau privalumų, tokių kaip vidiniai žmogiškieji ištekliai arba stambiųjų tarptautinių veiklos partnerių tokių kaip *Microsoft, Cisco, Symantec, McAfee* kompanijos ir pan. kompetencijos bei žinios. Temos aktualumą taip pat didina greitai plintanti daiktų Interneto technologija (IoT), taip pat debesų kompiuterija (angl. Cloud Computing), kuri spartina organizacijų informacijos išteklių perkėlimą į elektroninę erdvę, tačiau tuo pačiu yra stebima incidentų kibernetinėje erdvėje augimo dinamika, kas didina grėsmes minėtiems ištekliams.

Problema – Organizacijoms kyla efektyvių kibernetinės gynybos priemonių pasirinkimo iššūkiai. Nepaisant to, kad yra sukurta daugybė technologinių kibernetinio saugumo sprendimų, standartų ir metodikų, organizacijoms, ypač mažoms ir vidutinėms, kurių veikla nėra tiesiogiai susijusi su IT, kyla klausimų kokias priemones pasirinkti, kokius aspektus įvertinti, kuriant efektyvias kibernetinės gynybos sistemas.

Magistro baigiamojo darbo temos ištirtumas: organizacijų kibernetinės erdvės gynybos problematika Lietuvoje nėra ištyrinėta. Artimiausiuose darbuose yra nagrinėjami informacijos saugos aspektai. Yra tyrinėta informacijos saugumo valdymo viešojo sektoriaus organizacijose problematika (Kranauskienė, 2004). Išanalizuota informacijos saugos užtikrinimo problematika kuriant elektroninės valdžios infrastruktūrą, išnagrinėti saugios sistemos kūrimo praktiniai bei teoriniai aspektai (Damkus, 2006). Išnagrinėta informacijos saugos problema viešajame ir privačiajame sektoriuje bei palygintas informacijos apsaugos lygis viešosiose ir privačiose organizacijose (Selskaitė, 2008).

Tyrimo objektas – Organizacijos X kibernetinės erdvės gynybos sistema.

Magistro baigiamojo darbo tikslas – ištirti vidutinio dydžio organizacijos, kurios veikla nėra tiesiogiai susijusi su informacinėmis technologijomis, pasirengimą gintis nuo grėsmių kylančių kibernetinėje erdvėje, kad nustatyti priemones efektyvios gynybos sistemos sukūrimui.

Tikslui pasiekti keliami **uždaviniai**:

1. Išnagrinėti grėsmes kylančias organizacijoms kibernetinėje erdvėje ir identifikuoti kibernetinių grėsmių vektorius organizacijose;
2. Nustatyti organizacijų kibernetinės erdvės gynybos organizavimo principus;
3. Ištirti organizacijos pasirengimą kibernetinės erdvės gynybai;
4. Pateikti organizacijai siūlymus dėl priemonių efektyviam kibernetinės erdvės gynybos organizavimui.

Magistro baigiamajame darbe keliama **hipotezė**, kad mažo ir vidutinio dydžio organizacijos kibernetinės erdvės gynybos sistemoje silpniausia grandis yra žmonės, todėl kyla grėsmė, kad išnaudojant žmogiškąjį faktorių per socialinės inžinerijos atakas, organizacija taps kibernetinių atakų taikiniu ir/arba gali būti panaudota kaip placdarmas vykdyti kibernetines atakas.

Ginamasis teiginys – holistinio požiūrio į kibernetinę gynybą taikymas padeda organizacijoms sukurti patikimas kibernetinės gynybos sistemas.

Tyrimo subjektas – viešojo sektoriaus *Organizacija X* (organizacija autoriui yra žinoma). Pasirinkimas sąlygotas tuo, kad organizacija yra vidutinio dydžio ir jos veikla nėra tiesiogiai susijusi su informacinėmis technologijomis.

Tyrimo metodika. Kibernetinės erdvės gynybos tyrimas yra sudėtingas procesas, kuris kelia aukštus reikalavimus tyrėjo kompetencijai. Rengdamas magistro baigiamąjį darbą, autorius naudojo teorinius ir empirinius tyrimo metodus. Teoriniame tyrime buvo vykdoma dokumentų analizė, kurios metu autorius tyrė mokslinės literatūros šaltinius bei norminius dokumentus, kad atskleistų svarbius tiriamos problemos aspektus. Informacijos buvo ieškoma mokslo žurnalų ir kitų mokslo leidinių duomenų bazėse, tokiose kaip *EBSCO Publishing*, *Oxford Journals, Cambridge Journals Online, Elektroninių tezių ir disertacijų informacinė sistemoje (ETD IS)* ir kituose informaciniuose ištekliuose. Empiriniai tyrimai buvo vykdomi pasitelkiant kiek įmanoma patikimus empirinius duomenis. Autorius rengdamas magistro baigiamąjį darbą atliko elektroninėje erdvėje kilusių incidentų analizę, kad identifikuoti pavojingiausias kibernetines grėsmes organizacijoms, o taip pat apklausė organizacijos darbuotojus, kad nustatyti organizacijos kibernetinės erdvės gynybos sistemos padėtį, ir kad padidinti tyrimo patikimumą, vykdė organizacijos kibernetinės erdvės stebėjimą bei atliko keturis eksperimentus.

Darbo struktūra. Magistro baigiamąjį darbą sudaro įvadas, dėstomoji, tiriamoji ir baigiamoji dalys. Dėstomojoje dalyje apžvelgiama mokslinė literatūra, nagrinėjami kibernetinės erdvės gynybos teoriniai aspektai bei analizuojami mažų ir vidutinių organizacijų kibernetinės erdvės gynybos organizavimo principai. Tiriamojoje dalyje aprašoma tyrimo metodologija, aptariami tyrimo metu gauti rezultatai. Baigiamojoje dalyje pateikiamos išvados ir rekomendacijos.

1. KIBERNETINĖS ERDVĖS GYNYBOS TEORINIAI ASPEKTAI

Autoriaus nuomone, prieš pradedant nagrinėti kibernetinės gynybos klausimus, svarbu apibrėžti kibernetinės erdvės sąvoką ir kibernetinės gynybos sampratą, išsiaiškinti kibernetinių grėsmių tendencijas bei nustatyti kibernetinių grėsmių vektorius organizacijos kontekste. Šioje darbo dalyje autorius nagrinėja organizacijos kibernetinės erdvės gynybos teorinius aspektus.

1.1. MOKSLINĖS LITERATŪROS APŽVALGA

Lietuvoje nėra pakankamai išplėtota kibernetinės gynybos tematika, tačiau, neskaitant KTU išleistų mokomųjų knygų „Informacijos saugos vadyba“ ir „Elektroninės valdžios sauga“, galima rasti kitų autorių darbų, kuriuose nagrinėjama kibernetinio saugumo problematika. Saugios kibernetinės erdvės įgyvendinimo problematika nagrinėjama straipsnyje „Kibernetinė sauga ir Lietuva“ (Japertas, 2010). Straipsnyje mokslininkas teigia, kad kibernetinė sauga yra sudėtingas uždavinys, kurį įtakoja politiniai, finansiniai, struktūriniai ir personaliniai aspektai. Saugios kibernetinės erdvės įgyvendinimas reikalauja bendrų pastangų ne tik iš aukščiausių valstybės pareigūnų ir organizacijų, bet ir iš atskirų ūkinių subjektų koordinuojant veiksmus kibernetinio saugumo užtikrinime. Pažymima, kad kibernetinės erdvės saugumo įgyvendinime būtinas veiksmų koordinavimas ne tik šalies viduje, bet ypatingai svarbu veiksmus koordinuoti užsienio valstybių ir tarptautinių organizacijų partneriais. Pasak mokslininko, rengiantis kibernetinės erdvės gynybai, svarbu nuspręsti ką turime ginti, kodėl turime ginti, nuo ko turime ginti ir kaip turime ginti.

Moksliniame straipsnyje „Elektroninės erdvės saugumo ekonominiai aspektai“ elektroninės erdvės saugumo problemos svarstomos per elektroninės erdvės saugumo ekonomikos prizmę, nagrinėjamas ekonominis pagrindas investicijų dydžiui bei investavimo krypčių sprendimams (Amilevičius, 2012).

Atliktas kibernetinio saugumo teisinio reguliavimo tyrimas, kuriame buvo analizuojamos bei lyginamos Europos Sąjungos, Jungtinės Karalystės, Vokietijos ir Prancūzijos kibernetinio saugumo strategijos ir Lietuvos kibernetinio saugumo programa (Štitilis, 2013). Pastaroji vertintina kaip teigiamas žingsnis reglamentuojant kibernetinį saugumą, tačiau yra įvardinama daug jos trūkumų, vienas jų tai, kad programoje nėra numatyta išsami ir sisteminė kibernetinės gynybos politika, neišskirti prioritetai saugant kritinę infrastruktūrą nuo kibernetinių atakų, nenustatyti institucijų ir privataus sektoriaus veiksmai kibernetinių atakų atveju, nėra padalintos institucijų funkcijos ir atsakomybės, todėl šis trūkumas turi būti kaip įmanoma skubiau pašalintas.

Kibernetinės gynybos tematika Lietuvos mokslinėje literatūroje sudaro neužpildytą nišą, todėl magistro baigiamojo darbo autorius medžiagos paiešką tęsė užsienio literatūroje. Mokslininkų

grupė iš Karnegio Universiteto, Programinės įrangos inžinerijos instituto parengė dokumentą, kuriame pateikiamos gairės kaip formuoti ir valdyti kompiuterių saugumo incidentų reagavimo komandas (West-Brown, et al, 2003). Šis dokumentas padeda organizacijoms apibrėžti ir dokumentuoti kompiuterių saugumo incidentų reagavimo tarnybos, kuri yra komandos pagrindas, pobūdį bei apimtį. Dokumente aiškinamos tarnybos funkcijos ir kaip jos siejasi, taip pat pateikiami įrankiai, procedūros ir rolės būtinos tarnybos realizavimui. Darbe yra išnagrinėta kaip kompiuterių saugumo incidentų reagavimo komandos bendradarbiauja su kitomis organizacijomis ir kaip yra tvarkoma jautri informacija. Taip pat yra apžvelgti operaciniai ir techniniai iššūkiai, tokie kaip įranga, saugumas ir personalo formavimas. Šis dokumentas yra sukurtas kaip vertingas informacijos šaltinis tiek naujai formuojamoms komandoms, tiek esamoms komandoms, kurių paslaugos, politikos ir procedūros nėra aiškiai apibrėžtos arba dokumentuotos.

Microsoft kompanija savo veikloje daug dėmesio skiria mažom ir vidutinėm organizacijoms, yra sukurta specializuotų produktų, tokių kaip operacinė sistema, pritaikyta mažo ir vidutinio verslo poreikiams, *Windows Small Bussiness Server*. Kompanija taip pat daug dėmesio skiria edukacijai saugumo srityje, yra išleista nemažai publikacijų, pavyzdžiui 2006 m. išleido du leidinius skirtus vidutinio verslo saugumui, viename jų pateikiama susisteminta informacija apie strategijas, taikomas valdant kenkimo programinės įrangos rizikas, o kitas yra vadovą kaip apsaugoti organizacijos narius nuo socialinės inžinerijos grėsmių.

JAV Nacionalinis standartų ir technologijų institutas išleido standartą *SP 800-83,* kuriame pateikiamos rekomendacijos organizacijoms dėl priemonių, skirtų pagerinti incidentų, susijusių su kenkimo programine įranga, prevenciją. Dokumentas taip pat pateikia išsamias rekomendacijas kaip stiprinti esamus incidentų reagavimo pajėgumus organizacijoje, kad ji būtų geriau pasirengusi valdyti dėl kenkimo programinės įrangos kilusius incidentus. Rekomendacijose sprendžiami klausimai apimantys skirtingų formų kenkimo programas, įskaitant virusus, kirminus, trojos arklius, mobiliuosius kenkimo kodus, mišrias atakas, šnipinėjimo slapukus bei specializuotas kibernetinio puolimo priemones. Dokumente išanalizuoti įvairūs kenkimo kodo perdavimo mechanizmai, įskaitant tokias tinklo paslaugas kaip pvz.: elektroninis paštas, interneto naršymas, dalijimasis kompiuterinėmis rinkmenomis ir kt. bei duomenų laikmenos. Įgyvendintos šios rekomendacijos leis organizacijai efektyviau ir veiksmingiau reaguoti į kenkimo programinės įrangos sukeltus incidentus. 2014 m. buvo publikuota kritinės infrastruktūros kibernetinio saugumo stiprinimo sistema, kuri suteikia galimybę organizacijoms, priklausomai nuo jų dydžio ir kibernetinio saugumo rizikos, pritaikyti rizikos valdymo principus ir geriausias praktikas stiprinant kritinės infrastruktūros kibernetinį saugumą ir atsparumą. Dokumentas į vieningą struktūrą surinko kibernetinio saugumo metodus, paremtus standartais, gairėmis ir geriausiomis praktikomis. Dėl naudojamų nuorodų į

pasaulinius kibernetinio saugumo standartus, dokumentas gali būti taikomas kaip tarptautinio bendradarbiavimo stiprinant kritinės svarbos infrastruktūros objektų kibernetinį saugumą modelis.

Ekspertai savo darbe perteikia ne tik savo techninę patirtį, bet ir nagrinėja kaip pažeidžiamumo valdymą suderinti su verslo valdymu (Manzuik, et al, 2007). Jų teigimu nors yra svarbu žinoti visus naujausius įsilaužimo metodus, tačiau šios žinios yra vertingos tik tada, jei įsibrovėlių keliamos grėsmės susiejamos su jų rizika organizacijai. Darbe teigiama, kad pataisymų, konfigūracijų ir saugumo valdymas evoliucionavo iš vienos disciplinos, tačiau dažnai konkuruoja tarpusavyje, taip kyla šiandieninė IT problema – pažeidžiamumo valdymas.

Atliktas aktyvios kibernetinės gynybos taikymo tyrimas (Wong, 2011), kuriame teigiama, kad didėjanti priklausomybė nuo interneto daro kibernetines atakas patraukliomis dėl galimybės nuslėpti įsibrovėlio tapatybę. Nepaisant to fakto, kad vyriausybės visame pasaulyje deda didžiules pastangas stiprinant nacionalinę kibernetinę gynybą, tačiau naudojamos pasyvios gynybinės priemonės nėra pakankamos atremti šiuolaikines grėsmes. Darbe tyrinėjamos galimybės taikyti aktyvios kibernetinės gynybos priemones, kad sustiprinti kibernetinę gynybą valstybiniu lygiu. Teigiama, kad aktyvioje gynyboje reikia naudoti puolamuosius veiksmus, tokius kaip įsilaužimas į įsibrovėlio sistemas ar prevencinis įsibrovimas. Šiame darbe tyrinėjamos aktyvios kibernetinės gynybos topologijos ir nagrinėjama kaip toks požiūris gali sustiprinti valstybės kibernetinės gynybos pozicijas.

Sjouwerman (2011) teigia, kad ne tik rinkų griūtis ir recesija turėjo įtakos verslo klimato atšalimui 2008 m. Amerikos verslas susidūrė su rimta grėsme – elektroniniais nusikaltimais. Jo teigimu mažos ir vidutinės įmonės sunkiai nukentėjo, nuostoliai siekė dešimtis milijonų dolerių, kurie buvo pavogti iš verslo banko sąskaitų. Knygoje nagrinėjamos grėsmės verslui, kylančios kibernetinėje erdvėje, svarbiausiu laikomas klastojimas kaip tam tikros rūšies socialinės inžinerijos ataka, kurios metu naudojamas elektroninis paštas arba internetas. Knygoje analizuojama kaip pavieniai asmenys ir organizacijos gali atpažinti kylantį pavojų, kai naudojamasi internetu, ypač vykdant finansinę veiklą, kokių apsauginių veiksmų pagalba galima apsaugoti organizaciją. Nagrinėjamos rizikos apima jautrios informacijos, prekių ir paslaugų vagystes, intelektinės nuosavybės ir pinigų iš banko sąskaitų praradimus (Sjouwerman, 2011).

„Gray Hat Hacking The Ethical Hacker's Handbook Third Edition" knygoje nagrinėjami etiškųjų įsilaužimų metodai, technologijos, teisiniai bei etiniai aspektai. Knygos autoriai teigia, kad kibernetiniam saugumui užtikrinti būtina išanalizuoti naudojamos infrastruktūros esamus pažeidžiamumus ir pabandyti atlikti įsibrovimo į informacines sistemas bei įrangą testus (Harper, et al, 2011). Saugumo testuotojams siūloma „perimti" įsibrovėlių mąstymą, kad saugumo testavimas būtų kiek įmanoma sėkmingesnis. Knygoje pateikti duomenys rodo, kad saugumo užtikrinimas vien tik antivirusinės programinės įrangos įdiegimu yra neefektyvus, tai yra sąlygota tuo, kad šiuo metu

yra kuriama žymiai rafinuotesnė kenkimo programinė įranga, išnaudojanti sistemose esančias saugumo spragas. Todėl vienintelis efektyvus apsisaugojimo būdas – pažeidžiamumų identifikavimas ir spragų eliminavimas. Knygoje yra apžvelgiami JAV teisės aktai, kuriuos būtina žinoti prieš vykdant įsibrovimų testavimą, taip pat aptariami etiniai aspektai, apimantys testavimo rezultatų informacijos dalinimąsi tarp suinteresuotųjų šalių bei informacijos neviešinimo klausimai.

Kosina savo darbe nagrinėjo kibernetinio karo problematiką, analizavo kibernetines atakas ir jų vykdytojus, atliko *Stuxnet* atakos tyrimą bei įvardino kibernetinių karų istorinius etapus (Kosina, 2012). Pasak jo, iki *Stuxnet* atakos tai yra pirmasis žiniatinklio karas (angl. Web War One), po *Stuxnet* – antrasis kibernetinis karas (angl. Cyber War 2.0).

Knygoje „Cyber Security Policy Guidebook“ pateikta susisteminta kibernetinio saugumo politikų kūrimo ir taikymo patirtis, perimta iš akademinės bendruomenės, verslo ir vyriausybinių organizacijų (Bayuk, et al, 2012). Mokslininkai nagrinėja aktualius organizacinius kibernetinio saugumo politikų formavimo klausimus pasauliniu mastu, analizuojami dabartiniai kibernetinės erdvės saugumo metodai, pateikiami išsamūs aprašymai su nurodytais privalumais ir trūkumais. Gilinamasi į organizacinius politikų įgyvendinimo klausimus, pateikiami konkrečių politikų pasirinkimo teigiamo ir neigiamo poveikio aprašymai.

Knygoje „The Fog of Cyber Defence“ nagrinėjami kibernetinės erdvės, kibernetinio saugumo ir kibernetinio karo klausimai (Rantapelkonen, et al, 2013). Knygoje analizuojamos Šiaurės Europos šalių sąsajos su svarbiu ir tuo pačiu komplikuotu bei miglotu reiškiniu – kibernetiniu saugumu. Tai prideda svarbių perspektyvų į vykstančią diskusiją apie kibernetinį saugumą ir sukuria galimybes stiprinti bendradarbiavimą tarp Šiaurės šalių kibernetinės gynybos srityje. Šios knygos straipsniai prisideda prie diskusijų dėl kibernetinio saugumo poveikio nacionaliniam saugumui. Knygos redaktoriai publikuoja įvairių autorių straipsnius, kuriuose diskutuojamos svarbios temos, įtakojančios kasdieninį gyvenimą. Kiravuo ir Särelä straipsnyje „The Care and Maintenance of Cyberweapons“ teigia, kad kibernetiniai ginklai yra specializuota programinė įranga, kuri yra tikslingai sukurta. Toliau straipsnyje analizuojama tokių ginklų architektūra, jų kūrimo bei panaudojimo aspektai. Hyppönen straipsnyje „The Exploit Marketplace“ analizuoja programinio kodo, skirto išnaudoti operacinių sistemų ir taikomosios programinės įrangos pažeidžiamumus, rinką. Jis teigia, kad toks programinis kodas tapo kibernetinio ginklavimosi pramonės kasdienės prekybos preke. Pasak jo, įvairiose šalyse egzistuoja smulkios įmonės, kurios specializuojasi nulinės dienos[1] pažeidžiamumų paieškoje ir ginklų sukūrimu aptiktų saugumo spragų išnaudojimui. Šios įmonės nesidalina informacija apie aptiktus pažeidžiamumus su

[1] Nulinės dienos pažeidžiamumas (angl. Zero-Day), tai toks atakos tipas, kai išnaudojamas dar plačiai nežinomas pažeidžiamumas, kuriam dar nesukurtas pataisymų rinkinys.

programinės įrangos gamintojais, informacija yra specialiai slepiama, kad gamintojai negalėtų sukurti pataisų.

Denning (2013) nagrinėjo aktyvios kibernetinės gynybos principus. Darbe pateikiamas platesnis požiūris į aktyvią kibernetinę gynybą, kuris lyginamas su aktyvia oro ir priešraketinės gynybos koncepcija. Vietoj aktyvios kibernetinės gynybos būdo, kai bandoma įsilaužti į įsibrovėlio sistemas (angl. Hack Back), šis platesnis aiškinimas skolinasi sąvokas iš aktyviųjų ir pasyviųjų oro ir priešraketinės gynybos koncepcijų, bandant jas pritaikyti elektroninėje erdvėje. Autorė savo darbe siūlo vadovautis tinkamais teisiniais ir etiniais principais, vykdant aktyvią kibernetinę gynybą (Denning, 2013).

Straipsnyje „Failed Cyberdefense“ analizuojamos nepavykusios kibernetinės gynybos nuo priešiškų veiksmų galimos pasekmės aplinkai. Pateikiamos įžvalgos kaip neapginta kritinė kibernetinė infrastruktūra, gali padaryti didelę žalą aplinkai, nagrinėjami galimų kibernetinių atakų prieš hidroelektrinių užtvankas ir cheminės pramonės objektus atvejai (Kallberg ir Burk, 2014).

Knygoje „Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks“ giliai analizuotos realios rizikos kibernetiniam saugumui tiek valstybiniame, tiek verslo sektoriuose, identifikuoti aspektai kurie turi būti įvertinti, kad išlaikyti informacijos vientisumą (MacDonnell, 2014). Knygoje rašoma, kaip verslas ir vyriausybinės organizacijos turi saugoti savo turtą, kad išvengti katastrofiškų padarinių. Knygos autorius teigia, kad vyriausybės ir verslo organizacijos privalo siekti veikti kartu ir protingai, siekiant bendro tikslo – kibernetinio saugumo. Atskleidžiamas problemos mastas ir pateikiamas planas kaip pakeisti kursą, kad geriau valdyti ir saugoti kritinę informaciją.

„Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions“ knygoje sufokusuotas dėmesys į praktinius, kasdieniniame gyvenime reikalingus tinklų, sistemų ir duomenų apsaugojimo nuo kibernetinių grėsmių įgūdžius (Mowbray, 2014). Knygoje perduodama praktinė, pažangi tinklų saugumo patirtis, kuri yra JAV akademinės ir pramoninės grupės *CyberWatchCenter.org* narių labai vertinama. Ši organizacija yra viena iš atsakingų už JAV Nacionalinės kibernetinio saugumo iniciatyvos (angl. The Comprehensive National Cybersecurity Initiative, CNCI) dėl kibernetinio saugumo švietimo programos vystymo. Knygoje daug dėmesio skiriama pažeidžiamumų aptikimui ir įsibrovimo į sistemas testavimui, aptariamos kibernetiniame saugume dažniausiai pasitaikančios klaidos. Trečiame knygos skyriuje pateikiamos įžvalgos apie paprastų vartotojų, smulkaus verslo ir stambių korporacijų kibernetinio saugumo užtikrinimo ypatumus. Knygoje taip pat teigiama, kad būtina rūpintis slaptažodžių pažeidžiamumo mažinimu, išskiriamas elektroninio pašto panaudojimas socialinės inžinerijos tikslais, taip pat perspėjama dėl grėsmių, naudojantis internetine bankininkyste ar vykdant pirkimus internetu, taip pat atkreipiamas dėmesys, kad socialiniai tinklai atakų vykdytojams yra labai svarbūs dėl galimybės rasti informaciją

apie taikinius, pavyzdžiui galima rasti svarbias datas, vardus ir juos panaudoti bandant atspėti slaptažodžius.

„Incident Response & Computer Forensics“ trečiajame knygos leidime kruopščiai nagrinėjami naujausios ir veiksmingiausios reagavimo į kibernetinius incidentus ir kompiuterių skaitmeninės ekspertizės priemonės bei metodai. Knygoje pateikiama informacija, suteikia organizacijai galimybes išvengti problemų, kylančių dėl saugumo pažeidimų, arba sumažinti jų poveikį (Luttgens, et al, 2014). Šį darbą galima laikyti praktiniu vadovu, kuris apima visą reagavimo į incidentus ciklą, įskaitant paruošimą, duomenų rinkimą, duomenų analizę ir atkūrimą. Realių pasaulinių atvejų tyrimai atskleidžia labiausiai klastingiausių išpuolių metodus ir sistemų atkūrimo strategijas.

Eksponentinis elektroninių nusikaltimų augimas per paskutinį dešimtmetį iškėlė daugybę klausimų ir iššūkių teisei ir teisėsaugai (Brenner, 2012). Brenner remdamasi savo, kaip teisininkės, patirtimi ir konkrečių rinkmenų atvejais, identifikuoja įvairių elektroninių nusikaltimų spektrą, įskaitant nusikaltimus, nukreiptus prieš kompiuterius (virusai, kirminai, „trojos arkliai“, kenkimo programinė įranga ir DDOS atakos) ir nusikaltimus, kurių įrankis yra kompiuteris (elektroninis priekabiavimas[2], elektroninis turto prievartavimas[3], elektroninė vagystė[4]). Nušviesdama teisines problemas, būdingas tyrimams elektroninėje erdvėje, ji nagrinėja tiek nacionalines teisėsaugos institucijas, tiek tarptautinį nusikalstamumą. Ji parodo, kaip kibernetinė erdvė griauna funkcinius ir empirinius skirtumus, kurie jau seniai atskyrė nusikalstamumą nuo terorizmo, o terorizmą nuo karo.

Etsebeth (2011) analizuoja labiausiai paplitusias kibernetines grėsmes su kuriomis susiduria organizacijos ir kokius esminius klausimus turi jų vadovybė išspręsti, kad įvertinti potencialų teisinį poveikį saugumo pažeidimų atveju). Pasak mokslininkės šiandien organizacijos saugo didžiulius jautrios, konfidencialios ar slaptos informacijos kiekius savo tinkluose, kuri kibernetinių atakų metu gali būti prarasta. Kadangi dabar kibernetinių nusikaltėlių motyvacija yra pasipelnymas, todėl organizacijoms tenka balansuoti tarp svarbios informacijos saugumo ir jos pasiekiamumo. Organizacijos informacijos ir jos vientisumo apsaugojimo nuo vis didėjančių rizikų ir grėsmių svarba reikalauja, kad organizacijos imtųsi visų reikiamų priemonių informacijai apsaugoti, nes priešingu atveju organizacijai ir/arba jos nariams gali kilti teisinė atsakomybė (Etsebeth, 2011).

Lerner (2014) savo darbe, remdamasis *Microsoft* kompanijos patirtimi, diskutuoja apie viešojo ir privataus sektoriaus bendradarbiavimo aspektus, kovojant su *botnet* tinklais. Darbe

[2] Elektroninis priekabiavimas (angl. Cyberstalking) – nenutrūkstamas elektroninių ryšių naudojimas asmens įbauginimui arba priekabiavimui.
[3] Elektroninis turto prievartavimas (angl. Cyberextortion) – nusikaltimas apimantis tiek pačią kibernetinę ataką, tiek grasinimą ją įvykdyti, su tikslu reikalauti pinigų už jos išvengimą arba vykstančios atakos nutraukimą
[4] Elektroninė vagystė (angl. Cybertheft) – finansinės arba asmeninės informacijos pasisavinimas kompiuterio pagalba su tikslu ją neteisėtai panaudoti.

analizuojamas *botnet* tinklų naudojimas paskirstytųjų paslaugos trikdymo atakų vykdymui, nagrinėjami įvairūs šių atakų tipai bei įvairūs jų prevencijos metodai (Lerner, 2014).

Mokslininkai identifikavo pagrindinius kibernetinės erdvės grėsmių analizės ir perspėjimo pajėgumų požymius bei palygino juos su *US-CERT* tarnybos pajėgumais, kad nustatytų spragas (Catwell ir Norwood, 2009). Jie taip pat nustatė kokie iššūkiai kyla *US-CERT* tarnybai vystant sėkmingus valstybinius kibernetinės erdvės grėsmių analizės ir perspėjimo pajėgumus. Mokslininkai tyrimo eigoje analizavo dokumentus, vykdė įvairių subjektų veiklos stebėjimą bei atliko atsakingų asmenų ir ekspertų apklausas.

Kasmet JAV Gynybos departamentas, siekdamas padidinti savo veiklos efektyvumą, atnaujina savo informacinių technologijų sistemas. Nepaisant to, kad sistemų atnaujinimas daro teigiamą poveikį nacionalinio saugumo interesams, tuo pačiu kyla naujų sistemų grėsmės išnaudojimo pavojus. Dažniausiai grėsmės yra aptinkamos tik po to, kai sistemos jau būna įdiegtos, o jų pašalinimas yra santykinai brangus (Panton, et al, 2014). Mokslininkai pateikia rekomendacijas JAV Gynybos departamentui kaip taikyti ekonominę strategiją, vadinamą pažeidžiamumų rinka (angl. Vulnerability Market), kad sustiprinti informacijos užtikrinimo (angl. Information Assurance) priemones. Abipusis bendradarbiavimas tarp pramonės ir kariuomenės informacijos apsaugos srityje, leistų Gynybos departamentui optimizuoti investicijas į saugumą, apsaugotų svarbią informaciją bei sukurtų efektyvius ir patikimus kovinius pajėgumus.

Išnagrinėti pažangių patvarių grėsmių metodai, taikomi šiuolaikinėse kibernetinės erdvės atakose (Smiraus ir Jasek, 2011). Darbe pateikiami pagrindinių pastarųjų metų kibernetinių atakų, kurios siejamos su *APT*, pavyzdžiai. Mokslininkai ne tik diskutuoja apie *APT* atakų metodologijas, bet ir pateikia savo įžvalgas kaip išvengti *APT* atakų ateityje. Pateikiami pagrindinių saugumo politikų variantai, galintys sustiprinti gynybą ir apsaugoti nuo pažangiųjų patvariųjų grėsmių.

1.2. KIBERNETINĖS ERDVĖS GYNYBOS SAMPRATA

Kibernetinės erdvės gynybos tyrimo pradžioje svarbu nustatyti sąvokas, kuriomis bus operuojama baigiamajame darbe. Visų pirma apibrėšime kas yra kibernetinė erdvė. Darbe (Starrs ir Anderson, 1997) kibernetinę erdvę apibrėžia kaip „pasaulį, sudarytą iš elektroninės informacijos, duomenų ir ryšių tarp šių duomenų. Tai gali būti įvairi informacija, pavyzdžiui kiekybinės rinkmenos moksliniams tyrimams, rinkų transakcijos, interaktyvūs žaidimai, elektroninės bibliotekos, palydoviniai ryšiai, rinkodara ir prekyba Internetu“.

Tuo tarpu (Strate, 1999) pateikia kitokią kibererdvės sampratą, pagal kurią *yra išskiriami trys kibernetinės erdvės lygmenys, pirmasis yra ontologija, kuri apima tokias erdvės sampratas kaip netikra erdvė (angl. Paraspace) arba neerdvė (angl. Nonspace), o taip pat ir kibernetinės erdvės laiko (angl. Cyberspacetime) koncepciją. Antrame lygmenyje yra tokie blokai, kaip pavyzdžiui,*

fizinis konceptualus ir virtualios erdvės suvokimo. Trečiasis lygmuo tai sintezė, apimanti kibernetinės erdvės įvairovę, kaip antai žiniasklaidos erdvė, estetinė erdvė, duomenų erdvė, asmeninė ir socialinė erdvė.

Butler (2013), nagrinėdamas JAV karinių oro pajėgų kibernetinę koncepciją, kibererdvę pateikia kaip „globalią erdvę informacinėje aplinkoje, sudarytoje iš tarpusavyje susijusių informacinių technologijų infrastruktūrų, įskaitant ir Internetą, telekomunikacijų tinklus, kompiuterių sistemas bei integruotus procesorius ir valdiklius“ (Butler, 2013).

Kaip matome sąvokos yra pakankamai skirtingos, o Butler (2013) pateikta traktuotė labiausiai atitinka 2015 sausio 1 d. įsigaliojusiame LR Kibernetinio saugumo įstatyme įtvirtintą kibernetinės erdvės sąvoką, kuri apibrėžiama kaip „aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą“. Toliau savo darbe autorius nusprendė remtis įstatyme įtvirtinta sąvoka.

Kitos dvi svarbios sąvokos kibernetinės erdvės gynybos kontekste yra kibernetinė gynyba ir kibernetinė ataka. Priešingai nei kibernetinės erdvės sąvokos apibrėžimas, šios dvi sąvokos nėra apibrėžtos LR Kibernetinio saugumo įstatyme, nors pačiame įstatyme abi sąvokos yra naudojamos. Kadangi išsamaus kibernetinės gynybos ir kibernetinės atakos sąvokų apibrėžimų autoriui nepavyko rasti nei LR Kibernetinio saugumo įstatyme, nei kituose LR teisės aktuose, todėl autorius apibrėžimų ieškojo LR Karinėje strategijoje ir Lietuvos karinėje doktrinoje (LR Kibernetinio saugumo įstatyme Krašto apsaugos sistema pasirinkta kaip viena svarbiausių institucijų). Nepavykusi paieška, autorių paskatino remtis JAV kariškių naudojamomis sąvokomis. JAV kariškiai išskiria penkias savo veiklos interesų dimensijas: oras, žemė, vanduo, kosmosas ir penktoji – kibernetinė erdvė, kur taikomi tokie patys karinės veiklos principai kaip ir kitose keturiose dimensijose.

