MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERLSO FAKULTETAS

DEIVIDAS AMBRULEVIČIUS

KIBERNETINĖS GRĖSMĖS IR KIBERNETINIO SAUGUMO UŽTIKRINIMAS ĮMONĖSE: DAIKTŲ INTERNETO ASPEKTAS

Magistro baigiamasis darbas

Darbo vadovas

Prof. dr. Darius Štitilis

Vilnius, 2020

MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

KIBERNETINĖS GRĖSMĖS IR KIBERNETIIO SAUGUMO UŽTIKRINIMAS ĮMONĖSE: DAIKTŲ INTERNETO ASPEKTAS

Verslo ir vadybos magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas

Prof. dr. Darius Štitilis

2020 04 …

Atliko

KSVvmis18-1

D. Ambrulevičius

2020 04 16

VILNIUS, 2020

TURINYS

ĮVADAS ... 6
1.KIBERNETINIO SAUGUMO IR DAIKTŲ INTERNETO TEORINIAI ASPEKTAI ... 9
1.1 Kibernetinis saugumas ir jo raidos tendencijos ... 9
1.2 Daiktų interneto sąvoka ir naudojimas versle ... 11
1.2.1 Daiktų interneto reikalavimai verslui ... 13
1.3 Nauji iššūkiai kibernetiniam saugumui – daiktų interneto plėtra. ... 16
2. DAIKTŲ INTERNETO ĮTAKA KIBERNETINIAM SAUGUMUI. PASAULINĖ ANALIZĖ ... 18
2.1 Naujų IoT įrenginių gausa pasaulyje – grėsmė kibernetiniam saugumui. ... 18
2.2 JAV pavyzdys ... 21
2.3 Kinija ... 22
2.3 Vokietija ... 23
2.4 Lietuva ... 25
2.6 Pasirinktų šalių apibendrinimas, išvados ... 29
3. DAIKTŲ INTERNETO SAUGUMO PROBLEMOS, SPRENDIMO BŪDAI. ... 31
3.1 Pažeidžiamiausios daiktų interneto naudotojų sritys. ... 31
3.2 IoT įrenginių pažeidžiamumo tipai ir atakų galimybės ... 37
3.3 Daiktų interneto įrenginių saugumo architektūra ... 40
3.3.1 Saugaus įrenginio modelis ... 47
4. KIBERNETINIO SAUGUMO UŽTIKRINIMAS ĮMONĖSE: DAIKTŲ INTERNETO ASPEKTAS. TYRIMAS ... 49
4.1 Tyrimo metodologija ... 49
4.2 Tyrimo duomenų analizė ... 52
IŠVADOS ... 57
REKOMENDACIJOS ... 59
LITERATŪROS SĄRAŠAS ... 60
SANTRAUKA LIETUVIŲ KALBA ... 65
SANTRAUKA ANGLŲ KALBA ... 66
ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS ... 67
PRIEDAI ... 68

PAVEIKSLAI

1 PAV. DAIKTŲ INTERNETO POVEIKIS KIBERNETINĖMS ATAKOMS. TENDENCIJA 2025M. ŠALTINIS: CYBER SECURITY RADAR TINKLAPIS. 11
2 PAV. DAIKTŲ INTERNETO REIKALAVIMAI VERSLUI. SUDARYTA AUTORIAUS PAGAL LAIMĄ ZALIECKIENĘ IR RAIMUNDĄ ŽILISNKĄ. 14
3 PAV. DAUGIAUSIAI ATAKŲ PATIRIANČIOS ŠALYS PASAULYJE. ŠALTINIS: ĮMONĖS „COMPARITECH“ TINKLAPIS 18
4 PAV. ŠALYS KURIOMS KIBERNETINĖS ATAKOS DAUGIAUSIAI KAINUOJA. ŠALTINIS: ĮMONĖS „COMPARITECH“ TINKLAPIS. 19
5 PAV. DAUGIAUSIAI KIBERNETINIŲ ATAKŲ PATIRIANTYS SEKTORIAI. ŠALTINIS „FIREEYE“ TINKLAPIS. 20
6 PAV. 10 DAŽNIAUSIAI PATIRIANČIŲ DAIKTŲ INTERNETO KIBERNETINIUS IŠPUOLIUS SRIČIŲ. ŠALTINIS: „PENTON“ TINKLAPIS 31
7 PAV. DAIKTŲ INTERNETO ĮRENGINIŲ ATAKŲ TIPAI. SUDARYTAS AUTORIAUS PAGAL ĮMONĖS „ALLERIN“ KIBERNETINIO SAUGUMO SPECIALISTŲ ĮŽVALGAS. 37
8 PAV. 6 DAIKTŲ INTERNETO ĮRENGINIŲ APSAUGOS PRICIPAI. ŠALTINIS: „IOT ANALYTICS“ TINKLAPIS 41
9 PAV. SAUGAUS IOT ĮRENGINIO MODELIS. SUDARYTAS AUTORIAUS PAGAL „ARDEX“ VADOVO GEORGE CORE ANALIZĘ. 47
10 PAV. ANKETOS SUDARYMO SCHEMA PAGAL VYTAUTĄ DIKČIŲ, 2011. 49
11 PAV. EKSPERTŲ VERTINIMO NUOKRYPIO PRIKLAUSOMYBĖ NUO EKSPERTŲ SKAIČIAUS. ŠALTINIS: PAGAL ŽALIMAITĘ IR BALEŽENTĮ 51
12 PAV. DAIKTŲ INTERNETO ĮRENGINIŲ SKAIČIUS TIRTOSE VERSLO ĮMONĖSE. 52
13 PAV. BANDYMAI ĮSILAUŽTI Į ĮMONIŲ IOT ĮRENGINIUS 53
14 PAV. DAŽNIAUSIAI NAUDOJAMI ATAKŲ TIPAI ĮMONĖSE. 53
15 PAV. DAŽNIAUSIAI KIBERNETINES ATAKAS PATIRIANTYS ĮRENGINIAI 54
16 PAV. ĮMONIŲ APSISAUGOJIMO BŪDAI NUO KIBERNETINIŲ INCIDENTŲ. 55

PRIEDAI

PRIEDAS 1. TYRIME NAUDOTA ANKETA..... 68

ĮVADAS

Temos aktualumas. Vystantis išmaniosioms technologijoms kibernetinė erdvė paveikė visas sferas, kurios didžiąją veiklos dalį perkėlė į virtualią erdvę. Bene didžiausios galimybės atsivėrė verslo subjektams, jų elektroninės prekės ar paslaugos be vargo tapo pasiekiamos iš bet kurio pasaulio krašto. Šių dienų naujosios technologijos šiuolaikiniam verslui leidžia visus procesus atlikti dar greičiau ir patogiau daiktų interneto pagalba. Daiktų internetas viena greičiausiai ir pažangiausiai besivystanti informacinių ir komunikacinių technologijų krypčių, kurios plitimo mastai kasmet auga. Tarpusavyje sujungti išmanieji daiktai sudaro lengvai pasiekiamą ir valdomą daiktų interneto tinklą, kuriame įrenginiai siųsdami informaciją vienas kitam padeda efektyviau organizuoti veiklą, taip spartindami verslo komunikacinius procesus bei veiklos efektyvumą. Be daugybės naudingų padarinių daiktų interneto įsiveržimas į kibernetinę erdvę sukėlė daugybę naujų saugumo uždavinių kibernetinio saugumo ekspertams pasaulyje. Daugėjant daiktų prijungtų prie tinklo, verslui iškilo naujas uždavinys, kaip juos visus tinkamai apsaugoti jog jie neatneštų daugiau bėdų nei naudos, nes su kiekvienu nauju daiktu tinkle atsiranda naujas kelias kibernetiniams nusikaltėliams patekti į įmonės sistemas. Saugios kibernetinės erdvės užtikrinimo uždavinys palietė daugybę sričių, tarp jų ir pačius politikus, kurie yra priversti kurti bei keisti įstatymus norint užtikrinti elektroninės erdvės saugumą.

Temos naujumas. Informacinių technologijų galimybės bei plėtra verčia verslą keltis į naują elektroninio verslo lygmenį. Modernaus ir sėkmingo verslo neatsiejamas įrankis tampa daiktų internetas, kuris palengvina kasdieninius procesus bei verslui galimybes atlikti darbus greičiau ir kokybiškiau. Diegiant naujomis technologijomis pripildytus išmaniuosius daiktų interneto įrenginius tampame priklausomi nuo globalaus tinklo, kuris reikalingas įrenginiams veikti, todėl iškyla saugumo problemos tarptautiniu mastu, kai nusikaltėliai iš bet kurio pasaulio krašto, gali vykdyti atakas nutaikytas į daiktus esančius tinkle. Kibernetiniai nusikaltimai tapo daug pavojingesni ir pridarantys daugiau žalos nei fiziniai. Viena pagrindinių spartaus nusikaltimų skaičiaus augimo priežastimi elektroninėje erdvėje – daiktų internetas. Nes kasdien yra pagaminama ir prie tinklo prijungiama šimtai tūkstančių išmaniųjų įrenginių, kurie sudaro platesnes galimybes kibernetiniams nusikaltimams dėl netinkamos jų apsaugos. Saugi kibernetinė aplinka tiek versle, tiek politikoje ar bet kurioje kitoje srityje yra svarbus ir sudėtingas uždavinys, kurį išspręsti dėl kasdien augančio išmaniųjų įrenginių kiekio ir įvairovės tampa vis sunkiau.

Mokslinis temos ištirtumas. Apžvelgus pastarojo dešimtmečio kibernetinio saugumo ir daiktų interneto aspektus pastebima, kad kasmet moksliniame kontekste šios sąvokos atsiranda vis dažniau ir užima vis svarbesnį vaidmenį. Kibernetinio saugumo sąvokas savo moksliniuose darbuose gana plačiai nagrinėja lietuvių autoriai – Audronė Mikalauskienė, Zenonas Brazaitis, užsienio – Parker Donn, Basie von Solms, taip pat didžiųjų kibernetinio saugumo kompanijų kibernetinio saugumo specialistai: Jake Moore iš „Eset“, taip pat „Cisco“ ir „McAfee“ specialistų grupės, nuolat pateikia nemažai incidentų

ataskaitų, kurios patvirtina daiktų interneto keliamas problemas kibernetiniam saugumui. Lietuvoje teisines rekomendacijas pateikė MRU dėstytojų grupė: Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis, Inga Malinauskaitė. Apie naujausias daiktų interneto technologijas bei tendencijas plačiai dalinasi KTU mokslininkai – Algirdas Dobrovolskis, Juozas Dovydaitis, Rolandas Girčys kuriems vadovauja ir mokslo grupės „Daiktų ir paslaugų internetas“ įkūrėjas Egidijus Kazanavičius. Tačiau jų sutapatinimas ir tarpusavio priklausomybė vis dar yra nepakankamai ištirta. Retai kaip viena iš pagrindinių kibernetinio saugumo spragų yra minima daiktų internetas, todėl buvo pasirinkta ši problema tirti.

Mokslinė problema. Mokslo šaltiniuose nepakankamai išanalizuoti kibernetinio saugumo užtikrinimo metodai ir nenustatytos taisyklės, kaip tinkamai turi būti naudojami daiktai esantys tinkle. Daiktų interneto įrenginių įtaka naujos kartos kibernetinėms atakoms mažai išanalizuotas ir aprašytas procesas. Tinkamai neapsaugoti įrenginiai sukelia saugumo problemas tarptautiniu mastu, o jų spartus didėjimas rinkoje kuria itin prastas tendencijas kibernetinio saugumo klausimu. Dėl šių priežasčių įmonės, kuriose naudojamas daiktų internetas, dažnai susiduria su kibernetinio saugumo problemomis ir klausimais kaip tinkamai diegti ir naudoti daiktų internetą, kad jis atneštų daugiau naudos nei problemų?

Tyrimo tikslas. Išnagrinėti kaip daiktų internetas pakeitė verslą ir jo kibernetinį saugumą, kokios pagrindinės problemos ir kokias būdais bandoma apsisaugoti.

Pagrindiniai uždaviniai:

1. Išanalizuoti kokią įtaką daiktų internetas daro kibernetiniam saugumui.
2. Atlikti pasirinktų pasaulio šalių kibernetinio saugumo ir daiktų interneto apsaugos analizę, iškelti pagrindines daiktų prijungtų prie tinklo problemas kibernetiniam saugumui.
3. Atlikti kibernetinio saugumo kokybinį tyrimą verslo įmonėse Lietuvoje, išsiaiškinti kokia daiktų interneto įrenginių saugumo situacija, pagrindinės keliamos problemos.
4. Remiantis tyrimo rezultatais bei teorine medžiaga pateikti efektyvių sprendimo būdų bei sukurti įmonėms modelį, padėsiantį apsaugoti įrenginius prijungtus prie interneto tinklo nuo kibernetinių incidentų

Darbo objektas ir tyrimo metodai. Šio darbo tiriamasis objektas verslo įmonių naudojami nesaugūs daiktų interneto įrenginiai, bei apsaugos priemonės, kurių reikia imtis norint išvengti kibernetinių incidentų. Sąvokoms aptarti naudojamas lyginamasis ekspertų nuomonių metodas. Verslo subjektams naudojantiems daiktų internetą nagrinėti buvo pasitelkta statistiniais ir sociologiniais tyrimo metodais, pagrindinė statistika ir duomenys aprašyti remiantis kibernetinio saugumo ekspertų nuomone. Ištirti daiktų interneto saugumą verslo įmonėse Lietuvoje, buvo atliktas kokybinis tyrimas pagal ekspertų

vertinimų standartinio nuokrypio priklausomybės nuo ekspertų skaičiaus teoriją (Baležentis, Žalimaitė, 2011).

Darbo struktūra ir tyrimo rezultatų taikymo sritys. Darbą sudaro 4 dalys. Pirmoje dalyje pateikiama kibernetinio saugumo ir daiktų interneto teoriniai aspektai remiantis mokslininkų pateiktomis sąvokomis. Taip pat daiktų interneto ir verslo tarpusavio priklausomybė, keliamos grėsmės. Antroje dalyje buvo atlikta pasaulinė daiktų interneto versle saugumo analizė, išnagrinėtos šalys: (JAV, Kinija, Vokietija, Lietuva), pateiktos išvados bei apibendrinimas bendrai situacijai apžvelgti. Trečioje – nagrinėjamos daiktų interneto įrenginių problemos, atsiradimo verslo sektoriuose problemos, bei sprendimo būdai. Ketvirtoje dalyje pateikiami atlikto kokybinio tyrimo rezultatai. Atsižvelgiant į ekspertų žinias ir nuomones, pateikiamos pagrindinės problemos kylančios verslo subjektams, naudojantiems daiktų internetą.

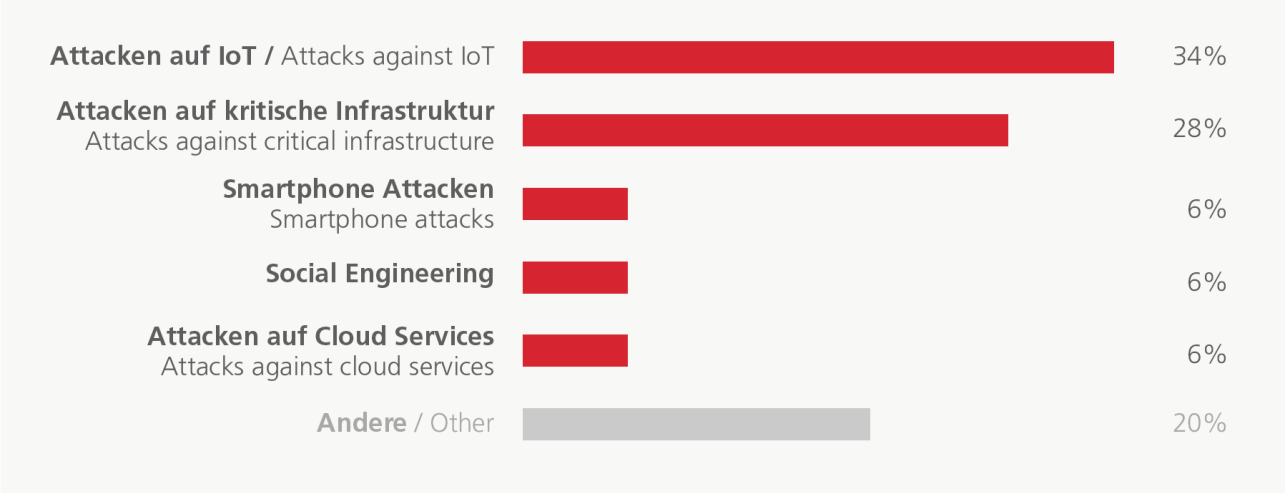
1.KIBERNETINIO SAUGUMO IR DAIKTŲ INTERNETO TEORINIAI ASPEKTAI

1.1 Kibernetinis saugumas ir jo raidos tendencijos

Kibernetinis saugumas – tai ,,visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.” (Lietuvos Respublikos Kibernetinio saugumo įstatymo 2str.10 p.).