- JAV Gynybos departamento „Bendrosios terminologijos operacijoms kibernetinėje erdvėje“ kibernetinė gynyba apibrėžiama kaip *integruotas JAV gynybos departamento arba JAV Vyriausybės kibernetinių pajėgumų ir procesų taikymas elektroninėje erdvėje siekiant išvystyti gebėjimą realiu laiku aptikti, išanalizuoti ir sumažinti grėsmes bei pažeidžiamumus ir pergudrauti priešininkus, siekiant apginti paskirtus tinklus, apsaugoti ypatingos svarbos užduotis ir suteikti laisvę JAV veiksmams. Kibernetinę gynybą sudaro:*

- *aktyvios tinklo operacijos – tai konfigūracijų valdymas, informacijos užtikrinimo priemonės, fizinė sauga ir saugios architektūros dizainas, įsibrovimų aptikimas, ugniasienės, antivirusinių aprašų naujinimas ir galiausiai duomenų šifravimas;*

- *gynybinės kibernetinės kovos – apima karinę apgaulę panaudojant „medaus puodynes“[5] bei kitus veiksmus, ir kenksmingo programinio kodo (angl. Malware), panaudoto priešiško veiksmo metu, nukreipimą, nukenksminimą arba pašalinimą.*
- *gynybinės atsakomosios priemonės* (Joint Terminology for Cyberspace Operations, 2010).

Toks kibernetinės gynybos sąvokos apibrėžimas tinkamas žiūrint iš karinės perspektyvos, todėl autorius siūlo šią sąvoką interpretuoti taip: kibernetinė gynyba, tai technologinių ir organizacinių priemonių komplekso panaudojimas, siekiant apsaugoti kibernetinę erdvę nuo kibernetinių atakų arba sumažinti jų žalingą poveikį.

Tame pačiame dokumente kibernetinė ataka apibrėžiama kaip *priešiškas veiksmas, panaudojant kompiuterį ar susijusius tinklus arba sistemas, ir skirtas suardyti ir/arba sunaikinti priešininko svarbias kibernetines sistemas, įrangą arba funkcijas. Numatomas kibernetinių atakų poveikis nebūtinai apsiriboja tikslinėmis kompiuterinėmis sistemomis arba pačiais duomenimis. Pavyzdžiui, išpuoliai prieš kompiuterines sistemas, kurių paskirtis yra naikinti infrastruktūrą arba trikdyti galimybę keistis duomenis. Kibernetinės atakos gali būti vykdomos išnaudojant tarpines priemones, įskaitant periferinius įrenginius, elektroninius siųstuvus, integruotus kodus ar žmogiškuosius vykdytojus. Kibernetinės atakos aktyvavimas arba poveikio rezultatas gali žymiai skirtis nuo realios atakos pradžios tiek laiko atžvilgiu, tiek geografiškai* (Joint Terminology for Cyberspace Operations, 2010).

Autorius mano, kad tęsiant kibernetinės gynybos nagrinėjimą yra svarbu nubrėžti takoskyrą tarp kibernetinio incidento ir kibernetinės grėsmės sąvokų, nes šiomis sąvokomis dažnai operuojama nagrinėjant kibernetinio saugumo klausimus ir kartais šios sąvokos yra painiojamos.

Kibernetinio incidento sąvoka nustatyta įstatyme (LR Kibernetinio saugumo įstatymas, 2014), kur kibernetinis incidentas apibrėžiamas kaip *įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims*.

Kibernetinės grėsmės sąvokos autoriui teko ieškoti kituose šaltiniuose, nes LR Kibernetinio saugumo įstatyme ši sąvoka neapibrėžta. *ISO 27000* standarte kibernetinė grėsmė apibrėžiama kaip „potenciali nepageidaujamo incidento, kuris gali sukelti žalą sistemai ar organizacijai, priežastis”

[5] Medaus puodynė (angl. Honeypot) yra kompiuterinė sistema, kurios paskirtis yra įvilioti į spąstus kompiuterinius įsibrovėlius, tokiu būdu sudaroma galimybė juos susekti.

(ISO, 2014). Tačiau autorius mano, kad išsamesnė kibernetinės grėsmės sąvoka pateikia *NIST*[6] *800-53* publikacijoje: „Kibernetinė grėsmė – bet kokia aplinkybė arba įvykis, kurių metu gali būti neigiamai įtakota organizacijos veikla (įskaitant misiją, funkcijas, įvaizdį ar reputaciją), organizacijos turtas, asmenys, kitos organizacijos ar valstybės, išnaudojant informacines sistemas per neteisėtos prieigos, sunaikinimo, atskleidimo, informacijos pakeitimo ir/arba paslaugos trikdymą“ (NIST, 2013).

Pagal (Catwell ir Norwood, 2009) „skirtingi kibernetinių grėsmių tipai, kylantys iš skirtingų šaltinių, gali neigiamai paveikti kompiuterius, programinę įrangą, tinklus, organizacijos veiklą, pramonę ar patį Internetą.“ Jie siūlo kibernetines grėsmes skirstyti:

1. Netyčinės grėsmės – gali kilti dėl programinės įrangos naujinimų arba priežiūros procedūrų sukeltų sistemų trikdžių.
2. Tyčinės grėsmės skirstomos:
    2.1. Tikslinės atakos – jas vykdo pavieniai asmenys ar asmenų grupės prieš pasirinktą kibernetinį turtą.
    2.2. Netikslinės atakos – jas sukelia virusai, kirminai arba Internete esanti kenkimo programinė įranga, kuri nėra sukurta konkrečiam taikiniui.

Tam, kad iš pateiktų sąvokų būtų galima nustatyti kibernetinio incidento santykį su kibernetine grėsme autorius daro prielaidą, kad trūksta vieno rišančiojo elemento – pažeidžiamumo sąvokos: „informacinės sistemos, sistemos saugumo procedūrų, vidaus kontrolės ar įgyvendinimo silpnybės, kurios gali būti išnaudotos arba iššaukiamas grėsmės šaltinio“ (NIST, 2013).

Toliau paanalizuokime pažeidžiamumo sampratą, štai (Hypponen, 2013) teigia, kad „pažeidžiamumai yra tiesiog programavimo klaidos (angl. Bug). Klaidos atsiranda todėl, kad programinę įrangą kuria žmonės, o žmonės klysta. Programinės įrangos defektai egzistuoja nuo tada, kai buvo sukurti programuojami kompiuteriai ir jie neišnyks“. Jis pažeidžiamumus siūlo skirstyti *pagal jų išnaudojimo būdą:*

1. Lokalūs pažeidžiamumai – gali būti išnaudoti tik vietinio vartotojo, turinčio fizinę prieigą prie sistemos.

2. Nuotoliniai pažeidžiamumai – gali būti išnaudojimai nuotoliniu būdu per tinklines technologijas.

Jis taip pat išskiria tris pažeidžiamumų tipus pagal jų poveikį sistemoms:

1. Paslaugos trikdymas (angl. Denial of Service) – šio tipo pažeidžiamumo išnaudojimas suteikia galimybę sulėtinti sistemą arba ją išjungti.

2. Teisių eskalavimas (angl. Privilege Escalation) – išnaudojus šio tipo pažeidžiamumus, gaunamos papildomos teisės sistemoje.

[6] NIST – JAV Nacionalinis standartų ir technologijų institutas (angl. National Institute of Standards and Technology)

3. *Kodo vykdymo (angl. Code Execution) – sudaroma galimybė įvykdyti programinį kodą sistemoje* (Hypponen, 2013).

Taip pat pabrėžiama, kad pažeidžiamumų aktualumas labiausiai išaugo kartu su Interneto plėtra. Tuo netruko pasinaudoti organizuoto nusikalstamumo atstovai, „pradėję uždirbti didelius pinigus iš klaviatūros sekimo įrangos (angl. Keylogger), bankų trojos arklių ir išpirkos prašančių (angl. Ransomware) trojos arklių. Kai pinigai tapo svarbiu elementu, naujus pažeidžiamumus išnaudojančių įrankių (angl. Exploit) paklausa sukūrė pogrindinę rinką“ (Hypponen, 2013). Žemiau pateiktame paveikslėlyje galime matyti kokios yra programinės įrangos pažeidžiamumų orientacinės kainos pagal gamintojus.

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Šaltinis: Greenberg, 2012

1 pav. Programinės įrangos pažeidžiamumų kainos

Mokslininkai akcentuoja ir teigiamą pažeidžiamumų rinkos, kuri tapo svarbiu pajamų šaltiniu saugumo tyrėjams ir programišiams, pusę kaip galimybę stiprinti kibernetinį saugumą. Jie išskiria tris pažeidžiamumų rinkos modelius: klaidų iššūkis (angl. Bug Challenge), klaidų premija (angl. Bug Bounty) ir klaidų aukcionas (angl. Bug Auction) (Panton, et al, 2014). Pasak mokslininkų, JAV Gynybos departamentas, reaguodamas į problemos mastą ir galimas pasekmes, kai valstybės remiami ar nepriklausomi programišiai išnaudoja pažeidžiamumus kritinėse sistemose, pasikliauja informacijos užtikrinimo sertifikavimo procesu bei daugiasluoksnės „Gynybos į gylį“ (angl. Defense-in-Depth) koncepcija, kurios pamatinis sluoksnis yra: žmonės, technologijos ir operacijos (Panton, et al, 2014).

Autorius siūlo apjungti kibernetinės grėsmės, pažeidžiamumo ir kibernetinio incidento elementus į vieną loginę visumą – kibernetinė grėsmė, veikdama per pažeidžiamumo elementą sąlygoja kibernetinį incidentą. Todėl autoriaus manymu, pažeidžiamumų valdymas yra svarbus elementas kibernetinės gynybos kontekste. Tai įrodo *Stuxnet* kirminas, kuris išnaudojo net šešis programinės įrangos pažeidžiamumus, o penki jų buvo nulinės dienos pažeidžiamumai (De Falco, 2012).

Dabar galime apžvelgti kokios grėsmės kyla organizacijoms kibernetinėje erdvėje. Teigiama, kad *kiekvienos organizacijos sprendimai yra paremti tikslia ir patikima informacija. Šiandien organizacijos saugo žymią dalį jautrios, konfidencialios ir slaptos informacijos savo kompiuterių*

sistemose ir tinkluose. Todėl darytina išvada, kad bet kas, kas kelia grėsmę organizacijos informaciniam turtui, tas tiesiogiai kelia pavojų organizacijos rezultatyvumui ir efektyvumui (Etsebeth, 2011). Pasak jos organizacijų informacinis turtas yra jautrus įvairių tipų kibernetinėms atakoms ir šie pažeidžiamumai yra susiję su išaugusiu Interneto naudojimu organizacijose. Todėl „organizacijoms tampa svarbu išlaikyti balansą tarp jautrios ir konfidencialios informacijos apsaugos ir šios informacijos prieinamumo suinteresuotosioms šalims“ (Etsebeth, 2011). Ji siūlo organizacijų kibernetines grėsmes klasifikuoti:

1. *Atakos apimančios trikdymą, apsimetinėjimą ir informacijos ir/ar duomenų perėmimą.*
    - 1.1. *Tapatybės vagystė*
    - 1.2. *Pramoninis ir korporatyvinis špionažas*
    - 1.3. *Socialinė inžinerija*
2. *Atakos trikdančios informacijos ir/ar duomenų prieinamumą*
    - 2.1. *Paslaugos trikdymo atakos*
    - 2.2. *Paskirstytosios paslaugos trikdymo atakos*
3. *Kenksmingas mobilus kodas*
    - 3.1. *Virusai*
    - 3.2. *Kirminai*
    - 3.3. *Trojos arkliai*
    - 3.4. *Loginės bombos*
4. *Konkurentai/priešininkai*
    - 4.1. *Išorinės grėsmės*
    - 4.2. *Vidinės grėsmės*
    - 4.3. *Netyčiniai organizacijos narių veiksmai*
    - 4.4. *Tyčiniai organizacijos narių veiksmai*

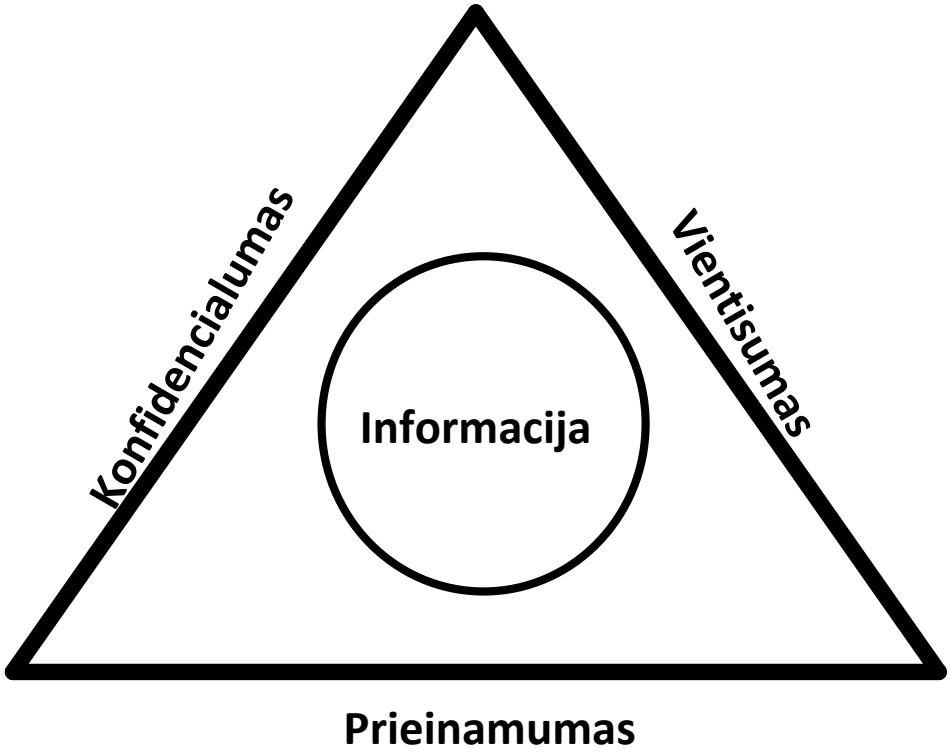
Autorius daro prielaidą, kad visos grėsmės organizacijoms yra pavojingos ir turėtų būti vertinamas jų galimas poveikis, tačiau vienareikšmiškai išskirti kokios grėsmės organizacijoms yra aktualiausios ar pavojingiausios negalima. Tarkim organizacijai, kuri neturi savo interneto puslapio, nėra svarbios paslaugos trikdymo atakos, nukreiptos į interneto prieglobos paslaugos tiekėjus, tuo tarpu kitai organizacijai, kuri užsiima prekyba Internetu, šio tipo atakų neigiamas poveikis yra žymus. Autorius mano, kad norint identifikuoti pavojingiausias grėsmes, reikia atlikti konkrečios organizacijos rizikų analizę.

1.3. ORGANIZACIJŲ KIBERNETINĖS ERDVĖS GRĖSMIŲ VEKTORIAI

Šiame poskyryje aptarsime kokie yra pagrindiniai organizacijos kibernetinės erdvės grėsmių vektoriai. Pradžioje apibrėžkime subjektų, kurie savo veikloje naudoja informacines sistemas,

saugos interesų spektrą arba kitaip tariant informacijos savybes, kurios sąlygoja informacijos vertę subjektui. Informacijos svarba organizacijai yra *didžiausias indėlis, kurį informacija suteikia organizacijoms yra ištekliai, gerinantys organizacijų ir asmenų, kurie dirba jose, efektyvumą. Organizacijos našumas gali būti pagerintas išnaudojant informacinius išteklius, kas leidžia teikti pelningiau aukštesnės kokybės produktus ar paslaugas. Asmeninis našumas gali būti pagerintas teikiant darbuotojams labiau aktualią ir savalaikę informaciją, kuri paremia jų sprendimus* (Chaffey ir Wood, 2004). Taigi galime teigti, kad šiuolaikinėje visuomenėje informacija traktuojama kaip ištekliai, padedantys organizacijoms ar pavieniams asmenims sėkmingai vykdyti savo veiklą.

Informacija yra nematerialiai vertybė, ją gali sudaryti duomenys, informacija ir žinios, turintys vertę informacijos valdytojui. Tačiau ši nematerialiai vertybė turi materialų pagrindą, tai informacijos saugojimo laikmenos, ryšio linijos, kuriomis informacija perduodama, taip pat informacinės sistemos, kuriose ta informacija yra apdorojama. Informacijos saugos savybes apibrėžia informacijos *CIA* (angl. Confidentiality, Integrity, Availability) triados modelis, kuris taikomas *ISO/IEC 27001* standarte, kuriant informacijos saugos valdymo sistemą. Kartais literatūroje galima aptikti šį modelį po *AIC* (angl. Availability, Integrity, Confidentiality) abreviatūra, taip yra todėl, kad JAV *CIA* trumpinys dažniausiai siejamas su centrinės žvalgybos agentūra (angl. Central Intelligence Agency).



Šaltinis: sudaryta pagal Microsoft, 2006

2 pav. CIA triados modelis

CIA triados modelį sudaro trys kertiniai informacijos saugumo principai:

1. Konfidencialumas – užtikrina, kad reikiama informacija bus prieinama tik tiems vartotojams, kuriems yra suteikta prieigos teisė.

2. Vientisumas – užtikrina, kad saugoma, apdorojama ar perduodama informacija nebus pakeista.

3. Prieinamumas – tai galimybė reikiamą informaciją pasiekti reikiamu metu.

Todėl apibendrindami galime teigti, kad *CIA* modelio esmė – prieiti prie tikslios (nepakeistos) informacijos, reikiamu laiku gali tik tas vartotojas, kuris turi tokią teisę.

Tam, kad identifikuoti organizacijos kibernetinės erdvės grėsmių vektorius, autorius siūlo nustatyti, kokie svarbūs elementai dalyvauja organizacijos informacijos valdymo procese. Pradėkime nuo „didžiųjų duomenų“ (angl. Big Data) sampratos, pasak mokslininkų, *kai žmonės girdi „didžiųjų duomenų“ terminą, jie pirmiausiai galvoja apie organizacijos duomenų tvarkymo technologines priemones. Tačiau, „didieji duomenys“ neapsiriboja vien tik duomenimis ir įrankiais, o tai yra kompleksinė sistema sudaryta ne vien tik iš technologijų, bet ir procesų bei žmonių, įtrauktų į duomenų rinkimą, analizę ir naudojimą. Tai tartum simfonija, kur trys pagrindiniai komponentai sudaro „didžiųjų duomenų“ sistemą: technologijos (instrumentai), procesai (natos) ir žmonės (atlikėjai)* (Rankin, et al, 2015). Kitas mokslininkas, analizuodamas Indijos bankų ryšių su klientais valdymo (angl. Customer Relationship Management, CRM) sistemų kūrimo problemas, išskiria žmones, procesus ir technologijas kaip tvirtą pagrindą sėkmingam CRM diegimui (Bihari, 2012).

Išskiriami trys išteklių tipai, reikalingi efektyviam informacijos valdymui, tai yra informacija, technologijos ir žmonės (Chaffey ir Wood, 2004). O štai mokslininkė, apibendrindama informacijos vadybos šiuolaikinėje organizacijoje tyrimą, teigia kad „didžiojoje dalyje ištirtų organizacijų svarbiausias efektyvios informacijos vadybos elementas yra žmonės, taip pat pabrėžiama informacijos ir technologijų svarba.“ (Girnienė, 2012).

Autorius siūlo informaciją vertinti kaip potencialų taikinį, kurį galima pažeisti išnaudojus pažeidžiamumus technologijose, procesuose ir žmonėse. Kitaip tariant, pagrindinės grėsmių kryptys organizacijų kibernetinėje erdvėje yra technologijos, procesai ir žmonės. Pastarąjį vektorių autorius vertina kaip svarbiausią ir mano, kad tai yra sėkmingos organizacijos kibernetinės erdvės gynybos sistemos pamatas.

Nustačius pagrindinę organizacijos kibernetinės erdvės grėsmės kryptį, autorius siūlo panagrinėti kaip ji gali būti išnaudota. Į žmogiškąjį vektorių yra nukreiptos socialinės inžinerijos atakos. Socialinė inžinerija tai „sėkmingi ar nesėkmingi bandymai priversti vieną ar daugiau asmenų atskleisti informaciją arba veikti taip, kad rezultate būtų gauta neteisėta prieiga prie informacinės sistemos, tinklo ar duomenų, neteisėtas naudojimas jų panaudojimas arba neteisėtas

paviešinimas“ (Tipton ir Krause, 2002). O štai (Sjouwerman, 2011) socialinę inžineriją apibrėžia, kaip „veiklą, kurios metu yra bandoma įkalbėti žmones atskleisti informaciją, kurios jie neturėtų atskleisti asmenis, neturintiems teisės disponuoti tokia informacija“.

Socialinė inžinerija įveikia informacijos apsaugą nenaudodama techninių saugumo mechanizmų. Organizacijos dažnai pamiršta, kad kompiuteriai ir technologijos yra tiktai įrankiai, naudojami žmonių. Šių įrankių problema yra ta, kad žmonės turi naudoti, konfigūruoti, diegti ir taikyti juos. Galiausiai, socialinė inžinerija manipuliuoja silpniausia organizacijos grandimi – jos pačios nariais teigia (Etsebeth, 2011). Socialinė inžinerija naudojama tam, kad sukurti pasitikėjimo ryšius, o daugelis žmonių tuos pasitikėjimo ryšius išnaudoja tokiai informacijai, kaip slaptažodžiai ar fizinis patekimas į saugomas zonas, gauti. Šiandieniniuose socialiniuose tinkluose daugybė žmonių dalinasi informacija su žmonėmis, kurių jie gerai nepažįsta ir net niekada nebuvo sutikę (Pastore, 2014).

Socialinės inžinerijos atakos gali būti vykdomos pasitelkiant skirtingus metodus, pvz.: elektroninis paštas, telefonas, šiukšlių paieška, bandymas prasmukti paskui darbuotoją pro duris, „pamestos“ *USB* laikmenos (Stasiukonis, 2006). Socialinės inžinerijos atakos metu stengiamasi išnaudoti žmogaus silpnybes, t. y. baimę, godumą, geranoriškumą ir pan. Todėl klastojimo atakos metu bandoma simuliuoti situacijas, kurios žmones galėtų paskatinti imtis veiksmų, kurių pasėkoje nusikaltėliai pasiektų jiems reikalingus tikslus, pvz.: gautų slaptažodžius, prisijungimo vardus, nukreiptų vartotojus į kenksmingas svetaines ar priverstų juos aktyvuoti kenksmingą kodą savo kompiuteriuose.

Kasdien organizacijų darbuotojai gauna dešimtis ar net šimtus elektroninių laiškų, toks laiškų kiekis sudaro prielaidas, kad vartotojai tiesiog nebespėja atidžiai peržiūrėti kiekvieno laiško, todėl elektroninis paštas yra viena populiariausių priemonių socialinės inžinerijos atakoms vykdyti. Atsiųstas suklastotas laiškas gali atrodyti kaip tikras, normalus laiškas iš patikimo siuntėjo. Žemiau esančiame paveiksle pavyzdys suklastoto *Swedbank* laiško, kuriame yra suklastotas siuntėjo adresas ir pateikta nuoroda į suklastotą svetainę (Sukčiai nusitaikė į Swedbank klientus, 2009).

From: "**AS Hansapank - SwedBank**" < **no-reply@hansapank.ee**Šis el.pašto adresas yra apsaugotas nuo Spam'o, jums reikia įjungti Javaskriptą, kad matytumėte tai >

Date: March 23, 2009 9:02:50 AM GMT+02:00

To: undisclosed-recipients: ;

Subject: AS Hansapank - SwedBank

Dear Valued Customer ,

On the 17th of March 2009 AS Hansapank will change its business name, the new operating name will be Swedbank AS. This move is the last phase in the brand changing process initiated last autumn. In Latvia the bank's new name will be Swedbank AS and in Lithuania "Swedbank" AB.

Until the full changes will be made to our system we will require some personal information of every account holder.

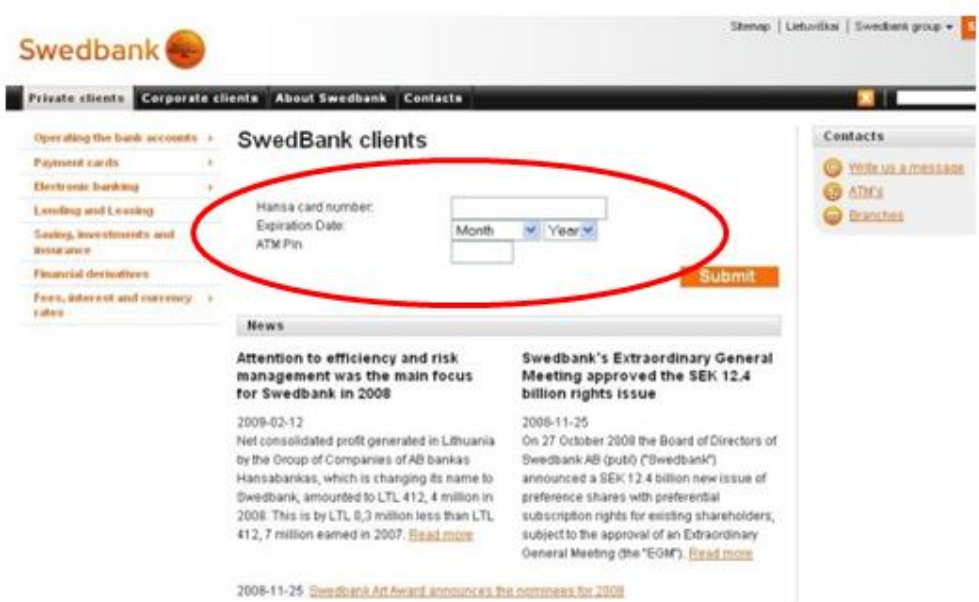
Click here and complete all the required data.

Account suspension will be applied if the necessary data will not be completed.

Šaltinis: technologijos.lt, 2009

3 pav. Suklastotas *Swedbank* laiškas

Vartotojas, paspaudęs nuorodą patenka į suklastotą *Swedbank* svetainę, kurioje prašoma suvesti mokėjimo kortelės numerį, galiojimo pabaigos datą ir *PIN* kodą. Šiuo atveju, atidesnis vartotojas, galėtų įtarti klastotę, nes svetainės adresas yra įtartinas **netuall-54-130.cnt.nerim.net/HansaBank-SwedBank/index.php**.



Šaltinis: technologijos.lt, 2009

4 pav. Suklastota *Swedbank* svetainė

Tačiau kruopščiau parengtose svetainių klastotėse adresas gali būti vizualiai labai panašus į tikrąjį, pvz.: suklastotas adresas **www.svedbank.lt** labai panašus į tikrąjį **www.swedbank.lt**. Suklastoti laiškai gali turėti nuorodas ne tik į suklastotas svetaines, bet ir nuorodas tiesiogiai atsisiųsti kenkimo programinę įrangą.

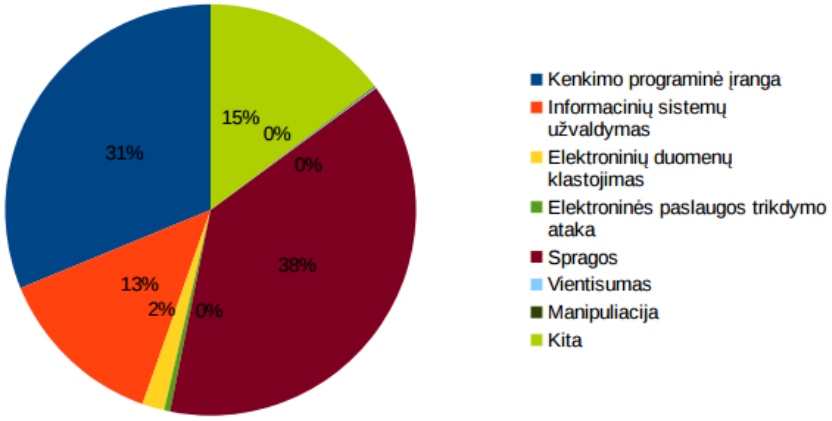
Taigi, socialinės inžinerijos grėsmė išnaudodama organizacijos narių, t. y. žmonių, pažeidžiamumus gali paversti niekais net ir geriausiai parengtą organizacijos kibererdvės gynybos sistemą, kuri orientuota į technologinius ir procesinius vektorius. Todėl autorius mano, kad vienas svarbiausių organizacijos prioritetų organizuojant gynybą turėtų būti nuolatinis narių edukacinis procesas, nukreiptas į kibernetinio saugumo sąmoningumo ugdymą ir gebėjimą atpažinti naujausias socialinės inžinerijos grėsmes.

1.4. GRĖSMĖS ORGANIZACIJOMS KIBERNETINĖJE ERDVĖJE

Kibernetinės grėsmės, išnaudojusios pažeidžiamumus, sąlygoja kibernetinius incidentus, kurių padariniai organizacijoms gali padaryti daug žalos. Pavyzdžiui McLean (2013) teigia, kad „kibernetiniai incidentai gali pažeisti infrastruktūrą, pertraukti veiklą, sudaryti prastovas, sąlygoti jautrių komercinių duomenų praradimą, intelektinės nuosavybės vagystes, sukčiavimą ir sukelti patikimumo abejones trečiosioms šalims“. Ji siūlo skirstyti kibernetinių incidentų organizacijoms žalą, atsižvelgiant į jų žalingą poveikį organizacijos veiklai:

- *Finansiniai nuostoliai (pinigų praradimas, žalos padarinių atkūrimo kaštai, poveikis akcijų vertei, pajamų praradimas ir kt.);*
- *Reputacijos praradimas (žalingas poveikis prekės ženklui, klientų pasitikėjimo praradimas, ir kt.);*
- *Žala verslo interesams (verslo klientų praradimas, neigiamas poveikis įmonių apsijungimui, konkurencinio pranašumo praradimas ir kt.);*
- *Teisinės nuobaudos (baudos ir kt.);*
- *Kompensacijos nukentėjusioms trečiosioms šalims* (McLean, 2013).

Siekiant nustatyti šiuolaikines grėsmes organizacijų kibernetinei erdvei, apžvelgsime Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio *CERT-LT* pateikiamą 2014 metų statistinę kibernetinių incidentų informaciją. *CERT-LT* pateikiamoje 2014 metų ataskaitoje galime išskirti dominuojančius kibernetinių incidentų tipus: spragos, kenkimo programinė įranga, elektroninės paslaugos trikdymo atakos, informacinių sistemų užvaldymas.



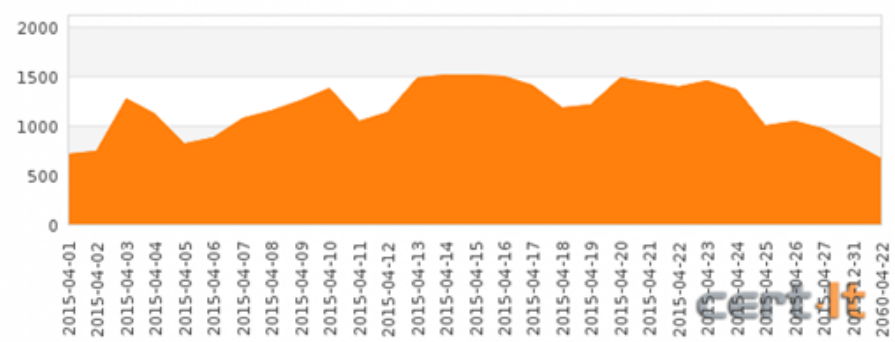
Šaltinis: CERT-LT, 2014

5 pav. CERT-LT 2014 m. gautų ir siųstų pranešimų tipai

CERT-LT 2006 m. fiksavo viso labo tik šeši kenkimo programinės įrangos atvejus, tuo tarpu 2014 m. užfiksuoti jau 11276 incidentai. Kenkimo *PĮ* incidentų augimo dinamika yra pakankamai įspūdinga – per minėtą laikotarpį šio tipo incidentų skaičius išaugo net 1879 kartus. *CERT-LT* pabrėžia, kad paskutiniu metu pastebima, jog pavojingas kodas antivirusinės programinės įrangos yra atpažįstamas tik po kelių dienų (pvz., taip buvo su *Geodo* ir *Feodo* virusu). *CERT-LT* prognozuoja, kad 2015 m. virusų kūrėjai dar aktyviau kurs žalingus kodus išmaniesiems telefonams ir planšetiniams kompiuteriams.

CERT-LT taip pat išskiria *botnet* tinklų veiklą. Pasak *CERT-LT* specialistų, dažniausiai naudotojų kompiuteriai įtraukiami į *botnet* tinklą, pasitelkiant kenkimo programinę įrangą, o apie dalyvavimą *botnet* tinkle kompiuterio savininkas ilgą laiką gali nieko nežinoti (kompiuteris veikia iš esmės normaliai, kartais gali sulėtėti interneto ryšys). 2006 m. buvo fiskuotas tik vienas dalyvavimo *botnet* tinkluose atvejis, tačiau jau 2010 m. kasdien Lietuvoje buvo fiksuojama 10000 įrenginių, dalyvaujančių *botnet* tinklų veikloje (CERT-LT, 2011). 2014 m. vidutiniškai buvo fiksuojama 2000 tokių įrenginių per dieną, o 2014 m. gruodžio mėnesį – 1500. 2015 m. balandžio mėnesį *botnet* tinkluose aptiktų Lietuvos *IP* adresų skaičius svyravo nuo 500 iki 1500 unikalių *IP* adresų (CERT-LT, 2015). Toks sumažėjimas grindžiamas tuo, kad *CERT-LT* pradėjo taikyti naujas kibernetinių incidentų sprendimo priemones (CERT-LT, 2015). Tačiau autorius mano, kad realus įrenginių, įtrauktų į *botnet* tinklus, skaičius gali gerokai viršyti minėtą skaičių, nes minimi *IP* adresai yra Interneto adresai, kurie gali būti priskirti tokiai tinklo įrangai, kuri leidžia sujungti vietinius kompiuterių tinklus su Internet tinklu (maršrutizatoriai, UTM įrenginiai, ugniasienės, *proxy* serveriai), o tai reiškia, kad vietiniame tinkle gali būti bet koks įrenginių, dalyvaujančių *botnet* tinkle, skaičius. Spėjama, kad vienas iš šešių šimtų kompiuterių yra kurio nors *botnet* tinklo dalis (Ryšių reguliavimo tarnyba, 2014). Kai kurie ekspertai teigia, kad pavyzdžiui JAV mažiausiai 25

procentai kompiuterių, turinčių Interneto ryšį, yra įtraukti į vieno ar daugiau *botnet* tinklų veiklą (Sjouwerman, 2011).



Šaltinis: CERT-LT, 2015

6 pav. Botnet tinkluose aptiktų Lietuvos *IP* adresų kiekis

2014 metais *CERT-LT* statistikoje pirmą kartą pradėjo skelbti incidentus susijusius su įrenginių saugumo spragomis, kurių buvo aptikti net 13827 atvejai. Pasak *CERT-LT* šio tipo incidentai iš principo nekelia grėsmės patiems tokių įrenginių savininkams, tačiau sudaro prielaidas piktavaliams šiuos įrenginius elektroninių paslaugų trikdymo atakų metu išnaudoti kaip stiprintuvus (CERT-LT, 2015).