Šiuolaikinėje visuomenėje vis daugiau dėmesio yra skiriama kibernetiniam saugumui. Atsakymas kodėl taip yra- gana paprastas. Statistiškai yra didesnė tikimybė tapti kibernetinio nusikaltimo auka negu fizinio nusikaltimo auka. Taip yra todėl, kad virtualioje erdvėje darant nusikaltimus šiuo metu yra mažesnė rizika būti „pagautam“ negu fiziniame pasaulyje ir tokio pobūdžio nusikaltimams reikalingas mažesnis piniginis biudžetas. Kad būtų geriau suprantama kibernetinio saugumo svarba visuomenėje, šiame darbe kibernetinio saugumo raida pateikiama per kibernetinių atakų prizmę. Kibernetinė ataka – tai ,,elektroninėje erdvėje pavienių asmenų arba organizacijų vykdomas informacinių sistemų, infrastruktūros objektų, kompiuterių tinklų, asmeninių kompiuterių puolimas įvairiomis kenkėjiškomis priemonėmis”. Šiuo metu tikriausiai būtų daug lengviau išvardinti gyvenimo sritis, kuriose nevyksta kibernetinės atakos, nes beveik visi gyvenimo aspektai jau yra persikėlę į internetinę erdvę. Dauguma žmonių jau suvokia, kad tai, ką paverčia skaitmenine informacija- tiesiogiai ar ne, prisijungia prie internetinio tinklo ir tai tampa interneto dalimi. Šis teiginys ir atsako į klausimą kodėl kibernetinis saugumas svarbus- kas yra pasiekiama internetu, gali būti užpuolama bet kuriuo metu ir iš bet kurios vietos. „Horizon“ konferencijoje tarptautinio IT saugumo eksperto Mikko Hypponeno teigimu, verslo sėkmė remiasi tuo, kaip efektyviai įmonė geba skaitmenizuoti savo veiklą ir visai nesvarbu, kuo įmonė užsiima, prekiauja akcijomis ar šaldytuvais. Tačiau atkreipia dėmesį į tai, kad kuo labiau skaitmenizuota įmonė -tuo didesnė kibernetinių įsilaužimų rizika. Ir tai liečia ne tik dideles įmones ar įstaigas. Svarbu suvokti ir kiekvienam fiziniam asmeniui, kad bet kuris prie interneto prisijungęs kompiuteris ar išmanusis telefonas, planšetė, kelia riziką patirti kibernetines atakas. Netrukus nebūsime saugūs nuo tokių atakų net ir svetainėje, virtuvėje, vonioje, nes šiuo metu esame „daiktų interneto“ amžiuje. Netgi išmanusis televizorius, modernus automobilis ar virtuvės įrangos prietaisas gali tapti kibernetinių įsilaužėlių taikiniais. It saugumo eksperto Mikko Hypponeno teigimu,

tikroji „daiktų interneto“ revoliucija prasidės, kai prie interneto jungsis dauguma kasdieniame gyvenime naudojamų įrenginių, prie kurių atsiras vis daugiau įvairių jutiklių, kamerų– ir šie daiktai jungsis prie interneto. Pavyzdžiui taip dauguma daiktų, kurie turės kameras gali būti puiki priemonė įsilauželiams stebėti aplinką kurioje gyvename. Kadangi technologijos tobulėja – nuo jų neatsilieka ir kibernetinės priežiūros specialistai. Vis daugiau dėmesio yra skiriama saugumo spragoms įvairiuose įrenginiuose taisymui. Pavyzdžiui, anksčiau kompiuteris su „Windows“ operacine sistema saugus buvo tik jeigu turėjo antivirusinę programa, o šiuo metu „Windows“ turi pakankamai efektyvią apsaugą ir pačios kibernetinės atakos labiau orientuotos į vartotojų psichologiją. Pastaruoju metu populiarėja Ransomware virusai, už kurių padarytą žalą yra reikalaujama išpirkų. Šio tipo virusų piko pradžia buvo 2017 metais, nes tuo metu padaugėjo net 2500%. Pradėti atakuoti tiek ir verslo subjektai tiek ir fiziniai asmenys. Pranešama, kad anksčiau šie virusai dažniausiai puldavo Windows sistemas, tačiau pastaruoju metu jie kellia grėsmę ir Mac, Linux bei Android/iOS išmaniuosiems telefonams bei planšetėms. Kibernetinio saugumo specialistė Eva Velasquez teigia, kad kibernetines atakas vykdantys subjektai pavogti duomenis gali ir pasinaudoję internete paplitusiomis naujienomis apie kitų nusikaltėlių įvykdytas atakas. Kada kibernetinių atakų sukelėjai manipuliuoja ir siunčia melagingus laiškus tik daugės. Kibernetinis saugumas turi stiprėti ir valstybiniu lygiu todėl, kad valstybių remiamos grupuotės gali pradėti atakuoti kitų šalių infrastruktūrą, gali būti sutrikdyta labia daug kasdienių paslaugų bei gali nukentėti paprasti žmonės. Valdžios rinkimų užgrobimas yra tik pradžia. „Stuxnet“ virusas, kuris buvo paplitęs dar 2010 metais įrodė, kad gali būti nulaužti miestų tinklai ir taip pažeidžiama infrastruktūra. Tačiau per šiuos 10 metų tobulėjant technologijoms ir atsiradus daugybei naujo tipo daiktų interneto įrenginių. 2020m. užfiksuota kad pasaulyje verslo objektuose daiktų prijungtų prie tinklo skaičius siekia 30 milijardų, o tendencijos rodo, kad per ateinantį dešimtmetį ir įvedus 5G ryšio tinklą, kuris leis daiktams dar greičiau veikti tinkle ir pagreitinti verslo procesus, jų skaičius padvigubės ir sieks 74 milijardus įrenginių verslo sektoriuje. (BrightTalk, 2020). O iki 2025m. kibernetinių incidentų skaičiaus didžiausią dalį sudarys daiktų interneto pagalba įvykdyti nusikaltimai. (Cyber Security Radar, 2020) (žr. 1 pav.)



1 pav. Daiktų interneto poveikis kibernetinėms atakoms. Tendencija 2025m. Šaltinis: Cyber Security Radar tinklapis.

Apibendrinant galima teigti, kad su kiekviena diena kibernetinis saugumas užima vis svarbesnį vaidmenį valstybių gyvavime. Kibernetinės atakos nuolat tobulėja ir įsilaužėliai tampa vis sumanesni ir pasitelkia skirtingus būdus kaip paveikti elektroninėje erdvėje esančius duomenis.

1.2 Daiktų interneto sąvoka ir naudojimas versle

Daiktų interneto sampratų literatūroje yra gausu. Daiktų internetas yra apibūdinamas kaip pavyzdžiui, „dinaminio globalaus tinklo infrastruktūra, kurioje fiziniai ir virtualūs „daiktai“ turi savo tapatybes ir fizinius atributus”, „ globalus tinklas, jungiantis išmaniuosius objektus”, „laiko momentas, kai objektų arba daiktų, prijungtų prie interneto, yra daugiau negu žmonių” .

Visose verslo srityse valdymas vykdomas internetu ir skaitmeniniais prietaisais, sąveikaujančiais per tinklą, todėl daiktų internetą galima apibūdinti kaip tinklų konfigūraciją, kuri apima fizinių objektų komunikaciją ir žmonių sąveiką internete. Daiktų internetui yra svarbios dvi sąvokos – fizinis daiktas ir virtualusis daiktas. Šiuo atveju daiktu yra laikomas fizinio pasaulio objektas ir informacijos pasaulio objektas, kuris gali būti identifikuotas ir integruotas į ryšių tinklus.

Kiekvienas objektas turi elektroninę žymą, yra nuolat prijungtas prie duomenų bazės ir tinklo, todėl objektus galima valdyti bei kontroliuoti. (Laima Zalieckaitė, Raimundas Žilinskas, 2015)

Istoriškai pirmiausia internetas atsirado žmonių namuose. Vėliau interneto ryšys atsirado mobiliuosiuose įrenginiuose ir tik vėliau atsirado daiktų internetas (angl. - Internet of Things). Daiktų interneto atsiradimui turėjo įtaką įvairialypės technologijos ir jų plėtra. Pavyzdžiui, daiktų interneto atsiradimui turėjo įtaką, IoT įrenginių kainų mažėjimas, duomenų apdorojimo greičio didėjimas

ir kainos mažėjimas internetinio ryšio kokybės ir pralaidumo didėjimas, nauji internetinio ryšio palaikymo standartai. Šiuo metu egzistuoja daug sensorinių prietaisų, kurie yra naudojami žmonių kasdienybėje ir patenka į daiktų interneto sampratą. Pavyzdžiui šiuo metu yra prietaisai kurie matuoja žmonių miego kokybę, aktyvumą, širdies ritmą, streso lygį, nueitų žingsnių kiekį. Prie interneto prijungti namų apyvokos prietaisai padeda gyventi patogiau - primena, kada palaistyti gėles, automatiškai palaiko temperatūrą namuose prieš grįžtant iš darbų ir panašiai. Kaip ir žmonių buitis, kasdienybė taip pat ir verslas tampa neatsiejamas nuo daiktų interneto. Nuo kompiuterių, telefonų, spausdintuvų iki vėdinimo, šaldymo-šildymo įrenginių, šaldytuvų, apšvietimo, apsaugos įrenginių (kamerų, signalizacijų) kurie visi palaipsniui yra prijungiami prie įmonės tinklo. Taigi, vis daugiau transporto priemonių, buitinių prietaisų, pastatų yra aprūpinti jutikliais ir yra sujungti su sumaniais matuokliais bei daiktų interneto platforma.

Daiktų internetas tai savotiška ateities technologijų viršūnė, kai tikri objektai, kurie supa mus - tiksliai identifikuojamai, rodoma jų buvimo vieta, taip pat galima juos pasiekti interneto tinklo pagalba iš bet kurios pasaulio vietos. Žinoma, kad šios išmaniosios paslaugos ir jų sudėtingumas kelia daiktų interneto technologijoms aukšto lygio reikalavimus (žr. 2 pav.) (Kraijak, 2015), (Raimundas Savukynas, Virginijus Marcinkevičius, 2017) .

Daiktų internetas vykdo perversmą ne tik asmens gyvenime, bet ir įvairiose verslo šakose, valstybės infrastruktūros lygmeniu. Daiktų internetas suteikia galimybę gauti duomenis apie tai, kaip naudojami fizinio pasaulio daiktai. Vartojamų daiktų aprūpinimas davikliais leidžia verslui gauti tikslesnę informaciją apie vartotojų įpročius, elgseną ir poreikius. Tai savo ruožtu padeda tobulinti produktus, efektyviau organizuoti jų tiekimą ir pan. Taigi, Daiktų internetas yra technologija, leidžianti valdyti ir verslo procesus, todėl šiame darbe svarbu išskirti daiktų interneto įtaką, privalumus ir trūkumus verslo srityje.

Daiktų interneto privalumai versle:

1. Informacijos pateikimas ir analizė. Daiktų interneto technologijos pagalba yra galimybė surinkti daug daugiau tikslesnės informacijos, kuri yra reikalinga gilioms analizėms priimant tinkamus sprendimus verslui. Kiekviena verslo sritis privalo kaupti ir analizuoti informaciją, kuri padeda įvertinti esamą situaciją rinkoje, bet ir priimti bū. Surinkta informacija
turi būti teisinga, patikima, nesidubliuojanti. Daiktų interneto pagalba kiekvienas IoT įrenginys, prijungtas prie daiktų interneto tinklo, pateikia savo veiklos informaciją ir visa tai yra padaroma automatiniu būdu.

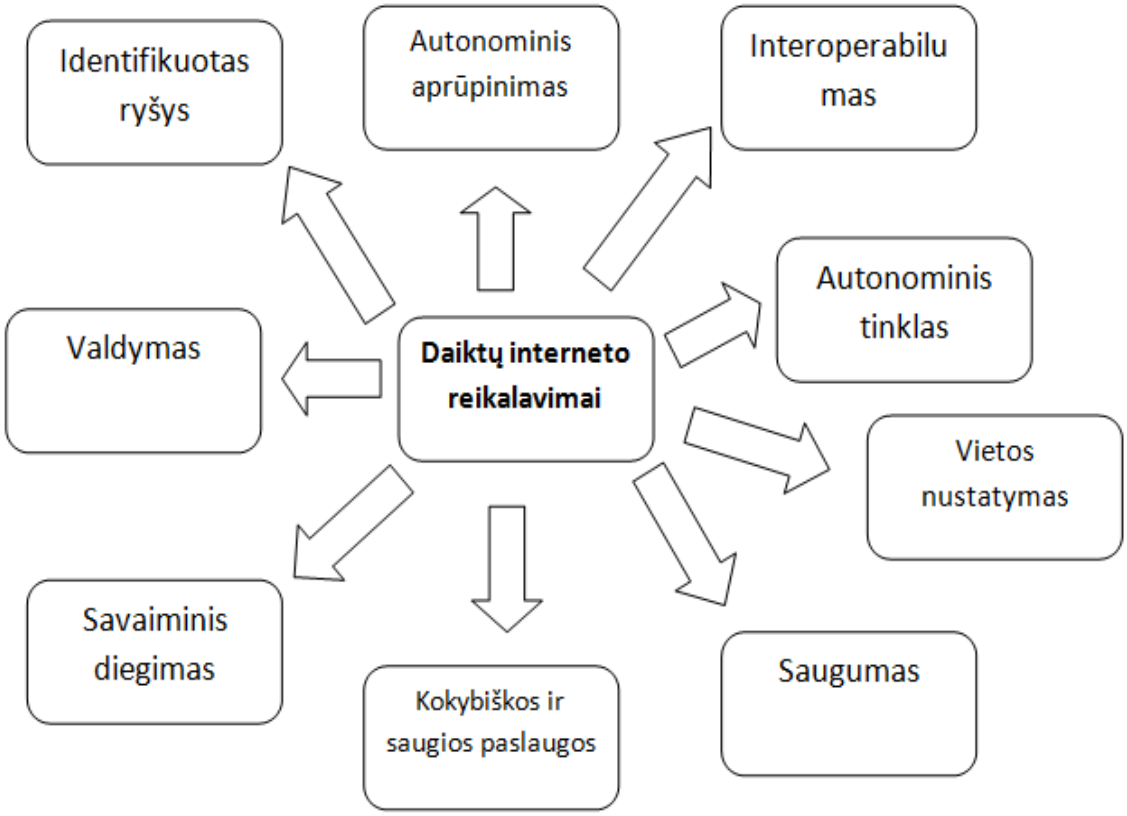
2. Nuolatinė stebėsena. Daiktų internetas savarankiškai gali vykdyti verslo objektų stebėseną. Versle stebėsena yra vykdoma norint laiku pamatyti problemą ir jos atsiradimo priežastis. Stebėti yra svarbu dėk to, kad laiku pastebėjus problemą ir atsiradimo priežastis pati problema yra lengviau ištaisoma ir

išvengiama didesnių neigiamų pasekmių verslo srityje. Daiktų interneto pagalba stebėsena yra lengvesnė, nes yra informuojama apie problemų atsiradimo židinius greitai, savarankiškai ir laiku.
3. Darbo laiko taupymas ir verslo sąnaudų mažinimas. Daiktų interneto technologija taupo verslo organizacijos laiką bei pinigus, nes renka informaciją savarankiškai bei informuoja darbuotojus apie atsiradusias problemas.

Daiktų internetas yra naujas darinys, kuris padeda verslui įgyvendinti išsikeltus tikslus. Tačiau pabrėžtina, kad taikant versle naują technologiją privalu atsižvelgti į keletą veiksnių.
Pirmiausia, daiktų internetas reikalauja didesnių duomenų saugumo reikalavimų ir naujų dalijimosi informacija tarp verslo įmonių standartų.
Antra, unikalios verslo patirties perkėlimas į daiktų interneto terpę yra sudėtingas procesas, kuriam reikia daug laiko.
Trečia, daiktų internetas suteikia verslui galimybę valdyti didelį duomenų kiekį ir daiktų interneto technologijos diegimas į verslo procesus gali sukelti grėsmę unikaliems verslo duomenims.
Didelė daiktų internetas taikomas įvairiuose verslo sektoriuose ir jo teikiama nauda verslui yra
Didžiulėm nes skatina ekonominį efektyvumą. Daiktų interneto įtaka ekonomikai
didėja, kai verslas randa naujų daiktų interneto technologijų pritaikymui.

1.2.1 Daiktų interneto reikalavimai verslui

Daiktų internetas puikus įrankis verslui, kuris remdamasis naujausiomis technologijomis leidžia darbus atlikti greičiau, patogiau, taip pat padeda analizuoti verslo procesus, atlikti stebėseną. Pasaulinės tendencijos rodo, jog palaipsniui verslas ir daiktų internetas taps neatsiejami. Žinoma, kad šios išmaniosios paslaugos ir jų sudėtingumas kelia daiktų interneto technologijoms aukšto lygio reikalavimus (žr. 2 pav.) (Kraijak, 2015), (Raimundas Savukynas, Virginijus Marcinkevičius, 2017)



2 pav. Daiktų interneto reikalavimai verslui. Sudaryta autoriaus pagal Laimą Zalieckienę ir Raimundą Žilinską.

1. **Identifikuotas ryšys**: IoT turi užtikrinti objekto ir tinklo tarpusavio bendravimą, kuris paremtas IoT identifikatoriais, taip sukuriant jų tinklą ir tvarkyti juos vieninga sistema

2. **Autonominis aprūpinimas**: IoT įrenginiai turi perteikti taisyklėmis paremtas ir tinkamai sukonfigūruotas paslaugas, kurios priklauso nuo automatinės duomenų sistemos.

3. **Interoperabilumas**: IoT turi turėti galimybę apimti ir apdoroti iš skirtingų sistemų gautą informaciją ir pasalaugas

4. **Autonominis tinklas:** toks IoT tinklas, kuris turi turėti savarankišką tinklą, galintį veikti skirtingose aplinkose ir prisitaikyti prie didelio ir skirtingais įrenginiais paremto įrenginių tinklo.

5. **Vietos nustatymas**: IoT privalo naudoti vietos nustatymo funkciją, nes įrenginių veikimo galimybės ir principai priklauso nuo esamos vietovės.

6. **Saugumas**: Kiekvienas įrenginys prijungtas prie tinklo kelia grėsmę saugumui, todėl IoT užtikrinti apsaugą nuo kibernetinių grėsmių bei apsaugoti vartotojų duomenų vientisumą ir konfidencialumą.

7. **Kokybiškos ir saugios paslaugos**: IoT turi užtikrinti aukštą įrenginių darbo kokybę, nes jie dirba su žmonių psichologinėmis savybėmis ir elgsena išvedami statistinius rezultatus, padedančius teikti kokybiškas ir saugias paslaugas.

8. **Savaiminis diegimas**: IoT turi užtikrinti ir turėti savaiminio diegimo galimybes, kad įrenginiai galėtų tarpusavyje veikti turi turėti bendros programos palaikymą bei laikytis bendrų reikalavimų.

9. **Valdymas**: Siekiant užtikrinti kokybišką ir saugų IoT naudojimą turi būti nustatyti valdymo ir pavaldymo principai bei procesai nuolatos turi būti kontroliuojami, nes įrenginiai valdymo programų pagalba veikia automatiškai, todėl būtina veiklos priežiūra.

Tačiau vieną svarbiausių vis tiek turime išskirti saugumo reikalavimą, kuri įmonėms tampa vis sunkiau įgyvendinti, nes dideliems įrenginių kiekiams sujungiamumas ir identifikacija tampa nebe pagrindine problema, o jų sistemos saugumo užtikrinimas – svarbiausias ir daugiausiai problemų keliantis reikalavimas. (Madakam 2015).

1.3 Nauji iššūkiai kibernetiniam saugumui – daiktų interneto plėtra.

Analizuojant kibernetini saugumo bei daiktų interneto teorinius aspektus pastebima tendencija kad vis dar daugumoje straipsnių, specialistų įžvalgų daiktų internetas kaip silpnoji kibernetinio saugumo vieta neminimas ir nukeliamas kaip ateities vizija. Tačiau šiomis dienomis pažvelgus aplinkui tiek verslo įmonėse tiek jau privačiuose namuose galime pastebėti, kad įrenginių, kuriems reikalinga prieiga prie tinklo – apstu. Žinoma didžiausias kiekis daiktų interneto įrenginių yra technologiškai pirmaujančiose šalyse – JAV, Kinija, Japonija, tačiau šiuo metu esant puikioms logistinėms galimybėms, išmanieji daiktai nesunkiai pasiekia ir mažiau technologiškai išsivysčiusias šalis, kur kibernetinio saugumo politika yra silpna. Todėl šio darbo tikslas – pateikti konkrečių pavyzdžių, kurie įrodytų, jog visuomenė susitelkusi į kompiuterių sistemų saugumą per mažai skiria dėmesio ne ką mažiau pavojingiems daiktų interneto įrenginiams, kurių dėka gali būti pažeistos ir pačios kompiuterių sistemos. Žinoma, kaip ir kiekviena nauja technologija, taip ir daiktų internetas skirtas pagerinti gyvenimo ar darbo kokybę. Tačiau šiais technologijai sėkmingai pasiekus naudotojus pradėjo kilti naujos – saugumo problemos. Daiktų interneto įrenginiai pradėjo kelti nepasitikėjimą dėl privatumo pažeidimų, prieigos prie asmeninių duomenų ir jų netinkamo panaudojimo. Galima teigti, kad šiomis dienomis daiktų internetas tarpusavyje sieja ne tik įrenginius, bet jų pagalba pačius jų vartotojus. Todėl daiktų internetas, kaip technologija, kuri gali sujungti kompiuterines technologijas ir žmonių santykius, taps nauja visuomenės problema. Problemų priežastimis taps daiktų interneto pernelyg didelis nematomumas, nes prietaisai kuriami vis mažesni, o kompiuterinės technologijos tampa vis skaidresnės ir nepastebimos žmogui, todėl jas taps vis sunkiau kontroliuoti, o tams prireiks specialių sudėtingų priemonių. Įrenginių, objektų ir žmonių kiekis kasdien vis didėja, todėl sparčiai auga ir perduodamų ir fiksuojamų duomenų kiekiai, todėl jų suvaldyti ir kontroliuoti jų srautus tampa sunku, todėl užpuolikams juos perimti tampa lengviau ir dažnai tai pavyksta padaryti nepastebėtiems. Todėl galima daryti išvada šiuo metu vyraujanti ir ateityje augsianti daiktų interneto įrenginių problema – jų valdymas ir kontrolė. Taip pat manoma, kad padaugės autorinių teisių pažeidimų, didžiuliai duomenų perdavimo kiekiai įtakos e. paslaugų tiekimo kokybę. Todėl specialistai yra įpareigoti tobulėti ir adaptuotis prie esamos ir būsimos situacijos ir kurti naujus tyrimo metodus bei priemones skirtas kovoti su skaitmeniniais daiktų interneto nusikaltimais.

Pietų Korėjos Songdo miestas 2018 metais buvo pirmasis pasiskelbęs pilnai išmaniuoju miestu, nes visi jo objektai: automobiliai, apšvietimas, eismo kontrolė, stovėjimo aikštelės, pastatai ir net šiukšlių konteineriai yra sujungti į vieną tinklą. Šiam tikslui įgyvendinti svarbiausias komponentas – realaus laiko kompiuterinės sistemos. Tai mažo dydžio daiktų interneto jutikliai, kurie dedami įvairiuose daiktuose. Tokio pobūdžio jutikliai Lietuvoje tikrai nėra svetimi, kitaip tariant mūsų šalies

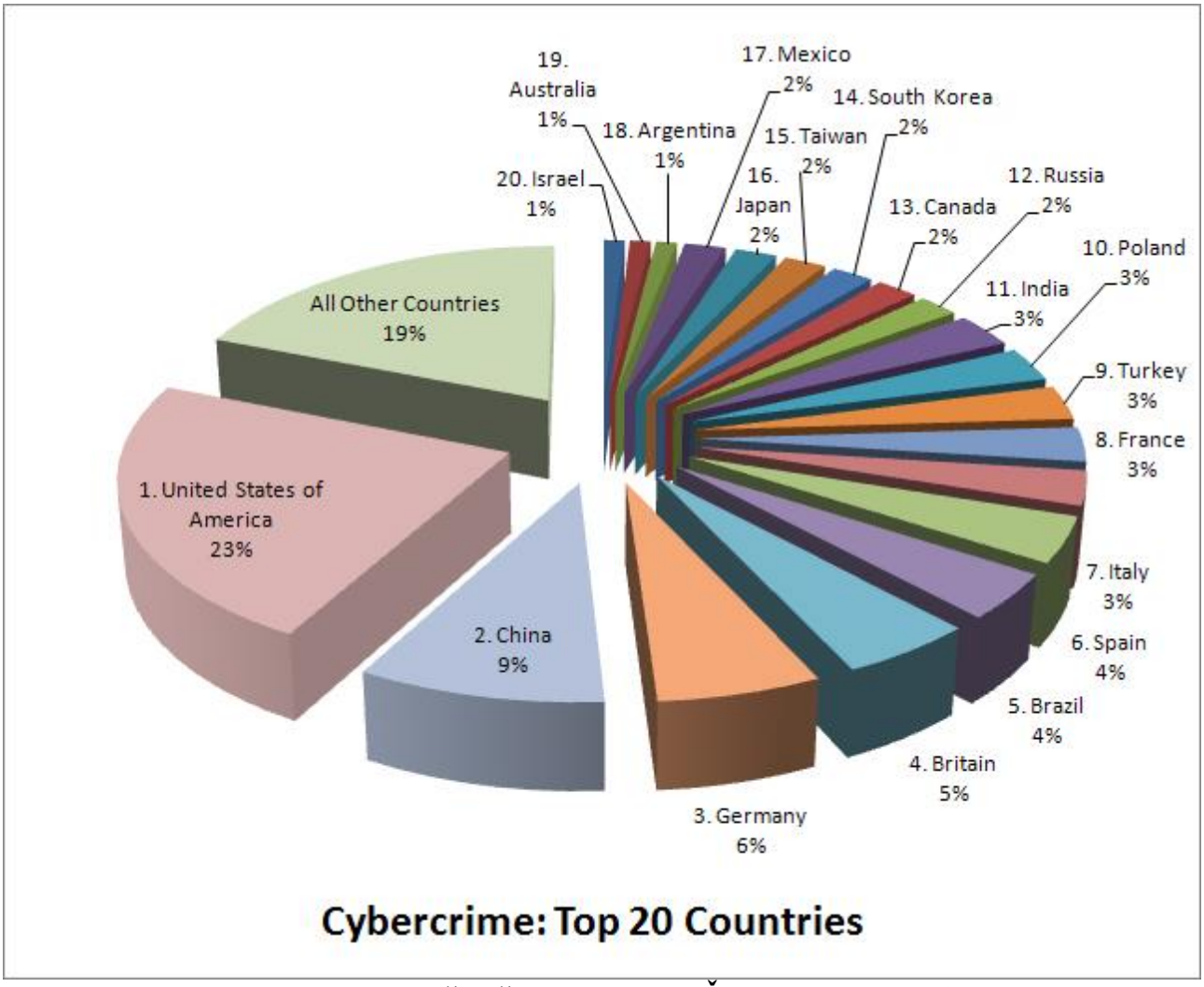
KTU mokslininkai patys juos kuria„ Norime iš tų daiktų vis daugiau funkcijų. Jie turi tarpusavy bendrauti. Kalbame ne tik apie daiktus, bet ir apie išmanią aplinką. Kaip jie bendrauja, teikia mums tam tikras paslaugas ir mes bendraujame su tų paslaugų tiekėjais aplinkoje“, – laidai „Mokslo ekspresas“ pasakojo KTU Realaus laiko kompiuterinių sistemų centro direktorius prof. Egidijus Kazanavičius. Mokslininkai pradėjo kurti nuo paprasčiausių namuose esančių išmaniųjų daiktų, žinoma, norint daiktams tarpusavyje rasti „bendrą kalbą“ reikia sukurti tinkamą tinklo architektūrą bei visus jungiančią bendrą sistemą. E. Kazanavičius taip pat pasidalino naujienomis, prie kurių šiuo metu dirba. Šiuo metu mokslininkai Lietuvoje yra sukūrę būsto aplinkos valdymo sistemą, kurios dėka tam tikri namų daiktai stebi žmogaus, kuris kartu su savimi turi jutiklį, būseną ir pagal ją pritaiko namų aplinką, šviesą, šilumą ir tt. KTU mokslininkai ir pats E. Kazanavičius pasaulyje yra garsūs dėl transporto sistemų kūrimo. Todėl būtent šiuo metu yra susitelkę į naujo transporto ir logistikos projekto tobulinimą. E. Kazanavičius teigia, kad labai svarbu žinoti apie eismo dalyvius kuo daugiau informacijos, apie jų elgseną, dalyvavimą, judėjimo sistemingumą. Nes kuriant logistikos internetą, labai svarbu buvimo vieta centimetrų tikslumu. Todėl šiuo metu mokslininkai stengiasi kurti centimetro tikslumu rodančias vietovės sistemas, nes kartais išvengti incidento pritrūksta kelių centimetrų tikslumo duomenų perdavimo procese. Taip pat E. Kazanavičius pabrėžia, kad nereikia vengti ir seniau jau sukurtų sistemų kaip – skaitmeninio radijo ryšio technologija. Kuri naudojama ne duomenims perduoti bet transliuoti radijo ryšiu svarbią informaciją vairuotojams, kas daugelyje Europos Sąjungos valstybių sėkmingai veikia.

Pastebima, kad Lietuvos mokslininkų šiuo metu pagrindinis tikslas – technologijų pagalba drausminti vairuotojus ir padėti jiems išvengti žmogiškų klaidų automobiliams bendraujant tarpusavyje o tai įgyvendinti padės daiktų internetas. Nes daiktų internetas – vienas pagrindinių 21a. naujovių. Daiktai esantys viename tinkle ne tik palengvina kasdieninę buitį, bet ir atveria naujas galimybes versle.“Huawei“ vadovas Baltijos šalyse Ricky Chen teigia, kad atsiradus 5G ryšiui, daiktų interneto plėtra patirs naują pagreičio bangą ir, kad jau 2021 metai benrą daiktų interneto tinklą sudarys 35,8 milijardo skirtingų įrenginių, o iki 2025 metų skaičiai padvigubės ir gali siekti 75 milijardus įrenginių. Todėl labai svarbus kuo greičiau reaguoti ir analizuoti naujus įrenginius ir kurti sistemas galinčias jas kontroliuoti ir apsaugoti nuo kibernetinių incidentų, nes tai padaryti daug sudėtingiau nei sukurti naują įrenginį.

2. DAIKTŲ INTERNETO ĮTAKA KIBERNETINIAM SAUGUMUI. PASAULINĖ ANALIZĖ

2.1 Naujų IoT įrenginių gausa pasaulyje – grėsmė kibernetiniam saugumui.

Analizuojant kibernetinio saugumo ir daiktų interneto plėtros statistinius žemėlapius kasmet susidaro tendencija, kad nusikaltimų ir naujų daiktų rūšių, kurie yra prijungti prie tinklo kiekis nenumaldomai auga. O kibernetiniai nusikaltėliai pasiekti savo tikslą vis dažniau renkasi daiktų interneto kelią. Šiais metais viena iš pirmųjų pateikė kibernetinių atakų statistiką šalyse „Enigmasoft“. Kurioje ryškiai matoma, kad JAV dominuoja šiame statistikos rodiklyje, kaip daugiausiai kibernetinių nusikaltimų patirianti šalis. Toliau rikiuojasi Kinija, kiek mažiau ir Europos šalys – Vokietija, Didžioji Britanija. (CompariTech, 2019) (žr. 3 pav.)



3 pav. Daugiausiai atakų patiriančios šalys pasaulyje. Šaltinis: įmonės „CompariTech“ tinklapis

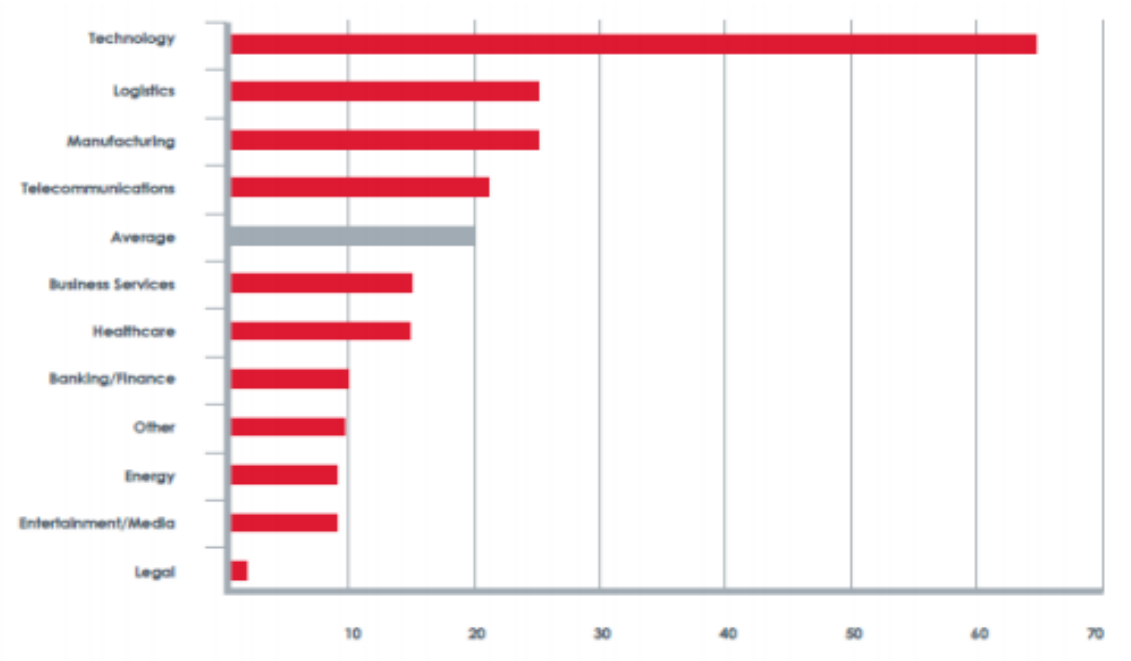
Išnagrinėjus statistikos diagramą, matoma tendencija, kad daugiausiai atakų patiria labiausiai technologiškai išsivystę šalys kaip JAV, Kinija, Vokietija. Nes daugiausiai daiktų interneto įrenginių pagaminanti šalis Kinija, daugiausiai jų parduoda JAV rinkai, tai ir patvirtina ši statistikos diagrama, kad kur daugiausiai nukeliauja daiktų prijungtų prie tinklo, ten daugiausiai kelių ir atsiveria kibernetiniams nusikaltėliams. Šią statistiką taip pat galima susieti ir su „CompariTech“ pateikta analize, kurioje išskirta šalys, kurioms kibernetiniai nusikaltimai daugiausiai kainuoja. (žr. 4 pav.)