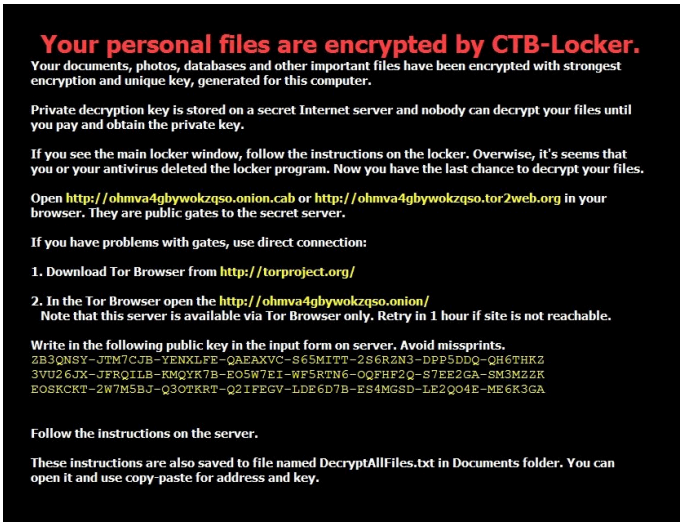
Autorius daro prielaidą, kad organizacijoms didžiausią grėsmę kelia kenkimo programinės įrangos incidentai, kurie plinta išnaudodami pažeidžiamumus ir gali padaryti įvairios žalos organizacijoms, pavyzdžiui gali būti prarasti duomenys arba organizacijos įranga tapti *botnet* tinklo dalimi. Todėl organizacijos turi sugebėti apginti savo kibernetinę erdvę nuo kenkimo programinės įrangos.

Mokslininkai teigia, kad *virusai, kirminai, kenkimo PĮ ir kitas kenksmingas kodas yra viena didžiausių grėsmių kompiuterių sistemoms nuo 1970 m., kai buvo aptiktas pirmasis kompiuterinis virusas. Dabartiniame Interneto amžiuje jie plinta ir dauginasi žymiai sparčiau ir lengviau nei kada nors anksčiau, nepaisant antivirusinės programinės įrangos patobulinimų ir plataus jos pasirinkimo* (Radvilavicius, et al, 2012).

Kaip vieną iš pavojingesnių organizacijoms kenksmingos *PĮ* tipų autorius išskirtų – išpirkos prašančią kenksmingą *PĮ,* kuri užšifruoja duomenis ir reikalauja vartotoją sumokėti išpirką, kad būtų iššifruoti duomenys. Lietuvoje buvo fiskuota tokio tipo kenksmingos *PĮ* atstovo *CBT-Locker* veikla (Ryšių reguliavimo tarnyba, 2015). Jis plinta elektroniniu paštu ir užšifruoja duomenis visuose pasiekiamose laikmenose (standieji, tinklo diskai, *USB* atmintinės). Užšifravus duomenis, vartotojui būdavo pateikiamas pranešimas anglų kalba, kuriame vartotojas raginamas, naudojant „Tor[7]“ tinklą, prisijungti prie svetainės, kurioje pateikiama informacija kaip sumokėti išpirką

[7] Tai populiarus tinklas anonimiškumui Internete užtikrinti, tai atviro kodo projektas suteikiantis anonimiškumo paslaugą TCP (angl. Transmission Control Protocol) protokolu veikiančioms aplikacijoms.

„bitcoin“[8] valiuta už duomenų iššifravimą. Tokio tipo kenksmingos *PĮ* taikiniu tapo ir Lietuvos organizacijos – buvo užšifruotos buhalterinės apskaitos duomenų bazės (Kauno apskrities Vyriausiasis policijos komisariatas, 2015).



Šaltinis: rrt.lt, 2015

7 pav. Pranešimas apie *CBT-Locker* užšifruotus duomenis

Kitas pavojingas kenkimo programinės įrangos tipas – pažangios patvarios grėsmės, *APT*. Mokslininkai teigia, kad *APT* atstovauja realų šiuolaikinio pasaulio pavojų, kurio atsiradimą sąlygojo Interneto plėtra, – tikslinį šnipinėjimą. *Kiekviena APT termino dalis yra tarpusavyje susijusi. Pažangumas reiškia galimybę išlaikyti prieigą gerai apsaugotame tinkle, o patvarumas rodo, kad tokio tipo grėsmėms yra sudėtinga uždrausti prieigą. Žinomi atakų būdai apima infekuotas laikmenas, tiekimo grandinės pažeidimus (angl. Supply Chain Compromise) ir socialinę inžineriją* (Smiraus ir Jasek, 2011).

ENISA[9] kaip pagrindinę *APT* savybę išskiria ilgą atakos trukmę, kuri gali trukti kelis mėnesius ar net metus. Kita svarbi charakteristika nurodoma *APT* diferenciacija – skirtingiems atakos taikiniams taikomos skirtingos *APT*, tai ypač susiję su atakoms naudojama kenkimo programine įranga (ENISA, 2015). Iš to seka, kad *APT* atakos gali turėti unikalius ir tik joms būdingus atakos rengimo ir jos vykdymo ypatumus.

Pavyzdžiui *Stuxnet* kirminas, pirmą kartą aptiktas 2008-11-20, yra labai pažangi kenksminga *PĮ,* kurią specialistai įvardino kaip pirmą kibernetinį ginklą, kuris buvo nutaikytas į pramonines valdymo sistemas – programuojamus loginius valdiklius (angl. Programmable Logic Controller, PLC). *Asmeniniai kompiuteriai būdavo infekuojami tik tokiu atveju, jei jie sujungti su pramoninėmis sistemomis ir atitikdavo visas reikiamas sąlygas. Kirminas išnaudojo šešis*

[8] Bitcoin – atviru kodu ir „peer-to-peer“ technologija paremtas mokėjimų tinklas, https://bitcoin.org/en/
[9] ENISA (angl. European Network and Information Security Agency) – Europos tinklų ir informacijos saugumo agentūra

pažeidžiamumus[10]*, iš jų net penki buvo nulinės dienos pažeidžiamumai*[11]*. Kirminas turėjo aukštą prisitaikymo laipsnį, t.y. naudojo skirtingas taktikas, kad padidintų sėkmingo infekavimo galimybę ir apeitų galimas apsaugos sistemas. 2012-06-24 Stuxnet savaiminio susinaikinimo diena leido padaryti prielaidą, kad tai yra tikslinis įrankis, kuris iki nurodytos datos turėjo atlikti suprogramuotas funkcijas ir pasinaikinti, nepaliekant įkalčių* (De Falco, 2012).

Yra siūloma *tobulinant organizacines priemones apsaugai nuo šiuolaikinių APT įtraukti pažangias saugumo praktikas ir politikas:*

- *Mokyti vartotojus ir bendradarbiauti su IT personalu, kad užkardyti socialinės inžinerijos metodus.*
- *Nustatyti keletą saugumo lygių, suteikiant daugiausiai apsaugos jautriausiai informacijai.*
- *Saugoti jautrią informaciją ne tinkle, jei įmanoma, arba atskirame tinkle.*
- *Reguliariai naujinti operacines sistemas ir programinę įrangą.*
- *Tinkamai suteikti teises vartotojams ir apibrėžti tinklo prieigos ribojimus kompiuteriams, kurie gali būti įjungiami į organizacijos tinklą tiek lokaliai, tiek nuotoliniu būdu.*
- *Kontroliuoti USB laikmenas, kurios gali būti naudojamos organizacijos tinkluose, ir sukurti jų naudojimo politikas bei nustatyti minimalius šifravimo reikalavimus.*
- *Vykdyti tiek kompiuterių, tiek tinklo įsibrovimų analizę, kad aptikti anomalią veiklą.*
- *Riboti vartotojų prieigą, vadovaujantis žemiausios privilegijos metodologija, remti gerą slaptažodžių kontrolę, periodiškai tikrinti prieigos įrašus ir peržiūrėti prieigos lygius.*
- *Taikyti SPF (angl. Sender Policy Framework) įrašo metodą, kad apsisaugoti nuo suklastotų laiškų* (Smiraus ir Jasek, 2011).

Kitas pavojingas kibernetinių incidentų tipas, tai dalyvavimas *botnet* tinklų veikloje. *Botnet* tinklai dažniausiai naudojami įvairiai nelegaliai, nusikalstamai veiklai vykdyti, pavyzdžiui:

- Paskirstytoms paslaugos trikdymo atakoms (DDOS).
- Nepageidaujamų elektroninių laiškų siuntimui.
- Persiųsti informacijai, kurią perduoda šnipinėjimo programinė įranga (angl. Spyware).
- Anoniminei Interneto prieigai gauti.
- Klastojimo atakoms vykdyti.
- Sukčiavimui su kreditinėmis kortelėmis.

[10] Pažeidžiamumas (angl. Vulnerability) tai saugumo spraga PĮ, kuri gali būti išnaudota atakos vykdymui.

[11] Nulinės dienos pažeidžiamumas (angl. Zero-Day), tai toks atakos tipas, kai išnaudojamas dar plačiai nežinomas pažeidžiamumas, kuriam dar nesukurtas pataisymų rinkinys. Juodojoje rinkoje aktyviai prekiaujama tokiais pažeidžiamumais, kurie paskui išnaudojami vykdant kibernetinius nusikaltimus. Priklausomai nuo pažeidžiamumo efektyvumo, naujumo ir kokias sistemas įtakoja, kainos gali svyruoti nuo kelių dešimčių iki kelių šimtų tūkstančių JAV dolerių.

Botnet tinklas apibrėžiamas kaip „tinklas, sudarytas iš nuotoliniu būdu valdomų kompiuterių, dažniausiai kenkimo tikslais“ (Sjouwerman, 2011). O štai kita mokslininkė teigia, kad „kibernetiniai nusikaltėliai šiuolaikines DDOS atakas vykdo pasitelkę užgrobtus kompiuterius, kitaip vadinamus „zombiais“, įtrauktus *botnet* tinklus. Tokie užgrobti kompiuteriai dažniausiai priklauso tokiems teisėtiems naudotojams, kaip pvz.: pavieniams fiziniams asmenims, verslo atstovams, vyriausybinėms, švietimo įstaigoms bei kitoms organizacijoms“ (Brenner, 2012). Kaip pavyzdys gali būti pateikiamas *Bredolab botnet* tinklas, kurį sudarė apie 30 mln. užgrobtų kompiuterių (Cluley, 2012). Tai parodo problemos mąstą bei leidžia daryti prielaidą, kad tiek viešojo, tiek privataus sektoriaus organizacijos yra patrauklus taikinys kibernetiniams nusikaltėliams, suteikiantis galimybę vykdyti nusikalstamas veikas maksimaliai išnaudojantis anonimiškumo faktorių.

Botnet tinklų galimybės vykdyti nusikalstamai veiklai, susiformavusi tokių tinklų paklausa juodojoje rinkoje, skatina nusikaltėlius taikyti pažangias technologijas, galinčias užtikrinti *botnet* tinklų saugumą ir patikimumą. Kovai su *botnet* tinklais vykdomomis nusikalstamomis veikomis, tokiomis kaip sukčiavimai su kreditinėmis ar dovanų kortelėmis, siūlo „taikyti kelių skirtingų gamintojų apsaugos priemones arba vieno gamintojo, tačiau naudojančias skirtingas apsaugos technologijas, jis taip pat teigia, kad vienas iš lemiamų apsaugos priemonių pasirinkimų faktorių yra sprendimo kaina. Jis kaip svarbų aspektą išskiria socialinį faktorių ir siūlo sutelkti dėmesį į internetinių prekybos centrų darbuotojų mokymą kaip atpažinti ir išvengti klientų duomenų atskleidimo grėsmių“ (Sjouwerman, 2011).

Todėl kyla prielaida, kad organizacijoms kyla dvigubas pavojus, visų pirma organizacija gali tapti *botnet* tinklais vykdomų kibernetinių atakų auka, kita vertus organizacijos kompiuterinė įranga gali būti įtraukiama į *botnet* tinklų veiklą ir tokiu būdu organizacija taptų tokių atakų vykdytojų „bendrininke“. Tai gali sudaryti organizacijai pakankamai daug nemalonumų, pradedant reputacijos praradimu ir baigiant sankcijomis ribojančiomis tinklo paslaugų tiekimą, kaip numatyta LR Kibernetinio saugumo įstatyme.

Pastaruoju metu stebimos dvejopos DDOS atakos, vienose naudojamos sudėtingos technologijos, jos vyksta keliomis fazėmis, pasitelkiant *APT*, šios atakos gali trukti dienas, savaites ar net ištisus mėnesius. Kitos DDOS atakos yra paprastos, kurių metu netaikomos pažangios technologijos, o jų trukmė iki 30 min. Toks dvilypumas yra siejamas su DDOS atakų vykdytojų tipais (Zeifman, 2015):

1. Profesionalūs kibernetiniai nusikaltėliai;
2. *Botnet* tinklų paslaugų (angl. Botnet-for-hire Services) abonentai (angl. Booters, Stressers).

Juodojoje rinkoje yra prekiaujama *botnet* tinklų paslaugomis, pavyzdžiui nusikaltėliai gali išsinuomoti reikiamo dydžio *botnet* tinklą, kad vykdyti prieš kokią nors įmonę nukreiptą DDOS

ataką su tikslu gauti išpirką už atakos nutraukimą. „Paslaugos nuomos modelis suteikia galimybę, bet kam įvykdyti kelias trumpas DDOS atakas vos už keliasdešimties dolerių mėnesinį mokestį. DDOS atakos įvykdytos, pasinaudojant tokiomis paslaugomis sudaro daugiau nei 40 proc. visų atakų“ (Zeifman, 2015). Juodojoje rinkoje esanti gausi *botnet* tinklų pasiūla sąlygoja „botentų“ panaudojimo kibernetinėms atakoms vykdyti augimą.

DDOS atakų evoliucija kelia nerimą tiek kibernetinio saugumo ekspertams, tiek organizacijoms. „Per pastarąjį dešimtmetį vykdomų DDOS atakų metu duomenų srautai išaugo beveik 5000 proc., nuo 8 Gbps 2004 m. iki 400 Gbps 2014 m.” (Arbor Networks, 2015). Didžiausia DDOS ataka, kurios srautas sudarė 500 Gbps, buvo nukreipta prieš nepriklausomas naujienų svetaines *Apple Daily* ir *PopVote*, pasak kompanijos *Cloudflare*, kuri atsakinga už minėtų portalų apsaugą, atstovo M. Prince „tai didžiausia kada nors Internete stebėta ataka“ (Olson, 2014). Tokio mąsto atakos gali sukelti itin daug žalos, ne tik organizacijoms, bet net ir valstybėms. Pasak KAM atstovo R. Černiausko, „jei būtų gerai koordinuota ataka (prieš Lietuvos Respubliką, aut. pastaba), galbūt reikėtų ir atsijungti“ (Alfa.lt, 2012). Todėl galime teigti, kad DDOS atakų metu generuojami duomenų srautai nuolat auga, o jų augimas fiksuojamas kartais.

Tradiciškai DDOS atakos buvo vykdomos siekiant sutrikdyti paslaugų teikimą, dažniausiai politiškai motyvuotos arba kriminaliniais sumetimais, kurių tikslas gauti išpirką už DDOS atakų nutraukimą prieš pasirinktą organizaciją. DDOS atakos taip gali būti išnaudojamos organizacijų veiklos trikdymui (Turton, 2014). Dabar stebimos kitos tendencijos, tokios kaip pavyzdžiui DDOS atakų panaudojimas užmaskuoti kitus kibernetinius nusikaltimus – „dūminė priedanga“ (angl. Smoke Screening). Tai tokio tipo DDOS ataka, kai naudojami palyginti nedideli duomenų srautai, nuo 1 iki 5 Gbps, nukreipiant puolamos organizacijos dėmesį būtent į gynybą nuo DDOS atakos, nors tikrasis taikinys yra visai kitas. Kompanijos *Neustar* tyrimų duomenimis 2013 m. “55 proc. nukentėjusių nuo DDOS atakų, taip pat tapo kibernetinių vagysčių aukomis, atakų rezultate buvo prarastos lėšos, klientų duomenys bei intelektinė nuosavybė“ (Neustar, 2015). Analogiškus tyrimus 2014 m. atlikusios kompanijos *Incapsula* duomenimis 33 proc. atvejais buvo pavogti klientų duomenys, o 19 proc. sudarė intelektinės nuosavybės praradimai (Matthews, 2014). Pasak R. Agarwal, tokių DDOS atakų metu „naudojama trumpesnių atakų strategija tam, kad padidinti atakos efektyvumą ir tuo pačiu atitraukti IT personalo dėmesį nuo tikrų atakos tikslų, kurie yra kenkimo *PĮ* įrangos įdiegimas ir duomenų vagystės“ (Bronson, 2015).

Taip pat stebimos ir technologinės DDOS atakų pokyčių tendencijos. 2015 m. DDOS atakoms vykdyti buvo naudojami išmanieji arba daiktų Interneto įrenginiai (Zeifman, 2015). Pagal *Gartner* prognozes IoT įrenginių įjungtų į Interneto tinklą 2020 m. sudarys ~25 mlrd. vnt. (Barker, 2014), kas leidžia daryti prielaidą, jog IoT įrenginiai vis dažniau bus naudojami DDOS atakoms vykdyti. Kitas DDOS atakų technologinis pokytis susijęs su atakoms naudojamais protokolais. Iki 2013 m.

DDOS atakoms vykdyti dažniausiai buvo naudojamas DNS protokolas ir didžiausias srautas iki 100 Gbps, tačiau 2014 m. DDOS atakų analizė parodė, kad tokioms atakoms vykdyti pradėti taikyti ir kiti protokolai (Arbor Networks, 2015).

1 lentelė. **Pažeidžiami protokolai, naudojami DDOS atakoms vykdyti.**

Protokolas	I ketv., %	II ketv., %	III ketv., %	IV ketv., %	Maks. ataka, Gbps
DNS (53)	2	4	4	< 1	104,28
NTP (123)	14	6	5	7	325,05
SSDP (1900)	< 1	< 1	4	9	131,2
SNMP (161)	< 1	< 1	< 1	< 1	18,61
Chargen (19)	1	1	2	1	96,27

Šaltinis: Arbor Networks, 2015

Kitas svarbus DDOS atakų aspektas yra jų poveikis organizacijoms. Viena pagrindinių sąlygų, kad būtų įvykdyta sėkminga DDOS ataka – Interneto ryšys. Pasak KAM atstovo R. Černiausko *Interneto ryšys nieko bendro neturi su vidiniais ryšiais. Nors nėra interneto, krašto apsaugos sistema pilnai funkcionuoja ir nejaučia jokio sutrikimo išskyrus tai, kad mes neišsiunčiame ir negauname elektroninių laiškų. Kelių valandų sutrikimas labai retais atvejais turėtų didesnės įtakos. O šiaip tinklai yra autonomiški ir mes nelabai nukentėtume* (Alfa.lt, 2012). Organizacijos, kurioms Interneto ryšys nėra gyvybiškai svarbus, todėl DDOS atakų poveikis būtų žymiai mažesnis. Tačiau, jei organizacija tiesiogiai nėra priklausoma nuo Interneto ryšio, bet naudojasi prieglobos paslaugų tiekėjų duomenų centrais, ji gali tapti netiesioginės DDOS atakos auka, kai ataka įvykdoma prieš paslaugų tiekėją.

Taigi DDOS atakų poveikis įvairioms organizacijoms yra skirtingas. Prieglobos paslaugas teikiančioms organizacijoms DDOS atakų, nukreiptų į jų duomenų centrus, poveikis gali pasireikšti per (Arbor Networks, 2015):

1. Padidėjusias eksploatacines išlaidas;
2. Klientų nepasitenkinimą;
3. Pajamų sumažėjimą;
4. Darbuotojų kaitą.

Tuo tarpu verslo, vyriausybinės bei švietimo organizacijos, išskiria šiuos aspektus kaip DDOS atakų poveikį (Arbor Networks, 2015):

1. Padidėjusias eksploatacines išlaidas;
2. Reputacijos ir/arba klientų praradimą;
3. Pajamų sumažėją;
4. Darbuotojų kaitą;
5. Akcijų kainų svyravimą;

6. Aukščiausio lygio vadovų praradimą.

Taigi matome, kad tiek prieglobos paslaugas teikiančios organizacijos, tiek privataus ir viešojo sektoriaus organizacijos DDOS atakų rezultate patiria finansinius nuostolius. 2014 m. vidutinė DDOS atakų trukmė buvo 6 val., o vidutiniai vieną valandą trunkančios DDOS atakos nuostoliai sudarė 40 tūkst. JAV dolerių. Iš to seka, kad vidutinės trukmės ataka 2014 m. trukusios DDOS atakos kaina organizacijai kainavo apie pusę milijono JAV dolerių. Prognozuojama, kad DDOS atakos intensyvės, joms vykdyti bus vis plačiau taikomi IoT įrenginiai, bus taikomos pažangios atakų vykdymo technologijos, o DDOS atakų metu organizacijų metu patiriami nuostoliai didės.

Mokslininkų teigimu "visi Interneto vartotojai, pradedant namų ar verslo kompiuterių vartotojais, sistemų administratoriais, programuotojais ir baigiant Web paslaugų/aplikacijų administratoriais, yra atsakingi už gynybą" (Akkaladevi ir Katangur, 2010). Jie taip pat išskiria tris gynybos nuo *botnet* atakų etapus:

1. Prevencija – šiame etape siekiama apsaugoti kompiuterius nuo įtraukimo į botnet tinklą. Svarbiausi aspektai yra apsauga nuo kenkimo programinės įrangos, vartotojų informavimas, keleto apsaugos lygmenų taikymas (programinės įrangos naujinimas, ugniasienės, Interneto naršyklių ir elektroninio pašto programų saugios konfigūracijos, minimalios vartotojų teisės sistemose ir kompiuteriuose).

2. Gynyba – šio etapo pagrindas yra tinklo politikų, apimančių aukščiau minėtas saugumo priemones, nustatymas.

3. Aptikimas – paremtas tokiomis technologinėmis priemonėmis, kaip tinklo srauto stebėjimas, įsibrovimų aptikimo sistemų įrašų analizė. Aptikus botnet ataką reikia nedelsiant atjungti pažeistus įrenginius nuo tinklo (Akkaladevi ir Katangur, 2010).

McLean (2013) savo įžvalgose nurodo, kad organizacijos neturi apsiriboti vien tik keleto saugumo lygių strategijos taikymu, bet taip pat svarbus yra holistinis požiūris, sutelkiantis dėmesį į žmones, procesus ir sistemas (McLean, 2013).

Autorius daro prielaidą, kad visi aukščiau minėti kibernetiniai incidentai yra tarpusavyje susiję. Neištaisytos saugumo spragos sistemose sudaro galimybę kenkimo programinei plisti organizacijų tinkluose ir sistemose, kuri savo ruožtu gali būti panaudota organizacijos kompiuterių ir kitos tinklo įrangos įtraukimui į *botnet* tinklų veiklą.

1.5. PIRMOS DALIES APIBENDRINIMAS

Pirmoje dalyje autorius, nagrinėdamas kibernetinės gynybos teorinius aspektus, apibrėžė kibernetinę gynybą kaip technologinių ir organizacinių priemonių komplekso panaudojimą, siekiant apsaugoti kibernetinę erdvę nuo kibernetinių atakų arba sumažinti jų žalingą poveikį.

Autorius, nagrinėdamas kibernetinio incidento ir kibernetinės grėsmės santykį, apjungė kibernetinės grėsmės, pažeidžiamumo ir kibernetinio incidento elementus į vieną loginę visumą, kas leido daryti prielaidą, kad kibernetinė grėsmė, veikdama per pažeidžiamumo elementą sąlygoja kibernetinį incidentą.

Autorius organizacijų valdomą informaciją ir jos apdorojimo priemones vertina kaip turtą, kuris yra patrauklus kibernetinių atakų taikinys ir kurį galima pažeisti ar užvaldyti išnaudojus pažeidžiamumus technologijose, procesuose ir žmonėse. Kitaip tariant, pagrindiniai grėsmių vektoriai organizacijose yra technologijos, procesai ir žmonės. Daugiausia kibernetinių atakų vykdoma per žmones, išnaudojant socialinės inžinerijos technologijas, todėl autorius mano, kad saugumo priemonės šioje kryptyje sudaro organizacijos kibernetinės erdvės gynybos sistemos pamatą.

Kibernetiniai incidentai neigiamai veikia organizacijų veiklą per finansinius nuostolius, reputacijos praradimą, žalą verslo interesams, teisines nuobaudas ir kompensacijas nukentėjusioms trečiosioms šalims. Augantis kibernetinių incidentų skaičius, ypač kenkimo programinės įrangos incidentų ir saugumo spragų suponuoja faktą, kad šių incidentų sinergijos efekto rezultate organizacijos įranga ar tinklai gali būti įtraukti į *botnet* tinklus, ko pasėkoje organizacija gali nevalingai tapti kibernetinių nusikaltėlių bendrininke. Todėl, autorius daro prielaidą, kad organizacijoms didžiausią grėsmę kelia kenkimo programinės įranga, neištaisytos saugumo spragos ir dalyvavimas *botnet* tinkluose.

2. MAŽŲ IR VIDUTINIŲ ORGANIZACIJŲ KIBERNETINĖS ERDVĖS GYNYBOS ORGANIZAVIMO PRINCIPAI

Šiame skyriuje autorius nagrinėja kokiais kibernetinės gynybos principais turi vadovautis mažos ir vidutinės organizacijos, kurdamos efektyvias kibernetinės erdvės gynybos sistemas. Autorius taip pat apžvelgia mažų ir vidutinių organizacijų kibernetinėje gynyboje taikytinas metodikos.

Pradžiai nustatykime kas yra mažo ir vidutinio dydžio organizacijos. Tuo tikslu autorius siūlo vadovautis Europos bendrijų komisijos rekomendacijoje 2003/361/EB „Dėl mikroįmonių, mažųjų ir vidutinių įmonių apibrėžimo“ siūlomu organizacijų skirstymu pagal jų narių skaičių:

1. 0 – 9 nariai – mikro;
2. 10 – 49 nariai – maža;
3. 50 – 249 nariai – vidutinė.

Mokslininkų teigimu stambios organizacijos gali apsaugoti savo kibernetinę erdvę kurdamos ir diegdamos gerai patikrintus saugumo sprendimus, nes priešingai nei mažos ir vidutinės organizacijos, gali pritraukti kvalifikuotus specialistus. Susidariusią padėtį jie paaiškina nepakankamu dėmesiu kibernetiniam saugumui ir finansinių išteklių trūkumu mažose ir vidutinėse organizacijose (Sangani ir Vijayakumar, 2012). Tačiau autorius daro prielaidą, kad mažos ir vidutinės organizacijos, taikydamos tinkamus kibernetinės gynybos principus, taip pat gali sukurti efektyvias kibernetinės gynybos sistemas.

2.1. PAGRINDINIAI KIBERNETINĖS GYNYBOS ELEMENTAI

Pirmas kibernetinės gynybos principas – „gynybos į gylį“ strategijos taikymas organizacijos kibernetinei erdvei ginti. „Gynybos į gylį“ strategija yra plačiai naudojama karinėse gynybos operacijose, siekiant ne išvengti lemiamo susidūrimo su puolančiosiomis priešo pajėgomis, bet atidėti su tikslu laimėti laiko. Šis principas lieka aktualus ir taikant „gynybos į gylį“ strategiją organizacijos kibernetinėje gynyboje.

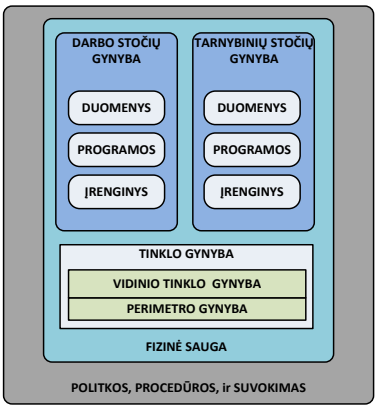
Mokslininko (Byres, 2014) teigimu *negalima pasikliauti vieninteliu kibernetinės gynybos sprendimu, nepaisant to kaip jis gerai suprojektuotas ir patikimas, nes jį pažeidus – pažeidžiama tampa visa sistema. Daug efektyvesnė strategija patikimam saugumui slypi „gynybos į gylį“ koncepcijoje, kuri remiasi trimis pagrindinėmis sąvokomis:*

1. Daugiasluoksnė gynyba. Keleto saugumo sprendimų paskirstymas skirtinguose sluoksniuose užtikrina, kad pažeidus saugumo priemonę viename sluoksnyje, kitame sluoksnyje veikianti priemonė tieks papildomą apsaugą. Sistemos negali remtis vienintele saugumo priemone, nepaisant to, kokia ji yra patikima.

2. *Gynybos sluoksnių diferencijavimas. Užtikrinama, kad sluoksniai tarpusavyje yra skirtingi. Pažeistas vienas gynybos sluoksnis nesuteikia automatinės galimybės pažeisti kitų sluoksnių.*

3. *Specifinių grėsmių sluoksniai. Kiekvienas sluoksnis turi būti projektuojamas atsižvelgiant į konkrečias grėsmes. Grėsmės gali varijuoti nuo nepatenkintų darbuotojų ir kenkimo programinės įrangos iki paslaugos trikdymo atakų ir duomenų vagysčių. Turi būti įvertinta kiekviena grėsmė ir pasiruošta ją atremti* (Byres, 2014).

Microsoft kompanijos „gynybos į gylį“ strategijos koncepcija (Microsoft, 2006) yra pakankamai lanksti, nes kiekvieno saugumo lygmens detalus apibrėžimas gali būti keičiamas, atsižvelgiant į skirtingus organizacijų saugumo reikalavimus ir prioritetus.



Šaltinis: sudaryta pagal Microsoft, 2006

8 pav. Microsoft kompanijos „gynybos į gylį“ modelis

Microsoft kompanijos „gynybos į gylį“ strategijos koncepcijoje išskiriami septyni lygmenys, kuriuose gali kilti rizikos saugumo pažeidimams:

1. Duomenys – šiame lygmenyje rizikos kyla dėl pažeidžiamumų, kurie gali būti išnaudoti tam, kad gauti prieigą prie konfigūracijų, organizacijos duomenų ar kitų specifinių duomenų.

2. Programos – čia kaip ir duomenų lygmenyje, rizikos kyla dėl potencialių pažeidžiamumų, tačiau jau programų lygmenyje. Bet kuris programišių sukurtas kenksmingas vykdomasis programinis kodas gali būti panaudotas įrenginių atakoms per juose veikiančios programinės įrangos pažeidžiamumus.

3. Įrenginiai – šiame lygmenyje rizikos kyla dėl pažeidžiamumų įrenginių valdymo programinėje įrangoje ir tvarkyklėse.

4. Vidinis tinklas – šiame lygmenyje rizikos dažniausiai susijusios su organizacijų jautriais duomenimis, kurie perduodami vidiniais tinklais.

5. Perimetras – čia rizikos kyla, kai programišiai gauna prieigą prie organizacijos globalių tinklų ir per juos gali pasiekti kitus organizacijos tinklus.

6. Fizinė sauga – šiame lygmenyje rizikos kyla, kai programišius fiziškai gali gauti prieigą prie fizinio įrenginio.

7. Politikos, Procedūros ir Suvokimas – visus saugumo lygmenis apjungia į visumą politikos ir procedūros, kurias organizacijos turi parengti ir taikyti, kad užtikrinti saugumo reikalavimus kiekviename lygmenyje.

Duomenų, Programų ir Įrenginių saugumo lygmenys gali būti apjungiami į dvi gynybines strategijas, padedančias organizacijai apsaugoti serverius ir vartotojų galinius įrenginius. Šios dvi strategijos turi bendrų bruožų, tačiau serverių ir vartotojų galinių įrenginių apsaugos skirtumai yra pakankamas pagrindas, kad būtų taikomi unikalūs gynybos metodai abejoms grupėms.

Perimetro ir Vidinio tinklo lygmenys, dėl vienodų technologijų taikymo abiejose lygmenyse, taip pat gali būti apjungiami į bendrą Tinklo gynybos strategiją. Tačiau realizavimo detalės, priklausomai nuo įrenginių ir technologijų pozicijų organizacijos infrastruktūroje, gali skirtis kiekviename lygmenyje.

Toks gynybos būdas charakterizuoja gynybos sistemą, kur saugumo priemonės yra taikomos skirtinguose sluoksniuose, kas leidžia sukurti darnią saugumo aplinką, kurioje nėra vienintelio pažeidimo taško (angl. Single Point of Failure).

Saugumo lygiai, formuojantys gynybos į gylį strategiją, turi numatyti kompleksinių saugumo priemonių taikymą organizacijos kibernetinėje erdvėje, pradedant technologinių priemonių diegimu perimetro tinkle ir galinėje įrangoje bei tarpiniuose taškuose, incidentų valdymo ir veiklos atkūrimo procedūrų bei saugos politikų nustatymu ir baigiant personalo kibernetinio saugumo sąmoningumo ugdymu. Kelių saugumo lygių taikymas leidžia užtikrinti saugumą taip, kad pažeidus saugumo priemones viename lygyje, kituose lygiuose esančios saugumo priemonės teiks apsaugą.

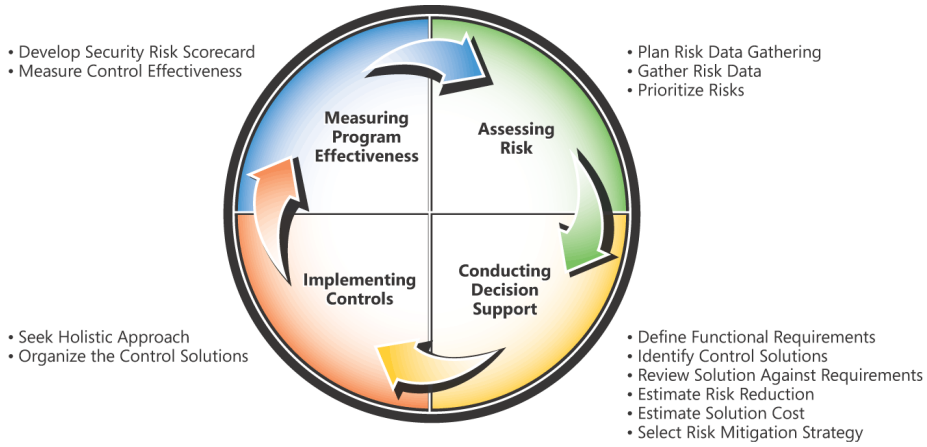
Sekantis kibernetinės gynybos principas yra rizikų valdymas, kurį *Microsoft* apibrėžia kaip procesą, kurio metu yra nustatomos rizikos ir įžvelgiamas galimas jų poveikis. Savo ruožtu rizika nusakoma kaip „tikimybė, kad pažeidžiamumas bus panaudotas esamoje aplinkoje, todėl atsiras tam tikro laipsnio turto konfidencialumo, vientisumo ar pasiekiamumo nuostoliai“ (Microsoft, 2006). Iš esmės rizikų valdymo procesas, tai grėsmių ir pažeidžiamumų, santykio įvertinimas, nustatantis rizikas organizacijai. Rizikos vertintojai, atlikdami rizikų poveikio organizacijai vertinimą, atsižvelgia į šias poveikio organizacijai keturias kategorijas: konkurencinį pranašumą, juridines/reguliavimo, veiklos prieinamumą ir rinkos reputaciją. Kiekvienai kategorijai priskiriama viena iš trijų rizikos poveikio grupių (Microsoft, 2006):

1. Didelis pavojus – žymus ar visiškas turto praradimas;
2. Vidutinis pavojus – riboti arba vidutiniai nuostoliai;
3. Mažas pavojus – maži nuostoliai arba nuostolių nėra.

Formaliai rizikų valdymo procesas padeda mažom ir vidutinėm organizacijoms vykdyti efektyvią finansiniu požiūriu veiklą, nustatant priimtinus veiklos rizikų lygius, taip pat suteikia išsamų ir aiškų ribotų išteklių valdymo būdą rizikų valdymo procese. Pagal (Microsoft, 2006) saugumo rizikų valdymo procesą sudaro keturios fazės, susidedančios iš tam tikrų žingsnių:

1. Rizikos įvertinimas – identifikuoti rizikas organizacijos veiklai ir suteikti joms prioritetus:
    1.1. Duomenų rinkimo planavimas – aptariami sėkmę lemiantys faktoriai ir sudaromas pasirengimo vadovas;
    1.2. Rizikos duomenų rinkimas – nustatomi duomenų rinkimo ir analizės principai;
    1.3. Prioritetų rizikoms suteikimas – nustatomi rizikų kiekybinio ir kokybinio vertinimo principai.
2. Sprendimo parama – identifikuoti ir įvertinti pasirinktų priemonių efektyvumą per kaštų prizmę:
    2.1. Funkcinių reikalavimų nustatymas – apibrėžiami funkciniai reikalavimai, nukreipti į rizikų poveikio sumažinimą;
    2.2. Galimų priemonių pasirinkimas – nustatomi rizikų poveikio mažinimo priemonių pasirinkimo metodai;
    2.3. Galimų priemonių vertinimas – įvertinamos galimos priemonės per funkcinių reikalavimų prizmę;
    2.4. Rizikos mažinimo vertinimas – daromos pastangos, kad įvertinti sumažintos rizikos poveikį ar jos tikimybę;
    2.5. Priemonių kaštų vertinimas – įvertinami tiesioginiai ir netiesioginiai kaštai, susiję su rizikos poveikio mažinimo priemonėmis;
    2.6. Rizikos poveikio mažinimo strategijos pasirinkimas – užbaigiama išlaidų ir gautos naudos analizė, kad nustatyti efektyviausią kaštų prasme priemonę.
3. Priemonių įdiegimas – įdiegti ir valdyti priemones organizacijos veiklos rizikos sumažinimui:
    3.1. Holistinių metodų paieška – rizikos poveikio mažinimo priemonės turi apjungti žmones, procesus ir technologijas;
    3.2. Organizavimas pagal „gynybos į gylį“ principus – priemonės paskirstomos po visą organizaciją.
4. Vertinti programos efektyvumą – analizuoti rizikos valdymo proceso efektyvumą ir įvertinti ar pasirinktos priemonės teikia tokį saugumo lygį, kurio buvo tikimasi:
    4.1. Sukurti rizikų rezultatų kortelę – padeda suprasti rizikų pozicijas ir jų poveikio mažinimo pažangas;

4.2. Matuoti programos efektyvumą – vertinamos galimybės tobulinti rizikų valdymo programą.



Šaltinis: sudaryta pagal Microsoft, 2009

9 pav. Keturių fazių rizikų valdymo procesas

Kaip matome, tai iš principo yra Demingo ciklo, žinomo kaip P-D-C-A (angl. Plan, Do, Check, Act) ciklas ir plačiai taikomo *ISO 27001* standarte, *Microsoft* kompanijos traktuotė. Kiekvieną fazę sudaro tam tikri žingsniai, o jų sinergija sudaro saugumo rizikų valdymo procesą.

Pasak kompanijos, rizikų valdymas mažoms ir vidutinėms organizacijos gali tapti nepakeliama našta dėl patirties stokos ar ribotų išteklių, kaip alternatyva gali būti rizikų valdymo perkėlimas į kitą kompetentingą bendrovę. Saugumo rizikų valdymas pateikia proaktyvų požiūrį, kuris gali padėti mažom ir vidutinėm organizacijoms planuojant gynybines strategijas.

Trečias kibernetinės gynybos principas, kurį turėtų praktikuoti ne tik organizacijos, bet ir fiziniai asmenys, yra kibernetinė higiena. Teigiama, kad „kibernetinės higienos trūkumas ir prastas saugumo valdymas sąlygoja kibernetinių atakų skaičiaus augimą ir nuostolius tiek privačiame, tiek viešajame sektoriuje, kas įrodo, jog abu sektoriai yra vienodai pažeidžiami“ (Eshoo, 2015). Ji taip pat aptaria JAV Geros kibernetinės higienos skatinimo įstatymo projektą (angl. The Promoting Good Cyber Hygiene Act), turintį nustatyti gerąsias tinklų saugumo praktikas, kurias savanoriškai taikytų valstybinės įstaigos, privataus sektoriaus atstovai, fiziniai asmenys ar organizacijos. Pasak jos, įstatymas sukurtų prielaidas sistemų administratoriams geriau pasaugoti savo tinklus ir įrenginius nuo žinomų kibernetinių grėsmių, o bet kokio dydžio organizacijoms leistų apsaugoti investicijas, reputaciją, klientus ir pelną.

Kitas mokslininkas nagrinėjo 2014 m. balandį startavusią JAV Kibernetinės higienos kampaniją (angl. The Cyber Hygiene Campaign), kurios pagrindiniai iniciatoriai Interneto saugumo centras (angl. The Center for Internet Security) ir Kibernetinio saugumo taryba (angl. The Council on Cybersecurity) dirbo kartu su vyriausybinėmis organizacijomis, kad padėtų tiek viešajam, tiek privačiam sektoriui greitai ir ženkliai patobulinti jų pasirengimą gintis nuo nuolat augančio kibernetinių atakų skaičiaus. Pasak jo „taikant penkis pakankamai paprastus ir nebrangius žingsnius

galima užkardyti 80 procentų programišių, siekiančių įsibrauti į kompanijų ar vyriausybės kompiuterines, vykdomų atakų“ (Magnuson, 2014). Jis įvardija penkis žingsnius:

1. Inventorizuoti visus įrenginius;
2. Inventorizuoti programinę įrangą;
3. Vystyti ir valdyti saugias įrenginių konfigūracijas;
4. Vykdyti nuolatinį (automatizuotą) pažeidžiamumų vertinimą ir taisymą;
5. Aktyviai valdyti ir kontroliuoti administravimo privilegijų naudojimą.

Ketvirtas principas autoriaus manymu būtų holistinių metodų taikymas. Autorius daro prielaidą, kad mažos ir vidutinės organizacijos, taikydamos holistinį požiūrį į kibernetinės erdvės gynybą, gali sukurti efektyvias gynybos sistemas. Kitaip tariant nepakanka į organizacijos kibernetinę gynybą žvelgti vien tik iš technologinių perspektyvų, o reikia įvertinti visus organizacijos grėsmių vektorius – žmones, procesus ir technologijas. Organizacijos turi pasirinkti tinkamas kibernetinio saugumo metodikas, kurios apimtų visas organizacijos grėsmių kryptis bei teiktų išsamius pasiūlymus saugumo priemonių diegimui. Saugumo standartų, dėl jų apimties ir sudėtingumo, autoriaus manymu mažos ir vidutinės organizacijos turėtų vengti, jei tik jos nėra įpareigotos juos atitikti. Pavyzdžiui, *LST ISO/IEC 27002:2014* standarte yra nustatyti 114 saugumo reikalavimų, suskirstytų į 14 kategorijų, o JAV *NIST SP 800-53* standarte yra nustatyti net 205 saugumo reikalavimai.

Tolimesniam nagrinėjimui autorius pasirinko tris kibernetinio saugumo metodologijas: *PCI DSS* duomenų saugumo standartą, *HIPAA* Saugumo taisykles, ir 20 Kritinių saugumo reikalavimų (angl. 20 Critical Security Controls, *20 CSC*). Mokslininkai (Whilley ir White, 2013) teigia, kad Mokėjimų kortelių pramonės taryba (angl. Payment Card Industry Council) pripažįsta, jog *PCI DSS* metodikos taikymas ženkliai sumažino duomenų vagysčių atvejus. Tuo tarpu (Hecker ir Erdwards, 2014) įvardina *HIPAA* taisykles kaip „sparčiai tampančiu pramoniniu standartu sveikatos priežiūros privatumo ir įrašų apsaugos srityje“. Remiantis (Basani, 2014) įžvalgomis, *SANS 20 CSC* metodikos taikymas, sprendžiant pagrindines organizacijų kibernetinio saugumo problemas, leis pakeisti saugumo situaciją iš esmės.

2.2. *HIPAA* SAUGUMO TAISYKLIŲ REIKALAVIMAI

1996 JAV priimtas Sveikatos draudimo mobilumo ir apskaitos įstatymas (angl. Health Insurance Portability and Accountability Act, *HIPAA*), kurio pirminė paskirtis supaprastinti sveikatos priežiūros sistemos administravimą. Savo ruožtu administravimo supaprastinimas sąlygojo perėjimą nuo popierinių dokumentų prie elektroninių dokumentų ir jų mainų, todėl JAV Sveikatos ir gyventojų aptarnavimo departamentui (angl. Department of Health and Human Services, HHS) buvo pavesta parengti ir paskelbti reikalavimus asmens elektroninės sveikatos

duomenų apsaugai, tuo pačiu užtikrinant sveikatos priežiūros paslaugų teikėjų ir kitų subjektų prieigą prie tų duomenų.

2002 m. buvo paskelbti reikalavimai asmens sveikatos informacijos privatumui, sutrumpintai *HIPAA* privatumo taisyklės, kurios nustato asmens sveikatos duomenų naudojimo ir viešinimo be asmens sutikimo apribojimus bei sąlygas, ir suteikia pacientui galimybę valdyti savo sveikatos informaciją, įskaitant teisę susipažinti su ja bei gauti įrašų kopijas ir reikalauti koregavimo.

2003 m. paskelbtos saugumo taisyklės elektroninės informacijos apsaugai – *HIPAA* saugumo taisyklės. Jose reikalaujama taikyti technines ir kitas apsaugos priemones elektroninės informacijos apsaugai. 2006 m. buvo publikuotos *HIPAA* saugumo reikalavimų vykdymo taisyklės. 2009 m. paskelbtas *HITECH* (angl. Health Information Technology for Economic and Clinical Health Act) nutarimas, 2009 m. – Informavimo apie pažeidimus taisyklės (angl. Breach Notification Rule), 2013 m. padaryti pakeitimai *HIPAA* privatumo, saugumo reikalavimų, įgyvendinimo ir informavimo apie įsibrovimus taisyklėse bei padaryti kiti *HIPAA* taisyklių pakeitimai, žinoma kaip Omnibus taisyklės.

HIPAA Saugumo taisyklės reikalauja tinkamų administracinių fizinių ir techninių saugumo priemonių taikymo, siekiant užtikrinti asmens sveikatos duomenų konfidencialumą, vientisumą ir prieinamumą. Taisyklės leidžia subjektams naudoti bet kokias saugumo priemones, suteikiančias galimybę tinkamai ir protingai įvykdyti reikalavimus ir taikymo specifikacijas, atsižvelgiant į subjekto dydį, kompleksiškumą, turimus pajėgumus, techninę infrastruktūrą (techninę ir programinę įrangą), saugumo priemonių kaštus, galimų rizikų tikimybę. Reikalavimai apibūdinami kaip lengvai pritaikomi bet kokio dydžio organizacijai ir yra nepririšti prie konkretaus gamintojo įrangos, kas suteikia galimybę subjektams pasirinkti tinkamas technologijas ir priemones savo infrastruktūros apsaugai (Greene, 2014).

Saugumo taisykles sudaro penkios kategorijos (standartai), nusakantys privalomus reikalavimus subjektams, bei reikalavimų įgyvendinimo instrukcijos, kurios savo ruožtu nusako kaip subjektas turi tuos reikalavimus įvykdyti.

I. Administracinės apsaugos priemones sudaro:

1. Saugumo valdymo procesas (rizikų valdymo procesas, sankcijų politika ir nuolatinė stebėsena).
2. Turi būti paskirtas saugumo pareigūnas.
3. Personalo saugumas.
4. Prieigos prie informacijos valdymas.
5. Saugumo sąmoningumo stiprinimas ir mokymas.
6. Saugumo incidentų procedūros.
7. Nenumatytų atvejų planavimas.
8. Vertinimas.

9. Verslo sutarčių su partneriais ir kitus susitarimų valdymas.

II. Fizinės apsaugos priemonės:

1. Patekimo į patalpas kontrolė.
2. Kompiuterių naudojimas.
3. Kompiuterių saugumas.
4. Įrenginių ir laikmenų kontrolė.

III. Techninės apsaugos priemonės:

1. Prieigos kontrolė.
2. Audito priemonės.
3. Vientisumo užtikrinimo priemonės.
4. Asmens ar elemento autentifikavimas.
5. Duomenų perdavimo saugumas.

IV. Organizaciniai reikalavimai nustato taisykles veiklos partnerių sutartims ir kitiems susitarimams.

V. Dokumentacijos reikalavimai. Nustato subjektams privalomų politikų ir procedūrų rengimo taisykles bei dokumentacijos valdymo reikalavimus.

Kaip ir daugelis standartų ir taisyklių, taip ir *HIPAA* saugumo taisyklės turi reikalavimų realizavimo instrukcijas, kurios iš esmės yra nuodugnus metodų, kuriuos subjektas gali taikyti, kad atitikti tam tikrus reikalavimus, aprašymas. Reikalavimų atitiktis yra būtina sąlyga, net jei kuriam nors reikalavimui nėra parengtų įgyvendinimo instrukcijų – jis vis tiek turi būti įgyvendintas. Realizavimo instrukcijos būna:

- Privalomos – jomis kaip ir reikalavimais, subjektas privalo vadovautis, siekiant atitikti reikalavimus.
- Nukreipiančiosios – subjektas privalo atlikti vertinimą, kad nustatyti ar apsaugos priemonės yra pagrįstos ir būtinos subjekto aplinkoje. Jų subjektas negali ignoruoti, jei jos pagrįstos ir būtinos – privalo įdiegti. Jei subjektas nustato, kad instrukcijos yra nepagrįstos ir nebūtinos, jis turi dokumentuoti pagristą sprendimą ir pritaikyti tolygias priemones, kurios siūlomos instrukcijose, arba būti pasiruošęs įrodyti, kad reikalavimai gali būti įgyvendinti nesivadovaujant instrukcija.

Metodikos kūrimo procese buvo įvertinta sąlyga, kad metodika bus taikoma įvairių dydžių organizacijų, todėl metodika neįpareigoja taikyti konkrečių veiksmų. Taisyklės sako, kad subjektas gali taikyti bet kokias saugumo priemones, kurios sudaro galimybę pagrįstai ir tinkamai įgyvendinti standartus ir specifikacijas, atsižvelgiant į:

- Subjekto dydį, kompleksiškumą ir pajėgumus;
- Techninę infrastruktūrą, programinę įrangą;
- Saugumo priemonių kainą;

- Potencialių rizikų tikimybę.

Metodika buvo kuriama, taip, kad ją galėtų taikyti įvairaus dydžio sveikatos priežiūros įstaigose. Ji yra neutrali technologijų ir gamintojų atžvilgiu, todėl subjektai gali laisvai pasirinkti tinkamą technologiją ir kontrolę. *HIPAA* nenumato formalaus sertifikavimo ar akreditavimo proceso. Kiekviena organizacija pati vertina kaip jos saugumo programos atitinka taisyklių reikalavimus, visa tai turi būti įforminta dokumentuose, kad vėliau prireikus būtų galima pagrįsti savo sprendimus.

2.3. *PCI DSS* DUOMENŲ SAUGUMO STANDARTAS

Kredito, debeto ir išankstinio mokėjimo kortelių naudojimas nuolat auga, kasmet įvykdoma keliasdešimties milijardų dolerių vertės transakcijų, tai sukuria kibernetiniams nusikaltėliams patrauklų taikinį – mokėjimo kortelių duomenys. Todėl, siekdami apsaugoti kortelių savininkus nuo jų asmeninės informacijos netinkamo naudojimo ir sumažinti nuostolius dėl mokėjimo kortelių, pagrindiniai mokėjimo kortelių prekinių ženklų atstovai, tokie kaip *Visa, MasterCard, Discover, JCB International* ir *American Express* įsteigė Mokėjimų kortelių pramonės saugumo reikalavimų tarybą (angl. Payment Card Industry Security Standards Council) ir sukūrė Mokėjimo kortelių pramonės duomenų saugumo reikalavimus (angl. Payment Card Industry Data Security Standard, *PCI DSS*). Pirmoji *PCI DSS* versija buvo išleista 2004, antroji versija – 2010, o 2013 publikuota trečioji reikalavimų versija (Greene, 2014).

PCI DSS metodika nustato sąlygas kaip turi būti saugomi, perduodami ir apdorojamai mokėjimo kortelių duomenys. Metodiką sudaro šeši pagrindiniai principai, kuriuose yra nustatyti techninių ir operacinių saugumo priemonių reikalavimai, testavimo reikalavimai ir sertifikavimo procedūros. Subjektai privalo įrodyti, kad atitinka reikalavimus, kurie priklauso nuo transakcijų skaičiaus, veiklos pobūdžio ir transakcijų tipo. Mokėjimo kortelių prekinių ženklų atstovai gali rinkti pinigines baudas ir taikyti kitas nuobaudas organizacijoms, kurios neatitinka reikalavimų, ir panaikinti teisę priimti mokėjimo korteles.

PCI DSS 3.0 versija buvo kuriama, atsižvelgiant į augančius atsiskaitymus elektroninėje erdvėje – mobilūs mokėjimai, elektroninė prekyba, debesų kompiuterija. Šioje versijoje pripažįstama, kad saugumas yra bendra atsakomybė, todėl yra suteikiamos atitinkamos pareigos kiekvienam mokėjimo grandinės dalyviui.

PCI DSS 3.0 versija pabrėžia, kad saugumo atitikimas yra nuolatinis procesas. Įprastinė veikla, tai rizikų vertinimo strategijos, kurią organizaciją valdo ir nuolat stebi, sudedamoji dalis. Įprastinės veiklos požiūris suteikia organizacijai galimybę išlaikyti pastovų reikalavimų atitikimą tarp *PCI DSS* atitikties vertinimų. Organizacijos turi vykdyti reikiamų priemonių nuolatinę

stebėseną, kad įsitikinti jog saugumo priemonių veikla yra efektyvi, ir greitai reaguoti į neveikiančias priemones.

PCI DSS 3.0 versiją sudaro dvylika reikalavimų susietų su šešiais pagrindiniais principais. Kiekvienas reikalavimas turi numatytas įgyvendinimo priemones. Reikalavimai paruošti remiantis gerosiomis informacijos saugumo praktikomis.

1. Sukurti ir eksploatuoti saugų tinklą ir sistemas. Šį principą sudaro du reikalavimai:
   1.1. Įdiegti ir naudoti ugniasienės konfigūraciją kortelių mokėtojų duomenims saugoti.
   1.2. Nenaudoti gamintojo standartinių slaptažodžių ir sisteminių parametrų.
2. Saugoti kortelių savininkų duomenis principas turi du reikalavimus:
   2.1. Saugoti kortelių duomenis.
   2.2. Kortelių savininkų duomenys perduodami atvirais, viešais tinklais, naudojant šifruotus kanalus.
3. Naudoti pažeidžiamumų valdymo programinę įrangą. Principas turi du reikalavimus:
   3.1. Saugoti sistemas nuo kenkimo programinės įrangos ir nuolat atnaujinti programinę ir antivirusinę įrangą.
   3.2. Sukurti ir naudoti saugias sistemas ir architektūrą.
4. Įdiegti griežtas prieigos kontrolės priemones. Principą sudaro trys reikalavimai:
   4.1. Riboti prieigą prie kortelių savininkų duomenų pagal principą „būtina žinoti“.
   4.2. Prieigos prie sistemos komponentų identifikavimas ir autentifikavimas.
   4.3. Fizinės prieigos prie kortelių savininkų duomenų ribojimas.
5. Principas. Nuolat stebėti ir testuoti tinklus:
   5.1. Stebėti ir sekti visas prieigas prie tinklo išteklių ir kortelių savininkų duomenų.
   5.2. Pastovus saugumo sistemų ir procesų testavimas.
6. Principas. Palaikyti informacijos saugumo politiką. Palaikyti informacijos saugos politiką, kuri nukreipta į visą personalą. Politika turi apimti visus likusius 11 *PCI DSS* reikalavimus, tačiau neturi jais apsiriboti. Politika turi būti patvirtinama organizacijos vadovybės ir kasmet peržiūrima ir atnaujinama, o personalas turi kasmet patvirtinti, kad yra susipažinęs ir supranta saugumo politikų ir procedūrų reikalavimus.

PCI DSS atitiktis yra sutartinis įsipareigojimas, kuris taikomas visiems mokėjimų kortelių grandinės subjektams: prekybininkams, finansinėms įstaigoms, paslaugų tiekėjams bei kitiems subjektams, kurie saugo, apdoroja ar perduoda kortelių savininkų duomenis ir/arba jautrius autentifikavimo duomenis. *PCI DSS* atitikties nereglamentuoja jokie teisės aktai ar įstatymai, tačiau mokėjimų kortelių prekinių ženklų atstovai reikalauja atitikti *PCI DSS* reikalavimus, kad subjektai galėtų vykdyti kortelių mokėjimus ir/arba tapti mokėjimų sistemos dalimi.

2.4. *20 CSC* KRITINIŲ SAUGUMO REIKALAVIMŲ

Indėlį į *20 CSC* metodikos kūrimą įnešė ekspertai iš kibernetinio saugumo organizacijų ir komercinių įsiskverbimų testavimo įmonių, taip pat ekspertai iš tokių organizacijų kaip *SANS* Institutas, Nacionalinė saugumo agentūra (angl. National Security Agency, NSA), JAV kariuomenės kibernetinių pajėgų vadovybė (angl. U. S. Cyber Command, USCYBERCOM), saugumo sprendimų gamintoja McAfee, JAV gynybos departamentas (angl. U. S. Department of Defense, DoD), gynybos pramonės atstovas *Lockheed Martin*. Juodraštinis metodikos variantas pasirodė 2009 m., o 2012 m. JAV valstybės departamentas (angl. U. S. State Department) ir Idaho nacionalinė laboratorija (angl. Idaho National Laboratories (SCADA R&D)) nuodugniai palygino metodikos saugumo priemones su realiais saugumo incidentais ir patvirtino šių priemonių efektyvumą.

2013 m. įsteigta nepriklausoma, pelno nesiekianti ekspertinė Kibernetinio saugumo taryba (angl. Council on Cyber Security), kuri įsipareigojusi vystyti, remti ir taikyti kritinius saugumo reikalavimus, kelti kibernetinės gynybos personalo kompetencijas ir vystyti politikas, suteikiančias reikšmingus patobulinimus ir galimybes vykdyti saugią ir patikimą veiklą kibernetinėje erdvėje. Šios metodikos didžiausia vertė yra tai, kad saugumo priemonės paremtos realių grėsmių atvejais, kuriuos patyrė stambios organizacijos.

Svarbiose saugumo reikalavimuose atsispindi penki kertiniai efektyvios kibernetinės gynybos sistemos principai (Council on Cybersecurity, 2014):

1. Puolimas informuoja gynybą – taikyti žinias, gautas iš realių sėkmingai įvykdytų atakų, kad sukurti efektyvią praktinę gynybą. Taikyti tik tas priemones, kurios gali sustabdyti žinomas realias atakas.

2. Prioritetų nustatymas – pirmiausia taikyti tas saugumo priemones, kurios labiausiai sumažina grėsmių riziką ir apsaugo nuo pavojingiausių atakų bei gali būti tinkamai įdiegtos organizacijos aplinkoje.

3. Metrikos – turi būti nustatytos metrikos, kurios suteikia galimybę naudoti bendrą kalbą organizacijos vadovams, IT specialistas, auditoriams ir saugumo pareigūnams, kad įvertinti saugumo priemonių efektyvumą organizacijoje ir greitai identifikuoti ir įdiegti reikiamus pakeitimus ar pataisymus.

4. Nuolatinė diagnostika ir grėsmių mažinimas – nuolat testuoti ir vertinti esamų saugumo priemonių efektyvumą ir padėti nustatyti prioritetus tolesniuose etapuose.

5. Automatizavimas – taikyti automatizuotas gynybos priemones, kad organizacija galėtų skurti patikimą, plečiamą ir nepertraukiamą saugumo priemonių atitikties vertinimo sistemą.

Kritinių saugumo reikalavimų metodika struktūrizuota taip, kad kiekvieną reikalavimą sudaro:

1. Aprašymas kaip reikalavime numatytos priemonės blokuoja arba identifikuoja atakos faktą ir paaiškinimas kaip atakuotojai aktyviai išnaudoja saugumo priemonių nebuvimą.

2. Sąrašas specifinių veiksmų, kuriuos organizacijos taiko diegiant, automatizuojant ir vertinant reikalavimo įgyvendinimo efektyvumą. Reikalavimas suskaidytas į keturias kategorijas:

2.1. Greiti laimėjimai – ženkliai sumažina riziką be didesnių finansinių, procedūrinių, architektūrinių ar techninių aplinkos pakeitimų arba greitai ir žymiai sumažina rizikas prieš dažniausiai pasitaikančias atakas, todėl labiausiai saugumu besirūpinančios organizacijos teikia jiems prioritetą.

2.2. Regimumo ir atributų matai pagerina organizacijos procesus, architektūrą ir techninius pajėgumus, stebint tinklus ir kompiuterių sistemas, kad aptikti bandymus atakuoti, nustatyti prasiskverbimo taškus, identifikuoti pažeistus mazgus, nutraukti įsibrovėlių veiklą ir gauti informaciją apie atakos šaltinį.

2.3. Geresnė informacijos saugumo konfigūracija ir higiena sumažina saugumo pažeidžiamumų skaičių bei reikšmingumą ir pagerina veiklą tinklinių kompiuterių sistemų, kurios orientuotos į apsaugą nuo blogųjų praktikų, taikomų sistemų administratorių bei vartotojų ir kurios gali atakuotojams suteikti pranašumo.

2.4. Pažangios priemonės, kurios naudoja naujas technologijas ar procedūras, suteikiančias didžiausią saugumo lygį, bet jas sunkiau įdiegti arba jos yra brangesnės ar reikalaujančios daugiau aukštos kvalifikacijos personalo nei kiti saugumo sprendimai.

3. Įrankiai ir procedūros, kurios įgalina diegimą ir automatizavimą.

4. Metrikos ir testas įdiegimo būsenai ir efektyvumui vertinti.

5. Subjektų tarpusavio ryšių diagramos, nusakančios įdiegimo komponentus.

SANS 20 CSC kritinių saugumo reikalavimų sudaro:

CSC 1. Leistinų ir nesankcionuotų įrenginių inventorizavimas.

CSC 2. Leistinos ir nesankcionuotos programinės įrangos inventorizavimas.

CSC 3. Saugios mobiliųjų įrenginių, nešiojamų kompiuterių, darbo stočių ir tarnybinių stočių techninės ir programinės įrangos konfigūracijos.

CSC 4. Periodinis pažeidžiamumų ieškojimas ir taisymas.

CSC 5. Gynyba nuo kenkimo programinės įrangos.

CSC 6. Taikomosios programinės įrangos saugumas.

CSC 7. Bevielių įrenginių kontrolė.

CSC 8. Duomenų atkūrimo pajėgumai.

CSC 9. Saugumo įgūdžių vertinimas ir atitinkamų mokymų organizavimas.

CSC 10. Saugios tinklo įrenginių (ugniasienės, kelvedžiai, komutatoriai) konfigūracijos.

CSC 11. Tinklo prievadų, protokolų ir paslaugų ribojimas ir kontrolė.

CSC 12. Administravimo teisių naudojimo kontrolė.

CSC 13. Tinklo perimetro gynyba.

CSC 14. Audito įrašų naudojimas, stebėjimas ir analizė.

CSC 15. Prieigos valdymas pagal principą „būtina žinoti“.

CSC 16. Paskyrų stebėjimas ir kontrolė.

CSC 17. Duomenų praradimo prevencija.

CSC 18. Reagavimas į incidentus ir jų valdymas.

CSC 19. Saugaus tinklo inžinerija.

CSC 20. Įsiskverbimų testai ir „raudonųjų komandų“ pratybos.

Kritinių saugumo reikalavimų metodika nėra visoms organizacijoms vienodai taikoma tiek turinio, tiek prioriteto atžvilgiu. Reikia suprasti kas yra svarbu kiekvienai organizacijai, duomenims, tinklams, infrastruktūroms ir reikia įvertinti atakuotojų veiksmus, kurie gali paveikti organizacijos veiklos sėkmę. Taikant šią metodiką nerekomenduojama įgyvendinti visus arba kelis reikalavimus vienu metu, o reikėtų parengti reikalavimo įgyvendinimo planą.

Kai kurie saugumo reikalavimai, ypač nuo pirmo iki penkto, yra sėkmės pagrindas ir turi būti vertinami kaip pirmi žingsniai metodikos taikyme. Tiems, kurie nori tiksliai žinoti nuo ko pradėti yra akcentuojami „pirmi penki greiti laimėjimai“ (angl. First Five Quick Wins), kurie turi didžiausią atakų prevencijos poveikį:

1. leidžiamų aplikacijų sąrašo sudarymas (*CSC* 2);
2. standartinių, saugių sistemų konfigūracijų naudojimas (*CSC* 3);
3. taikomosios programinės įrangos pataisų įdiegimas per 48 valandas (*CSC* 4);
4. sisteminės programinės įrangos pataisų įdiegimas per 48 valandas (*CSC* 4);
5. sumažintas vartotojų, turinčių administravimo teises, skaičius (*CSC* 3 ir *CSC* 12).

Apibendrinant aukščiau nagrinėtas metodikas, autorius siūlo jas palyginti tarpusavyje pagal šiuos kriterijus: lankstumą, turimas išsamias diegimo instrukcijas, dengiamus organizacijų kibernetinių grėsmių vektorius ir kt. (žr. 2 lent.).

***2 lentelė. PCI DSS, HIPAA* ir *20 CSC* metodikų palyginimas**

Metodika	Akreditavimo procesas	Privaloma atitiktis	Baudų sistema	Reguliavimas	Vektoriai			Išsamios diegimo instrukcijos	Lankstumas
					Žmonės	Technologijos	Procesai		
HIPAA	–	+	+	Įstatymas	+	+	+	+/–	–
PCI DSS	+	+	+	Standartas	+	+	+	+	–
20 CSC	–	–	–	–	+	+	+	+	+

Autorius siūlo pažvelgti į Portlendo (JAV, Oregono valstija) savivaldybės *20 CSC* metodikos diegimo atvejį (Hietala, 2013). Prieš pradedant taikyti *20 CSC* metodiką, IT saugumo valdymas buvo labiau intuityvus ir reaktyvus, t.y. orientuotas į gaisrų gesinimą arba kitaip tariant vyravo „ad hoc“ požiūris. Nebuvo laikomasi sistemingo požiūrio kokius saugumo projektus vystyti ir kodėl, taip pat nebuvo ilgalaikio planavimo kibernetiniam organizacijos saugumui užtikrinti. Įvairūs miestų skyriai taikė skirtingus saugos atitikties standartus ir metodikas, tarp jų *PCI DSS* ir *HIPAA*. Taip pat savivaldybę ribojo žmogiškųjų ir finansinių išteklių trūkumas.

PCI DSS metodika buvo taikoma visose miesto IT sistemose, tačiau buvo nuspręsta, kad tai nėra gera praktika, nes *PCI DSS* labiau koncentruota į mokėjimo kortelių savininkų duomenų apsaugą ir daugelis saugumą užtikrinančių priemonių yra sunkiai pritaikomos arba jų taikymo kaštai yra per dideli. Buvo nuspręsta pereiti prie *20 CSC* metodikos taikymo, nes tai leido miestui pasiekti „greitas pergales“ ženkliai pagerinant saugumo padėtį mažiausiomis pastangomis. Konkrečių saugumo priemonių pasirinkimą lėmė kiekvienos priemonės kainos ir naudos santykis, suteikiantis realų rizikos mažinimą (Hietala, 2013).

Miesto IT saugumo padėtis ženkliai pagerėjo nuo tada, kai buvo pradėta taikyti *20 CSC* metodika. Ženkliai sumažėjo incidentų skaičius galiniuose įrenginiuose, tai buvo pasiekta apribojus administravimo privilegijas ir dažniau diegiant naujinimus sistemose. Sumažėjo incidentų, susijusių su konfigūracijų problemomis, skaičius. Organizacija pradėjo taikyti standartines serverių ir galinių įrenginių konfigūracijas. Metodikos taikymas, leido suvienodinti organizacijos IT personalo žodyną. Organizacijos personalui tapo lengviau suprantami kiekvienos *20 CSC* priemonės tikslai ir kaip jų įdiegimas pagerina saugumo būklę (Hietala, 2013).

2.5. ANTROS DALIES APIBENDRINIMAS

Antroje dalyje autorius išskyrė ir apžvelgė keturis kibernetinės gynybos principus, kuriais mažos ir vidutinės organizacijos turėtų vadovautis, kurdamos savo kibernetinės erdvės gynybos sistemas. Kibernetinės gynybos principai yra:

1. Gynybos į gylį arba daugiasluoksnės gynybos taikymas.
2. Rizikų valdymas.
3. Kibernetinės higienos palaikymas.
4. Holistinio požiūrio taikymas.

Standartai, tokie kaip *ISO/IEC 27002* arba *NIST SP 800-53*, yra labai platūs ir didelės apimties. Jų reikalavimų įgyvendinimas reikalauja papildomų organizacijos išteklių, todėl organizacijoms, kurios neprivalo atitikti šių standartų reikalavimų, reikalingi kitokie įrankiai – metodikos, kurios remiasi minėtais standartais ir jose koncentruotos realių incidentų išmoktos pamokos bei gerosios praktikos.