And CompariTech has also prepared a list of countries which have the average cost of cyber crime in the world

United States-$17.36 million
Japan-$8.39million
Germany-$7.84 million
United Kingdom-$7.21 million
Brazil-$5.27million
Australia-$4.3 million

4 pav. Šalys kurioms kibernetinės atakos daugiausiai kainuoja. Šaltinis: įmonės „CompariTech“ tinklapis.

Matome, kad ir šioje grafoje viena statistika patvirtina kitą, kad JAV kaip daugiausiai patirianti kibernetinių nusikaltimų šalis, taip pat pirmauja ir statistinėje lentelėje kiek šalims kainuoja kibernetiniai nusikaltimai. Tačiau pastebimas ir dar vienas statistikos rodiklis, kad finansinėje statistikos lentelėje atsirado ir Japonija, kurios kaip daugiausiai patiriančios atakas nebuvo. Todėl galima daryti išvadą, kad Japonija kibernetiniams nusikaltimams ir jų prevencijai skiria daug finansų, nepaisant, kad atakų patiria mažiau nei kitos didžiosios šalys, kurie pasitvirtina ir atakų skaičių sumažina. Toliau rikiuojasi Vokietija, Didžioji Britanija - šalys, kurios taip pat pirmauja ir tarp daugiausiai patiriančių kibernetines atakas, todėl natūralu, kad nusikaltimai iš jų reikalauja daugiau finansų tiek nuostoliams atlyginti, tiek apsisaugoti. Taip pat verta paminėti, kad tarp daugiausiai lėšų skiriančių šalių nėra Kinijos, iš ko galime daryti išvadą, jog Kinija patiria daug atakų, bet mažesnio mąsto ir kurios neatneša tiek daug finansinių sunkumų.



5 pav. Daugiausiai kibernetinių atakų patiriantys sektoriai. Šaltinis „Fireeye“ tinklapis.

Išnagrinėjus kibernetinio saugumo ir daiktų interneto įtakos teorinę medžiagą, bei šių dienų pavyzdžius tapo aišku, kad įvairiems sektoriams diegiant naujas technologijas, kurios yra valdomos daiktų interneto prietaisų bei jutiklių pagalba, neišvengiamai didėja kibernetinių nusikaltimų grėsmė. Šios problemos tendenciją išanalizavo ir pavaizdavo kibernetinio saugumo organizacija „Fireeye“ ir informacija pateikė diagramoje (žr. 5 pav.) kurioje pavaizduota kurie sektoriai per valanda patiria daugiausiai atakų. Matome, kad daugiausiai atakų patiria tie sektoriai, kurie daugiausiai naudoja daiktų interneto jutiklių bei įrenginių, bei jais perduoda ir savo duomenų bazėse saugo daugybę asmens duomenų, kas kibernetiniams nusikaltėliams yra vienas iš pagrindinių nusikaltimo tikslų. Dažniausiai atakuojami – Technologinis, logistika, sveikatos priežiūra, gamyba, telekomunikacija. Nusikaltimų gausos pasekmė – daiktų interneto įrenginiai suteikia daugiau kelių įsilaužimams. Nusikaltėlių siekiamybė – asmens duomenys.

2.2 JAV pavyzdys

JAV galima vadinti kibernetinių atakų gimtine. Nes būtent čia buvo užfiksuotos pačios pirmosios kibernetinės atakos, jau 1988m. užkrato programa „Interneto kirminas“ sugadino 6000 interneto centrus. Žinoma, tuo metu dar nebuvo tiek daug vartotojų, todėl ataka masiškai nepaveikė vartotojų. Vykstant interneto revoliucijai masiškai pradėjo daugėti vartotojų, naujų įrenginių kas įtakojo nenumaldomą kibernetinio saugumo spragą. Nes jau 2014m. buvo užfiksuota 42,8mln. Kibernetinio saugumo pažeidimų, o po metų išaugo dvigubai – 84mln. Pažeidimų. Šiomis dienomis incidentų kiekis jau viršija 100mln. Per metus. (Forbes, 2020) Viena pagrindinių to priežasčių - sparti naujų įrenginių prijungtų prie tinklo plėtra, kuri kuria naujus kelius kibernetinėms atakoms, o juos apsaugoti darosi vis sunkiau, nes didelė dauguma jų yra tinkamai neparuošti apsisaugoti nuo kibernetinių incidentų. Gana ryškus to pavyzdys visai neseniai dar 2019m. įvykdyta „DDoS“ ataka prieš interneto srauto bendrovę „Dyn“, kuri buvo surengta per daiktų interneto įrenginius, tokius kaip skaitmeniniai vaizdo įrašymo įrenginiai, spausdintuvai ir kt. Ši ataka pridarė žalos ir užklupo nepasiruošusias tokias JAV ir viso pasaulio elektroninio verslo gigantes kaip „Amazon“, „Ebay“, „Netflix“, kas joms kelioms valandoms neleido prisijungti prie interneto tinklo nei vienam daiktų interneto įrenginiui ir atlikti jam priskirtų operacijų, kas per sąlyginiai atrodo trumpą laiko tarpą, padarė labai didelius finansinius nuostolius kompanijoms. (Deadline.com, 2017) Ataka puikiai parodo kokia yra didelė grėsmė, kuria sukelia prietaisai, kurie nėra tinkamai apsaugoti ir esantys tinkle. JAV suprasdama kibernetinių incidentų svarbą jau 2015m. įvertino kibernetinio saugumo rinką 9,5 milijardo JAV dolerių, kas yra didžiausia nevyriausybinės kibernetinio saugumo rinka. 2017m. JAV vyriausybės iniciatyva kibernetinio saugumo infrastruktūrai buvo skirta 19 milijardų JAV dolerių. Sritis, kuri yra išskiriama kaip didžiausią poveikį patirianti – sveikatos priežiūros sistemos. Bendras kibernetinių išpuolių poveikis ligoninėms ir kitoms sveikatos priežiūros įstaigoms kasmet siekia 6 milijardus JAV dolerių. Manoma, kad siekiant kovoti su šiomis milžiniškomis išlaidomis iki 2022m. kibernetinio saugumo rinka sveikatos priežiūros srityje viršys 10,85 milijardo JAV dolerių. (Forbes, 2019)

JAV pasaulio žemėlapyje išsiskiria ryškiai tarp lyderiaujančiųjų technologiniu pažangumu šalių. Taip pat rinkoje valdanti daugiausiai įrenginių kurie yra išmanieji ir prijungti prie interneto tinklo. Tačiau pažvelgus į kibernetinių atakų kiekį ir padaromus finansinius nuostolius ir kiek visa tai pareikalauja valstybės resursų JAV – pirmūnė. Dėl masinio įrenginių didėjimo, kurio nesustabdo kibernetinio saugumo reikalavimai situacija tampa nevaldoma. JAV kiekvienais metais skiria vis didesnę finansų dalį sumažinti šiai problemai, taip pat pradėjo taikyti tai ką moka geriausiai – kontražvalgybos metodą. JAV garsėja gera kontražavalgybos programa kovai prieš terorizmą, todėl

kibernetinėms atakoms skaičiumi ir nuostoliais aplenkus ir terorizmą imtasi šį metodą taikyti ir internetinėje erdvėje, kas statistikos duomenis jau atneša pirmuosius ir nemažus šios programos vaisus.

2.3 Kinija

Daugeliui žinoma, kad daugybė metų Kinija yra lyderė tarp daugiausiai elektroninių prietaisų pagaminančių valstybių pasaulyje. Tobulėjant tarptinkliniam ryšiui, visi elektronikos prietaisai tapo patogiau ir paprasčiau valdomi, nes atsirado galimybė juos sujungti ir valdyti tarpusavyje. Todėl šiomis dienomis didžioji dalis rinkoje pagamintų elektronikos prietaisų yra prijungti prie interneto tinklo arba kitaip – daiktų interneto. Kinija pasauliui siunčia daugybę išmaniųjų įrenginių, kurie yra nesaugūs taip sukeldami pavojus jų vartotojams. Tą patvirtina ir vienos didžiausių kibernetinio saugumo įmonių pasaulyje „McAfee“ atlikta šalių analizė, kuri tarp silpniausių galinčių atremti kibernetinius išpuolius šalių išskyrė Kinija, aplink kurią taip pat buvo paminėtos daug prasčiau technologiškai išsivystę šalys tokios kaip Meksika, Brazilija. Kas parodo, kad Kinija turinti daugybę technologinių galimybių gaminti įrenginius, labai mažai dėmesio skiria jų saugumo užtikrinimui. Tyrimą atlikę ekspertai teigia, kad didžiausia Kinijos kibernetinio saugumo problema yra vieningos strategijos neturėjimas. („McAfee“, 2019) Kinijos kibernetinio saugumo reagavimo komanda 2018m. pateikė daiktų interneto problemos atskaitą, kuri parodė, kad per metus lyginant su praėjusiais įrenginių pažeidžiamumas padidėjo 120 procentų arba kitaip tariant į per dieną yra pažeidžiama apie 27 000 išmaniųjų įrenginių. Pagrindine problema laikoma, kad maži bei vidutiniai gamintojai dėl konkurencijos ir vietos rinkoje teikia pirmenybę įrenginių įperkamumui ir tinkamumui, o ne jo saugumui. Tapo įprasta gaminti įrenginius, kurių net neįmanoma sutaisyti, o apsaugos slaptažodžiai yra paprasti ir primityvūs. Pasak ekspertų atlikusių tyrimą viename iš pramonės miestų Chongqing, kuris turi 30 mln. gyventojų 40 proc įrenginių esančių jame turi nesaugius gamintojo numatytuosius slaptažodžius. Kaip viena iš pagrindinių problemų taip pat galima išskirti, kad visi saugumo reikalavimai daugiau skirti nacionaliniai rinkai, o bendradarbiaujant su užsienio bendrovėmis propaguojamas nesąžiningas sąlygų pakeitimas, dėl geresnės abipusės verslo naudos. Tačiau sparčiai kovojanti su kibernetiniais nusikaltimais JAV, kuri su Kinija turi tarpusavio interneto tiekimo grandinę, šiuo metu bando įgyvendinti naują projektą Kinijoje pagamintų įrenginių saugumui užtikrinti, bendru susitarimu kelia naujas sąlygas bei saugumo reikalavimus daiktams prijungtiems prie tinklo ir pagamintiems Kinijoje. Pavyzdžiui, kaip sąlyga įsigyti tik atnaujintus ir patikrintus pagal paskutinius saugumo reikalavimus įrenginius. Taip pat pateikti kuo mažiau užkoduotų duomenų, programinės įrangos ir aparatinės įrangos komponentų. Taip Kinijos gamintojai bus priversti atsižvelgti į įrenginių saugumą, kad būtų įvykdyti JAV užsakymai, kurie sudaro didžiausią užsakymų rinką. Kaip pavyzdį galima išskirti jau šiemet nutikusį ir San Antonijaus

universitete ištirtą kibernetinį incidentą kai buvo įsilaužta per Kinijoje pirktą išmaniąją apšvietimo lemputę. Tyrimas parodė, kad įsilaužėliai pasinaudodami lemputės skleidžiamais infraraudonaisiais spinduliais sugebėjo juos taip modifikuoti, kad spindulių pagalba prisijungė prie kitų namuose esančių įrenginių prijungtų prie tinklo. Šis tyrimas tik dar kartą įrodo, kad nesvarbu koks daiktas yra prijungtas prie tinklo, jeigu jis yra netinkamai apsaugotas per jį atsiveria keliai į kitus, dažniausiai svarbesnius duomenis kaupiančius įrenginius. Todėl nesvarbu kokią svarbą ir funkcijas atlieka tas daiktas, bet jeigu jis yra prijungtas prie tinklo jis kelia tokia pat grėsmę, kaip ir kiti, galbūt svarbesnes funkcijas atliekantys daiktais.

Didžiųjų pasaulio pramonės šalių bendradarbiavimas vienas iš svarbiausių žingsnių, norint užkirsti kelią kibernetiniams incidentams.

2.3 Vokietija

Kita šiame darbe išskiriama valstybė, kuri garsėja aukšta technologijų, verslo kokybe bei procesus versle vykdo su daugybe daiktų interneto įrenginių yra Vokietija. Daiktų interneto galimybės yra neribotos ir tai puikiai įrodo Vokietijos verslininkai. Išmanioji automobilių stovėjimo aikštelė jau prieinama daugiau nei 50 Vokietijos miestų: naudodamiesi „Park and Joy“ vairuotojai gali lengvai rasti nemokamą stovėjimo vietą. Mokėjimas atliekamas naudojant programą „Deutsche Telekom“. Taip pat ši įmonė kartu su kita įmonę „IoT Venture“ sukūrė programėlę , kuri padeda savininkams surasti savo elektroninius dviračius. Pabrėžtina ir tai, kad dviračiai automatiškai „šaukiasi“ pagalbos registruodami dviratininko kritimą. (Telekom, 2020) Daiktų internetas taip pat pagerina priešgaisrinę saugą: „Lupus Electronics“ dūmų detektorius ne tik įspėja priešgaisrinę tarnybą ir nuomininkus, bet ir įspėja kitus nukentėjusio pastato gyventojus ir administraciją. Nuotolinė priežiūros funkcija taupo laiką ir išlaidas. Panašiai per daiktų internetą perduoda logistikos paslaugų teikėjo „Rhenus“ išmanioji duomenų saugykla. Šie intelektualūs konteineriai nustato savo užpildymo lygius ir jutiklio pagalba koordinuoja savo ištuštinimo ciklus.2019 m. Vokietijoje atlikus analizę paaiškėjo, kad nustatyta net 75 proc. kibernetinių kibernetinių incidentų, susijusių su duomenų vagystėmis, įmonių šnipinėjimu, sabotažu. Duomenų vagystės, pramoninis šnipinėjimas ir sabotažas per pastaruosius dvejus metus Vokietijos ekonomikai ir verslui padarė apie 205,7 milijardo eurų nuostolių. Skaitmeninės atakos paveikė septynias iš dešimties bendrovių. Taip pat statistika rodo, kad nusikaltėliams į pagalbą atėjo naujieji daiktų interneto įrenginiai, kurie naudojo silpnus slaptažodžius, kas leido sudaryti kelius į kitas tinkle esančias sistemas. Be to, 40 procentų visų verslo įmonių mato didelę rimtos žalos dėl elektroninių nusikaltimų riziką, kurios priežastimi paminėdami naujus daiktų interneto įrenginius. Pavyzdžiui, dar 2017 metais Vokietijos geležinkelių bendrovė patyrė kibernetinį incidentą, kuriuo pagalbininkas tapo išmanusis

traukinių srauto monitorius, kuris saugojo daugybė asmens duomenų kaip: kokie keleiviai šiuo metu turi vykti, kokie atvyksta ir panašiai, taip sutrikdydamas visą traukinių bei kelievių eismą, norint dirbti toliau ekranuose pasirodęs tekstas prašė išpirkos. Taip pat Vokietijoje garsėjanti „Winnti“ grupuotė naudojo kenksmingą programas IoT įrenginiams, kad gautų prieigą prie bendrovės informacijos. Tos pačios kenksmingos programos naudojimas buvo aptiktos dar mažiausiai trijose Vokietijos kompanijų skirtinguose įrenginiuose. Šie pavyzdžiai parodo, kad Vokietijoje nuo kibernetinių atakų kenčia labai didelės bendrovės, kurios naudoja daugybė daiktų interneto jutiklių, kurių apsaugos dėl didelio kiekio nespėja pasirūpinti. Taip pat pažymėtina, jog Vokietijoje yra numatoma, kad daiktų interneto (IoT) rinka prognozuojamu laikotarpiu 2020-2025 m. sparčiai augs dėl didėjančios išmaniųjų prietaisų, tokių kaip laikrodžiai, telefonai paklausos. Numatyta, jog kiekvienas Vokietijos vartotojas turės vidutiniškai 9,7 prijungtų prietaisų prie interneto. Remiantis tyrimais numatyta Vokietijos programa, kurioje yra pagrindiniai segmentai- verslo automatizavimas ir transportavimas. Tikimasi, kad paslaugų segmentas prognozuojamu laikotarpiu augs įspūdingai, nes vis daugiau organizacijų naudojasi prijungtais prietaisais. Kadangi daugelis verslo atstovų kenčia nuo kibernetinių atakų ir numatomas IoT rinkos dar didesnis augimas, Vokietija 2019m. pradėjo rengti naują kibernetinės gynybos strategiją. Strategijai būdinga daug aktyvesnė gynyba, nei buvo įprasta Vokietijoje, ir joje numatoma sunaikinti serverius, per kuriuos vykdomos kibernetinės atakos. Tai padarytų arba telekomunikacijų operatoriai, arba federalinė policijos valdžia. Šiuo metu didžioji dalis Vokietijos kompanijų imasi organizacinių, darbuotojų ir techninių saugumo priemonių, kad sumažintų išpuolių grėsmę. Be to, gamindamos prijungtus įrenginius prie tinklo, daugelis Vokietijos kompanijų laikosi principo „pagal dizainą sauga“. Taigi jie klientams teikia atsparesnius kibernetinėms atakoms produktus ir paslaugas. 2018 m. Atliktas „Bitkom“ tyrimas nurodė, kokias priemones Vokietijos pramonės įmonės naudoja apsisaugodamos nuo kibernetinių išpuolių. Vokietijoje bendrovės skatinamos užšifruoti savo el. pašto srautus, vykdyti saugumo sertifikatus. Tokios priemonės svarbios, nes darbuotojai vis dar kelia didžiausią grėsmę įmonės kibernetiniam atsparumui - pvz. paspaudę sukčiavimo elektroniniuose laiškuose esančias nuorodas, todėl Vokietijoje beveik 60 procentų visų įmonių veda mokymus darbuotojams saugumo klausimais. Vokietija išties daug pastangų deda kovojant su kibernetiniu saugumu. (Bitkom, 2018). 2012 m. Įkurtas kibernetinio saugumo aljansas (Allianz für Cybersicherheit) yra sėkmingas valstybinių ir nevalstybinių (verslo) dalyvių bendradarbiavimo kūrimo pavyzdys. Kibernetinio saugumo aljansas savo nariams siūlo naujausią informaciją apie IT saugumo situaciją, įvairius žinių ir geriausios patirties mainų renginius, taip pat platų konsultavimo ir palaikymo paslaugų spektrą. Prie iniciatyvos jau prisijungė keli tūkstančiai įmonių ir institucijų, tokių kaip Vokietijos pramonės federacija (BDI) - ir jų skaičius auga. Siekdami dar glaudesnio pramonės ir politikos bendradarbiavimo, BDI ir Federalinė vidaus reikalų ministerija kartu paskelbė projektą „Bündnis für Cybersicherheit“ 2018 m. stiprindami mainus tarptautinėmis kibernetinio saugumo temomis. Apibendrinant galima teigti, kad Vokietija yra viena daugiausiai

dėmesio skirianti ES valstybė būtent verslo sektoriaus daiktų interneto įrenginiams, kurie pastaruoju metu sukelia daug problemų, visai Vokietijos verslo pramonės sektoriui.

2.4 Lietuva

Kaip ir kiekvienoje valstybėje taip ir Lietuvoje yra svarbus kibernetinis saugumas. Kiekvienais metais Lietuvoje įsteigtos įmonės bei fiziniai asmenys patiria kibernetines atakas. Lietuva kovai su kibernetinėmis atakomis pirmiausiai pasitelkė teisės aktus. 2015m. Lietuva įtvirtino Kibernetinio saugumo įstatymą. Kibernetinio saugumo įstatyme įvardijami šie kibernetinio saugumo principai:

1) kibernetinės erdvės nediskriminavimo principas, kuris reiškia, jog teisės aktų nuostatos yra taikomos, ir gėriai yra saugomi vienodai tiek ir kibernetinėje tiek ir fizinėje erdvėje;

2) kibernetinio saugumo rizikos valdymo principas, kuris reiškia, kad taikomos kibernetinio saugumo priemonės privalo užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;

3) kibernetinio saugumo proporcingumo principas reiškia, kad taikomos techninės, organizacinės ir teisinės kibernetinio saugumo priemonės negali apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai privalomai būtina;

4) viešojo intereso viršenybės principas reiškia, kad viešojo intereso apsauga yra užtikrinama tada, kai jos nepažeidžia atskirų vartotojų teisių ar neproporcingai neapriboja jų laisvės kibernetinėje erdvėje;

5) standartizacijos ir technologinio neutralumo principas kuris reiškia, kad kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės tais atvejais, kai jie įgyvendina kibernetinio saugumo priemones;

6) subsidiarumo principas kuris reiškia, kad valdantys savo sistemas kibernetinio saugumo subjektai yra atsakingi už ryšių bei informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą. Tose srityse, kurios priklauso išimtinei kibernetinio saugumo subjektų kompetencijai, valstybinės institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

Kibernetinio saugumo įstatyme numatytos privalomos gairės padeda įmonės ir fiziniams asmenims suvokti kas yra kibernetinis saugumas, kokios yra teisės ir pareigos ir atsakomybė už kibernetinius pažeidimus.

2019m. liepos 3 d. Vyriausybė patvirtinto Nacionalinės kibernetinio saugumo strategijos įgyvendinimo 2019–2021 m. tarpinstitucinį veiklos planą, kuriame išskyrė konkrečias priemonės kovai su kibernetinėmis atakomis ir paskyrė atsakingas Lietuvos institucijas ir įstaigas kibernetinėje srityje.

Pagrindinės veiklos plano priemonės yra susijusios su nusikalstamų veikų elektroninėje erdvėje mažinimu, informacinės visuomenės plėtra , energetikos sektoriaus kibernetinio saugumo stiprinimu, mokslinės veiklos finansavimu, inovacijų diegimu finansinių technologijų sektoriuje ir kt. Svarbu pabrėžti tai, kad ketinama vystyti kibernetinės gynybos pajėgumus – įsteigti Regioninio kibernetinio saugumo centrą, kuris gyvuotų Kaune ir modernias ankstyvojo kibernetinių grėsmių aptikimo ir užkardymo sistemas. Taip pat planuose numatyta kibernetinės gynybos priemonėmis aprūpinti neseniai Lietuvos kariuomenėje įkurtą Ryšių ir informacinių sistemų batalioną. Valstybinės įmonės, kurios bus įtrauktos įgyvendinant strategijos veiklos planą ir veiks pagal savo kompetenciją yra- Vyriausybės kanceliarija, Vidaus reikalų, Krašto apsaugos ,Švietimo, mokslo ir sporto, Ekonomikos ir inovacijų, Užsienio reikalų ir Teisingumo ministerijos, Nacionalinis kibernetinio saugumo centras, Policijos departamentas, kitos Lietuvos valstybės ir savivaldybių institucijos, įstaigos ir organizacijos.

2018 metais patvirtinta Nacionaline kibernetinio saugumo strategija siekiama ekonominės ir socialinės gerovės, todėl didelis dėmesys skiriamas sustiprinti valstybės kibernetinį atsparumą, užtikrinti, kad efektyviai būtų reaguojama į kibernetinio saugumo incidentus, numatyti jų prevencijos priemones ir išteklius. Tai numatoma įgyvendinti bendradarbiaujant viešajam ir privačiam sektoriui, mokslo ir švietimo institucijoms tarpusavyje ir su užsienio valstybių ir tarptautinių organizacijų kompetentingomis institucijomis ir mūsų visuomenei.

Nacionalinės kibernetinio saugumo strategijos veiklos plano įgyvendinimas prisideda prie kryptingos Lietuvos kibernetinio saugumo plėtros, 17-osios Vyriausybės programos ir Europos Sąjungos Tinklų ir informacinių sistemų saugumo (TIS) direktyvos įgyvendinimo. Lietuvoje per artimiausius metus bus kuriamos geresnės sąlygos juridiniams asmenims ir visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis, sklandžiai ir veiksmingai bei laiku susekti kibernetinius išpuolius, plėtoti mokslo, technologijų bei naujovių vystymąsi.

Kibernetinis saugumo įstatymas ir jame įvardinti principai, Nacionalinė kibernetinio saugumo strategija ir numatyti jos tikslai įrodo, kad Lietuvoje į kibernetnį saugumą per teisinę prizmę yra žiūrima labai rimtai. Dar vienas teisinis žingsnis ir nemažas iššūkis Lietuvai tapo Bendrasis duomenų apsaugos reglamentas. Vienas didžiausių iššūkių bendrovėms šiuo metu yra duomenų apsauga. Lietuvoje yra ne viena įmonė, kuri nesugebėjo apsaugoti savo klientų ar partnerių duomenų ir dėl to patyrė didelių tiesioginių ir netiesioginių nuostolių. Pavyzdžiui- Grožio chirurgija, tv3 ir Gemus. Bendrovė Gemus teigė, kad, kai įvyko kibernetinis incidentas duomenys, esantys serveriuose, nebuvo pavogti nei pakeisti. Tačiau neatmetė galimybės, kad kibernetiniai įsilaužėliai gavo prieigą prie užšifruotų klientų slaptažodžių. Vienu naujausiu daiktų interneto pavyzdžiu pasidalino įmonės „Telia“ saugumo ekspertas

Giedrius Maškauskas: šiuo metu internete plinta vienas pavojingiausių ginklų per visą istoriją pavadinimu „Reaper“, tai interneto robotų „Botnet“ tinklas jungiantis šimtus tūkstančių išmaniųjų daiktų interneto įrenginių, iš kurių renkamai labai dideli kiekiai duomenų, šie srautai neaplenkė ir Lietuvos, „Telia“ pastebėjus tai viešina šią problemą ir skatina susirūpinti ypatingai verslo subjektams imtis rimtesnės išmaniųjų įrenginių apsaugos ir neprarasti savo duomenų. Šie pavyzdžiai parodo, jog yra labai svarbi duomenų apsauga. Manoma, kad tai jau įvykusios 2017m. „Mirai“ pobūdžio atakos atmaina. Ši ataka apėmė daiktų interneto įrenginius, kurie turėjo numatytuosius prisijungimo duomenis, kuo pasinaudojo užpuolikai ir sukūrė modifikacijas, kurios leido įsilaužti į vaizdo stebėjimo kameras, sensorius, išmaniąsias verslo valdymo sistemas. Rezultate tai pasiekė ir ne vieną užsienio kapitalo verslo įmonę Lietuvoje. („Telia.lt“, 2019m.)

Europos Sąjungos Bendrasis duomenų apsaugos reglamentas įsigaliojo 2018 m. gegužės 25 d. Šis reglamentas tapo esmine asmens duomenų apsaugos reforma, kuri palietė visas įmones, duomenų tvarkytojus ir valdytojus. Pagrindinis principas ir šio reglamento reguliavimo esmė atsispindi pirmame skirsnyje*: „Atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos“ (BDAR, 1 skirsnis, 24 str.).*

Reglamentas gana stipriai pakeitė iki tol laiko buvusį reguliavimą duomenų apsaugos srityje. Vieni svarbiausių pokyčių yra susiję su griežtesniais reikalavimais. Sugriežtinta tvarka sutikimams, leidžiantiems tvarkyti duomenis, atskaitomybės principo įvedimu, teisės į duomenų perkėlimą sukūrimu. Taip pat įtvirtintas privalomas pranešimas apie duomenų saugumo pažeidimus, pranešimais apie duomenų tvarkymą ir kt. Kaip ir minėta šiuo reglamentu sugriežtinama duomenų tvarkymo tikslo apibrėžtis. Pagrindinis principas yra toks ,kad subjektai norėdami naudoti asmeninius, tarkime konkretaus darbuotojo duomenis, privalo pateikti svarius argumentus, kam tai reikalinga ir kodėl tai yra būtina. Taip pat reglamentas asmenims numato naują teisę nesutikti su automatizuotu sprendimų priėmimu, o visgi esant automatizuotam duomenų tvarkymui, būtinas pranešimas apie tokio tvarkymo loginį pagrindimą ir galimas pasekmes. Atkreiptinas dėmesys į naujas priemones, kurios taikomos duomenų saugumo užtikrinimui. Dauguma bendrovių privalo paskirti duomenų apsaugos pareigūną bei užtikrinti tinkamų išteklių skyrimą jo darbui. Sekantis minėtas pasikeitimas – asmens duomenų valdytojo atskaitomybės principas. Šis principas reikalauja, kad duomenų valdytojas būtų proaktyvus ir ne tik užtikrintų numatyto reglamento reikalavimų laikymąsi, bet ir gebėtų tai įrodyti. Būtent šis principas sukėlė nemažą naštą įmonėms, kurios tvarko asmens duomenis. Kaip atsvarą minėtam sunkumui galima išskirti informavimo visuomenei naudingumą, Kadangi visuomenė tampa vis geriau

informuota apie savo asmens duomenų saugumą, mažėja pakantumas pažeidimams. Vis daugiau žmonių kreipiasi į Valstybinę duomenų apsaugos inspekciją su skundais. 2018 metais inspekcija gavo net 859 skundų dėl galimo duomenų apsaugos pažeidimo ir 619 iš jų buvo išnagrinėti. Pirmasis inspekcijos nubaudimas siekė 61 500 eurus. Šią baudą gavo įmonė, kuri veikė tarptautiniu mastu ir teikė mokėjimo paslaugas Lietuvos bei užsienio gyventojams. Šis atvejis yra pamoka ir kitoms bendrovėms, kurios atmestinai sutvarkė dokumentus ir reglamento reikalavimus įgyvendino tik formaliai. Neužtenka tik formaliai bendrovės viduje nusistatyti teorinę asmens duomenų tvarkymo tvarką, bet ir būtina gebėti tinkamai pritaikyti kasdienėje veikloje.

Taigi, visi šie teisiniai dokumentai parodo, jog Lietuvos valstybė su kibernetinėmis atakomis kovoti ir duomenų apsaugai dėmesio skirti pirmiausiai pasitelkė teisines priemones. Tačiau vien tik teisinių aktų priėmimo ir strategijų kūrimo kibernetinėje srityje neužtenka. 2018 m. Nacionalinis kibernetinio saugumo centras užregistravo 53 183 kibernetinius incidentus (atakas) . Nacionalinis kibernetinio saugumo centras nurodė, kad palyginus su 2017 m. kibernetiniai nusikaltimai tapo daug labiau pažangesniais ir dar sunkiau aptinkamais. Iki 21% išaugo pažeidžiamų interneto įrenginių skaičius.

Statistikos departamento atliktas „Informacinių technologijų naudojimas įmonėse 2019 m. tyrimas parodė, jog smulkiojo ir vidutinio verslo bendrovės yra daug mažiau pasiruošusios atremti kibernetines atakas. Vidutiniškai smulkios įmonės (10-49 darbuotojai), 36 proc. mažiau nei didelės įmonės (250+ darbuotojai) naudojo bent vieną kibernetinio saugumo / e. saugos priemonę.

Taigi, tokie duomenys parodo, jog Lietuvoje reikia atsižvelgti ne tik į teisinius dokumentus, bet ir į kitus aspektus, kad būtų gerinama situacija kibernetinėje srityje.

Vienas iš pasiūlymų yra didinti kibernetinio saugumo brandą. Mano nuomone tai yra vienas iš geriausių būdų išvengti kibernetinių incidentų. Taigi, yra svarbu skatinti viešojo bei mažo ir vidutinio privataus sektorių atstovus tikrintis kibernetinio saugumo būklę, taisyti kibernetinio saugumo spragas. Numatytoje strategijoje įsipareigojama kurti priemones, skirtas privataus sektorių (mažų bei vidutinių) verslo atstovų kibernetinio saugumo būklei gerinti. Pagrindinis siekis, kad 2021 m. būtų bent keturios, o 2023 m. bent šešios tokios priemonės.

„Samsung“ atliko apklausą kuri parodė, jog 30 proc. respondentų, patyrusių kibernetines atakas nežinojo, kaip įsilaužėliai pasiekė jų asmeninius duomenis, o netgi daugiau nei 60 proc. nenutuokė, kokių veiksmų imtis, jei įsilaužta į jų paskyras ar įrenginius. Lietuvos kibernetinio saugumo strategijoje išskirta, jog nuo kibernetinių incidentų negalima apsisaugoti net ir taikant visas esamas technines kibernetinio saugumo priemones. Dėl to be galo yra svarbu, kad privataus sektorių atstovai rūpintųsi savo darbuotojų kibernetinės kultūros kėlimu. Pabrėžtina, jog verslo subjektai dažniausiai

neįvertina žalos, kurią patirtų dėl kibernetinio incidento, nelaiko interneto svetainių, kaip svarbaus informacinio turto, reikalingo jų veiklai, taip pat neįvertina to, kad kai kurios interneto svetainėse yra saugomi asmens duomenys.