Autorius apžvelgė *HIPAA* saugumo taisyklių reikalavimus, kurie skirti JAV pacientų elektroninės sveikatos duomenims apsaugoti, ir *PCI DSS* metodiką, skirtą mokėjimo kortelių savininkų informacijos apsaugai. Nepaisant to, kad *PCI DSS* ir *HIPAA* reikalavimai kurti specifinei organizacijų kategorijai, juos gali taikyti bet kokios veiklos srities organizacija savo kibernetinės erdvės gynybos planavime.

20 CSC metodika nėra skirta konkrečios veiklos srities organizacijomis, todėl geriausiai tinka bet kokio tipo organizacijai. Ši metodika nėra pakaitalas standartams ar kitiems reikalavimams, kaip pvz. *HIPAA* ar *PCI DSS*. Metodika parengta, remiantis vyriausybinių, akademinių ir pramoninių organizacijų patirtimi. Ji, lyginant su standartais, yra žymiai mažesnės apimties, joje koncentruoti svarbiausi gynybos prioritetai ir pateiktos efektyviausios gynybos priemonės. Todėl ši metodika tinka bet kokio dydžio ir bet kokios veiklos srities organizacijoms, kurios siekia sukurti efektyvias kibernetinės erdvės gynybos sistemas.

3. ORGANIZACIJOS X KIBERNETINĖS ERDVĖS GYNYBOS TYRIMAS

Šiame skyriuje autorius pateikia *Organizacijos X* kibernetinės erdvės gynybos tyrimo metodus, aprašo tyrimo eigą ir aptaria gautus rezultatus. Atsižvelgdamas į gautus rezultatus, autorius pateikia siūlymus *Organizacijai X* dėl taikytinų priemonių kibernetinės erdvės gynybos sistemos stiprinimui.

3.1. ORGANIZACIJOS X TYRIMŲ METODOLOGIJA

Kibernetinės gynybos tyrimai yra sudėtingas procesas, todėl autorius siekdamas gauti kuo labiau patikimus empirinius duomenis, taikė skirtingus tyrimo metodus, kurie leido patikslinti bei papildyti vieni kitų duomenis. Empiriniai tyrimai buvo vykdomi pasitelkiant šiuos metodus:

1. Elektroninėje erdvėje kilusių incidentų analizė. Autorius remdamasis naujausiais *CERT-LT* duomenimis, analizavo incidentus elektroninėje erdvėje, kurie kėlė grėsmes organizacijų tinklų ir informacijos saugumui.

2. Patirties iš kibernetinės gynybos specialistų perėmimas. Autorius savo kasdienėje darbinėje veikloje bendradarbiaudamas su kibernetinio saugumo specialistais sėmėsi patirties iš kolegų kibernetinės gynybos srityje. O taip pat 2008 m. dalyvaudamas *EC-Council* Certified *Ethical Hacker* mokymuose ir 2015 m. kibernetinės gynybos kursuose *Undergraduate Cyber Training* (JAV) bei tarptautinėse kibernetinės gynybos pratybose *Locked Shields* perėmė tarptautinių kibernetinės gynybos specialistų patirtį.

3. Stebėjimas ir asmeninės profesinės patirties apibendrinimas. Autorius, pasitelkdamas asmeninius profesinius gebėjimus bei turimas kompetencijas, technologinių priemonių pagalba stebėjo organizacijos kibernetinę erdvę, o gauti rezultatai leido padidinti tyrimo patikimumą.

4. Eksperimentai. Tyrimo metu, panaudojant socialinės inžinerijos technologijų priemones, buvo atlikti natūralūs ir laboratoriniai eksperimentai, siekiant nustatyti kaip organizacija yra pasirengusi reaguoti į elektroninių laiškų klastojimo (angl. Phishing) incidentus bei tokias socialinės inžinerijos taikomas priemones kaip „pamestos“ *USB* laikmenos su kenkimo kodu.

5. Apklausa žodžiu ir raštu. Tyrimo metu apklausti respondentai padėjo atskleisti *Organizacijos X* kibernetinės gynybos sistemos būklę, identifikuoti silpniausias jos grandis bei įvertinti rekomenduotų kibernetinės gynybos stiprinimo priemonių efektyvumą.

Autorius, siekdamas įvertinti *Organizacijos X* esamą kibernetinės erdvės gynybos padėtį, kad pateikti rekomendacijas kibernetinės gynybos sistemos optimizavimui bei įvertinti pasiūlytų priemonių efektyvumą, magistrinio baigiamojo darbo empirinį tyrimą vykdė trimis etapais:

1. Pirmo etapo metu apklausti *Organizacijos X* atstovai, kurių atsakymai padėjo geriau įvertinti esamą kibernetinės erdvės gynybos padėtį.

2. Antro etapo metu buvo atlikta:

1.1. *Organizacijos X* tinklo stebėjimas;

2.1. trys natūralūs eksperimentai:

2.2.1. suklastoto elektroninio laiško, kuriame vartotojai raginami įvesti prisijungimo prie savo tarnybinio elektroninio pašto duomenis, eksperimentas Nr. 1;

2.2.2. suklastoto elektroninio laiško, kuriame vartotojai raginami atsisiųsti iš pateiktų nuorodų ir aktyvuoti savo kompiuteriuose programinį kodą, eksperimentas Nr. 2;

2.2.3. „pamestų“ *USB* laikmenų su programiniu kodu eksperimentas Nr. 3.

3. Trečio etapo metu apklaustas *Organizacijos X* atstovas, kurio atsakymai ir laboratorinio eksperimento Nr. 4 rezultatai padėjo nustatyti pasiūlytų *Organizacijai X* kibernetinės erdvės gynybos stiprinimo priemonių efektyvumą.

Organizacijos X tinklo stebėjimas ir eksperimentai buvo vykdomi vadovaujantis mokslinių tyrimų metodologija ir metodais (Kardelis, 2002) ir kibernetinės gynybos ekspertų (Harper, et al, 2011) rekomendacijomis.

Siekiant nustatyti *Organizacijos X* esamą kibernetinio saugumo padėtį buvo atliktas kokybinis tyrimas. Tikslinės atrankos būdu atrinktiems respondentams buvo elektroniniu paštu pateikta anketa su iš anksto parengtais atviro tipo klausimais (žr. priedus 5 – 6). Tokiu būdu buvo apklausti *Organizacijos X* IT tarnybos vadovas ir jo pavaduotojas. IT tarnybą sudaro vedėjas, vedėjo pavaduotojas, trys inžinieriai ir vyriausiasis technikas, visi tarnybos darbuotojai yra įgiję aukštąjį universitetinį arba neuniversitetinį išsilavinimą informatikos ar elektronikos inžinerijos srityje. *Organizacija X* neturi dedikuotos pareigybės kibernetinio saugumo klausimams spręsti. IT tarnybos pagrindinis uždavinys yra IT ūkio palaikymas: kompiuterinių darbo vietų bei serverių ir tinklo įrangos diegimas ir priežiūra, informacinių sistemų monitoringas ir palaikymas, vartotojų konsultavimas. IT tarnyba taip pat atsakinga už IT įrangos ir paslaugų pirkimo proceso organizavimą ir vykdymą.

Kadangi apklausos metodas turi tam tikrų trūkumų, kurie gali nulemti bendrą tyrimo patikimumą, nes respondentai gali vengti pateikti tikslų atsakymą dėl asmeninių priežasčių, pavyzdžiui nenori sukelti abejonių dėl savo kompetencijos ir pan., todėl autorius papildomai tyrime taikė stebėjimo ir natūralių eksperimentų metodus, kas leido padidinti tyrimo patikimumą.

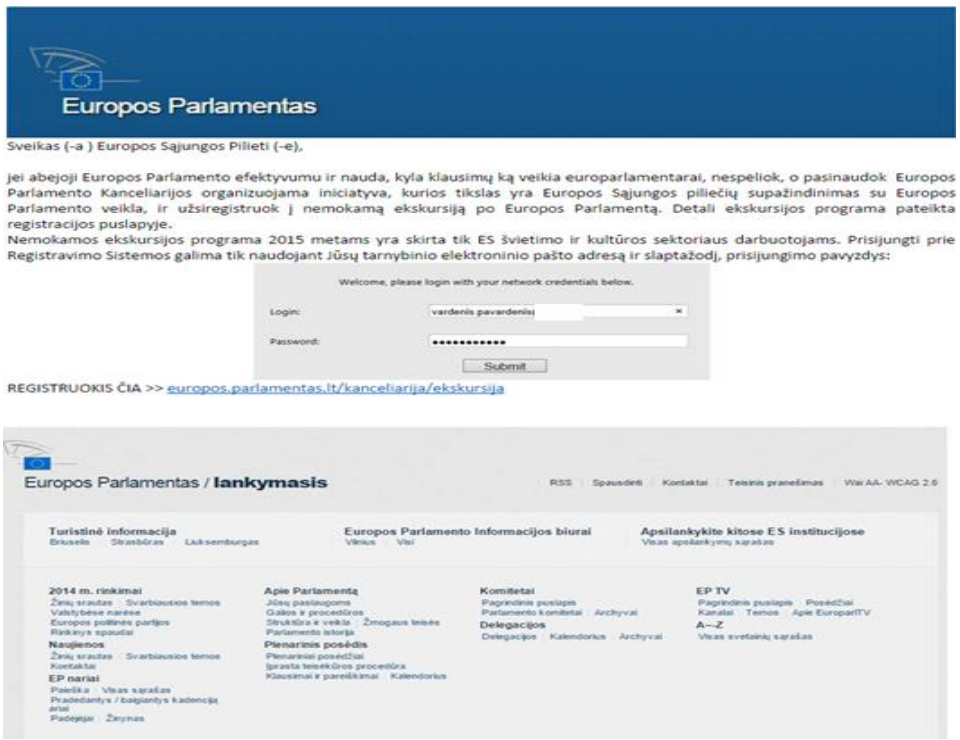
Autorius, apklausęs *Organizacijos X* IT tarnybos atstovus, atliko *Organizacijos X* kompiuterių tinklo stebėjimą. Kadangi *Organizacijoje X* nėra vykdomas pažeidžiamumų valdymas, autorius nusprendė atlikti *Organizacijos X* tinklo dalies (33 kompiuteriai) pažeidžiamumų skenavimą, kad nustatyti pažeidžiamas vietas skenavimui buvo panaudota *Microsoft Baseline Security Analyzer 2.3,*

MBSA programinė įranga, o stebėjimo metu gauti rezultatai leido patikslinti tyrimo išvadas, gautas po IT atstovų apklausos analizės, ir pasiruošti natūraliesiems eksperimentams.

Natūralieji eksperimentai buvo vykdomi pasitelkiant socialinės inžinerijos metodus, t.y. nukreipti į *Organizacijos X* žmogiškąjį grėsmių vektorių, o taip pat lygiagrečiai leido patikrinti technologinį bei procesinius vektorius. Autorius pasirinko natūralaus eksperimento metodą todėl, kad tyrimas atliekamas natūralioje aplinkoje, todėl gauti duomenys yra objektyvūs.

Suklastoto elektroninio laiško, raginančio įvesti prisijungimo duomenis eksperimento Nr. 1 (2 priedas) tikslas patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai atsiunčiamas suklastotas elektroninis laiškas, kuriame vartotojai raginami įvesti prisijungimo prie savo tarnybinio elektroninio pašto duomenis. Eksperimento Nr. 1 rezultate buvo nustatytas rizikos organizacijos kibernetinei erdvei laipsnis. *Organizacija X* atrinko 20 vartotojų, kurie dalyvavo eksperimente.

Eksperimentui Nr. 1 vykdyti buvo sukurta pašto paskyra su elektroninio pašto adresu **eur0parlament@outlook.com**, iš kurio buvo išsiųstas laiškas atrinktiems eksperimento Nr. 1 dalyviams. Laiške buvo siūloma nemokama ekskursija į Europos parlamentą, į kurią reikia užsiregistruoti įvedant savo tarnybinio elektroninio pašto adresą ir slaptažodį. Eksperimento Nr. 1 metu dalyvių skaičius išaugo, nes vienas iš atrinktų dalyvių persiuntė elektroninį laišką visiems savo padalinio darbuotojams.



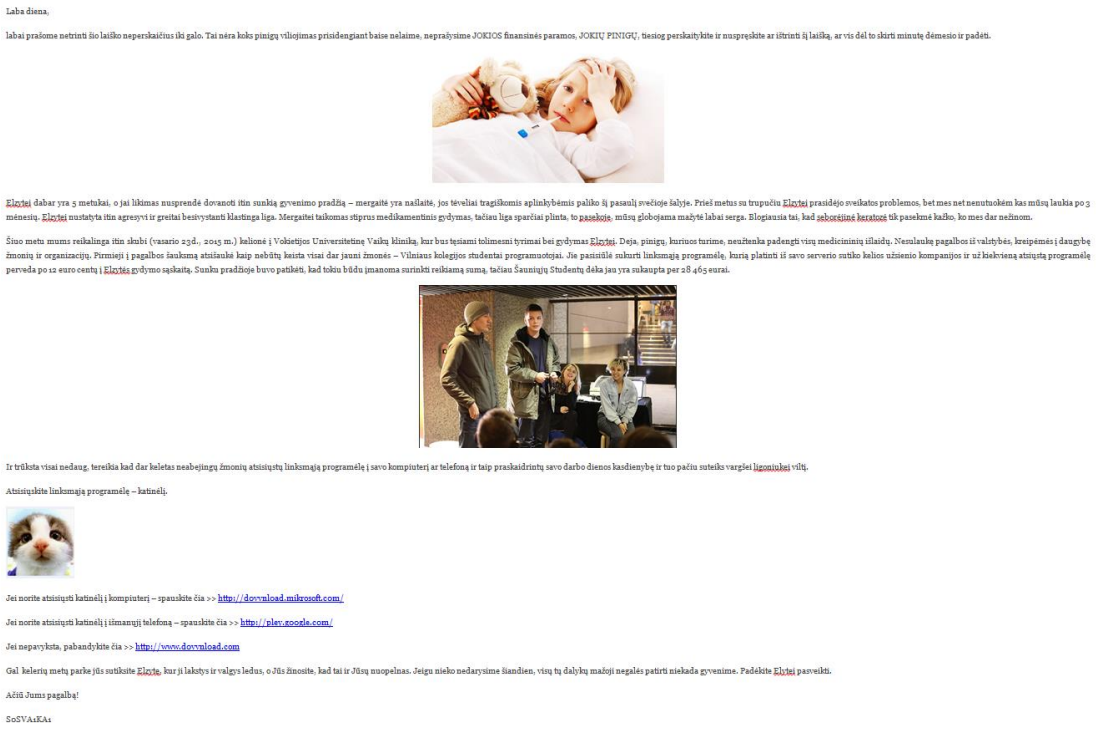
10 pav. Suklastotas laiškas, naudotas eksperimente Nr. 1

Eksperimento Nr. 1 rezultatai buvo registruojami specialiai šiam tikslui skirtame *Organizacijos X* kompiuteryje, kuriame buvo įdiegta nemokama programinė įranga *MSI Simple*

Phish, kurios pagalba buvo registruojami vartotojų, apsilankiusių suklastotojo svetainėje, *IP* adresai, paskyrų pavadinimai bei pirmi trys paskyros slaptažodžio simboliai.

Suklastoto elektroninio laiško, raginančio atsisiųsti programinį kodą eksperimento Nr. 2 (3 priedas) tikslas patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai atsiunčiamas suklastotas elektroninis laiškas, kuriame vartotojai raginami atsisiųsti iš pateiktų nuorodų ir aktyvuoti savo kompiuteriuose programinį kodą. Eksperimento Nr. 2 rezultate buvo nustatytas rizikos organizacijos kibernetinei erdvei laipsnis. *Organizacija X* atrinko 20 vartotojų, kurie dalyvavo šiame eksperimente Nr. 2.

Eksperimentui Nr. 2 vykdyti buvo sukurta pašto paskyra su elektroninio pašto adresu **s0sva1ka1@outlook.com**, iš kurio buvo išsiųstas laiškas atrinktiems eksperimento Nr. 2 dalyviams. Laiškas ragino vartotojos atsisiųsti iš suklastotos svetainės programinį kodą ir jį aktyvuoti savo kompiuteryje.



Laba diena,

labai prašome netrinti šio laiško neperskaičius iki galo. Tai nėra koks pinigų viliojimas prisidengiant baise nelaime, neprašysime JOKIOS finansinės paramos, JOKIŲ PINIGŲ, tiesiog perskaitykite ir nuspręskite ar ištrinti šį laišką, ar vis dėl to skirti minutę dėmesio ir padėti.

Elytei dabar yra 5 metukai, o jai likimas nusprendė dovanoti itin sunkią gyvenimo pradžią – mergaitė yra našlaitė, jos tėveliai tragiškomis aplinkybėmis paliko šį pasaulį svečioje šalyje. Prieš metus su trupučiu Elytei prasidėjo sveikatos problemos, bet mes net nenutuokėm kas mūsų laukia po 3 mėnesių. Elytei nustatyta itin agresyvi ir greitai besivystanti klastinga liga. Mergaitei taikomas stiprus medikamentinis gydymas, tačiau liga sparčiai plinta, to pasekoje, mūsų globojama mažytė labai serga. Blogiausia tai, kad seborėjinė keratozė tik pasekmė kažko, ko mes dar nežinom.

Šiuo metu mums reikalinga itin skubi (vasario 23d., 2015 m.) kelionė į Vokietijos Universitetinę Vaikų kliniką, kur bus tęsiami tolimesni tyrimai bei gydymas Elytei. Deja, pinigų, kuriuos turime, neužtenka padengti visų medicininių išlaidų. Nesulaukę pagalbos iš valstybės, kreipėmės į daugybę žmonių ir organizacijų. Pirmieji į pagalbos šauksmą atsiliepė kaip nebūtų keista visai dar jauni žmonės – Vilniaus kolegijos studentai programuotojai. Jie pasiūlė sukurti linksmąją programėlę, kurią platinti iš savo serverio sutiko kelios užsienio kompanijos ir už kiekvieną atsiųstą programėlę perveda po 12 euro centų į Elytės gydymo sąskaitą. Sunku pradžioje buvo patikėti, kad toku būdu įmanoma surinkti reikiamą sumą, tačiau Šauniųjų Studentų dėka jau yra sukaupta per 28 465 eurai.

Ir trūksta visai nedaug, tereikia kad dar keletas neabejingų žmonių atsisiųstų linksmąją programėlę į savo kompiuterį ar telefoną ir taip praskaidrintų savo darbo dienos kasdienybę ir tuo pačiu suteiks vargšei ligonukei vilį.

Atsisiųskite linksmąją programėlę – katinėlį.

Jei norite atsisiųsti katinėlį į kompiuterį – spauskite čia >> http://dovvnload.mikrosoft.com/

Jei norite atsisiųsti katinėlį į išmanųjį telefoną – spauskite čia >> http://play.google.com/

Jei nepavyksta, pabandykite čia >> http://www.dovvnload.com

Gal kelerių metų parke jūs sutiksite Elyte, kur ji laksty ir valgys ledus, o Jūs žinosite, kad tai ir Jūsų nuopelnas. Jeigu nieko nedarysime šiandien, visų tų dalykų mažoji negalės patirti niekada gyvenime. Padėkite Elytei pasveikti.

Ačiū Jums pagalbą!

SoSVAtKAt

11 pav. Suklastotas laiškas, naudotas eksperimente Nr. 2

Eksperimento Nr. 2 rezultatai buvo registruojami specialiai šiam tikslui skirtame *Organizacijos X* kompiuteryje, kuriame *Microsoft Internet Information Services* platformoje buvo sukurta suklastota svetainė, kurioje patalpinta kompiuterinė rinkmena **katinukas.exe**. Vartotojui atsisiuntus ir aktyvavus šią kompiuterinę rinkmeną, *Organizacijos X* bendrame tinklo kataloge būtų sukuriamas katalogas, kuris pavadinamas vartotojo vardu, o tame kataloge sukuriamos dvi kompiuterinės rinkmenos, kuriose registruojamas kompiuterio vardas, *IP* adresas, *MAC* adresas ir įdiegtos vartotojo kompiuteryje *PĮ* sąrašas.

„Pamestų“ *USB* laikmenų eksperimento Nr. 3 (4 priedas) tikslas patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai vartotojai randa *USB* laikmeną su programiniu kodu.

Eksperimento Nr. 3 rezultate buvo nustatytas rizikos organizacijos kibernetinei erdvei laipsnis. Eksperimentui Nr. 3 buvo skirtos penkios *USB* laikmenos, kurias rado atsitiktiniai eksperimento Nr. 3 dalyviai. *Organizacijos X* skirtingose vietose (bendro naudojimo patalpose) buvo paliktos penkios *USB* laikmenos su programiniu kodu, *USB* laikmenoms buvo suteiktas pavadinimas **SVARBU**. Kiekvienoje *USB* laikmenoje buvo penkios kompiuterinės rinkmenos, kurias vartotojui aktyvavus, *Organizacijos X* bendrame tinklo kataloge buvo registruojami eksperimento Nr. 3 rezultatai:

1. **kamasutra.pdf.exe** – pateikiama vartotojui kaip tekstinė, PDF formato, rinkmena. Aktyvavus sukuriama tekstinė kompiuterinė rinkmena, kurioje registruojamas vartotojo vardas ir kompiuterio vardas.

2. **MUZIKA\geriausiosdainos.mp3.exe** – pateikiama vartotojui kaip muzikinė, MP3 formato, rinkmena. Aktyvavus sukuriama tekstinė kompiuterinė rinkmena, kurioje pateikiamas vartotojo darbalaukyje esančių kompiuterinių rinkmenų sąrašas.

3. **FILMAI\50pilkuatspalviu.avi.exe** – pateikiama vartotojui kaip video, AVI formato, rinkmena. Aktyvavus sukuriama tekstinė kompiuterinė rinkmena, kurioje pateikiamas vartotojo kompiuteryje įdiegtos programinės įrangos sąrašas.

4. **ZAIDIMAI\angrybirds.exe** – pateikiama vartotojui kaip vykdomoji, EXE formato, rinkmena. Aktyvavus sukuriama tekstinė kompiuterinė rinkmena, kurioje registruojamas *IP* adresas.

5. **FOTO\intymi.jpg.exe** – pateikiama vartotojui kaip grafinė, JPG formato, rinkmena. Vartotojui aktyvavus kompiuterinę rinkmeną sukuriama tekstinė kompiuterinė rinkmena, kurioje registruojamas *MAC* adresas.

Tam, kad nustatyti *Organizacijai X* pasiūlytų kibernetinės erdvės gynybos stiprinimo priemonių efektyvumą, autorius naudojo kryptingo interviu metodą (klausimai priede 7). Siekdamas kuo tikslesnių duomenų apie taikytų kibernetinės gynybos stiprinimo priemonių efektyvumą, autorius atliko eksperimentą Nr. 4. Buvo pasirinktas laboratorinio eksperimento metodas, kuris tinkamas esant laiko ribotumui, tačiau autoriaus manymu tai neturėtų iškreipti tyrimo rezultatų, nes tikrinamos įdiegtos saugumo priemonės, kurios vienodai veikia tiek natūralioje, tiek testavimo aplinkose. Eksperimentui Nr. 4 buvo panaudota eksperimento Nr. 3 metodologija ir technologijos. *Organizacijos X* IT tarnybos atstovo apklausos metu buvo surinkti duomenys apie taikytas priemones ir pagal tai sumodeliuotas eksperimento Nr. 4 scenarijus:

1. Paruošiama *USB* laikmena su imituojamu kenkimo *PĮ* kodu;
2. *Organizacija X* skiria kompiuterį ir sukuria vartotojo paskyrą;
3. *USB* laikmena prijungiama prie kompiuterio;
4. Aktyvuojama kenkimo *PĮ* imitacija;
5. Sėkmingo kenkimo *PĮ* imitacijos aktyvavimo rezultatai registruojami *Organizacijos X* bendrame tinklo kataloge.

Eksperimentas Nr. 4 buvo papildytas *Organizacijos X* antivirusinės *PĮ* testavimo priemone, *EICAR* antivirusiniu testavimo kodu:

Šaltinis: eicar.org, 2015

12 pav. EICAR AV PĮ testavimo kodas

Eksperimento Nr. 4 metu taip pat buvo naudojama *MBSA 2.3 PĮ,* kurios pagalba buvo patikrintas *PĮ* naujinimo procesas. Minėtos priemonės, naudotos šiame eksperimente, leido padaryti išvadas apie daugiasluoksnės gynybos priemonių efektyvumą kiekviename lygmenyje.

Tyrimo metu naudoti apklausos, stebėjimo, natūralių ir laboratorinių eksperimentų metodai papildė vieni kitų duomenis, o tai sudarė galimybes padidinti bendrą tyrimo patikimumą

3.2. ORGANIZACIJOS X ESAMOS KIBERNETINĖS ERDVĖS GYNYBOS PADĖTIES ANALIZĖ

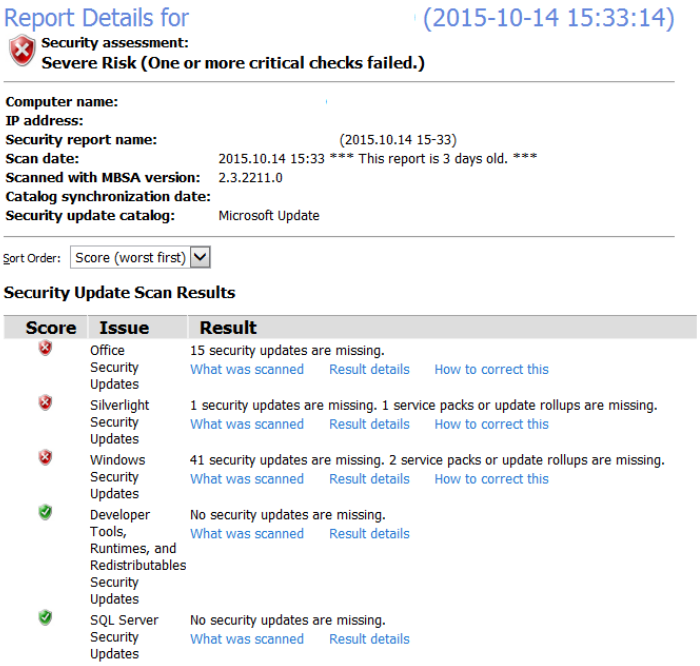
Tyrimo metu nustatyta, kad *Organizacija X* turi 220 kompiuterinių darbo vietų, kas atitinka vidutinės organizacijos sąvoką. Kritinėmis paslaugomis įvardinta Interneto prieiga, buhalterinės apskaitos sistema bei personalo valdymo sistemos duomenys. *Organizacija X* savo elektroninio pašto sistemą yra perkėlusi į „debesį“, t.y. naudojasi trečios šalies teikiama elektroninio pašto prieglobos paslauga, kuri taip pat užtikrina elektroninio pašto saugą nuo virusinių atakų.

IT tarnybos vadovas apsaugą nuo duomenų nutekinimo ir kenkimo programinės įrangos atakų išskyrė kaip aktualiausias kibernetinės gynybos kontekste. *Organizacija X* netaiko jokios kibernetinės gynybos metodikos, tačiau atsižvelgia į teisės aktus, vadovaujasi LR Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 patvirtintais „Bendraisiais elektroninės informacijos saugos reikalavimų, saugos dokumentų turinio gairių bei valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašais“ (toliau – Bendrieji elektroninės informacijos saugos reikalavimai) bei kitais kibernetinę saugą reglamentuojančiais teisės aktais. Viduje vadovaujamasi direktoriaus patvirtintomis „Naudojimosi kompiuteriais *Organizacijoje X* taisyklėmis“ (2010 m.) ir „Tarnybinių mobiliųjų telefonų ir mobiliojo ryšio *SIM* kortelių naudojimo taisyklėmis“ (2014 m.).

Tyrimo metu nustatyta, kad *Organizacija X* neturi patvirtintos kibernetinių incidentų valdymo procedūros. Vartotojai pastebėję sutrikusį kompiuterio ar sistemos veikimą, kreipiasi tiesiogiai į tarnybą telefonu arba registruoja organizacijos vidiniame tinkle esančioje sistemoje. Tačiau *Organizacija X* turi patvirtintas veiklos atkūrimo ir tęstinumo valdymo procedūras, kuriomis vadovaujantis yra daromos kritinių sistemų atsarginės kopijos ir atliekami periodiniai šių kopijų atkūrimo testai. Autorius taip pat pastebi, kad *Organizacijoje X* IT ūkio valdymas nėra paremtas

pripažintomis metodikomis, tokiomis kaip *ITIL*[12] arba *CoBIT*[13], todėl galima daryti prielaidą, kad IT ūkis organizacijoje yra valdomas ne sistemingai, bet intuityviai ir yra paremtas „gaisrų gesinimu“, t.y. kai problema yra sprendžiama ne prieš jai iškylant, bet kai jau juntami problemos padariniai, tai pasakytina ir apie kibernetinę gynybą.

Taip pat paminėtina, kad organizacijoje nėra nustatyto rizikų valdymo proceso, ši prielaida buvo suformuluota autoriui atlikus organizacijos tinklo stebėjimą. Aptiktos spragos pavaizduotos 8 paveikslėlyje, kur matome programinės įrangos saugumo naujinimo skenavimo rezultatus, iš kurių galime spręsti apie aukštą saugumo riziką, nes neįdiegta net 41 operacinės sistemos *Microsoft Windows* saugumo naujinimas, 15 raštinės paketo *Microsoft Office* saugumo naujinimų bei trūksta vieno *Microsoft Silverlight* saugumo naujinimo. Tokia padėtis, autoriaus manymu, yra itin pavojinga, nes sukuria prielaidas, kad esančios saugumo spragos *Organizacijos X* tinkle gali būti išnaudotos kenkimo programinės įrangos įdiegimui ar užgrobiant organizacijos pažeidžiamus kompiuterius.


Report Details for (2015-10-14 15:33:14)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:
IP address:
Security report name: (2015.10.14 15-33)
Scan date: 2015.10.14 15:33 *** This report is 3 days old. ***
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date:
Security update catalog: Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

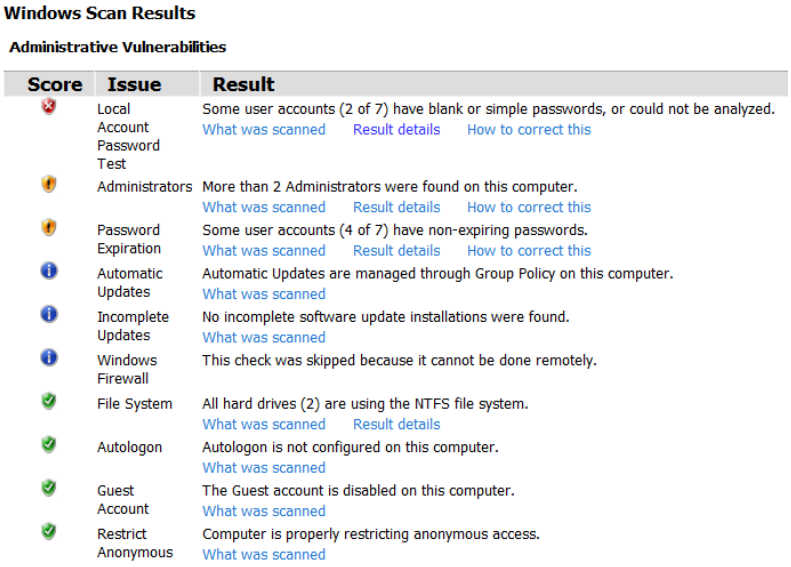
Score	Issue	Result
	Office Security Updates	15 security updates are missing. What was scanned Result details How to correct this
	Silverlight Security Updates	1 security updates are missing. 1 service packs or update rollups are missing. What was scanned Result details How to correct this
	Windows Security Updates	41 security updates are missing. 2 service packs or update rollups are missing. What was scanned Result details How to correct this
	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. What was scanned Result details
	SQL Server Security Updates	No security updates are missing. What was scanned Result details

13 pav. Organizacijos X saugumo naujinimų ataskaita

Toliau apžvelkime *Microsoft Windows* operacinės sistemos saugios konfigūracijos skenavimo rezultatus (9 pav.). Ataskaitoje matoma, kad sistemoje dvi vietinių vartotojų paskyros turi nesudėtingus slaptažodžius arba jų visai neturi, o tai sudaro palankias sąlygas perimti sistemos valdymą tų vartotojų teisėmis, ypač aukštas pavojaus lygis kyla, jei tai yra administratoriaus teisės. Kita saugumo problema susijusi su vartotojų paskyromis yra nesikeičiantys keturių vartotojų

[12] ITIL (angl. the IT Infrastructure Library), tai dokumentų rinkinys, kuris naudojamas IT paslaugų valdymui organizuoti. Sulygiuota su ISO 20000 standartų seriją. http://www.itil.org.uk/
[13] CoBIT yra pasaulyje pripažįstama kaip viena efektyviausių IT ūkio valdymo organizacijoje metodika, kuri paremta patvirtintomis geriausiomis praktikomis. http://www.isaca.org/cobit/pages/default.aspx.

paskyrų slaptažodžiai. Sistemoje yra dvi administratoriaus paskyros, tai nėra saugumo pažeidimas, jei administravimo teises turintys vartotojai apsaugoti sudėtingais slaptažodžiais. Taip pat pabrėžtina, kad jei nėra būtinybės sistemoje turėti papildomų administravimo paskyrų – jas reikėtų panaikinti. Autorius mano, kad gauti rezultatai, rodo jog organizacija turėtų nustatyti vartotojų paskyrų ir slaptažodžių kūrimo ir naudojimo politiką, kurios vykdymą organizacijoje būtų galima realizuoti pasitelkiant technines priemones.