Tam, kad didėtų kibernetinio saugumo branda svarbu stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą. Šių sektorių bendradarbiavimo įgyvendinimui užtikrinti naudojamas Kibernetinio saugumo informacinis tinklas. Šiame tinke galima dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir tinklo narių bendradarbiavimą kibernetinio saugumo srityje. Įdiegus priemones, užtikrinančias efektyvų tinklo narių bendravimą bus puiki galimybė išvengti kibernetinių incidentų.

Atsižvelgiant į situaciją Lietuvoje, mūsų valstybė turi puikius teisinius instrumentus kovoti su kibernetiniais incidentais. Tačiau vien tik įstatymų ir kitų teisės aktų mažinti kibernetiniam incidentų skaičiui nepakanka todėl svarbu yra skatinti viešojo ir privataus sektoriaus subjektus bendradarbiauti tarpusavyje ir nenuvertinti kibernetinių grėsmių pavojaus. Tobulinant įmonių vidinius saugiklius tiek duomenų apsaugos srityje tiek ir kibernetinio saugumo srityje bus pasiektas tikslas išvengti didesnių kibernetinių incidentų pasekmių.

2.6 Pasirinktų šalių apibendrinimas, išvados

Šiame darbe buvo pasirinktos trys šalys susijusios su kibernetinio saugumo problemomis:

1. JAV – viena iš lyderiaujančių pasaulyje išmaniųjų technologijų srityje. Šiame darbe ši valstybė išskiriama ir todėl, kad joje užfiksuotos pačios pirmosios daiktų interneto kibernetinės atakos. Šiuo metu kibernetinių incidentų JAV įvyksta daugiau nei šimtą milijonų kartų per metus ir apima įvairias sritis- nuo sveikatos priežiūros institucijų iki didžiausių pasaulyje verslo kompanijų, kurios sparčiai diegia naująsias daiktų interneto technologijas ir palengvinti darbams naudoja milijonus, dažniausiai iš Kinijos tiekėjų, įsigytus daiktų interneto įrenginius. Problema kibernetinio saugumo srityje yra tokia, kad didėja masiniai įrenginiai, kurie neatitinka saugumo reikalavimų. Pagirtina, kad JAV kiekvienais metais skiria didelę finansų dalį sumažinti šiai problemai. Taip pat, JAV šiuo metu didelį dėmesį skiria kontražavalgybos programai, kuri yra skirta kovoti prieš kibernetinį terorizmą.
2. Kinija- viena daugiausiai elektroninių prietaisų pagaminančių valstybių pasaulyje, kuri kelia grėsmę kibernetiniam saugumui. Kadangi Kinijos verslas turi daugybę technologinių galimybių gaminti stambiu mastu išmaniuosius įrenginius, todėl ji labai mažai dėmesio skiria jų saugumo

užtikrinimui. Pagrindinės problemos taip pat išskirtinos tos, kad Kinija neturi vieningos kibernetinio saugumo užtikrinimo strategijos, taip pat maži bei vidutiniai gamintojai dėl konkurencijos ir vietos rinkoje teikia pirmenybę įrenginių įperkamumui ir tinkamumui, o ne jų saugumui. Kadangi ši problema paliečia ir kitas valstybes, JAV ištiesė pagalbos ranką ir šios šalys sudarė tarpusavio interneto tiekimo grandinę. Didžiųjų pasaulio pramonės šalių bendradarbiavimas vienas iš svarbiausių žingsnių, norint užkirsti kelią kibernetiniams nusikaltimams.

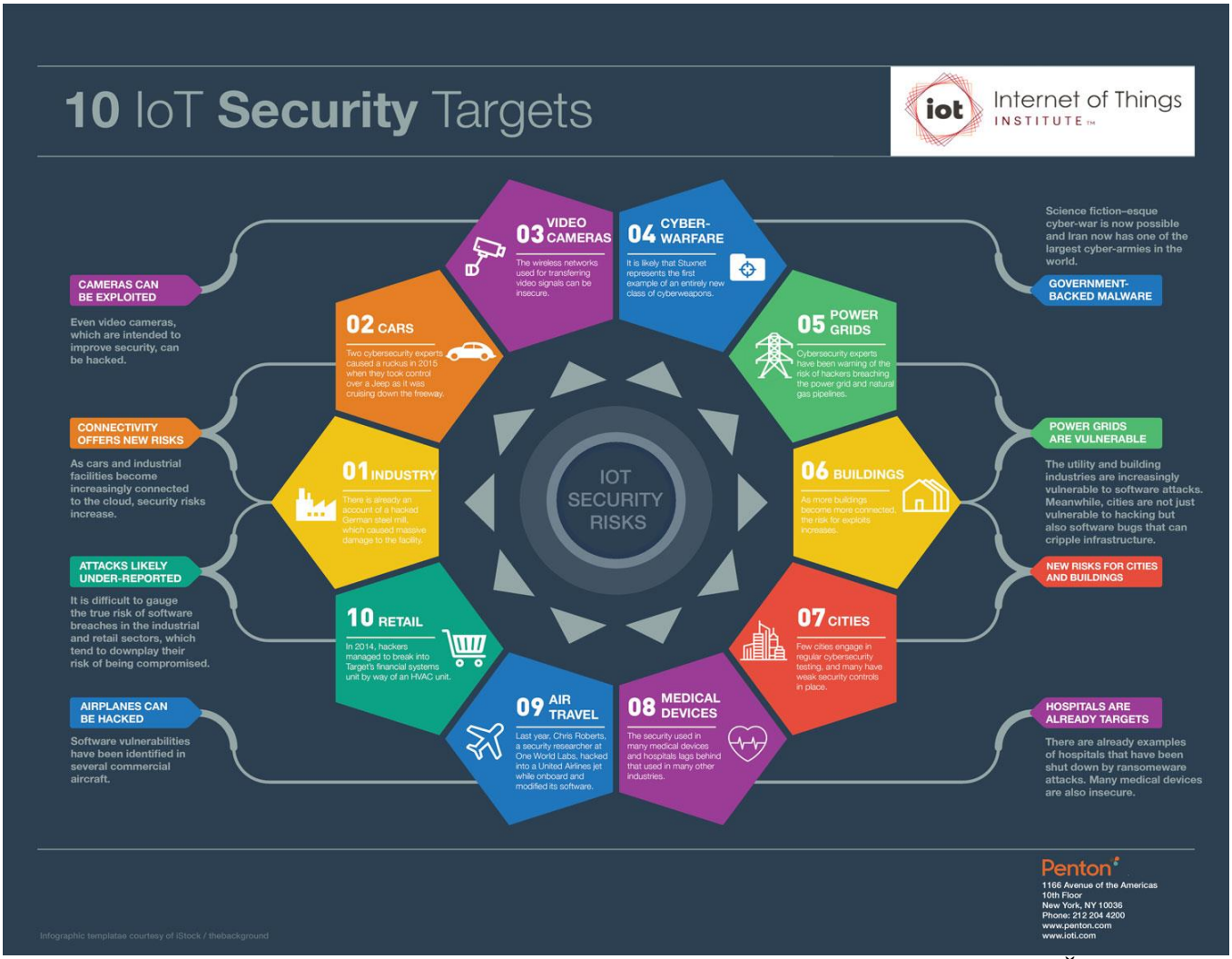
3. Vokietija. Ši valstybė buvo pasirinkta, dėl išskirtinio dėmesio daiktų internetui pramoninio verslo sektoriuje. Vokietija garsėja savo puikiai išvystyta pramone ir yra viena daugiausiai turinčių stiprių ir sėkmingų verslo įmonių šalis. Didžiųjų įmonių milžiniškus duomenų srautus reguliuoja – daiktų interneto prietaisai. Kuriems sparčiai daugėjant, buvo pastebėta, kad verslo sektorius dažnai patiria kibernetines atakas, kurios trikdo įrenginių darbą, bei įmonės patiria pastovius nuostolius dėl to. Todėl Vokietija išskirtinai daug dėmesio šiuo metu skiria daiktų interneto prietaisų reikalavimams ir matydama įrenginių augimą, kuria naujus įstatymus bei reikalavimus verslo saugumui užtikrinti, diegiant daiktų internetą. Taip pat šalyje norima galutinai sunaikinti visus serverius per kuriuos vyksta kibernetinės atakos ir juos pakeisti į naujus, sukurtus pagal griežtesnius saugumo reikalavimus ir saugesnius naudoti daiktų interneto prietaisus.

4. Lietuva. Ši valstybė pasirinkta todėl, kad mums yra aktualiausias kibernetinis saugumas artimoje aplinkoje. Palyginus su kitomis valstybėmis, Lietuvoje kibernetinių atakų yra mažiau, tačiau jų grėsmė su kiekviena diena didėja ir pavyzdžiai rodo, kad daiktų interneto integracija versle iššaukia naujus kibernetinius incidentus, nes šiuo metu Lietuvoje įskūrę nemažai užsienio kapitalo verslo subjektų, kurie plačiai naudoja daiktų interneto įrenginius operacijoms vykdyti. Lietuvos valstybė su kibernetinėmis atakomis pirmiausiai pasitelkė teisines priemones. Teisės aktai yra teigiama priemonė kovoti su kibernetiniais incidentais, tačiau to neužtenka. Lietuvoje visuomenės supratimas, kad tai yra pavojinga jų asmeniniams duomenims yra nepakankamas. Todėl svarbu skatinti viešojo ir privataus sektoriaus subjektus – bendrovių vadovus bei darbuotojus šviestis kibernetinėje srityje, bendradarbiauti tarpusavyje ir nenuvertinti kibernetinių grėsmių pavojaus.

3. DAIKTŲ INTERNETO SAUGUMO PROBLEMOS, SPRENDIMO BŪDAI.

3.1 Pažeidžiamiausios daiktų interneto naudotojų sritys.

Šiomis dienomis daugelis įmonių net neįsivaizduoja savo darbo dienos be daiktų interneto įrenginių pagalbos, didžioji dalis jų nutrūkus interneto ryšiui net negali tęsti savo darbų. Arba galima tik įsivaizduoti kokia sumaištis kiltų jei kibernetiniai nusikaltėliai įsilaužtų į šalies elektros tiekimo įrenginius ir paliktų visus žmones be elektros tiekimo. Praėjusiais metais į šia situaciją pasigilino ir analizę pateikė Lloyds „Bussines Blackout“, kurioje teigiama, jog JAV elektros tinklu gręsia „stuxnet“ stiliaus ataka, kuri gali padaryti žalos už trilijoną JAV dolerių! Taigi, tai dar kartą parodo kaip yra svarbu saugoti išmaniuosius įrenginius nuo kibernetinių nusikaltėlių. Todėl remiantis IoT (daiktų interneto) instituto „Penton“ atlikta analize bus apžvelgtos dešimt populiariausių tarp kibernetinių nusikaltėlių paplitusių daiktų internetą naudojančių sričių. (IoTWorldToday, 2019) (žr. 6 pav.)



6 pav. 10 dažniausiai patiriančių daiktų interneto kibernetinius išpuolius sričių. Šaltinis: „Penton“ tinklapis

1. Pramoniniai įrenginiai.

Vienas iš pavyzdžų Vokietijos plieno gamykla. Nusikaltėliams naudojant „phishing“ ir socialinės inžinerijos sukčiavimo metodus buvo įsilaužta į gamyklos biurų tinklą, iš kur gavo prieigą prie gamybos sistemos ir perėmė gamykloje esančius pramoninės kontrolė komponentus. Kas objektui padarė ypatingai didelę žalą. Pasak Marina Krotofilo iš Hamburgo technologijos universiteto, sunku sužinoti kaip yra nulaužiamos gamyklos dėl turto prievartavimo, nes apie tokius išpuolius pranešama retai, dažniausiai gamyklos neviešina tokių incidentų ir stengiasi susitvarkyti viduje.

Šioje srityje savo tinklus turime eksploatuoti taip, tarsi kasdien patirtume išpuolius. Sukčiavimo ir socialinės inžinerijos išpuoliai taip greitai neišnyks , pasak Thomas Pore, „Plixer“ IT pasaulgų direktoriaus, komercinės patalpos kaip ir kiekviena organizacija turi mokyti vartotojus atpažinti sukčiavimo išpuolius ir kaip išvengti socialinės inžinerijos išpuolių. Kaip pavyzdžiui nespaudinėti ant kiekvieno gauto el. laiško, reklamų ir panašiai. Mokymai turėtų būti periodiniai, o ne vienkartiniai renginiai, taip pat juose turi aktyviai dalyvauti darbuotojai, jiems turi būti pateikta konkretūs atpažinimo pavyzdžiai. Taip pat turi įmonėse veikti įrenginių apribojimo politika, autentifikavimas ir privilegijos turi būti sukonfigūruotos didėjimo tvarka, siekiant užkirsti kelią į svarbius išteklius įvykus incidentui. („Plixer“, 2019)

2. Automobiliai

Šiuo metu naujausi duomenys rodo, kad automobilių fizinės vagystes parengtos kompiuteriais ir „keyless go“ beraktėmis sistemomis prijungus užpuoliko kompiuterį su automobilyje esančiu, tačiau daugėja automobilių su visiškai pilnu prijungimu ir valdymu tinkle, kas sukuria dar naujų kelių kibernetiniams nusikaltėliams. 2015m. Du kibernetinio saugumo ekspertai kartu su kaskadininkų komanda „Wired“ atliko kibernetinio išpuolio eksperimentą, kaip automobiliui „Jeep“ važiuojant greitkeliu buvo perimtas visiškas jo valdymas, kai vairuotojas nieko negalėjo padaryti, pamatęs kad automobilis visiškai „neklauso“ jo komandų. Išpuolis parodė atakų pavojaus svarbą ir galią, kas įmonę paskatino sustabdyti 1,4 milijono transporto priemonių gamybą. Kita automobilių gamintojų kompanija „Fiat – Chrysler“ netgi paskelbė aukcioną kibernetinio saugumo specialistams, kuriems radus ir pranešus apie saugumo spragas esančias automobiliuose skiriama iki 1500 JAV dolerių premija. Žinoma, atsiradus naujoms technologijoms programišiai ėmė tyrinėti esamų sistemų pažeidžiamuma, vienas tokių – Troy Huntas, kuris visai neseniai automobilio „Nissan Leaf“ bateriją ištuštino, naudodamas tiesiog automobilio identifikavimo (VIN) numerį ir pasiekdamas klimato kontrolės sistemą, žinoma tai nėra pavojinga gyvybei ar sveikatai, tačiau tai puikus pavyzdys kaip panaudojant šiek tiek šoninio mąstymo viena automobilio dalis gali būti panaudojama patekti į kitą,

kas žinoma gali sukelti ir pavojingų padarinių, jei nusikaltėliai ras kelių į svarbesnes automobilio sistemas kaip stabdžiai ar vairavimo mechanizmas, ką grįžtant prie „Jeep“ pavyzdžio jau išbandė kaskadininkai greitkelyje.

Taigi, saugumo ekspertas Thomas Pore „Plixer“ IT direktorius apžvelgęs ir išnagrinėjęs pavyzdžius pateikia ne itin malonią ateities vizija apie automobilius kaip daiktus prijungtus prie tinklo. Kad padėtis darosi vis prastesnė, nes daugelis inžinierių, kurių užduotis yra kurti ir projektuoti sistemas, nėra tinklo ir protokolų ekspertai ir mažai išmanantys jų saugumą. Jie puikiai žino kaip išdėlioti komponentus, tačiau TCP / IP protokolų saugus įgyvendinimas reikalauja šios srities specialistų plataus derinimo bei testavimo. Kas kuria ne kokias prognozes naujiesiems automobiliams, nes netgi pakankamai gerai sukonfigūruotas programinis kodas, nereiškia visiškos apsaugos, nes kas šiandien atrodo saugu, rytoj gali būti panaudotas kaip spraga įsilaužti ir sugadinti sistemą. O jau minėtos 1500 JAV dolerių premijos už rastas saugumo spragas tikrai nevilioja rimtų specialistų dėmesio ieškant sistemos pažeidžiamumų.

3. Vaizdo stebėjimas

Vaizdo kameros visada asocijuojasi su saugumo užtikrinimu vienoje ar kitoje mūsų aplinkoje. Tačiau pažvelgus iš kitos pusės turime pripažinti, kad tai dar vienas daiktas prijungtas prie tinklo, kas daro jį nesaugiu, o kartais mums patiems pavojingu įrankiu.

Įžvalgomis apie vaizdo stebėjimo kameras dalijasi „PRPL“ fondo vyriausiasis direktorius Cesare Garlati, kuris teigia, kad kameros atveria naujas galimybes kuriant robotinius tinklus, kad būtų galima siųsti į sistemas šlamštą, išpirkos programas, paleisti DDoS atakas ir panašiai. Todėl vaizdo stebėjimo įrenginių saugumas turi būti kuriamas jau lusto kūrimo stadijoje, norint išvengti pasekmių vėliau, ypač jei išpuolis nukreiptas į kritinę infrastruktūrą, nes kameros visada bus vienas iš pagrindinių įsilaužėlių taikinių, nes jos fiksuodamos vaizdą kuria potencialiai jautrų turinį. Taip pat ekspertas nustatė, kad dažniausiai į vaizdo stebėjimo tinklą įsilaužiama dėl pardavėjo diegimo klaidų, dažnai įrenginiai net neturi atnaujinimo galimybių. (Cesare Garlati, 2018)

4. Kibernetinis atakos kariniame kontekste

Mokslininkai iki šių dienų vis dar nagrinėja vienas pavojingiausių „Stuxnet“ kirmino atakas kurios yra nukreiptos į kritinę infrastruktūrą. Pirmą kartą ši ataka buvo aptikta prieš 6 metus Irane, kai buvo sunaikinta penktadalis branduolinių įrenginių, manoma, kad šis kenkėjas buvo sukurtas JAV ir Izraelio kibernetinių nusikaltėlių. „Stuxnet“ veikimo principas leidžia perimtii programuojamus loginius valdiklius (PLCs) ir priežiūros kontrolės bei duomenų kaupimo (SCADA) sistemas.

Manoma, kad „Stuxnet“ yra pirmasis kibernetinių ginklų pavyzdys. Jo gimtine laikomas Iranas, nes jame pirmą kartą buvo sučiupti 7 kibernetiniai nusikaltėliai kūrę ginklą prieš didžiausią naftos kompaniją Saudo Arabijoje, anksčiau šiems iraniečiams buvo pateikti kaltinimai dėl atakų prieš JAV bankus bei užtvankos darbo sustrigdymo Niujorke. „In a Black Hat“ 2015m. pristatyme tyrėjai Runa Sandvik ir Michaelas Augeris teigė ir pristatė radę kelią į išmaniąją snaiperių taikymo programą „ShotView“. Nors šio karinio produkto kūrėjai iš dalies paneigė tai , tyrėjai vis tiek įrodė, kad galbūt visiško ginklo valdymo perimti nepavyko, tačiau naudojantis Wi – Fi ryšiu ir programinės įrangos pažeidžiamumu sugebėjo pakenkti ginklui pakeisdami jo taikinį. Žinoma iki didelės nelaimės saugiklis išliko, nes ginklui šaudyti vis tiek reikėjo fizinio paspaudimo., tačiau vis tiek buvo įrodyta, kad net kariniame sektoriuje daiktų internetas ir jo saugumas kelia naujus reikalavimus. (Runa Sandvik ir Michaelas Augeris, 2015)

5. Elektros tinklai ir komunalinės paslaugos

Tai viena jautriausių šakų, kalbant apie incidento mąstą, nes žvelgiant nacionaliniu lygmeniu šalyse elektros tiekimas ir komunalinės paslaugos priklauso vienam tiekėjui, todėl sutrikdžius įrenginių darbą be elektros ar kitų paslaugų gali likti visi šalis ar miestas. 2016m. Sausio mėnesį Ukrainos elektros tiekimo infrastuktūra patyrė kibernetinę ataką, kurios metu buvo sutrikdyta 30 iš 135 pastočių veikla. Dėl šios atakos Ukraina įtaria bei kaltina Rusijos kibernetinius nusikaltėlius. Taip pat JAV įsilaužėlių komanda „RedTeam“ pademonstravo kaip per kelias dienas įsilaužtį į energetikos įmonę. Šie pavyzdžiai tik rodo kokia svarbi yra šių infrastruktūrų sauga. Ir kad iki šiol buvę darbų sutrikdymai dėl voverių ar graužikų žalos yra tik maža dalis, ką gali padaryti kibernetiniai incidentai. („Penton“, 2018)

6. Pastatai

Statybos pramonė taip pat sėkmingai naudojasi skaitmeninėmis technologijomis. Pastatai sėkmingai automatizuojami, kas padeda juos patogiai valdyti, matyti iškilusias problemas sistemoje. Tačiau žinoma kaip ir kitose daiktų internetą naudojančiose srityse, taip ir šioje pastatų sujungiamumo problema tampa saugumas. Jau 2013m. pirmieji „Google“ pastebėjo, kad į jų „Wharf 7“ biurą Australijoje buvo įsilaužta ir perimta pastato valdymo sistema. Vienas iš įsilaužėlių Billy Riosas „BBC“ televizijoje sakė, kad pastatų sistemos buvo lengvai pažeidžiamos bei sugadinamos. Taip pat paminėjo, kad jo skaičiavimais kad pasaulyje yra apie 50 tūkstančių tokių sujungtų sistemų iš kurių 2000 neturi net menkiausios apsaugos tokios kaip slaptažodžiai. Kas leidžia be didesnio vargo valdyti pastatų šildymo/aušinimo sistemas ar net prijungtas durų spynas, nes verslo sektorius per mažai dėmesio skiria savo biurų apsaugai nuo daiktų interneto išpuolių.

7. Miesto infrastruktūra

Daiktų interneto laboratorijos „IOActive LAB“ vadovas Cezaris Cerrudo paskelbė, kad daugeliui miestų gresia kibernetiniai išpuoliai, netgi tiems, kurie savęs nelaiko „Smart cities“. Didžioji dalis viso pasaulio miestų naudoja tam tikras jungties technologijas, kad valdytų nuo eismo srauto daviklių, apšvietimo iki viešojo transporto judėjimo. Visgi tik nedaugelis iš jų vykdo kibernetinio saugumo bandymus, o daugelyje iš jų saugumo kontrolė silpna. Tačiau tam kad kiltų problemas, ne visada turi būti vykdoma kibernetinė ataka. Programinės įrangos klaidos taip pat gali sukelti rimtų problemų. Pavyzdžiui, 2013m. Lapkričio 22d. San Francisko įlankos greitojo tranzito sistema (BART) buvo laikinai sustabdyta dėl programinės įrangos trikdžių, kas lėmė 500 iš 1000 keleivių kelionių sustabdymą. Taip pat daiktų interneto kibernetinio saugumo įmonės vadovas Cesare Garlati pastebėjo, kad vienas didžiausių miestų transporto infrastruktūros milžinas „Transporto f London“ ieško naujų daiktų interneto jutiklių, kurie pagerintų priemiesčių spūstis, tačiau jie neturi pamiršti didesnio saugumo ir privatumo poveikio, kurį miestas turės įsivedęs naujus įrenginius. Nes gamintojams skubant pateikti į rinką naujus daiktų interneto įrenginius dažnai saugumas paliekamas antrame plane.

8. Medicinos įrenginiai ir ligoninės

Daugelyje medicinos prietaisų ir ligoninių saugumas atsilieka nuo kitų pramonės šalių. Paprastai medicinos prietaisuose slaptažodžiai yra nekeičiami ir primityvūs gamykliniai. Taip pat medicinos darbuotojai į kibernetinį saugumą per daug nesigilina ir papildomiems mokymas neskiria savo laiko ir kaip praktika rodo dėl to dažnai nukenčia. Gydymo įstaigos yra puikus taikinys nusikaltėliams reikalaujantis išpirkų, nes jos saugo daugybę asmens duomenų. Žinoma, sveikatos priežiūra yra viena iš labiausiai reikalaujančių naujų daiktų interneto jutiklių, kurie prisidėtų nuo efektyvesnės pacientų priežiūros. Tačiau saugumo spragos šioje srityje ypač riboja naujų įrenginių įvedimą. Pavyzdžiui jau 2015m. JAV maisto ir vaistų administracija įspėjo ligonines nesinaudoti populiaria internetine vaistų infuzijos pompa, po to kai Billy Rios tyrimai parodė, kad ją galima nulaužti nuotoliniu būdu ir reguliuoti vaistų dozes. Tokie išpuoliai gali lemti žmogaus gyvybę, todėl tokie įsilaužimai vadinami mirtinais ginklais. Šio įrenginio gamintojas „Hospira Symbiq“ teigia, kad vykdomas nuolatinis sistemos atnaujinimas ir bus išleista nauja versija leidžianti saugiai naudotis sistema. Tačiau žinant kibernetinių nusikaltėlių įgūdžius naujos sistemos spragų suradimas ir panaudojimas gali ilgai neužtrukti.

9. Lėktuvai

Saugumo tyrinėtojas iš „One World Labs“ Chrisas Robertsas pasiskelbė, kad sugebėjo įsilaužti į „United Airlines“ lėktuvą ir modifikavo lėktuvo traukos kodą esantį valdymo kompiuteryje. FTB

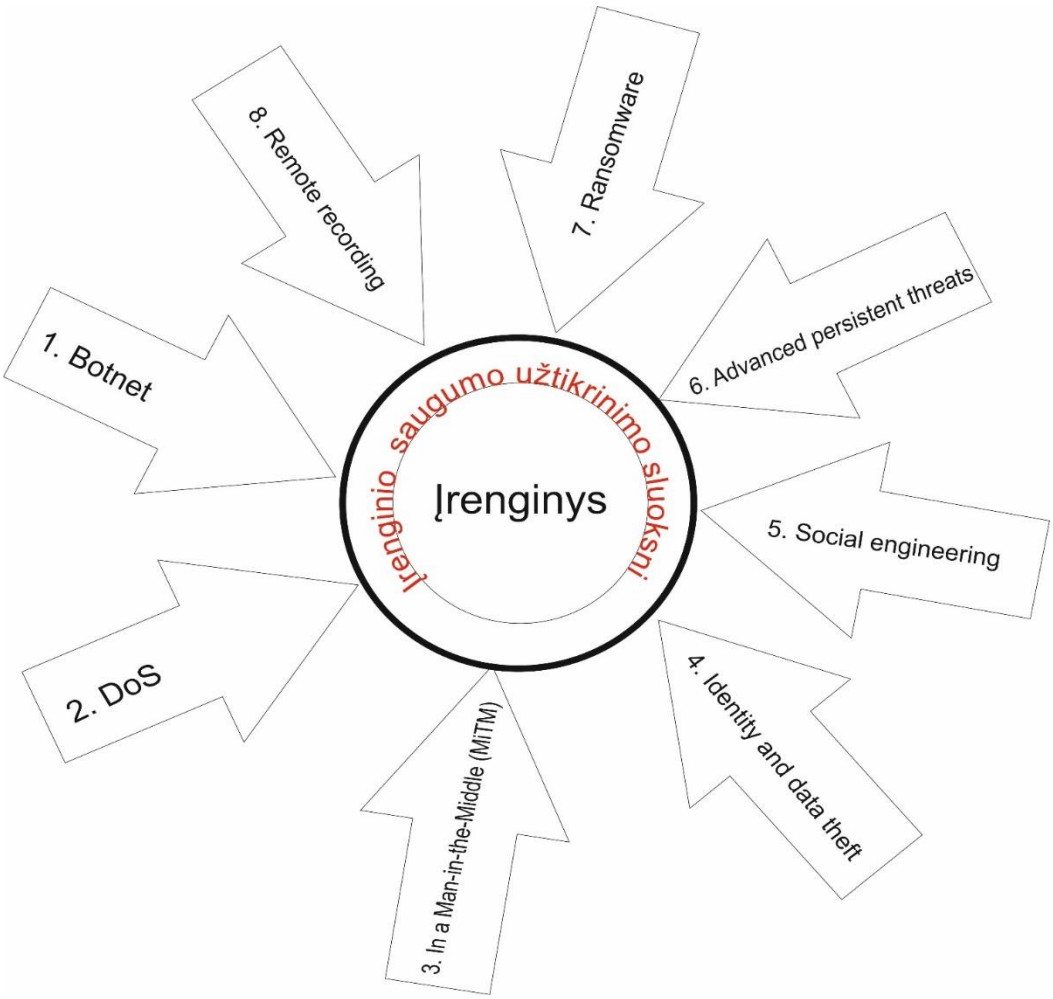
kratos orderyje teigiama, kad Robertsui pavyko įsakyti lėktuvui kilti, bei keisti kursą. Atlikus tyrimus paaiškėjo, kad Robertso kalbos pasitvirtino, lėktuvo valdymo kompiuteris buvo iš tikro pažeistas, taip pat tokio pobūdžio kompiuteriai yra naudojami daugelyje populiariausių orlaivių. Saugumo specialistas Garlati taip pat išanalizavo šį incidentą ir pateikė savo išvadą, kad lėktuve yra labai daug jutiklių pradedant navigacija ir baigiant salono temperatūra, kurie yra tarpusavyje sujungti, todėl neaišku per kurį iš jų buvo rastas kelias ir iki sistemoje esančio traukos valdymo kompiuterio, kas leido pakeisti lėktuvo judėjimo kryptį. Lėktuvų gamyboje dalyvauja tik atrinkti ir geriausi inžinieriai, kurie turi viską apgalvoti milimetrų tikslumu, kas leidžia sukurti patikimus lėktuvus, tačiau kaip rodo praktika incidentų vis daugėja, todėl prie stiprios inžinierių komandos kuriant lėktuvą, turi prisijungti tokie pat patikrinti ir stiprūs kibernetinio saugumo inžinerijos sprendimų specialistai, kurie sukurtų saugią kompiuterių struktūrą lėktuve.(OneWorldLabs, 2019m.)

10. Mažmeninės parduotuvės ir duomenų bazės.

Mažmeniniai prekiautojai ir smulkieji verslai palaipsniui tampa kibernetinių nusikaltėlių traukos objektais, nes savo duomenų bazėse kaupia didelius kiekius finansinių duomenų. O atsiradus daiktų interneto prietaisams ir jutikliams gaunamų duomenų kiekis tik dar labiau padidėjo. Apie šią sritį nuomonę pateikė dar vienas saugumo specialistas Pore, kuris pastebėjo, kad jeigu organizacijos dės tik į perimetrą nukreiptus įrankius, kad išvengtų grėsmės, jos greičiausiai taps kita auka. Svarbu, kad be tradicinių technologijų, tokių kaip ugniasienės, IDS, IPS ir antivirusinės, reikia įgyvendinti pagrindinio turto apsaugą naudojant analizę. Tai gali būti įgyvendinta naudojant tinklo elgseną su indikatorių koreliacija, kad būtų galima nustatyti grėsmes ir nepageidaujamą elgesį, Turtą stebėti ir profiliuoti.

3.2 IoT įrenginių pažeidžiamumo tipai ir atakų galimybės

Įdiegus daiktų internetą įvairioms pramonės šakoms, padidėjo produktyvumas, efektyvumas darbo vietų kokybė. Daiktų internetas paplito ligoninėse, miestų infrastruktūrose, kurių kasdieninė veikla ir darbas tapo priklausomas nuo tinkle veikiančių jutiklių. Žinoma, kaip ir minėta anksčiau taip sparčiai augant daiktų interneto galimybėms didžiausia problema ne jų sujungiamumas o saugumo problemos. Todėl svarbu analizuoti ir mokytis iš kitų klaidų bei pavyzdžių. IT specialistų jungtinė organizacija „Allerin“ išanalizavo daiktų interneto įrenginius pažeidžiančias atakas ir atrinko 8 dažniausiai naudojamus būdus pažeisti daiktų interneto įrenginius. (Allerin tinklapis, 2019m.) (zr. 7pav.)



7 pav. Daiktų interneto įrenginių atakų tipai. Sudarytas autoriaus pagal įmonės „Allerin“ kibernetinio saugumo specialistų įžvalgas.

1. Botnet robotai

„Botnet“ – tinklas jungiantis įvairias sistemas, kad nuotoliniu būdu būtų galima valdyti aukos sistemą ir platinti kenkėjiškas programas. Kibernetiniai nusikaltėliai kontroliuoja robotų tinlus naudodami "Command-and-Control-Server“, kad pasisavintų konfidencialius duomenis, gautų bankininkystės duomenis ir vykdytų įvairaus pobūdžio tokias kaip DDos ar „phishing“. Kibernetiniai nusikaltėliai naudoja robotinius tinklus, kad galėtų užpulti daiktų interneto įrenginius, kurie yra sujungti su kitais įrenginiais tokiai kaip nešiojamamieji ir stacionarūs kompiuteriai ar išmanieji telefonai. Kokio pavojingumo tai ataka parodė „Mirai“ robotas kuris užkrėtė 2,5 mln įrenginių, įskaitant maršrutizatorius spausdintuvus ir išmaniąsias kameras. Užpuolikai naudojo robotų tinklą, kad paleistų paskirstytus paslaugų atsisakymo išpuolius keliuose daiktų interneto įrenginiuose. (Allerin tinklapis, 2019m.)

2. Denial of service (Paslaugų neigimo (DoS) ataka.

Paslaugų neigimo (DoS) ataka sąmoningai bando sukelti pajėgumų perkrovą tikslinėje sistemoje, siųsdama kelias užklausas. Skirtingai nuo kitų išpuolių, šios atakos nesiekia pavogti svarbių duomenų. DoS atakos naudojamos norint sulėtinti ar išjungti paslaugą, kad pakenktų verslui. Pavyzdžiui, oro linijų bendrovė patyrusi tokio tipo ataką, turimų duomenų nepraranda, tačiau sutrikdomas daiktų interneto įrenginių darbas, todėl sutrinka tokios operacijos kaip, bilietų būsenos tikrinimas, atšaukimas ar rezervavimas. Todėl tokios atakos gali sugadinti įmonių reputacija, paveikti pajamas.