Windows Scan Results

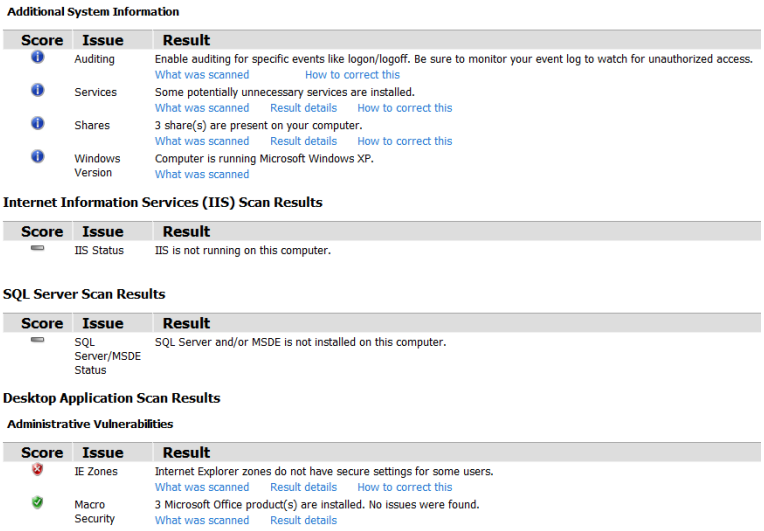
Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (2 of 7) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
	Password Expiration	Some user accounts (4 of 7) have non-expiring passwords. What was scanned Result details How to correct this
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Windows Firewall	This check was skipped because it cannot be done remotely.
	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

14 pav. Organizacijos X operacinės sistemos pažeidžiamumai

Informacija apie kitus sistemos saugumo nustatymus pateikta 10 pav. Pagal gautus rezultatus matome, kad sistemoje nėra registruojami vartotojų prisiregistravimo ir išsiregistravimo duomenys, kas apsunkina kibernetinių incidentų tyrimą. Taip pat sistemoje veikia nesaugi nuotolinio administravimo *Telnet* tarnyba, kuri neužtikrina saugaus ryšio, todėl ją būtina išjungti, jeigu ji nėra reikalinga. Sistemoje veikianti operacinės sistemos *Microsoft Windows XP* versija yra nebepalaikoma gamintojo nuo 2014-04-08[14], todėl tokios sistemos naudojimas tinkle yra itin pavojingas, nes gamintojas nebekuria sistemos saugumo naujinimų. Dar kita svarbi saugumo problema sistemoje yra nesaugūs naršyklės nustatymai, kas sudaro galimybes sistemoje įdiegti kenkimo programinę įrangą, vartotojui naršant nesaugiose svetainėse.

[14] http://windows.microsoft.com/en-us/windows/end-support-help



Additional System Information

Score	Issue	Result
ℹ	Auditing	Enable auditing for specific events like logon/logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
ℹ	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
ℹ	Shares	3 share(s) are present on your computer. What was scanned Result details How to correct this
ℹ	Windows Version	Computer is running Microsoft Windows XP. What was scanned

Internet Information Services (IIS) Scan Results

Score	Issue	Result
–	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
–	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
✓	Macro Security	3 Microsoft Office product(s) are installed. No issues were found. What was scanned Result details

15 pav. Organizacijos X kiti sistemos pažeidžiamumai

Autorius, apibendrindamas gautus tinklo stebėjimo rezultatus, teigia, kad visi 33 kompiuteriai turi po vieną ar daugiau aukšto rizikos pažeidžiamumų, tačiau 4 kompiuterių būklė yra itin pavojinga, nes juose aptikta daug įvairių saugumo problemų, kurias išnaudojus galima įdiegti kenkimo programinę įrangą arba perimti sistemos valdymą. Šio stebėjimo rezultatus, autorius panaudojo planuodamas eksperimentus Nr. 2 ir Nr. 3, kurių metu buvo imituojamas kenkimo programinės įrangos diegimas *Organizacijos X* tinkle.

Organizacijos X vartotojai ir IT tarnybos darbuotojai nedalyvauja specializuotose kibernetinio saugumo mokymo programose. Kibernetinio saugumo ugdymas yra ribotas, dažniausiai vykdomas tik pasklidus viešoje erdvėje informacijai apie kokią pavojingą kibernetinę grėsmę, ši informacija vartotojams pateikiama elektroniniu paštu arba talpinama organizacijos vidiniame tinkle. Autorius daro prielaidą, kad švietimo programų kibernetinio saugumo srityje deficitas sudaro organizacijoje palankią terpę kibernetiniams incidentams, šią prielaidą patvirtino eksperimentų, Nr. 1 ir Nr. 3, rezultatai.

Eksperimento Nr. 1 metu buvo nustatyta, kad suklastotoje svetainėje apsilankė 7 unikalūs vartotojai, iš kurių vienas suvedė savo tarnybinio elektroninio pašto paskyros duomenis. Remdamasis eksperimento Nr. 1 rezultatais autorius teigia, kad rizikos organizacijos kibernetinei erdvei, kai vartotojai yra raginami įvesti savo paskyrų prisijungimo duomenis, laipsnis yra aukštas, nes gauti prisijungimo duomenys suteikia galimybę prisijungti prie *Organizacijos X* elektroninio pašto sistemos. Taip pat paminėtina, kad organizacijos IT tarnyba neužregistravo nei vieno vartotojo kreipinio dėl gauto laiško, todėl autorius mano, kad organizacijoje nėra nustatyto reagavimo į kibernetinius incidentus proceso, o tai vėlgi parodo kibernetinio švietimo programų trūkumo pasekmes.

Eksperimento Nr. 3 metu buvo užregistruotas vienas programinio kodo aktyvavimo atvejis, kai vienas vartotojas aktyvavo PDF rinkmenos su kenksmingo kodo imitacija. Remdamasis

eksperimento Nr. 3 rezultatais autorius teigia, kad rizikos organizacijos kibernetinei erdvei, kai vartotojai randa *USB* laikmenas su programiniu kodu, laipsnis yra aukštas. *Organizacijos X* IT tarnyba gavo vartotojų pranešimus dėl rastų *USB* laikmenų, tačiau pasak *Organizacijos X* IT tarnybos vedėjo pavaduotojo, tai veikiausiai susiję su žmonių geranoriškumu.

Paprašytas įvardinti kibernetinių incidentų pavyzdžius, IT tarnybos vadovas negalėjo to padaryti, nes *Organizacija X* neturi duomenų apie prieš ją vykdytas kibernetinės atakas ar bandymus jas įvykdyti. Tokia situacija susiklosčiusi todėl, kad *Organizacija X* neturi pakankamų kibernetinės gynybos išteklių. *Organizacija X* 2008 – 2011 m. ekonominės krizės laikotarpiu vykdė taupymą ne tik kibernetinio saugumo, bet ir bendrai IT ūkio sąskaita. IT tarnybos vadovas pasidžiaugė, kad bent jau pavyko išlaikyti IT personalą. Bendrai *Organizacija X* savo pasirengimą vykdyti kibernetinę gynybą vertina šešetu dešimtbalėje skalėje, nes organizacija, praėjus ekonominei krizei, skyrė lėšų techninių saugumo priemonių įsigijimui, tačiau kaip silpniausią vietą nurodė socialinį faktorių. Tačiau, autorius mano, kad vien tik techninių priemonių taikymas, negarantuoja sėkmingos kibernetinės gynybos, tam reikalingas holistinis požiūris, kuris apimtų techninį, procedūrinį ir socialinį vektorių. Tokiu būdu būtų galima kurti daugiasluoksnės kibernetinės gynybos sistemą, kas padidintų bendrą kibernetinės gynybos patikimumą.

Tyrimo metu paaiškėjo, kad organizacija yra įsigijusi *Fortigate* kompanijos ugniasienę, kuri atskiria organizacijos vidinį tinklą nuo Interneto ir turi antivirusinės apsaugos funkcionalumą, leidžiantį vykdyti virusų paiešką Interneto sraute. Organizacijos kompiuteriuose ir serveriuose dominuoja *Microsoft Windows* šeimos operacinės sistemos, kurias nuo virusų saugo *ESET* kompanijos antivirusinės sistemos sprendimas, kuris suteikia centralizuotą valdymą, automatizuotus antivirusinės *PĮ* naujinimus bei virusų aprašų duomenų bazės naujinimus, kurie tikrinami kas tris valandas. Tačiau, organizacija neturi techninių sprendimų, kurie suteiktų galimybę blokuoti tinklo prieigą, kompiuteriams neturintiems veikiančios antivirusinės *PĮ* arba įdiegtų kritinių naujinimų. Taip pat organizacijoje nėra taikomos papildomos priemonės apsaugai nuo virusų.

Organizacijoje vartotojų paskyros valdomos centralizuotai, tam naudojama *Microsoft Active Directory* technologija. Vartotojų paskyros yra kuriamos gavus kreipinį iš vartotojo padalinio vadovo arba IT tarnybos vadovo nurodymu, vartotojui nereikia pildyti jokio dokumento dėl paskyros sukūrimo. Administravimo teisės vartotojams nėra suteikiamos, bet yra tam tikra grupė vartotojų, kurių programinės ar techninės įrangos konfigūracijų ypatumai reikalauja administravimo teisių.

Atlikus *Organizacijos X* dokumentų analizę nustatyta, kad pagal kompiuterių naudojimo taisykles, vartotojams yra draudžiama diegti programinę įrangą į tarnybinius kompiuterius, todėl programinę įrangą į kompiuterius diegia administratoriai lokaliai, dažniausiai pagal vartotojų kreipinius. Eksperimento Nr. 2 metu nebuvo užregistruotas nei vienas bandymas prisijungti,

atsisiųsti ar aktyvuoti kompiuterinę rinkmeną. Remiantis eksperimento Nr. 2 rezultatais galima teigti, kad rizikos organizacijos kibernetinei erdvei, kai vartotojai raginami atsisiųsti ir aktyvuoti programinį kodą, laipsnis yra žemas. Autorius daro prielaidą, kad toks rezultatas veikiausiai yra organizacijos patvirtinų procedūrų ir vartotojų sąmoningumo pasekmė, nes pagal „Naudojimosi kompiuteriais *Organizacijoje X* taisykles“ kompiuterių vartotojams draudžiama diegti programinę įrangą tarnybiniuose kompiuteriuose. Kaip ir pirmojo eksperimento metu, organizacijos IT tarnyba neužregistravo nei vieno vartotojo kreipinio dėl gauto laiško. Pagal eksperimento Nr. 2 rezultatus galima daryti prielaidą, kad organizacinės priemonės, konkrečiu atveju „Naudojimosi kompiuteriais *Organizacijoje X* taisyklės“, yra efektyvi kibernetinės gynybos priemonė.

Paminėtina, kad organizacija neturi patvirtinto leistinos programinės įrangos sąrašo, o taip pat neturi techninio sprendimo centralizuotam programinės įrangos diegimui ir naujinimui į vartotojų kompiuterius ar tarnybines stotis. Tyrimo metu nustatyta, kad programinė įranga naujinama arba administratoriams diegiant ją lokaliai, arba pasikliaujant programinės įrangos automatinių naujinimų nustatymais. Autoriaus mano, kad reikėtų keisti *Organizacijos X* programinės įrangos diegimo ir valdymo procedūras, taikyti centralizavimo principą. Programinės įrangos diegimas iš vienos centralizuotos vietos užtikrintų *PĮ* versijų kontrolę, taip pat procedūrą autorius rekomenduoja papildyti *PĮ* rinkmenų integralumo patikros procesu, kas leistų užtikrinti, kad naudojama *PĮ* nėra pakeista ir neturi kenkimo kodo.

3.3. KIBERNETINĖS ERDVĖS GYNYBOS STIPRINIMO REKOMENDACIJOS ORGANIZACIJAI X

Autorius, apklausęs *Organizacijos X* IT tarnybos vadovus bei atlikęs tinklo stebėjimą ir tris natūralius eksperimentus, pagrįstus socialinės inžinerijos technologijomis, išskiria šias *Organizacijos X* kibernetinės gynybos problemas:

1. *Organizacijos X* tinklo stebėjimo rezultatai parodė, kad organizacija neturi rizikos valdymo proceso, kurio metu būtų vykdomi tinklo pažeidžiamumų patikrinimai, todėl tinkle yra įrenginių, turinčių kritinių pažeidžiamumų, kurie gali būti išnaudoti kenkimo programinės įrangos arba programišių.

2. Eksperimentai Nr. 1 ir Nr. 3 parodė, kad *Organizacijos X* darbuotojai neturi gebėjimų atpažinti socialinės inžinerijos atakų, todėl kyla didelė rizika, kad gali būti perimti vartotojų paskyrų prisijungimo duomenys arba įdiegta kenkimo programinė įranga, kas savo ruožtu sudaro prielaidas duomenų nutekinimui arba sistemų užgrobimui.

3. Eksperimento Nr. 2 rezultatai parodė, kad *Organizacijos X* darbuotojai žino ir vadovaujasi nustatytomis procedūromis. Tačiau pačios procedūros, nustatytos „Naudojimosi kompiuteriais

Organizacijoje X taisyklėse“, yra pasenusios ir jas būtina atnaujinti ir papildyti, o tada supažindinti visus darbuotojus.

4. Eksperimento Nr. 3 metu nustatyta, kad *Organizacija X* kibernetinėje gynyboje netaiko „gynybos į gylį“ principo, todėl pažeidus kibernetinės gynybos priemones viename lygmenyje, pažeidžiama tapo visa organizacijos kibernetinė erdvė.

5. *Organizacija X* netaiko holistinio požiūrio savo kibernetinės erdvės gynyboje, daugiausia pastangų yra nukreipta į technologinį grėsmių vektorių.

Autorius siūlo *Organizacijai X* taikyti *20 CSC* metodiką, kuri naudoja holistinį metodą, savo kibernetinės erdvės gynybos sistemos stiprinimui. *Organizacijai X* rekomenduojamos kibernetinės gynybos priemonės pateiktos 3 lentelėje (žr. 8 priedą). *Organizacijai X* pasiūlytos kibernetinės erdvės gynybos priemonės apima visus tris grėsmių vektorius: žmones, technologijas ir procesus. Pasiūlytų priemonių įdiegimas organizacijoje nereikalauja papildomų finansinių išteklių, autorius stengėsi parinkti ekonomiškai efektyvias priemones, tačiau jos reikalauja laiko sąnaudų, todėl priemones galima diegti ne visas iš karto, o palaipsniui.

Autorius siūlo vadovautis gynybos į gylį principu, pavyzdžiui stiprinant gynybą nuo kenkimo programinės įrangos taikyti *CSC* 2-1, 2-6, 3-10, 4-5, 5-3, 5-4, 5-6, 5-7 ir 12-7 priemones. *CSC* 12-7 priemonės taikymas sudarytų pirmą gynybinį sluoksnį, kuriame būtų atskiriamos administravimo ir paprastos vartotojų paskyros, ribojamas administravimo paskyrų naudojimas Internetui naršyti ir elektroniniam paštui pasiekti. Tokiu atveju sekančiame gynybos sluoksnyje veiktų *CSC* 2-1 priemonė, kuri užtikrintų, kad sistemose naudojama tik leistina programinė įranga, o *CSC* 2-6 priemonė blokuotų pavojingų rinkmenų tipus. Kitame lygmenyje *CSC* 3-10 priemonė užtikrintų saugių konfigūracijų, tokių kaip pvz.: Interneto naršyklių saugos nustatymai taikymą sistemose, kas apsunkintų kenkimo programinės įrangos pateikimą į sistemas per Interneto naršykles. *CSC* 4-5 priemonė per programinės įrangos naujinimo ir pataisų diegimo procesą suteiktų papildomą apsauginį sluoksnį, o *CSC* 5-6 priemonė saugotų programinę įrangą nuo bandymų išnaudoti pažeidžiamumus. Ketvirtame saugumo lygmenyje priemonės *CSC* 5-3, 5-4 ir 5-7 apribotų kenkimo programinės įrangos patekimą per išorines laikmenas, tokias kaip *USB* atmintinės, *CD/DVD* diskai ir pan. Taip pat *Organizacija X* gali taikyti ir kitas priemones, kurios formuotų papildomus gynybinius lygmenis, pavyzdžiui *CSC* 13-1 (blokuojama tinklo prieiga prie žinomų kenksmingų Interneto adresų) ir *CSC* 13-6 (išeinančio į Internetą srauto valdymas) priemonės sukurtų papildomą sluoksnį organizacijos tinklo pakraštyje.

Aukščiau paminėtos technologinės rekomendacijos turi koreliuoti su procedūrinėmis, tai leis ne tik pagrįsti technologinių priemonių būtinumą, bet ir dokumentuoti jas, kas padės užtikrinti, kad įdiegtos visos numatytos priemonės ir jos veikia taip kaip numatyta. Tyrimo metu buvo nustatyta,

kad organizacija turi 2010 m. patvirtintas „Naudojimosi kompiuteriais *Organizacijoje X* taisykles“, todėl autorius siūlo organizacijai atnaujinti taisykles, jas papildant:

1. Vartotojų paskyrų valdymo procesu, kuriame būtų nustatyta privaloma naujų vartotojų kibernetinio saugumo ugdymo procedūra, o taip pat būtų numatyta slaptažodžių politika ir sąlygos kaip kuriamos ir valdomos administravimo paskyros.
2. Rizikų valdymo procesu, kuriame būtų numatytos nuolatinės rizikų vertinimo ir trūkumų šalinimo procedūros.
3. Incidentų valdymo procesu, kuriame būtų paskirtos incidentų valdymo funkcijos konkrečiam personalui bei nustatytos incidentų valdymo fazės, o taip pat numatyta kaip ir kada aktyvuojamos patvirtintos organizacijos veiklos atkūrimo ir tęstinumo procedūros.
4. Programinės įrangos valdymo procesu, kuriame būtų numatytas leistinos *PĮ* sąrašas bei diegimo procedūros, užtikrinančios naudojamos *PĮ* versijų kontrolę bei integralumą.
5. Reikalavimus standartinėms konfigūracijoms, kuriose būtų numatytos privalomos darbo ir tarnybinių stočių saugumo konfigūracijos.
6. Interneto ir elektroninio pašto naudojimo organizacijoje tvarka.
7. Antivirusinės saugos politika, kurioje būtų numatyti reikalavimai *AV PĮ,* jos nustatymams, bei virusų paieškos procedūros. Taip pat rekomenduojama įtvirtinti, kad skirtinguose lygiuose turi būti naudojami skirtingų gamintojų antivirusiniai varikliai.
8. Išorinių laikmenų naudojimo politika, kurioje turi būti nustatytos taisyklės *USB, CD/DVD* ir kt. išorinių laikmenų naudojimui.

Kadangi holistinio požiūrio taikymas yra vienas iš kibernetinės gynybos principų, todėl autorius siūlo organizacijai technologines ir procedūrines kibernetinės gynybos priemones papildyti socialinio vektoriaus gynybos priemonėmis. Visų pirma tai turėtų būti personalo kibernetinio saugumo ugdymo planai, kurie būtų vykdomi ir atnaujinami periodiškai. Visas dabartinis organizacijos personalas turėtų būti supažindintas su organizacijos taisyklėmis pasirašytinai, o naujiems darbuotojams būtų privalomas ir testavimas prieš sukuriant vartotojų paskyras. Taip pat autorius siūlo numatyti sankcijas už grubius organizacijos kibernetinės erdvės saugumo pažeidimus.

3.4. KIBERNETINĖS GYNYBOS STIPRINIMO PRIEMONIŲ EFEKTYVUMO VERTINIMAS

Organizacijos X kibernetinės gynybos tyrimo rezultatai privertė susimąstyti apie realią kibernetinio saugumo padėtį organizacijoje. Kaip viena iš didžiausių spragų įvardijamas žmogiškasis faktorius, todėl yra rengiamas kibernetinio saugumo ugdymo planas bei ieškoma kas galėtų vesti užsiėmimus su *Organizacijos X* darbuotojais.

Organizacijai X didžiausią susirūpinimą sukėlė eksperimentų Nr. 1 ir Nr. 3 rezultatai. Būtent todėl buvo pradėtas rengti darbuotojų kibernetinio saugumo ugdymo planas, tačiau tai yra laikui imlus procesas, o tai paskatino lygiagrečiai taikyti kibernetinės „gynybos į gylį“ principą, nes *Organizacija X* mano, kad technologinės priemonės turi dubliuoti procedūrines.

Pirmiausiai buvo peržiūrėtas administravimo paskyrų naudojimas ir apribotas administravimo paskyrų naudojimas Internetui naršyti ir elektroniniam paštui pasiekti. Taip pat buvo įdiegta *CSC* 2-6 priemonė ir dabar grupių politikos pagalba blokuojami pavojingų rinkmenų tipai, tokie kaip ***.exe**, ***.bat**, ***.com** ir pan. Šiuo metu *Organizacija X* baigia ruošti pagrindą *CSC* 2-1 priemonės taikymui, t.y. sudaromas leistinos *PĮ* sąrašas, kuris įtrauktas į atnaujinamų „Naudojimosi kompiuteriais *Organizacijoje X* taisyklių“ projektą. Tikimasi, kad pradėtas taikyti *Microsoft EMET v5.2* įrankis padės apsaugoti nuo naudojamos *PĮ* pažeidžiamumų išnaudojimo.

Organizacijos tinkle išjungtas *Autoplay* funkcionalumas bei nustatyta, kad antivirusinė *PĮ* automatiškai pradėtų virusų paiešką prijungtose išorinėse laikmenose, taip pat svarstoma galimybė uždrausti arba bent jau minimizuoti *USB* laikmenų naudojimą organizacijoje, tačiau susiduriama su dideliu vidiniu pasipriešinimu.

Saugios konfigūracijos valdomos grupinių politikų pagalba, kaip pavyzdys gali būti paminėtas *Restricted Groups* funkcionalumas, kuris periodiškai tikrina vartotojų paskyrų priklausymą administratorių grupei, jei aptinkama vartotojo paskyra, kuriai „neteisėtai“ suteiktos administravimo privilegijos, tokia paskyra yra automatiškai pašalinama iš administratorių grupės.

Organizacija X jau kurį laiką taiko išeinančio į Internetą srauto valdymą, dabar papildomai taikoma *CSC* 13-1 priemonė – blokuojami žinomi kenksmingi Interneto adresas, kad vartotojai negalėtų jų pasiekti.

Organizacija X dėl išteklių trūkumų, konkrečiai – talpos (diskinės vietos) ribotumo, pradėjo naudoti *Microsoft WSUS* funkcionalumą, leidžiantį valdyti *Microsoft PĮ* naujinimų diegimo parametrus, bet pačias naujinimų rinkmenas saugoti *Microsoft* tinkle ir parsiųsti jas į kompiuterius tik diegimui vykdyti. Taip *Organizacija X* sutaupo diskinės vietos Interneto ryšio apkrovimo sąskaita, tačiau naujinimų diegimo laiko nustatymas nedarbo valandomis šią problemą išsprendžia. Kitų gamintojų *PĮ* diegimas vykdomas per *Microsoft* grupinių politikų *Software Installation* funkcionalumą, jei nėra techninių galimybių *PĮ* diegti tokiu būdu, *Organizacija X* skyrė tinklo diske vietą į kurią saugomos diegimo rinkmenos, taip siekiama turėti vieną centralizuotą *PĮ* diegimo rinkmenų talpyklą, kur saugomos patikrintos diegimo rinkmenos.

Organizacijoje X buvo sukurta testavimo aplinka, kurioje tikrinami visi nustatymai prieš perkeliant juos į darbinę aplinką. Didžiausia kliūtis kibernetinės gynybos priemonių diegimui įvardintas vidinis pasipriešinimas, daugelis kolegų neigiamai reaguoja į bet kokius ribojimus ar draudimus, tačiau IT tarnyba stengiasi komunikuoti, aiškinti taikomų priemonių būtinumą. Taip pat

visos priemonės įtraukiamos į „Naudojimosi kompiuteriais *Organizacijoje X* taisyklių“ atnaujinimo projektus.

Organizacija X 20 CSC metodiką įvertino kaip pakankamai efektyvią, nes ji yra lengviau suprantama ir paprasčiau įgyvendinama todėl, kad kiekviena saugumo priemonė turi jos realizavimo aprašymą, kas palengvina priemonės diegimą. Būtent to buvo pasigendama „Bendruosiuose elektroninės informacijos saugos reikalavimuose“, todėl nuo šiol *Organizacija X* planuoja taikyti *20 CSC* metodiką, tam kad atitikti šiuos reikalavimus.

Organizacijos X IT tarnybos vedėjo pavaduotojo pastebėjimu be išorinės pagalbos, t.y. jei nebūtų šio tyrimo, greičiausiai *Organizacijoje X* nebūtų įvykę jokių pokyčių kibernetinės gynybos srityje. Dabar organizacija mato, kad yra pakankamai efektyvių ir papildomų kaštų nereikalaujančių priemonių, tuo pačiu pabrėžiama pagalbos iš išorės svarba.

Organizacijoje X buvo atliktas eksperimentas Nr. 4, kuris leido praktiškai patikrinti kibernetinio principo „gynyba į gylį“ efektyvumą, konkrečiai buvo tikrinamos *Organizacijos X* įdiegtos priemonės: *CSC* 2-6 , 3-2, 3-3, 3-10, 5-3, 5-4, 12-7 ir 13-1.

Eksperimentui Nr. 4 *Organizacija X* skyrė kompiuterį ir sukūrė vartotojo paskyrą, tokiomis pačiomis sąlygomis, kaip naujam darbuotojui. Pastaroji paskyra buvo įtraukta į vietinių kompiuterių administratorių grupę, kad patikrinti kaip veikia 3-3, 3-10 ir 12-7 priemonės. Bandymas naršyti vartotojo paskyra, kuri priklauso administratorių grupei, buvo nesėkmingas, nes prieiga nebuvo suteikta, ugniasienė reikalavo įvesti paskyros, kuriai suteikta teisė naršyti, duomenis:

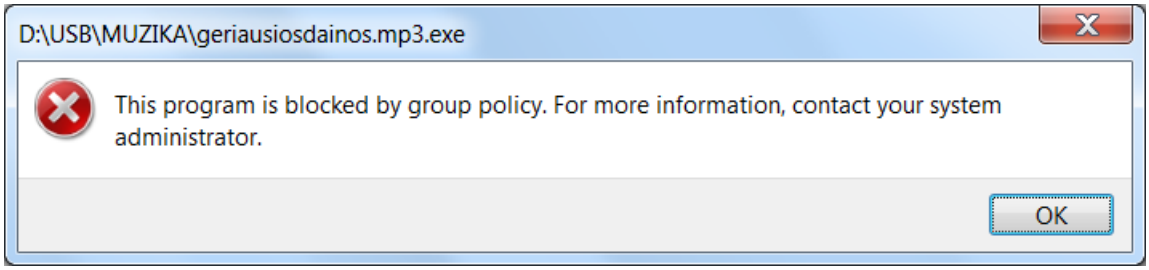
16 pav. Ugniasienės vartotojo autentifikavimo langas

Patikrinus vartotojo paskyros priklausymą vietinių administratorių grupei po 15 min., buvo nustatyta, kad ji automatiškai buvo pašalinta iš minėtos grupės. Todėl galima teigti, kad priemonės *CSC* 3-3, 3-10 ir 12-7 yra įdiegtos ir veikia.

Toliau buvo tikrinamas *CSC* 2-6, 5-3 ir 5-4 priemonių efektyvumas. Prijungus *USB* laikmeną, joje esantis turinys nebuvo automatiškai vykdomas ir startavo *AV PĮ ESET*, kuri aptiko ir pašalino *EICAR* testavimo rinkmeną:

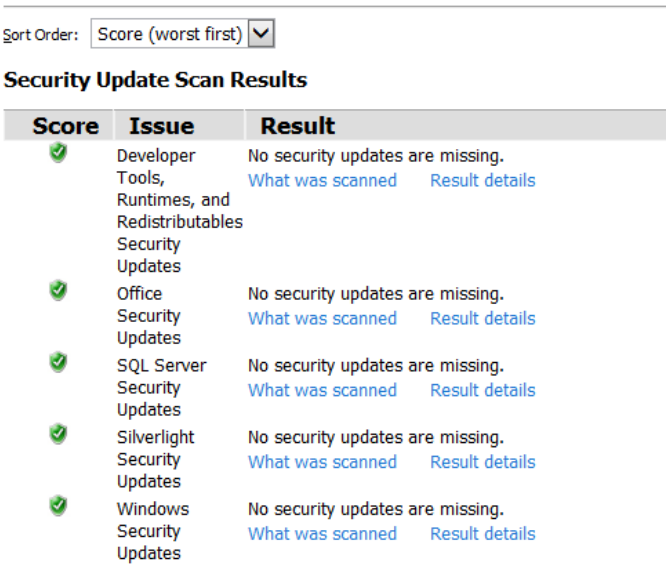
17 pav. AV PĮ ESET pranešimas apie pašalintą *EICAR* rinkmeną

Bandymai aktyvuoti *USB* laikmenoje esančias ***.exe** rinkmenas buvo nesėkmingi, 18 pav. matome pranešimą apie blokuotą **geriausiosdainos.mp3.exe** rinkmeną.



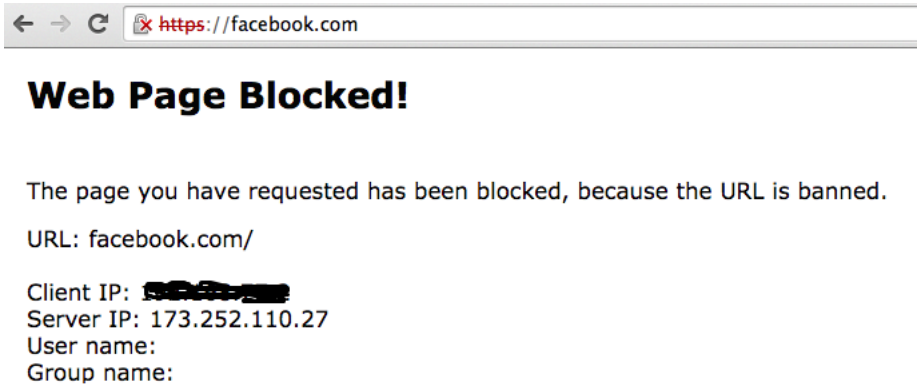
18 pav. Pranešimas apie blokuojamą ***.exe** rinkmeną.

Gauti rezultatai patvirtina įdiegtų *CSC* 2-6, 5-3 ir 5-4 priemonių efektyvumą, kas leidžia daryti prielaidą, kad šios technologinės priemonės, jeigu būtų įdiegtos *Organizacijoje X* prieš atliekant tyrimą, būtų padėjusios apsisaugoti nuo eksperimente Nr. 3 taikytos kenkimo *PĮ* imitacijos. Eksperimento metu taip pat buvo patikrintas *Organizacijos X PĮ* naujinimo procesas, t.y. *CSC* 3-2 priemonės pritaikymas. Patikrinus *Organizacijos X* skirtą kompiuterį, nustatyta, kad jame sėkmingai įdiegti visi naujausi saugumo naujinimai, kas patvirtina, jog *CSC* 3-2 priemonė yra įdiegta. Programinės įrangos naujinimo procesas padeda apsisaugoti nuo organizacijos kompiuteriuose veikiančios *PĮ* žinomų saugumo spragų išnaudojimo.



19 pav. *PĮ* naujinimo ataskaita

Paskutinis testas skirtas *CSC* 13-1 priemonės, kuri blokuoja vartotojų prieigą prie kenksmingų Interneto adresų, patikrai. Testavimo sumetimais portalas **facebook.com** buvo laikinai įtrauktas *Organizacijos X* ugniasienėje į blokuojamų adresų sąrašą, bandant naršyklėje pasiekti minėtą portalą gaunamas pranešimas. Tokiu būdu vartotojams blokuojama prieiga prie kenksmingų Interneto adresų, kas didina bendrą organizacijos gynybos sistemos efektyvumą.



20 pav. Pranešimas apie blokuotą prieigą prie **facebook.com** portalo.

Eksperimento Nr. 4 rezultatai leidžia daryti išvadą, kad *20 CSC* priemonių įdiegimas yra efektyvus, nes dabar *Organizacijoje X* automatiškai yra valdomos administravimo teisės, administratorių paskyroms draudžiama Interneto prieiga, blokuojamos pavojingų tipų rinkmenos, vykdoma automatinė virusų paieška prijungtose išorinėse laikmenos, draudžiama prieiga prie kenksmingų Interneto adresų. Šios priemonės, skirtos technologinės *Organizacijos X* grėsmių krypties apsaugai yra efektyvios, tačiau dar didesnis efektas bus pasiektas, kai *Organizacija X* baigs diegti gynybos priemones žmogiškajame ir procedūriniame vektoriuje, atnaujindama taisykles ir organizuodama personalo ugdymo programas.

IŠVADOS

Apibendrinant magistro baigiamąjį darbą, autorius teigia, jog visiškai pasitvirtino darbe iškelta **hipotezė**, kad mažo ir vidutinio dydžio organizacijos kibernetinės erdvės gynybos sistemoje silpniausia grandis yra žmonės, nes tai įrodo eksperimentų Nr. 1 ir Nr. 3 rezultatai. Taip pat autorius teigia, kad pasitvirtino **ginamasis teiginys,** jog holistinio požiūrio į kibernetinę gynybą taikymas padeda organizacijoms sukurti patikimas kibernetinės gynybos sistemas, nes: eksperimento Nr. 4 rezultatai patvirtino priemonių, nukreiptų į technologinio grėsmių vektoriaus gynybą, efektyvumą, o eksperimento Nr. 2 rezultatai leidžia daryti išvadą, kad organizacijoje veikia nustatytos *PĮ* diegimo procedūros ir vartotojai jas žino ir jomis vadovaujasi.

1. Teorinio tyrimo metu išanalizavus incidentus kibernetinėje erdvėje galima teigti, kad organizacijoms didžiausią grėsmę kelia kenkimo programinės įranga ir neištaisytos saugumo spragos, kurių sinergijos efekto rezultatas yra organizacijos įrangos ar tinklų įtraukimas į *botnet* tinklą, ko pasėkoje organizacija gali nevalingai tapti kibernetinių nusikaltėlių bendrininke.

2. Kibernetiniai incidentai neigiamai veikia organizacijų veiklą per reputacijos praradimą, žalą verslo interesams, vartotojų praradimą, teisines nuobaudas ir kompensacijas nukentėjusioms trečiosioms šalims, finansinius nuostolius. Užsienio tyrėjai įvardina kiek kainuoja kibernetinės atakos organizacijoms, tuo tarpu Lietuvoje yra ekonominio kibernetinių incidentų poveikio organizacijoms tyrimų deficitas, kas savo ruožtu atveria plačias galimybes Lietuvos tyrėjams vykdyti tyrimus šioje srityje.

3. Organizacijų valdoma informacija ir jos apdorojimo priemonės yra turtas, patrauklus kibernetinių atakų taikinys ir kurį galima pažeisti ar užvaldyti išnaudojus pažeidžiamumus technologijose, procesuose ir žmonėse. Todėl pagrindiniai grėsmių vektoriai organizacijose yra technologijos, procesai ir žmonės. Daugiausia kibernetinių atakų vykdoma pasinaudojant socialinės inžinerijos priemonėmis, todėl saugumo priemonės šioje kryptyje turi sudaryti organizacijos kibernetinės erdvės gynybos sistemos pamatą.

4. Organizacijos, kurdamos savo kibernetinės erdvės gynybos sistemas, turėtų vadovautis kibernetinės gynybos principais: gynybos į gylį arba daugiasluoksnės gynybos taikymas; rizikų valdymas; kibernetinės higienos palaikymas; holistinio požiūrio taikymas. Holistinio požiūrio taikymas, kai įvertinami visi organizacijos grėsmių vektoriai, t.y. žmonės, procesai ir technologijos, padeda sukurti efektyvias organizacijų kibernetinės erdvės gynybos priemones.

5. Tinkamos kibernetinio saugumo metodikos, kuri apimtų visas organizacijos grėsmių kryptis bei teiktų išsamius pasiūlymus saugumo priemonių diegimui, pasirinkimas sąlygoja patikimos kibernetinės erdvės gynybos sistemos sukūrimą. SANS 20 CSC metodika parengta, remiantis vyriausybinių, akademinių ir pramoninių organizacijų patirtimi, todėl tinka bet kokio

dydžio ir bet kokios veiklos srities organizacijoms, kurios siekia sukurti efektyvias kibernetinės erdvės gynybos sistemas.

6. Organizacijos X kibernetinės erdvės gynyboje prioriteto suteikimas technologinėms priemonėms, neatnaujintos procedūrinės priemonės ir ugdymo programų trūkumas leidžia daryti prielaidą, kad organizacijai trūksta kompetencijų kibernetinės erdvės gynybos organizavime ir valdyme. Kompetencijų trūkumas gali būti sprendžiamas apmokant personalą arba pasitelkiant pagalbą iš išorės.

7. Eksperimento Nr. 3 rezultatai įrodė, kad organizacija nesivadovauja kibernetinės gynybos principais, pavyzdžiui „gynybos į gylį“ principu ar holistinių metodų taikymu, nes pažeidimas viename gynybos lygmenyje leido imituoti kenkimo programinės įrangos įdiegimą organizacijos tinkle.

8. Atlikus Organizacijos X kibernetinės erdvės gynybos tyrimą, galima teigti, kad Organizacija X nėra pasirengusi ginti savo kibernetinę erdvę, o Organizacijos X kibernetinės gynybos sistemoje silpniausia grandis yra žmonės.

9. Eksperimento Nr. 4 rezultatai įrodė, kad Organizacijai X pradėjus taikyti kibernetinės „gynybos į gylį“ principą, diegiant SANS 20 CSC metodikoje numatytas priemones, bendra kibernetinės erdvės gynybos sistema buvo ženkliai sustiprinta.

REKOMENDACIJOS

1. *Organizacijai X* savo kibernetinės erdvės gynybos sistemos stiprinimui siūloma taikyti *20 CSC* metodiką, nes naudojamas holistinis metodas pateikia organizacijai kibernetinės erdvės gynybos priemones visuose vektoriuose: technologiniame, procedūriniame ir socialiniame.

2. *Organizacijai X* rekomenduojama stiprinti procedūrines kibernetinės gynybos priemones atnaujinant 2010 m. patvirtintas „Naudojimosi kompiuteriais *Organizacijoje X* taisykles“ ir jas papildant: vartotojų paskyrų, rizikų, incidentų ir programinės įrangos valdymo procesais, antivirusinės saugos ir išorinių laikmenų naudojimo politikomis, reikalavimais standartinėms konfigūracijoms ir Interneto ir elektroninio pašto naudojimo organizacijoje tvarka.

3. Kadangi holistinio požiūrio taikymas yra vienas iš kibernetinės gynybos principų, todėl autorius siūlo organizacijai technologines ir procedūrines kibernetinės gynybos priemones papildyti socialinės krypties gynybos priemonėmis, kurios apimtų personalo kibernetinio saugumo ugdymo planus, naujų darbuotojų testavimą prieš sukuriant vartotojų paskyras. Taip pat autorius siūlo numatyti sankcijas už grubius organizacijos kibernetinės erdvės saugumo pažeidimus.

4. *Organizacijai X* rekomenduojama periodiškai vykdyti savo kibernetinės erdvės tyrimus, periodiškai peržiūrėti ir atnaujinti kibernetinės gynybos procedūras ir personalo kibernetinio ugdymo planus, nes tai leistų nuolat tobulinti ir vystyti kibernetinės erdvės gynybos sistemą.

5. Tyrimų rezultatai parodė, kad *SANS 20 CSC* metodika yra pakankamai efektyvi, kuriant organizacijų kibernetinės erdvės gynybos sistemas, padeda užtikrinti „Bendrųjų elektroninės informacijos saugos reikalavimų“ atitiktį organizacijoms, kurioms tokia atitiktis yra privaloma. Kadangi tyrimas atliktas tik vienoje organizacijoje, autorius siūlo vystyti metodikos taikymo tyrimus organizacijose, kad patvirtinti metodikos efektyvumą, kas leistų įvertinti jos populiarinimo tarp organizacijų galimybes.

6. Kadangi Lietuvoje kibernetinės erdvės gynybos problematika nėra plačiai ištyrinėta, todėl rekomenduojama plėsti kibernetinės erdvės gynybos tyrimus – tyrinėti valstybės ir organizacijų atvejus. Organizacijų tyrimus galima skirstyti pagal organizacijų veiklos tipą, dydį, nuosavybės formas, kas leistų suprasti kokios yra tendencijos, skirtumai bei bendrumai ir koks santykis su bendra valstybės kibernetinės gynybos sistema.

LITERATŪROS SĄRAŠAS

Moksliniai šaltiniai (knygos, moksliniai straipsniai, leidiniai ir kt.):

1. Kranauskienė R. (2010). *Informacijos saugumo valdymas X organizacijoje* (magistro darbas). Prieiga per internetą:
http://vddb.laba.lt/obj/LT-eLABa-0001:E.02~2005~D_20050518_105648-27939

2. Damkus M. (2006). *Informacijos saugumas elektroninės valdžios infrastruktūros kūrime* (magistro darbas). Prieiga per internetą:
http://vddb.laba.lt/obj/LT-eLABa-0001:E.02~2006~D_20061221_160444-80115

3. Selskaitė I. (2010). *Informacijos sauga viešajame ir privačiame sektoriuje* (magistro darbas). Prieiga per internetą:
http://vddb.laba.lt/obj/LT-eLABa-0001:E.02~2008~D_20090908_201752-31444

4. Amilevičius, D. (2012). Elektroninės erdvės saugumo ekonominiai aspektai. *Visuomenės saugumas ir viešoji tvarka (7): mokslinių straipsnių rinkinys, 5-22*. Prieiga per internetą: https://www.mruni.eu/kpf_dokumentai/fakultetas/Leidiniai/MRU_VSVT__7__2012-06-25.pdf

5. Štitilis, D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. *SOCIALINĖS TECHNOLOGIJOS 2013, 3(1), 189–207*. doi:10.13165/ST-13-3-1-13

6. West-Brown, M., et al. (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs).* Software Engineering Institute. Prieiga per internetą:
http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

7. Manzuik, S. et al. (2007). *Network Security Assessment: From Vulnerability to Patch.* Syngress Publishing, Inc.

8. Wong, T. P. (2011). *ACTIVE CYBER DEFENSE: ENHANCING NATIONAL CYBER DEFENSE* (Master's thesis). Prieiga per internetą:
http://calhoun.nps.edu/bitstream/handle/10945/10713/11Dec_Wong_T.pdf?sequence=1

9. Sjouwerman, S. (2011). *Cyberheist: the biggest financial threat facing American businesses since the meltdown of 2008*. KnowBe4.

10. Harper, A., et al. (2011). *Gray Hat Hacking The Ethical Hacker's Handbook Third Edition*. McGraw-Hill.

11. Kosina, K. (2012). *Wargames in the Fifth Domain* (Master's thesis). Prieiga per internetą: http://kyrah.net/da/wargames.pdf

12. Bayuk, J. L., et al. (2012). *Cyber Security Policy Guidebook*. John Wiley & Sons, Inc.

13. Rantapelkonen, J. & Salminen M. (2013). *THE FOG OF CYBER DEFENCE*. Helsinki: National Defence University. Prieiga per internetą:

http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf

14. Denning, D. E. (2013). *Framework and Principles for Active Cyber Defense.* Prieiga per internetą: http://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20Active%20Cyber%20Defense%20-%2011Dec2013.pdf

15. Kallberg, J., & Burk, R. A. (2014). Failed Cyberdefense. *Military Review, 92(3), 22.*

16. MacDonnell, U. (2014). *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks.* John Wiley & Sons, Inc.

17. Mowbray, T. J. (2014). *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions.* John Wiley & Sons, Inc.

18. Luttgens, J. T., et al. (2014). *Incident Response & Computer Forensics, Third Edition.* McGraw-Hill Education.

19. Brenner, S. W. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston: Northeastern.

20. Etsebeth, V. (2011). Defining the Current Corporate IT Risk Landscape. *Journal of International Commercial Law & Technology. 6 (2), 62-73.*

21. Lerner, Z. (2014). MICROSOFT THE BOTNET HUNTER: THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN MITIGATING BOTNETS. *Harvard Journal Of Law & Technology, 28(1), 237-261.*

22. Catwell, S. P., & Norwood, K. T. (2009) *Cybersecurity, Cyberanalysis, and Warning.* New York: Nova Science Publishers, Inc.

23. Panton, B. C., et al. (2014) Strengthening DoD Cyber Security with the Vulnerability Market. *Defense Acquisition Research Journal: A Publication of the Defense Acquisition University, 21(1) 465-484.*

24. Smiraus, M., & Jasek, R. (2011). RISKS OF ADVANCED PERSISTENT THREATS AND DEFENSE AGAINST THEM. *Annals Of DAAAM & Proceedings, 1589-1590.*

25. Starrs, P. F., & Anderson, J. (1997). The words of cyberspace. *Geographical Review, 87(2), 146-154.* http://dx.doi.org/10.2307/216002

26. Strate, L. (1999). The Varieties of Cyberspace: Problems in Definition and Delimitation. *Western Journal Of Communication, 63(3), 382-413.* doi:10.1080/10570319909374648

27. Butler, S. C. (2013). Refocusing Cyber Warfare Thought. *Air & Space Power Journal, 27(1), 44-57.*

28. Hypponen, M. (2013) The Exploit Marketplace. Rantapelkonen, J., Salminen, M., *THE FOG OF CYBER DEFENCE*. Helsinki: National Defence University. 231-234.

29. Chaffey, D., Wood, S. (2004) *Business information management.* Pearson Canada.

30. Rankin, J. G., Johnson, M., Dennis, R. (2015 kovo 3 d.). *Research on Implementing Big Data: Technology, People, & Processes*. Pranešimas konferencijoje Society for Information Technology & Teacher Education (SITE) International Conference. Prieiga per internetą: http://files.eric.ed.gov/fulltext/ED555544.pdf

31. Bihari, S. C. (2012) CRM is all about bringing people, processes & technology together a case study of banking sector in India. *Romanian Journal of Marketing. (1), 50-56.*

32. Girnienė, I. (2012). Informacijos vadyba šiuolaikinėje organizacijoje. *Elektroninis mokymasis, informacijos ieška ir komunikacija: teorija ir praktika. 1-23.*

33. Tipton, H. F., Krause, M. (2002). *Information Security Management Handbook, 4th Edition, Volume 3*. Boca Raton: CRC Press LCC.

34. McLean, S. (2013). Beware the Botnets: Cyber Security Is a Board Level Issue. *Intellectual Property & Technology Law Journal, 25(12), 22-27.*

35. Radvilavicius, L., Marozas, L., & Cenys, A. (2012). Overview of Real-Time Antivirus Scanning Engines. *Journal Of Engineering Science & Technology Review, 5(1), 63-71*.

36. Akkaladevi, S., & Katangur, A. K. (2010). DEFENDING AGAINST BOTNETS. *Journal Of Applied Global Research, 3(7), 50-61*.

37. McLean, S. (2013). Beware the Botnets: Cyber Security Is a Board Level Issue. *Intellectual Property & Technology Law Journal, 25(12), 22-27.*

38. Sangani, N. K., & Vijayakumar, B. (2012). Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informatica Economica, 16(2), 58-71.*

39. Byres, E. (2014). Defense-In-Depth: Reliable Security To Thwart Cyber-Attacks. *Pipeline & Gas Journal, 241(2), 58.*

40. Eshoo, A. (2015). Promoting cyber hygiene. *Hill*. p. 22.

41. Magnuson, S. (2014). New Cyber Hygiene Campaign Seeks to Curtail Attacks. *National Defense, 98(726), 18.*

42. Hecker, L. L., & Edwards, A. B. (2014). The Impact of *HIPAA* and *HITECH*: New Standards for Confidentiality, Security, and Documentation for Marriage and Family Therapists. *American Journal Of Family Therapy, 42(2), 95-113.* doi:10.1080/01926187.2013.792711

43. Willey, L., & White, B. J. (2013). Teaching Case Do you take credit cards? Security and compliance for the credit card payment industry. *Journal Of Information Systems Education, 24(3), 181-188.*

44. Basani, V. (2014). CURBING EVOLVING CYBER ATTACKS AND INFRASTRUCTURE VULNERABILITIES. *Siliconindia, 14*.

45. Greene, S. (2014) *Security Program and Policies: Principles and Practices, Second Edition*. Pearson Certification.

46. Kardelis, K. (2002). *Mokslinių tyrimų metodologija ir metodai*. Kaunas: Judex.

Teisės ir kiti normatyviniai aktai, standartai:

47. Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). *Teisės aktų registras, 20553.*

48. Lietuvos Respublikos karinė strategija (2012). *Krašto apsaugos ministerija.* Prieiga per internetą: http://www.kam.lt/download/30845/lietuvos%20karine%20strategija.doc

49. Lietuvos karinė doktrina (2010). *Lietuvos kariuomenė.* Prieiga per internetą: http://kariuomene.kam.lt/download/14513/lietuvos%20karine%20doktrina.pdf

50. Lietuvos standartizacijos departamentas. (2014). *LST ISO/IEC 27002:2014. Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai*.

51. Joint Terminology for Cyberspace Operations. (2010). *The Vice Chairman of the Joint Chiefs of Staff.* Prieiga per internetą: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

52. International Organization for Standardization. (2014). *ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Prieiga per internetą: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

53. National Institute of Standards and Technology. (2005). *Guide to Malware Incident Prevention and Handling.* Prieiga per internetą: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

54. National Institute of Standards and Technology. (2013). *NIST.SP.800-53r4. Security and Privacy Controls for Federal Information Systems and Organizations.* Prieiga per internetą: http://dx.doi.org/10.6028/NIST.SP.800-53r4

55. National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Prieiga per internetą: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Interneto šaltiniai:

56. Lamothe, D. (2015, sausio 12). *U.S. military social media accounts apparently hacked by Islamic State sympathizers.* The Washington Post. Prieiga per internetą: http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/

57. Tsagourias, N. (2014). *State Responsibility for Cyber Operations: International Law Issues.* British Institute of International and Comparative Law. Prieiga per internetą: http://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf

58. Japertas, S. (2010, kovo 22 d.) *Kibernetinė sauga ir Lietuva*. Technologijos.lt. Prieiga per internetą:

http://www.technologijos.lt/n/technologijos/it/S-12007/straipsnis/Saulius-Japertas-Kibernetine-sauga-ir-Lietuva?l=2&p=1

59. De Falco, M. (2012) *Stuxnet Facts Report. A Technical and Strategic Analysis.* Prieiga per internetą:

https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf

60. Microsoft. (2006). *Midsize Business Security Guidance. Strategies for Managing Malware Risks.* Prieiga per internetą: http://go.microsoft.com/fwlink/?LinkId=71175

61. Microsoft. (2006). *The Security Risk Management Guide.* Prieiga per internetą: http://www.microsoft.com/en-us/download/confirmation.aspx?id=6232

62. Pastore, M. (2014) Think You're Too Small to Get Hacked? Think Again. *Protecting Your Mid-Size Business from Today's Security Threat.* Prieiga per internetą:

http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-0994ENW.pdf?ver=1.0

63. Stasiukonis, S. (2006) Social Engineering, the USB way. *Dark Reading.* Prieiga per internetą: http://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081?

64. Sukčiai nusitaikė į Swedbank klientus. (2009, kovo 23 d.). *Cybersecurity*. Prieiga per internetą: http://www.technologijos.lt/n/technologijos/it/straipsnis/Sukciai-nusitaike-i-Swedbank-klientus?name=straipsnis-6875

65. Greenberg, A. (2012, kovo 23 d.) Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. *Forbes.* Prieiga per internetą:

http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

66. Saugumo incidentų tyrimo skyriaus (CERT-LT) 2014 metų veiklos ataskaita. (2015) *CERT-LT*. Prieiga per internetą: https://www.cert.lt/doc/2014.pdf

67. „Botnet" tinkluose ir pavojingų spragų turintys įrenginiai aptikti Lietuvoje. (2015). *CERT-LT*. Prieiga per internetą: https://www.cert.lt/botnet.html

68. 2010 metų CERT-LT incidentų statistika. (2011). *CERT-LT*. Prieiga per internetą: https://www.cert.lt/doc/2010.pdf

69. „Botnet“ tinklai. (2014, gruodžio 2 d.) *Lietuvos Respublikos Ryšių reguliavimo tarnyba*. Prieiga per internetą: http://esaugumas.lt/lt/botnetai.html

70. Dėmesio: plinta virusas, užšifruojantis kompiuterio failus. (2015, sausio 20 d.) *Lietuvos Respublikos Ryšių reguliavimo tarnyba.* Prieiga per internetą: http://rrt.lt/lt/pranesimai-spaudai/demesio-plinta-virusas-8zds.html

71. Lietuvoje plinta duomenis šifruojantis kompiuterinis virusas. (2015, rugpjūčio 26 d.). *Kauno apskrities Vyriausiasis policijos komisariatas.* Prieiga per internetą: http://www.kaunas.policija.lt/ww/index.php/lt/4343-lietuvoje-plinta-duomenis-sifruojantis-kompiuterinis-virusas

72. ENISA Threat Landscape 2014. (2015) *ENISA* . Prieiga per inernetą: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

73. Cluley, G. (2012, kovo 23 d.)**.** Bredolab: Jail for man who masterminded botnet of 30 million computers. *Naked Security.* Prieiga per internetą: https://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/

74. The Critical Security Controls for Effective Cyber Defense Version 5.0. (2014). *Council on Cybersecurity.* Prieiga per internetą: https://www.sans.org/media/critical-security-controls/CSC-5.pdf

75. Hietala, J. D. (2013). *Implementing the Critical Security Controls.* SANS Institute. Prieiga per internetą: https://www.sans.org/reading-room/whitepapers/analyst/implementing-critical-security-controls-35125

76. EICAR Anti-Malware test file. *The European Institute for Computer Anti-Virus Research.* Prieiga per internetą: http://www.eicar.org/86-0-Intended-use.html

77. Neustar Annual DDoS Attacks and Impact Report. (2015). *Neustar*. Prieiga per internetą: https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

78. Worldwide Infrastructure Security Report, Volume X. (2015) *Arbor Networks*. Prieiga per internetą: http://e38359e99afe1badad5e-ae996a181c8de7a2fc21d75cdeef1b4d.r61.cf2.rackcdn.com/WISR2014_EN2014.pdf

79. KAM atstovas: per didelę „botnet“ ataką Lietuvai turbūt tektų atsijungti nuo interneto. (2012, sausio 29 d.). *Alfa.lt*. Prieiga per internetą: http://www.alfa.lt/straipsnis/13660195/kam-atstovas-per-didele-botnet-ataka-lietuvai-turbut-tektu-atsijungti-nuo-interneto?p=1

80. Bronson, G. (2015, birželio 25 d.). The accessibility of the Internet has led to a rapid evolution of cyber criminals. *The Network, Cisco's Technology News Site*. Prieiga per internetą: http://newsroom.cisco.com/feature-content?articleId=1659898

81. Olson, P. (2014, lapkričio 20 d.). The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites. *Forbes*. Prieiga per internetą:

http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/

82. Turton, W. (2014, gruodžio 30 d.) Lizard Squad's Xbox Live, PSN attacks were a 'marketing scheme' for new DDoS service. *The Daily Dot*.. Prieiga per internetą:

http://www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/

83. Barker, C. (2014, lapkričio 11 d.). 25 billion connected devices by 2020 to build the Internet of Things. *ZDNET*. Prieiga per internetą: http://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/

84. Zeifman, I. (2015, birželio 9 d.). Q2 2015 Global DDoS Threat Landscape: Assaults Resemble Advanced Persistent Threats. *Incapsula*. Prieiga per internetą: https://www.incapsula.com/blog/ddos-global-threat-landscape-report-q2-2015.html

85. Matthews, T. (2014, lapkričio 12 d.). DDoS Impact Survey Reveals the Actual Cost of DDoS Attacks. *Incapsula*. Prieiga per internetą: https://www.incapsula.com/blog/ddos-impact-cost-of-ddos-attack.html

Ropė Ž. Organizacijos X kibernetinės erdvės gynyba / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. D. Štitilis. – Vilnius: Mykolo Romerio universitetas, Verslo ir medijų mokykla, 2015. – 99 p.

SANTRAUKA

Kibernetinio saugumo valdymo magistro baigiamojo darbo tema „Organizacijos X kibernetinės erdvės gynyba“ yra aktuali, kadangi sparčiai tobulėjant technologijoms organizacijos iškelia savo veiklą į kibernetinę erdvę. Tačiau kibernetinių incidentų dinamika rodo, kad kibernetinės erdvės patrauklumas neteisėtai veiklai vykdyti nuolat didėja, o organizacijoms kibernetinėje erdvėje kyla realios grėsmės. Organizacijoms, ypač mažoms ir vidutinėms, kurių veikla nėra tiesiogiai susijusi su IT, kyla iššūkiai kuriant efektyvias kibernetinės erdvės gynybos sistemas.

Magistro baigiamajame darbe yra nagrinėjama kibernetinės erdvės gynybos samprata, nustatomi organizacijų kibernetinės erdvės grėsmių vektoriai, analizuojami kibernetiniai incidentai ir identifikuojamos pavojingiausios kibernetinės grėsmės. Apžvelgiamos ir palyginamos organizacijų kibernetinės erdvės gynybai taikytinos metodikos bei identifikuojami efektyvios kibernetinės gynybos principai. Tiriamas *Organizacijos X* pasirengimas vykdyti kibernetinės erdvės gynybą, teikiamos rekomendacijos ir vertinamas jų efektyvumas.

Šis darbas padės *Organizacijai X* pamatyti realias kibernetines grėsmes bei įvertinti esamos kibernetinės erdvės gynybos sistemos būklę. Atlikti tyrimai padės identifikuoti silpnąsias *Organizacijos X* kibernetinės erdvės gynybos sistemos grandis ir sustiprinti kibernetinę gynybą, taikant efektyvios kibernetinės gynybos principus. Kitoms organizacijoms, kurioms kelia nerimą jų kibernetinės erdvės gynybos sistemos būklė, šis tyrimas leis pamatyti aspektus, kurie sąlygoja efektyvios kibernetinės erdvės gynybos sistemos sukūrimą.

Darbą sudaro įvadas, dvi dėstymo dalys, tiriamoji dalis ir išvados bei rekomendacijos. Pirmojoje magistrinio baigiamojo darbo dalyje nagrinėjami teoriniai kibernetinės erdvės gynybos aspektai. Antrojoje dalyje nagrinėjami mažų ir vidutinių organizacijų kibernetinės erdvės gynybos organizavimo principai. Trečiojoje darbo dalyje aprašoma atlikto tyrimo metodologija ir analizuojami tyrimo metu gauti rezultatai. Darbo pabaigoje pateikiamos išvados ir rekomendacijos *Organizacijos X* kibernetinės erdvės gynybos sistemos stiprinimui.

Ropė Ž. Cyber Defence in X Organization / Master‘s work in Cyber Security Management. Supervisor prof. dr. D. Štitilis – Vilnius: Business and Media School, Mykolas Romeris University, 2015. – 99 p.

SUMMARY

Cyber security management master thesis on "Cyber Defence in X Organization“ is relevant, since the fast development of technology puts your organization's activities in cyberspace. However, the dynamics of cyber incidents show that cyber attractiveness of illegal activity is increasing and organizations in cyberspace faces a real threat. Organizations, especially small and medium-sized, which are not directly related to IT, face a challenge in developing effective cyber defence systems.

This master thesis presents an examined cyber defence concept, determined cyber threat vectors in organizations, analyses cyber incidents and identifies the most dangerous cyber threats. The thesis also provides an overview and comparison of methodologies that are used for cyber defence in organizations and identifies effective cyber defence principles. The research is made on readiness of “X Organization” to carry out cyber defence. The author gives recommendations and assesses their effectiveness.

This work will help “X Organization” to see real cyber threats and evaluate the existing cyber defence system status, as well as renders help to identify weaknesses in “X Organization” cyber defence chain, and enhances cyber defence system by applying an effective cyber defence principles. Concerning other organizations that are concerned about their cyber defence system status, this study will help them to see the aspects that lead to effective cyber defence framework.

The work consists of an introduction, two enunciation parts, a research part, as well as findings and recommendations. Master thesis in the first part deals with the theoretical aspects of cyber defence. The second part deals with the cyber defence principles of small and medium-sized organizations. The third part describes the techniques of the research and the analysis of study results. At the end are given conclusions and recommendations for the “X Organization” cyber defence system strengthening.

PRIEDAI

1 PRIEDAS

KIBERNETINĖS ERDVĖS GYNYBOS TYRIMO SUSITARIMAS

Šis susitarimas sudarytas tarp Mykolo Romerio Universiteto Socialinių technologijų instituto Kibernetinio saugumo valdymo magistranto Žilvino Ropės (Studento identifikacinis numeris **141992**), toliau vadinamu Tyrėju, ir Organizacijos X IT skyriaus vedėjo _____ (darbo pažymėjimo nr. _____), toliau vadinamu Užsakovu.

Šalys sutaria, kad:

1. Užsakovas patvirtina, kad Organizacijos X vadovybė supažindinta su atliekamu kibernetinės erdvės gynybos tyrimu.
2. Tyrėjas sutinka ir patvirtina, kad tyrimą atliks visiškai nemokamai ir nereikalaus iš Užsakovo jokio atlyginimo.
3. Tyrėjas patvirtina, kad neatskleis jokios informacijos trečiosioms šalims apie Užsakovo tinklą ir tyrimo rezultatus, gautus tyrimo metu. Visi rezultatai yra konfidencialūs ir bus panaudoti tik magistro baigiamajame darbe „Organizacijos X kibernetinės erdvės gynyba“.
4. Tyrimo ataskaitą Tyrėjas perduos Užsakovui iki 2016-01-31.
5. Užsakovas sutinka atlikti socialinės inžinerijos (angl. Social Engineering) testus, kurių tikslas patikrinti organizacijos reakciją į galimus kibernetinius incidentus:

5.1. Suklastoto elektroninio laiško, kuriame vartotojai raginami įvesti prisijungimo prie elektroninio pašto duomenis, išsiuntimas į Užsakovo atrinktų vartotojų tarnybinio elektroninio pašto dėžutes (Priedas 1);

5.2. Suklastoto elektroninio laiško, kuriame vartotojai raginami atsisiųsti testui skirtą programinę įrangą ir ją aktyvuoti kompiuteryje, išsiuntimas į Užsakovo atrinktų vartotojų tarnybinio elektroninio pašto dėžutes (Priedas 2);

5.3. Palikti Organizacijos X bendro naudojimo patalpose, Tyrėjo paruoštas USB laikmenas su testui skirta programine įranga (Priedas 3); Tyrėjas nereikalaus grąžinti ar bet kaip kitaip atlyginti už eksperimente panaudotas USB laikmenas.

5.4. Užsakovas patvirtina, kad gauti socialinės inžinerijos testo rezultatai bus panaudoti tik vartotojų švietimo ir technologinių priemonių taikymo tikslais. Socialinės inžinerijos testo rezultatai nebus panaudoti baudžiant ar kitaip persekiojant vartotojus.

6. Užsakovas sutinka atlikti tinklo pažeidžiamumų aptikimo (angl. Network Vulnerability Assesment) testus, kurių tikslas aptikti organizacijos tinkle esančias spragas.

7. Užsakovas sutinka atlikti tinklo įsibrovimų aptikimų (angl. Network Intrusion Detection) testus, kurių tikslas išsiaiškinti kibernetinių atakų mastą.
8. Užsakovas testo rezultatams rinkti ir saugoti skirs reikiamus techninius ir programinės įrangos išteklius;
9. Esant tyrimo poreikiui Užsakovas sudarys galimybę, iš anksto suderinus, naudoti Tyrėjo įrangą;
10. Esant tyrimo poreikiui Užsakovas skirs kontaktinį(-ius) asmenį(-ius), tyrimo veiksmų derinimui su Tyrėju;
11. Kiekvieną testą Tyrėjas suderins su Užsakovu, bus atlikti bandomieji testai, kad įsitikinti jog testas neįtakoja įrangos ar duomenų sugadinimo, sunaikinimo ar kito neigiamo poveikio. Suderindamas testą Užsakovas patvirtina, kad neturi jokių pretenzijų Tyrėjui;
12. Atsižvelgiant į besikeičiančią kibernetinio saugumo situaciją Užsakovas sutinka, kad tyrimo metu gali būti neaptiktos visos saugumo ar konfigūracijų problemos ir tai nebus laikoma Tyrėjo atsakomybe;
13. Užsakovas patvirtina, kad organizacija reaguos įprastu būdu, kai aptinkami kibernetiniai incidentai, kurie kyla testo metu, kad nebūtų iškreipti bandymo rezultatai. Užsakovas pasižada neinformuoti atsakingų teisėsaugos ar kitų institucijų ir patvirtina, kad neturi pretenzijų Tyrėjui dėl kibernetinių incidentų, kurie yra vykdyto testo pasekmė;
14. Atsiradus papildomų tyrimų poreikiui, šalys sudarys atskirus susitarimus.

Tyrėjas:	**Užsakovas**
(Vardas, Pavardė, Parašas)	(Vardas, Pavardė, Parašas)
Mykolo Romerio Universiteto	Organizacijos X
Socialinių technologijų instituto	Informacinių sistemų tarnybos vedėjas
Kibernetinio saugumo valdymo magistrantas	
Studento identifikacinis numeris **141992**	Darbuotojo pažymėjimas Nr. _____
2015-__-__	2015-__-__

2 PRIEDAS

KIBERNETINĖS ERDVĖS GYNYBOS TYRIMO SUSITARIMAS
Priedas Nr.1
2015-02-24

EKSPERIMENTAS NR.1

TIKSLAS: patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai atsiunčiamas suklastotas elektroninio laiško, kuriame vartotojai raginami įvesti prisijungimo prie savo tarnybinio elektroninio pašto duomenis.

ATRINKTI DALYVIAI: Respondentas 1, Respondentas 2, Respondentas 3, Respondentas 4, Respondentas 5, Respondentas 6, Respondentas 7, Respondentas 8, Respondentas 9, Respondentas 10, Respondentas 11, Respondentas 12, Respondentas 13, Respondentas 14, Respondentas 15,Respondentas 16, Respondentas 17, Respondentas 18, Respondentas 19, Respondentas 20.

EIGA: Eksperimentas vykdomas tokia eiga:

1. Siuntėjas, kurio adresas yra **eur0parlament@outlook.com** atsiunčia laišką atrinktiems eksperimento dalyviams:

2. Organizacijos X vidiniame tinkle yra kompiuteris [Kompiuterio vardas: _____ IP adresas: _____ MAC adresas: _____], kuriame viekia kompanijos **MICROSOLVED, INC.** nemokama programinė įranga *MSI Simple Phish* įdiegta **C:\MSISimplePhish**. Svetainėje vartotojai galės įvesti savo tarnybinio elektroninio pašto adresą ir slaptažodį.

3. **C:\MSISimplePhish\MSISimplePhishLog.txt** byloje bus registruojami: vartotojo apsilankiusio svetainėje IP adresas, vartotojo įvestas prisijungimo vardas (Login) ir pirmi trys vartotojo įvesto slaptažodžio simboliai.

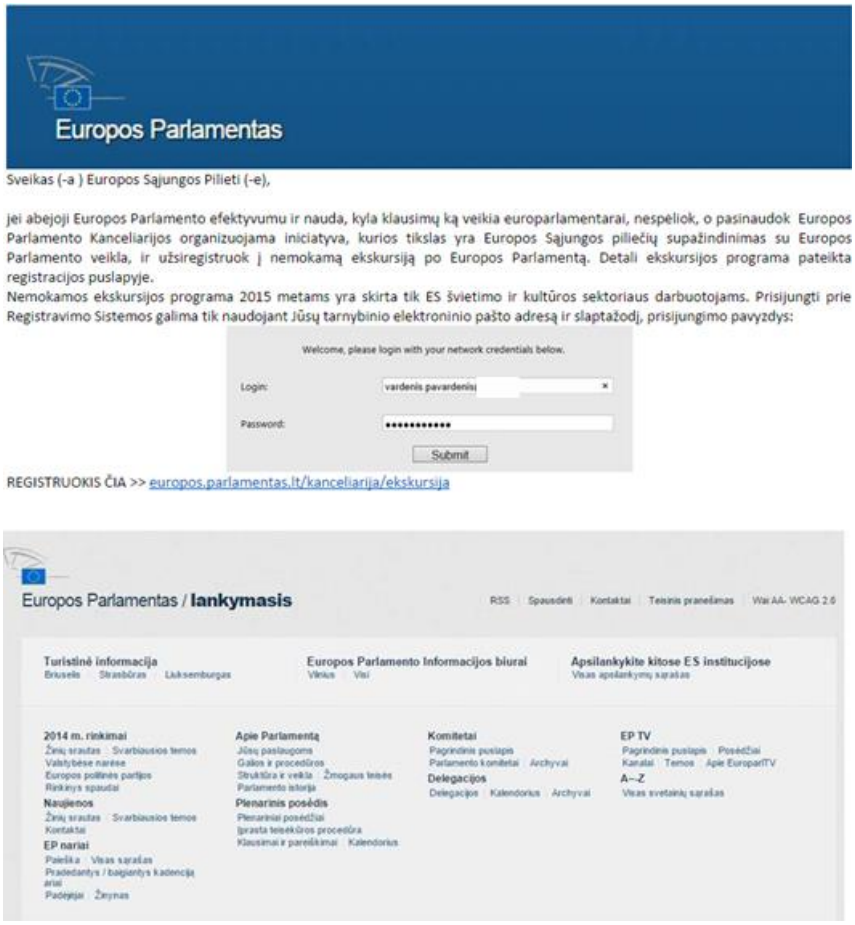
REZULTATAS: Eksperimento rezultate bus nustatytas rizikos organizacijos kibernetinei erdvei laipsnis.

KRITERIJAI: Rizikos organizacijos kibernetinei erdvei laipsnis bus nustatytas remiantis kriterijais:

1. Aukštas – jei:
    a. suklastotame laiške nuorodą į svetainę bus atidaryta ir suvesti prisijungimo prie tarnybinio elektroninio pašto duomenys.
2. Vidutinis – jei:
    a. suklastotame laiške nuoroda į svetainę bus atidaryta, tačiau nebus suvesti prisijungimo prie tarnybinio elektroninio pašto duomenų ir apie incidentą nebus pranešta Informacinių sistemų tarnybai.
3. Žemas – jei:
    a. Nei vienas vartotojas neatidarys suklastotame laiške nuorodos į svetainę

b. nuoroda bus atidaryta, bet neįvesti prisijungimo prie tarnybinio elektroninio pašto duomenys ir apie incidentą informuota Informacinių sistemų tarnybą.

ATRINKTIEMS VARTOTOJAMS SIUNČIAMAS LAIŠKAS:



Tyrėjas:

(Vardas, Pavardė, Parašas)

Mykolo Romerio Universiteto

Socialinių technologijų instituto

Kibernetinio saugumo valdymo magistrantas

Studento identifikacinis numeris **141992**

2015-__-__

Užsakovas

(Vardas, Pavardė, Parašas)

Organizacijos X

Informacinių sistemų tarnybos vedėjas

Darbuotojo pažymėjimas Nr. _____

2015-__-__

3 PRIEDAS

KIBERNETINĖS ERDVĖS GYNYBOS TYRIMO SUSITARIMAS
Priedas Nr.2
2015-02-24

EKSPERIMENTAS NR. 2

TIKSLAS: patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai atsiunčiamas suklastotas elektroninio laiško, kuriame vartotojai raginami atsisiųsti iš pateiktų nuorodų ir aktyvuoti savo kompiuteriuose programinį kodą.

ATRINKTI DALYVIAI: Respondentas 1, Respondentas 2, Respondentas 3, Respondentas 4, Respondentas 5, Respondentas 6, Respondentas 7, Respondentas 8, Respondentas 9, Respondentas 10, Respondentas 11, Respondentas 12, Respondentas 13, Respondentas 14, Respondentas 15,Respondentas 16, Respondentas 17, Respondentas 18, Respondentas 19, Respondentas 20.

EIGA: Eksperimentas vykdomas tokia eiga:

1. Siuntėjas, kurio adresas yra **s0sva1ka1@outlook.com** atsiunčia laišką atrinktiems eksperimento dalyviams:

2. Organizacijos X vidiniame tinkle yra kompiuteris [Kompiuterio vardas: _____ IP adresas: _____ MAC adresas: _____], kuriame Microsoft Internet Information Services pagrindu sukurta svetainė, kurioje patalpinta kompiuterinė byla **katinukas.exe**.

3. Vartotojui atsisiuntus ir aktyvavus kompiuterinę bylą **katinukas.exe,** Organizacijos X bendrame tinklo kataloge [Kompiuterio vardas: _____ IP adresas: _____ MAC adresas: _____]. Sukuriamas katalogas, kuris pavadinamas vartotojo vardu, tame kataloge sukuriamos dvi kompiuterinės bylos kuriose registruojamas kompiuterio vardas, IP adresas, MAC adresas ir programinė įranga instaliuota vartotojo kompiuteryje.

REZULTATAS: Eksperimento rezultate bus nustatytas rizikos organizacijos kibernetinei erdvei laipsnis.

KRITERIJAI: Rizikos organizacijos kibernetinei erdvei laipsnis bus nustatytas remiantis kriterijais:

1. Aukštas – jei:
    a. nors vienas vartotojas atsisiunčia kompiuterinę bylą **katinukas.exe** iš suklastotame laiške esančios nuorodos ir ją aktyvuoja savo kompiuteryje.
2. Vidutinis – jei:
    a. suklastotame laiške nuoroda bus atidaryta ir bus atsiųsta, tačiau nebus aktyvuota kompiuterinė byla **katinukas.exe** ir apie incidentą nebus pranešta Informacinių sistemų tarnybai.
3. Žemas – jei:
    a. Nei vienas vartotojas neatidarys suklastotame laiške esančios nuorodos.

b. nuoroda bus atidaryta ir bus atsiųsta, bet nebus aktyvuota kompiuterinė byla **katinukas.exe** ir apie incidentą informuota Informacinių sistemų tarnyba.

ATRINKTIEMS VARTOTOJAMS SIUNČIAMAS LAIŠKAS:

Laba diena,

labai prašome netrinti šio laiško neperskaičius iki galo. Tai nėra koks pinigų viliojimas prisidengiant baise nelaime, neprašysime JOKIOS finansinės paramos, JOKIŲ PINIGŲ, tiesiog perskaitykite ir nuspręskite ar ištrinti šį laišką, ar vis dėl to skirti minutę dėmesio ir padėti.

Elytei dabar yra 5 metukai, o jai likimas nusprendė dovanoti itin sunkią gyvenimo pradžią – mergaitė yra našlaitė, jos tėveliai tragiškomis aplinkybėmis paliko šį pasaulį svečioje šalyje. Prieš metus su trupučiu Elytei prasidėjo sveikatos problemos, bet mes net nenutuokėm kas mūsų laukia po 3 mėnesių. Elytei nustatyta itin agresyvi ir greitai besivystanti klastinga liga. Mergaitei taikomas stiprus medikamentinis gydymas, tačiau liga sparčiai plinta, to pasekoje, mūsų globojama mažytė labai serga. Blogiausia tai, kad seborėjinė keratozė tik pasekmė kažko, ko mes dar nežinom.

Šiuo metu mums reikalinga itin skubi (vasario 23d., 2015 m.) kelionė į Vokietijos Universitetinę Vaikų kliniką, kur bus tęsiami tolimesni tyrimai bei gydymas Elytei. Deja, pinigų, kuriuos turime, neužtenka padengti visų medicininių išlaidų. Nesulaukę pagalbos iš valstybės, kreipėmės į daugybę žmonių ir organizacijų. Pirmieji į pagalbos šauksmą atsiliaukė kaip nebūtų keista visai dar jauni žmonės – Vilniaus kolegijos studentai programuotojai. Jie pasiūlė sukurti linksmąją programėlę, kurią platinti iš savo serverio sutiko kelios užsienio kompanijos ir už kiekvieną atsiųstą programėlę perveda po 12 euro centų į Elytės gydymo sąskaitą. Sunku pradžioje buvo patikėti, kad tokiu būdu įmanoma surinkti reikiamą sumą, tačiau Šauniųjų Studentų dėka jau yra sukaupta per 28 465 eurai.

Ir trūksta visai nedaug, tereikia kad dar keletas neabejingų žmonių atsisiųstų linksmąją programėlę į savo kompiuterį ar telefoną ir taip praskaidrintų savo darbo dienos kasdienybę ir tuo pačiu suteiks vargšei ligonukei vilį.

Atsisiųskite linksmąją programėlę – katinėlį.

Jei norite atsisiųsti katinėlį į kompiuterį – spauskite čia >> http://dovvnload.mikrosoft.com/

Jei norite atsisiųsti katinėlį į išmanųjį telefoną – spauskite čia >> http://pley.google.com/

Jei nepavyksta, pabandykite čia >> http://www.dovvnload.com

Gal kelerių metų parkė jūs sutiksite Elytę, kur ji lakstys ir valgys ledus, o Jūs žinosite, kad tai ir Jūsų nuopelnas. Jeigu nieko nedarysime šiandien, visų tų dalykų mažoji negalės patirti niekada gyvenime. Padėkite Elytei pasveikti.

Ačiū Jums pagalbą!

SoSVAsKAs

NUORODOS:

Nuoroda ant paveiksliuko su katinu
http://dovvnload.mikrosoft.com/
http://pley.google.com/
http://www.dovvnload.com

Tyrėjas:

(Vardas, Pavardė, Parašas)

Mykolo Romerio Universiteto

Socialinių technologijų instituto

Kibernetinio saugumo valdymo magistrantas

Studento identifikacinis numeris **141992**

2015-__-__

Užsakovas

(Vardas, Pavardė, Parašas)

Organizacijos X

Informacinių sistemų tarnybos vedėjas

Darbuotojo pažymėjimas Nr. _____

2015-__-__

EKSPERIMENTAS NR. 3

TIKSLAS: patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai vartotojai randa USB laikmeną su programiniu kodu.

ATRINKTI DALYVIAI: atsitiktiniai vartotojai, kurie ras paliktas USB laikmenas su programiniu kodu.

EIGA: Eksperimentas vykdomas tokia eiga:

4. Organizacijos X skirtingose vietose (bendro naudojimo patalpose) bus palikti 5 vnt. USB laikmenų su programiniu kodu, USB laikmenoms suteiktas pavadinimas **SVARBU**.
5. USB laikmenoje yra kompiuterinės bylos:
    a. kamasutra.pdf.exe
    b. MUZIKA\geriausiosdainos.mp3.exe
    c. FILMAI\50pilkuatspalviu.avi.exe
    d. ZAIDIMAI\angrybirds.exe
    e. FOTO\intymi.jpg.exe
6. Duomenys apie kompiuterinių bylų aktyvavimą rastoje USB laikmenoje registruojami Organizacijos X bendrame tinklo kataloge [Kompiuterio vardas: _____ IP adresas: _____ MAC adresas: _____].
7. Vartotojui aktyvavus kompiuterinę bylą**:**
    a. kamasutra.pdf.exe – sukuria %username%.txt, kuriame registruojamas vartotojo vardas ir kompiuterio vardas;
    b. geriausiosdainos.mp3.exe – sukuria %username%_desktopfiles.txt, kuriame pateikiamas vartotojo darbalaukyje esančių kompiuterinių bylų sąrašas;
    c. 50pilkuatspalviu.avi.exe – sukuria %username%_softas.txt, kuriame pateikiamas vartotojo kompiuteryje įdiegtos programinės įrangos sąrašas;
    d. angrybirds.exe – sukuria %username%_ip.txt, kuriame registruojamas IP adresas;
    e. intymi.jpg.exe – sukuria %username%_mac.txt, kuriame registruojamas MAC adresas.

REZULTATAS: Eksperimento rezultate bus nustatytas rizikos organizacijos kibernetinei erdvei laipsnis.

KRITERIJAI: Rizikos organizacijos kibernetinei erdvei laipsnis bus nustatytas remiantis kriterijais:

4. Aukštas – jei:
    a. nors vienas vartotojas aktyvuoja bent vieną kompiuterinę bylą, esančią USB laikmenoje.
5. Vidutinis – jei:
    a. nebus aktyvuota nei viena kompiuterinė byla, esanti USB laikmenoje, ir apie rastą USB laikmeną nebus pranešta Informacinių sistemų tarnybai.

6. Žemas – jei:
    a. nei vienas vartotojas neaktyvuos kompiuterinių bylų, esančių USB laikmenoje, ir apie incidentą informuota Informacinių sistemų tarnyba.

KOMPIUTERINĖS BYLOS kamasutra.pdf.exe PROGRAMINIS KODAS:

```
REM USB failai
REM sukuriam kataloga pavadinta vartotojo vardu \\_____\cyber$\USB\
if not exist \\_____\cyber$\USB\%username%\ md
\\_____\cyber$\USB\%username%\
REM
REM gaunam vartotojo varda
REM
echo "vartotojo vardas:" %username% >
\\_____\cyber$\USB\%username%\%username%.txt
REM
REM gaunam kompiuterio varda
REM
echo "kompiuterio vardas:" %computername% >>
\\_____\cyber$\USB\%username%\%username%.txt
```

KOMPIUTERINĖS BYLOS geriausiosdainos.mp3.exe PROGRAMINIS KODAS:

```
REM USB failas
REM gaunam Destop failu saraša
if not exist \\_____\cyber$\USB\%username%\ md
\\_____\cyber$\USB\%username%\
dir %userprofile%\Desktop\ /b /s >
\\_____\cyber$\USB\%username%\USB\%username%_desktopfiles.txt
```

KOMPIUTERINĖS BYLOS 50pilkuatspalviu.avi.exe PROGRAMINIS KODAS:

```
REM USB failas
REM gaunam kompiuteryje instaliuotos PI saraša
REM
if not exist \\_____\cyber$\USB\%username%\ md
\\_____\cyber$\USB\%username%\
wmic /output:\\_____\cyber$\USB\%username%_Softas.txt product get name,version
```

KOMPIUTERINĖS BYLOS angrybirds.exe PROGRAMINIS KODAS:

```
REM USB failai
REM gaunam IP adresa
if not exist \\_____\cyber$\USB\%username%\ md \\_____\cyber$\USB\%username%\
@echo off
call :get_ip_address
echo "IP adresas:" %ip_address% >> \\_____\cyber$\USB\%username%\%username%_ip.txt
goto :eof
:get_ip_address
FOR /f "tokens=1 delims=:" %%d IN ('ping %computername% -4 -n 1 ^| find /i "reply"') do (FOR /F
"tokens=3 delims= " %%g IN ("%%d") DO set ip_address=%%g)
goto :eof
```

KOMPIUTERINĖS BYLOS intymi.jpg.exe PROGRAMINIS KODAS:

```
REM USB failai
REM gaunam MAC adresa
if not exist \\_____\cyber$\USB\%username%\ md \\_____\cyber$\USB\%username%\
echo off
call :get_mac_address
echo "MAC adresas:" %mac_address% >>
\\_____\cyber$\USB\%username%\%username%_mac.txt
goto :eof
:get_mac_address
For /f "tokens=1" %%a in ('getmac /NH') do set mac_address=%%a
goto :eof
```

Tyrėjas:

(Vardas, Pavardė, Parašas)

Mykolo Romerio Universiteto

Socialinių technologijų instituto

Kibernetinio saugumo valdymo magistrantas

Studento identifikacinis numeris **141992**

2015-__-__

Užsakovas

(Vardas, Pavardė, Parašas)

Organizacijos X

Informacinių sistemų tarnybos vedėjas

Darbuotojo pažymėjimas Nr. ____

2015-__-__

5 PRIEDAS

Anketa

Organizacijos X dabartinė situacija – IT tarnybos vadovas, IT tarnybos vadovo pavaduotojas

Magistriniam darbui „Organizacijos X kibernetinės erdvės gynyba“ atlieku tyrimą, todėl labai prašau Jūsų prisidėti ir skirti kelias minutes, atsakyti į anketos klausimus. Mūsų susitikimas truks iki 30 min. Garantuoju visišką anonimiškumą – visi duomenys bus išanalizuoti ir universitetui pateikiami tik apibendrinti.

Papasakokite apie jūsų skyriaus funkcijas?

Papasakokite apie skyriaus personalą. Kokių sričių specialistai dirba? Kokia personalo kvalifikacija? Ar turite pareigybę, dedikuotą kibernetinio saugumo klausimams spręsti?

Apibūdinkite organizacijos IT ūkį: Kiek IT vartotojų? Kiek kompiuterizuotų darbo vietų? Kiek serverių? Kokios yra kritinės paslaugos? Kokias kompiuterinės debesijos paslaugas naudojate?

Kokie Jūsų manymu organizacijos informaciniai ištekliai, į kuriuos gali būti nukreiptos tikslinės kibernetinės atakos? Jei taip įvardinkite juos.

Kaip valdomas organizacijos kibernetinis saugumas?

Kokie kibernetiniai incidentai Jūsų organizacijoje buvo fiksuoti? Kaip apie tai sužinojote? Kokių ėmėtės priemonių?

Ar jūsų organizacija turi patvirtintas kibernetinių incidentų valdymo procedūras? Papasakokite kaip realybėje vyksta tokių incidentų valdymas.

Ar jūsų organizacija turi patvirtintas veiklos atkūrimo ir tęstinumo valdymo procedūras? Papasakokite plačiau.

Kokias saugumo priemones taiko jūsų organizacija?

Kaip vyksta personalo (ir techninio, ir kito) kibernetinio saugumo mokymas ir ugdymas? Ar darbuotojai supažindinami su kibernetinėmis grėsmėmis, kaip jas atpažinti ir ką daryti atpažinus?

Kokią įtaką 2008-2011 m. krizė turėjo įtakos jūsų organizacijos IT ūkiui ir kibernetiniam saugumui? (pvz.: jokios įtakos; sumažėjo lėšos, skiriamos IT, todėl kibernetinio saugumo sąskaita buvo bandoma palaikyti IT infrastruktūrą .....)

Kaip jūs vertinate jūsų organizacijos pasirengimą vykdyti kibernetinės erdvės gynybą? Kokios Jūsų manymu stipriosios ir silpnosios pusės?

Papasakokite plačiau apie antivirusinės apsaugos technines priemones? Kokią antivirusinę įrangą naudojate, kokiu dažnumu atsinaujina, ar yra centralizuotas valdymas, kaip pranešama apie fiksuotus incidentus, ar visi įrenginiai turi antivirusinę įrangą? Ar yra galimybė, kad tinklo prieiga bus suteikta įrenginiui be veikiančios antivirusinės sistemos? Ar yra tikrinamas antivirusiniais varikliais Interneto srautas, ar jie to paties gamintojo kaip ir įrenginių antivirusinė įranga? Kaip

vykdoma elektroninio pašto antivirusinė sauga? Kokias dar papildomas priemones taikote apsaugai nuo virusų ir kitos kenkimo programinės įrangos?

Kaip valdomos vartotojų teisės? Kaip kuriamos naujų vartotojų paskyros? Kaip suteikiamos administratorių teisės? Ar vartotojai turi administratoriaus teises kompiuteriuose?

Kaip diegiate programinę įrangą į kompiuterius? Ar kiekvieną kartą atsiunčiama naujausia iš Interneto? Ar yra koks centralizuotas sprendimas? Kokia programinės įrangos naujinimo strategija vadovaujatės?

Kaip organizacijoje valdomi pažeidžiamumai?

Gal turite dar ką pasakyti svarbaus?

Ačiū Jums išsamius atsakymus.

6 PRIEDAS

Anketa

Organizacijos X eksperimentų rezultatai – IT tarnybos vadovo pavaduotojas

Magistriniam darbui „Organizacijos X kibernetinės erdvės gynyba“ atlieku tyrimą, todėl labai prašau Jūsų prisidėti ir skirti kelias minutes, atsakyti į anketos klausimus. Mūsų susitikimas truks iki 30 min. Garantuoju visišką anonimiškumą – visi duomenys bus išanalizuoti ir universitetui pateikiami tik apibendrinti.

Pagal susitarimą su Jūsų tarnyba buvo atlikti trys eksperimentai. Prašyčiau Jūsų pakomentuoti pastebėjimus. Pradėkime nuo eksperimento Nr. 1, kurio tikslas buvo patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai atsiunčiamas suklastotas elektroninio laiško, kuriame vartotojai raginami įvesti prisijungimo prie savo tarnybinio elektroninio pašto duomenis. (kokie rezultatai? Kokia darbuotojų reakcija – ar buvo informuojama Jūsų tarnyba, kokie rezultatai (kiek vartotojų bandė atiduoti prisijungimo duomenis, kiek atidavė).

Papasakokite apie eksperimentą Nr. 2, kurio tikslas patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai atsiunčiamas suklastotas elektroninio laiško, kuriame vartotojai raginami atsisiųsti iš pateiktų nuorodų ir aktyvuoti savo kompiuteriuose programinį kodą. (kokie rezultatai – ar buvo atsiųsta, aktyvuota kenkimo programinės įrangos imitacija, kokia vartotojų reakcija).

Papasakokite apie eksperimentą Nr. 3, patikrinti kaip organizacija reaguoja į kibernetinį incidentą, kai vartotojai randa *USB* laikmeną su programiniu kodu. (kaip vyko eksperimentas, kokia vartotojų reakcija, kokie rezultatai (vienas vartotojas aktyvavo)).

Gal turite dar ką pridurti dėl vykdytų eksperimentų.

Ačiū Jums išsamius atsakymus.

7 PRIEDAS

Interviu

Organizacijai X pasiūlytų kibernetinės gynybos priemonių efektyvumo vertinimas – IT tarnybos vadovo pavaduotojas

Magistriniam darbui „Organizacijos X kibernetinės erdvės gynyba“ atlieku tyrimą, todėl labai prašau Jūsų prisidėti ir skirti laiko susitikimui, kuris truks iki 30 min. Garantuoju visišką anonimiškumą – visi duomenys bus išanalizuoti ir universitetui pateikiami tik apibendrinti.

Prašau papasakokite kaip sekėsi taikyti praktikoje Jūsų organizacijai pasiūlytas kibernetinės erdvės gynybos stiprinimo priemones?

Kokias priemones nusprendėte diegti pirmiausiai? Kodėl?

Ar patikrinote praktiškai priemonių efektyvumą? Kaip? Kokie rezultatai?

Jūs nieko nepaminėjote apie programinės įrangos naujinimus, ar ėmėtės kokių nors priemonių, jei taip tai kokių, jei ne – dėl kokių priežasčių?

Jūs kalbėjote apie *Microsoft PĮ,* o kaip dėl kitų gamintojų PĮ?

Ar susidūrėte su kokiomis nors kliūtimis diegdami priemones? Jei taip, tai kokiomis?

Kaip vertinate *20 CSC* metodikos taikymo galimybes Jūsų organizacijoje?

Gal dar turite ką svarbaus paminėti?

Ar neprieštarausite, jei dabar atliktume trumpą eksperimentą, kad galėtume patikrinti kaip veikia „gynybos į gylį“ principo priemonės?

8 PRIEDAS

3 lentelė. *Organizacijai X* rekomenduojamos kibernetinės gynybos priemonės

#	Priemonė	Pastabos
***CSC* 1**	**Leistinų ir nesankcionuotų įrenginių inventorizavimas**	
***CSC* 1-1**	Įdiegti automatizuotą tinklo inventorizavimo sistemą, kuri leistų inventorizuoti tinkle veikiančius įrenginius.	*Organizacija X* gali naudoti atviro kodo programinę įrangą *Spiceworks* www.spiceworks.com.
***CSC* 1-6**	Įdiegti tinklo prieigos kontrolės sistemą, kuri įgalintų saugumo reikalavimų neatitinkančių įrenginių tinklo prieigos ribojimą.	Organizacija gali taikyti *Microsoft Windows Server 2008 R2* esantį NAP (angl. *Network Access Protection*) funkcionalumą: https://msdn.microsoft.com/en-us/library/dd314175(v=ws.10).aspx
***CSC* 2**	**Leistinos ir nesankcionuotos programinės įrangos inventorizavimas**	
***CSC* 2-1**	Įdiegti leistinos programinės įrangos kontrolės technologiją, kuri leistų sistemose naudoti tik leistiną programinę įrangą, o visa kita įranga būtų blokuojama automatiškai.	*Organizacija X* gali išnaudoti turimos operacinės sistemos *Microsoft Windows Server 2008 R2* funkcionalumą *Applocker*: https://technet.microsoft.com/en-us/library/dd723686(v=ws.10).aspx
***CSC* 2-2**	Sukurti *Organizacijoje X* leistinos programinės įrangos ir jų versijų sąrašą kompiuteriams, serveriams, nešiojamiems kompiuteriams ir mobiliesiems įrenginiams.	*Organizacija X* turėtų patvirtinti leistinos programinės įrangos sąrašą (gali būti kaip priedas prie Naudojimosi kompiuteriais *Organizacijoje X* taisyklių).
***CSC* 2-4**	Įdiegti programinės įrangos inventorizavimo sistemą, kuri gebėtų ne tik aptikti įdiegtą programinę įrangą, bet ir nustatyti jų versijas bei įdiegtas pataisas.	Žr. priemonę ***CSC* 1-1.**

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

#	Priemonė	Pastabos
***CSC* 2-5**	Programinės įrangos inventorizavimo sistema turi būti integruota su techninės įrangos inventorizavimo sistema, kas leistų stebėti techninės įrangos būklę su joje įdiegta programine įranga.	Žr. priemonę ***CSC* 1-1.**
***CSC* 2-6**	Pavojingi rinkmenų tipai, tokie kaip ***.exe** ar ***.msi** turi būti blokuojami.	*Organizacija X* gali išnaudoti turimos operacinės sistemos *Microsoft Windows Server 2008 R2* funkcionalumą *Software Restriction Policies*: https://technet.microsoft.com/en-us/library/hh994606.aspx.
***CSC* 3**	**Saugios mobiliųjų įrenginių, nešiojamų kompiuterių, darbo stočių ir tarnybinių stočių techninės ir programinės įrangos konfigūracijos.**	
***CSC* 3-1**	Naudoti tik standartines saugias operacinių sistemų konfigūracijas. Nenaudojamos sisteminės paskyros ar tarnybos turi būti išjungtos, blokuojami nenaudojami tinklo prievadai, turi būti diegiami atnaujinimai ir pataisos.	*Organizacijos X* IT tarnyba turi paruošti ir nuolat naujinti operacinių sistemų standartinės konfigūracijos atvaizdus (angl. Images).
***CSC* 3-2**	Turi būti įdiegta programinės įrangos naujinimo sistema. Turi būti naujinamos ne tik operacinės sistemos, bet ir taikomosios programos.	*Organizacija X* gali naudoti operacinėje sistemoje *Microsoft Windows Server 2008 R2* esančią atnaujinimų tarnybą *Windows Server Update Services, WSUS*: https://technet.microsoft.com/en-us/library/dd939822(v=ws.10).aspx ir grupinės politikos programinės įrangos diegimo funkcionalumą: https://support.microsoft.com/en-us/kb/816102.

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

#	Priemonė	Pastabos
***CSC* 3-3**	Riboti administratoriaus privilegijas. Administratoriaus teises suteikti tik kompiuterines sistemas administruojančiam personalui.	Naudojimosi kompiuteriais *Organizacijoje X* taisyklėse ši sąlyga yra įtvirtinta, tačiau realiai yra keli vartotojai, turintys administratoriaus privilegijas.
***CSC* 3-5**	Programinės įrangos rinkmenas saugoti tik saugios konfigūracijos serveriuose. Naudoti integralumo patikros įrankius, kad užtikrinti jog atvaizdai nėra nesankcionuotai pakitę.	*Organizacijos X* IT tarnyba turi sukurti vieningą prieigą tinkle, kur būtų saugomi patikrintos programinės įrangos rinkmenos.
***CSC* 3-10**	Taikyti automatines sistemų konfigūravimo priemones, kurios užtikrintų saugių konfigūracijų įgalinimą tose sistemose.	*Organizacija X* gali taikyti *Microsoft Windows Server 2008 R2* grupinių politikų objektus: https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx
***CSC* 4**	**Periodinis pažeidžiamumų ieškojimas ir taisymas.**	
***CSC* 4-1**	Periodinis pažeidžiamumų tinkle tikrinimas automatizuotais įrankiais.	Galima taikyti *MBSA* programinę įranga: http://www.microsoft.com/en-us/download/details.aspx?id=7558, kuri kartą per savaitę vykdytų pažeidžiamumų skenavimą, o rezultatus saugotų centralizuotoje vietoje.
***CSC* 4-5**	Įdiegti automatinius pataisų diegimo ir programinės įrangos naujinimo įrankius.	Žr. ***CSC* 3-2** priemonę.
***CSC* 4-9**	Prieš diegiant darbinėje aplinkoje, kritinius atnaujinimus diegti testavimo aplinkoje.	Tai padės organizacijai išvengti kritinių atnaujinimų sukeltų sistemų sutrikimų.
***CSC* 4-10**	Nustatyti pažeidžiamumų rizikų vertinimo procesą, kuris paremtas pažeidžiamumų išnaudojimo galimybės ir potencialaus poveikio vertinimu pagal atskiras sistemų grupes.	Pirmiausiai turi būti diegiamos pataisos aukščiausios rizikos pažeidžiamumams.

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

#	Priemonė	Pastabos
***CSC* 5**	**Gynyba nuo kenkimo programinės įrangos.**	
***CSC* 5-3**	Drausti kompiuteriams ir serveriams automatiškai vykdyti keičiamų išorinių laikmenų (*USB, CD/DVD,* tinklo diskai) turinį.	Naudoti *Microsoft* grupinių politikų nustatymus: https://support.microsoft.com/en-us/kb/2328787
***CSC* 5-4**	Sukonfigūruoti sistemas taip, kad prijungus išorinę laikmeną, būtų vykdomas automatinė kenkimo programinės įrangos paieška.	*ESET* nustatymai: http://support.eset.com/kb3449/
***CSC* 5-6**	Įgalinti pažeidžiamumų išnaudojimo apsaugos mechanizmus (DEP, ASLR ir pan.)	Įdiegti *Microsoft EMET* įrankį: https://technet.microsoft.com/en-us/security/jj653751
***CSC* 5-7**	Riboti išorinių laikmenų naudojimą, naudoti tik esant būtinybei, nustatyti naudojimo kontrolės procesą.	*Organizacija X* turėtų patvirtinti išorinių laikmenų naudojimo taisykles (gali būti kaip priedas prie Naudojimosi kompiuteriais *Organizacijoje X* taisyklių).
***CSC* 9**	**Saugumo įgūdžių vertinimas ir atitinkamų mokymų organizavimas.**	
***CSC* 9-1**	Atlikti darbuotojų IT saugos žinių spragų analizę, kad parengti darbuotojų IT saugos mokymo planą.	Eksperimentų Nr. 1 ir Nr. 3 rezultatai atskleidė vartotojų IT saugos žinių spragas.
***CSC* 9-2**	Pravesti darbuotojų IT saugos mokymus, mokymus gali pravesti vietinis personalas, dėstytojas iš išorės arba mokymai gali būti surengti nuotoliniu būdu.	IT saugos mokymai turi apimti klausimus kaip elgtis su rastomis *USB* laikmenomis ir kaip saugoti savo paskyrų duomenis.
***CSC* 9-3**	Įdiegti IT saugos ugdymo sistemą, kurioje būtų vartotojai perspėjami apie socialinės inžinerijos grėsmes. Nauji vartotojai, prieš sukuriant paskyras, turėtų baigti įvadinius IT saugos mokymus, vėliau kasmet juos pakartoti.	Išnaudoti *Organizacijos X* vidinio tinklo išteklius, pvz.: vidinį portalą.

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

#	Priemonė	Pastabos
***CSC* 9-4**	Tikrinti ir tobulinti IT saugos ugdymo sistemą. Periodiškai tikrinti vartotojų elgseną, imituojant socialinės inžinerijos atakas.	Pakartoti eksperimentus Nr. 1, 2 ir 3, pvz.: po metų.
***CSC* 12**	**Administravimo teisių naudojimo kontrolė.**	
***CSC* 12-1**	Sumažinti administravimo privilegijų naudojimą, naudoti tik administravimo tikslams.	Sutampa su priemone ***CSC* 3-3**.
***CSC* 12-3**	Visi administratorių paskyrų slaptažodžiai turėtų būti sudėtingi, juos turėtų sudaryti iš skaitmenų, raidžių ir specialiųjų simbolių.	Įgyvendinama per *Microsoft* grupines politikas: https://technet.microsoft.com/en-us/library/cc783512(v=ws.10).aspx. Reikalavimai slaptažodžiams turėtų būti įtvirtinti organizacijos taisyklėse.
***CSC* 12-4**	Visuose naujai į tinklą jungiamuose įrenginiuose turi būti pakeičiami gamykliniai slaptažodžiai.	Tai turi apimti tinklo įrangą, kompiuterius ir serverius.
***CSC* 12-5**	Užtikrinti, kad visos tarnybinės paskyros turi sudėtingus, sunkiai atspėjamus slaptažodžius, kurie keičiami periodiškai.	Įgyvendinama per *Microsoft* grupines politikas: https://technet.microsoft.com/en-us/library/dd548356(v=ws.10).aspx
***CSC* 12-7**	Užtikrinti, kad administravimo paskyros naudojamos tik administravimo tikslams. Drausti naudoti administravimo paskyras elektroniniam paštui skaityti arba naršyti Internete.	Įtraukti administravimo paskyras ugniasienėje į blokuojamų paskyrų sąrašą.
***CSC* 12-8**	Užtikrinti, kad administratoriai naudoja skirtingus slaptažodžius administravimo ir paprastoms paskyroms.	Naudoti unikalias administravimo paskyras. Slaptažodžių politika valdoma *Microsoft* grupinių politikų pagalba.
***CSC* 12-9**	Operacinės sistemos turi drausti naudoti tuos pačius slaptažodžius pusės metų laikotarpyje.	Slaptažodžių politika valdoma *Microsoft* grupinių politikų pagalba: https://technet.microsoft.com/en-us/library/hh994571.aspx

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

#	Priemonė	Pastabos
***CSC* 12-14**	Drausti prisiregistruoti sistemoje administratoriaus paskyroms. Administratoriai turi naudoti paprastų vartotojų paskyras registruodamiesi į sistemas.	Vykdant administravimo užduotis naudoti ***Run As Administrator*** komandą.
***CSC* 18**	**Reagavimas į incidentus ir jų valdymas.**	
***CSC* 18-1**	Užtikrinti, kad būtų sukurtos rašytinės incidentų valdymo procedūros, kuriose aprašytos atsakingo personalo funkcijos. Procedūrose turėtų būti numatytos incidentų valdymo fazės.	Turi būti sukurtas ir patvirtintas reagavimo į incidentus planas, kuriame būtų numatyti incidentų valdymo etapai. Taip pat reikėtų numatyti sąlygas kada turi būti aktyvuotos *Organizacijos X* veiklos atkūrimo ir tęstinumo procedūros.
***CSC* 18-2**	Priskirti incidentų valdymo funkcijas konkretiems darbuotojams.	Reagavimo į incidentus plane turi būti paskirstytos atsakomybės personalui.
***CSC* 18-3**	Numatyti vadovaujantį incidentų valdymo personalą, kuris dalyvautų sprendimų priėmimo procesuose.	Ši priemonė ypač svarbi, kai reikalinga aukščiausios vadovybės parama priimant sprendimus.
***CSC* 18-6**	Paskelbti visam organizacijos personalui pranešimų apie kompiuterių veiklos anomalijų ir incidentų tvarką. Šią informaciją įtraukti į periodinį darbuotojų ugdymo planą.	Susieti su ***CSC* 9-3** priemone.
***CSC* 18-7**	Periodiškai tikrinti incidentų valdymo komandos žinias apie grėsmes ir rizikas bei pasirengimą reaguoti į incidentus.	Susieti su ***CSC* 9-1** priemone.

„Sudaryta autoriaus“

9 PRIEDAS

Forma patvirtinta Mykolo Romerio universiteto

Senato 2012 m. lapkričio d. nutarimu Nr.1SN-

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2015 m. gruodžio 10 d.

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

_*Verslo ir medijų mokyklos, Kibernetinio saugumo valdymo*_____

(fakulteto / instituto, programos pavadinimas)

Studentas (-ė) _*Žilvinas Ropė*_____,

(vardas, pavardė)

patvirtinu, kad šis magistro baigiamasis darbas *„Organizacijos X kibernetinės erdvės gynyba“*:

1. Yra atliktas savarankiškai ir sąžiningai;

2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;

3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

_____ _____

(parašas) *(vardas, pavardė)*

Žilvinas Ropė

LT: Organizacijos X kibernetinės erdvės gynyba.

EN: Cyber Defence in X Organization.