3. In a Man in the Middle (MiTM) (Bendravimo perėmimas)

Tai toks atakų būdas kaip užpuolikas pažeidžia ryšio kanalą tarp dviejų atskirų kanalų bandydamas perimti jų siunčiamas žinutes. Užuolikams perėmus bednravimo kontrolę jie gali siųsti neteisėtas žinutes dalyvaujančioms sistemoms. Tokie išpuoliai dažniausiai naudojami tokiems daiktų interneto įrenginiams kaip išmanieji šaldytuvai ir autonominės transporto priemonės. Taip pat MiTM ataka gali būti naudojama norint atakuoti kelis daiktų interneto įrenginius, kurie dalijasi duomenimis realiuoju laiku taip perimdami kelių daiktų interneto prietaisų ryšius. Pavyzdžiui užpuolikas gali valdyti išmaniuosius namų aksesuarus tokius kaip lemputes ir kiti išmanieji daiktai namuose, kas atrodo ne itin pavojinga tačiau tokiu pačiu principu gali įsilaužti į pramonės ar medicinos įrangą, kur tokie įsilaužimai gali būti kritiškai pavojingi įmonių vientisumui ar net žmonių gyvybei (kalbant apie mediciną). (Allerin tinklapis, 2019m.)

4. Identity and data theft (Asmens tapatybės ir duomeų vagystės)

Dėl daugybės duomenų pažeidimų buvo pakenkta milijonams žmonių. Buvo pavogtos konfidencialios informacijos, kaip asmens duomenys, kredito ir debeto kortelių informacija, el. pašto adresai. Užpuolikams dabar daiktų internetas atvėrė naujas galimybes ir kelius, kaip išmanieji laikrodžiai, išmanieji namų ir biuro įrenginiai gauti informacijai apie vartotojus ir organizacijas. Surinkę tokius duomenis užpuolikai toliau gali vykdyti sudėtingesnes ir detalesnes tapatybės vagystes. Taip pat jie ieško silpniausių organizacijoje esančių daiktų interneto jutiklių per kuriuos galėtų patekti į verslo sistemos tinklą. Patekus į tokias sistemas, toliau atsiveria galimybės patekti ir į kitas įmones esančias bendrose verslo sistemose. (Allerin tinklapis, 2019m.)

5. Social engineering (Socialinė inžinerija)

Šiomis dienomis socialinės inžinerijos metodas vis plačiau naudojamas, nes kaip rodo statistika, jis yra vienas iš efektyviausių būdų išvilioti svarbius banko duomenis, slaptažodžius ar konfidencialią informaciją. Paprastai tai yra įtikinimai el. laiškai. Tačiau esant daiktų interneto prietaisams šis procesas palengvinamas užpuolikams atlikti savo darbą. Tinkliniai interneto įrenginiai, ypač nešiojamieji, renka didelius kiekius asmenį identifikuojančios informacijos (PII), kad vartotojams būtų sukurta asmeniniams poreikiams pritaikyta informacija, paslaugos. Todėl kibernetiniai nusikaltėliai gali pasiekti PII duomenų bazę per tam tikrą įrenginį ir gauti konfidencialią informaciją apie gyvenamąją vietą, pirkimo istorijas, banko informaciją. Todėl tai leidžia surengti pažangų socialinės inžinerijos išpuolį, kuris gali būti nukreiptas prieš patį vartotoją ar jo šeimą, draugus pasitelkiant jo nesaugius daiktus prijungtus prie tinklo.

6. Advanced persistent threats (APTs) (Pažangios nuolatinės grėsmės)

Šio tipo atakos kelia susirūpinimą įvairioms, daugiau didesnio mąsto organizacijoms. Pažangi nuolatinės grėsmės kibernetinė ataka – tikslinė ataka, kai įsibrovėlis įgyja nelegalią prieigą prie tinklo ir ilgą laiką lieka nepastebėtas. Užpuolikai siekia stebėti tinklo veiklą ir palaipsiui pasisavinti svarbius duomenis. Tokioms atakos svarbu užkirsti kelią ar jas išvis aptikti, nes daiktų interneto įrenginių dideliais kiekiais kasdien perduoda svarbius duomenis, todėl kibernetiniai nusikaltėliai būtent juos pasirenka pradinės prieigos taškais prie svarbių asmeninių ar įmonės tinklų. (Allerin tinklapis, 2019m.)

7. „Ransomware“ atakos

„Ransomware“ atakos tapo vienos žinomiausių ir daugiausiai nuostolių padarančiomis kibernetinėmis atakomis šiomis dienomis. Šios atakos principas – naudoti kenkėjišką programą ir priverstinai užšifruoti duomenis, kurie reikalingi organizacijoms atlikti tam tikras verslo operacijas. Tokios atakos reikalauja išpirkos mainais į duomenų grąžinimą (iššifravimą). Daiktų interneto įrenginiams tai labai pavojingą ataka, ypač tiems, kurie gali įtakoti vartotojo sveikatą ar net gyvybę.

Pavyzdžiui, buvo surengta „Ransomware“ išpirkos ataką prie išmaniuosius termostatus, kurių pagalba įmonėje buvo smarkiai užkelta temperatūra, o norint sugražinti ją į normalią, organizacijai reikia susimokėti išpirką. Tai pat tokie išpuoliai pavojingi išmaniuosius užraktus turintiems pastatams, kur įvykdžius tokio tipo ataką vartotojas nesumokėjęs išpirkos negalėtų ten patekti. (Allerin tinklapis, 2019m.)

8. Remote recording (Nuotolinis įrašymas)

Šis atakos tipas išnaudoja programinės įrangos versijos pažeidžiamumą – zero-day. Tokios atakos nutaikytos į įrenginius, kurie turi balso ar vaizdo įrašymo galimybes. Tai gali būti pokalbių įrašinėjimas arba, pavyzdžiui, labai dažnas atvejis įsilaužti į išmaniąją vaizdo stebėjimo sistemą, kur įrašinėjama kasdieninė verslo veikla, taip įgyjant konfidencialią verslo informaciją. Nuo šių zero-day atakų galima apsisaugoti vykdant pastovią tinklo įrenginių analizę bei vykdyti planuotus ir nuoseklius programinės įrangos atnaujinimo darbus.

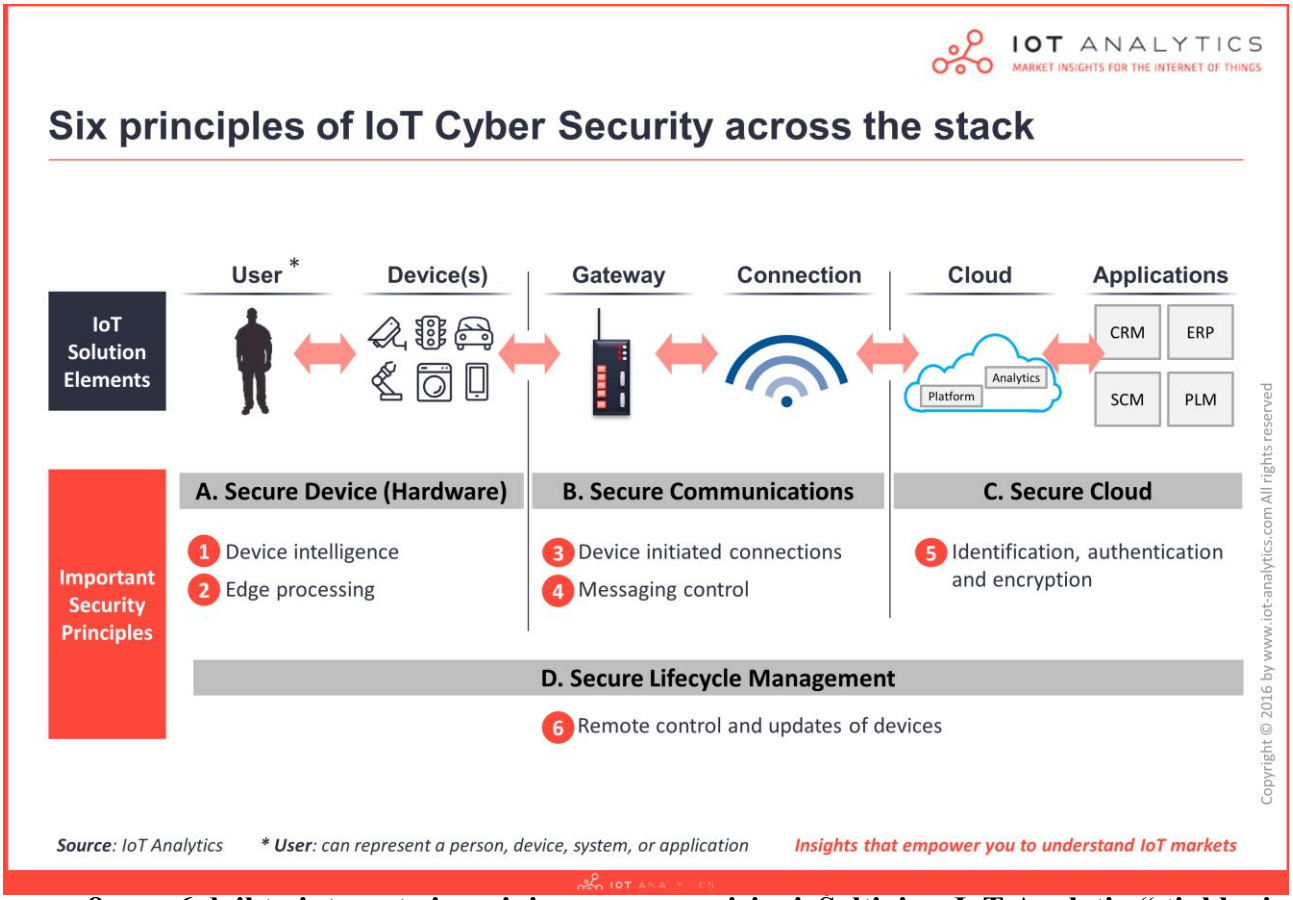
Taigi, išanalizavus IT specialistų iš jungtinės organizacijos „Allerin“ pateiktus pavojingiausius ir dažniausiai naudojamus atakų tipus prieš daiktų interneto įrenginius, galima teigti, kad šuo metu, esant daugybei daiktų interneto įrenginių ir daviklių tiek verslo tiek privačiame sektoriuose, kibernetinių atakų skaičius smarkiai išaugo, nes atsirado daugiau galimybių patekti netgi į tokias sistemas, kurių saugumas atrodė tvirtas ir sunkiai pažeidžiamas, bet vienas nesaugus įrenginys ar jutiklis, gali atverti į tą sistemą kelią kibernetiniams nusikaltėliams, o galimybių ir kelių kaip parodė analizė yra apstu. (Allerin tinklapis, 2019m.)

3.3 Daiktų interneto įrenginių saugumo architektūra

Tūkstančiai naujos kartos įrenginių internete, prekybos centruose ir kitose pardavimo vietose vilioja pirkėjus savo naujomis galimybėmis, kurios palengvina kasdieninius darbus, už mus padaro nemėgstamus ar mūsų laisvalaikiui suteikia įdomesnių spalvų. Žinoma tokiems išmaniems daiktams norint atlikti visas funkcijas reikalingas interneto ryšys, kas ir lemia naujas saugumo problemas. Pagrindinė sparčiai daugėjančių išmaniųjų įrenginių saugumo spraga yra silpna IoT (ang. Internet of Things) daiktų interneto saugumo architektūra. Su šia problema nusprendė susitvarkyti viena iš nedaugelio įsikūrusi daiktų interneto saugumo kompanijų „Ardexa“. Išnagrinėję JAV daiktų interneto rinką buvo pastebėta, kad dėl netinkamos daiktų saugumo architektūros principų naujus kelius kibernetiniams incidentams atvėrė apie 150tūkst. daiktų interneto įrenginių. Todėl buvo sukurtas 6

principų modelis, kuris apjungia svarbias IoT saugos architektūros funkcijas keturiuose skirtinguose sluoksniuose (IoT Analytic, 2019) (žr. 8 pav.):

A. „Device“
B. „Communications“
C. „Cloud“
D. „Lifecycle Management“



8 pav. 6 daiktų interneto įrenginių apsaugos pricipai. Saltinis: „IoT Analytics“ tinklapis

A. Secure Device Layer (Saugus įrenginio sluoksnis)

Įrenginio sluoksnis nurodo IoT techninės įrangos lygį, ty fizinį „daiktą“ ar gaminį. ODMs ir OEMs (kurie projektuoja ir gamina įrenginius) vis labiau integruoja daugiau saugos funkcijų į savo aparatinę ir programinę įrangą (kuri veikia įrenginyje), kad padidintų įrenginio sluoksnio saugos lygį.

Svarbios daiktų interneto saugumo architektūros savybės:

- Kai kurie gamintojai įdiegia lustų saugumą kaip TPM (Trusted Platform Modules), kurie veikia kaip pasitikėjimo šaltinis, saugant neskelbtiną informaciją (t.y. Neišleidžiant šifravimo raktų už lusto).

- Užtikrinti, kad įrenginyje veiktų tik patikrinta programinė įranga.
- Apsaugai nuo klastojimo, jei įsibrovėlis gauna fizinę prieigą prie įrenginio, gali būti naudojama net fizinė apsauga (pvz., Metalinis korpusas kaip skydas, apimantis visas vidines schemas).
- Nors šios įdiegtos ar fizinės apsaugos gali būti vertingos konkrečiose situacijose, rizikos laipsnį lems siūlomas duomenų judėjimas ir įrenginio galimybė atlikti sudėtingas saugumo užduotis. Tačiau fizinis korpuso apdorojimas ir sudėtingos įrenginio saugos funkcijos yra svarbūs principai, kuriuos reikia naudoti nuo pat pradžių.

Į šį sluoksnį patenka du svarbūs saugos principai, kuriuos įvertina ir savo nuomonę pateikia George Cora įmonės „Ardexa“ vadovas: (IoT Analytics, 2018m.)

1) **Device Intelligence (įrenginio žvalgyba)**

   „Daugelis šiandien prieinamų prietaisų, prietaisų, įrankių, ar kitų įtaisų turi galimybę komunikuoti su tam tikra paslauga, debesimi ar serveriu per„ Ethernet “ar„ wi-fi tinklą. Tačiau daugelį šių įrenginių maitina ne kas kitas, o mikroprocesorius, kuris yra netinkamai pritaikytas sudėtingiems interneto ryšiams apdoroti, todėl jie neturėtų būti naudojami svarbius duomenis apdorojančių kompanijų IT struktūrose.

   Veiksmingą ir saugų ryšį turi užtikrinti pats „išmanusis“ įrenginys, galintis valdyti savo apsaugą, šifravimą, autentifikavimą, laiko žymes, talpyklos kaupimą, tarpinius serverius, ugniasienes, ryšio praradimą ir kt. Įrenginiai taip pat turi būti tvirti ir gebėti veikti skirtingose vietose, nepriklausomai nuo ryšio kokybės bei aplinkos temperatūros ir kitų veiksnių, kurie gali lemti įrenginio saugumą.

2) **Edge processing (duomenų apdorojimas „kraštuose“)**

   Išmaniųjų įrenginių turėjimas reiškia, kad jūsų įrenginiui bus suteikta galimybė vystytis, todėl bėgant laikui jis taps galingesnis, naudingesnis, atliekantis naujas funkcijas. Pavyzdžiui, nauji algoritmai dabar gali leisti šiems mažiems įrenginiams apdoroti vaizdo įrašų srautus tokiu būdu, kokio prieš kelerius metus nebuvo galima. Duomenų apdorojimas „kraštuose“ reiškia, kad šie išmanieji įrenginiai gali apdoroti duomenis lokaliai prieš juos siunčiant į debesį, todėl nereikia perduoti didžiulės apimties įrašų į debesį. Bet ar tai gali užtikrinti saugumą? Absoliučiai. Tai reiškia, kad neskelbtinos informacijos nereikia siųsti į debesį. Be to, dabar tai reiškia apdorotus duomenis, supakuotus į atskirus pranešimus, saugiai siunčiamus įvairiems subjektams. Apgalvotas apdorojimo galios panaudojimas įrenginio sluoksnyje padeda sustiprinti bendrą tinklą. (Ardexa, 2019)

B. Saugios komunikacijos ryšių sluoksnis.

Ryšio komunikacijos sluoksnis nurodo IoT sprendimo jungiamuosius tinklus, t.y. Terpes, kuriomis saugiai perduodami / gaunami duomenys. Nesvarbu, ar neskelbtini duomenys yra perduodami per fizinį sluoksnį, tinklo sluoksnį ar programos lygmenį, nesaugūs ryšių kanalai gali būti pažeidžiami. Svarbios daiktų interneto saugumo architektūros savybės:

- Į duomenis orientuoti saugumo sprendimai užtikrina saugų duomenų užšifravimą, kai jie yra šifruojami ne tik eigoje bet ir „ramybės būsenoje“, taigi, net jei jie perimami, jie neturi prasmės, išskyrus vartotojus (ty asmenį, įrenginį, sistemą ar programą), kurie turi tinkamą šifravimo raktą atrakinti kodą.
- Ugniasienės ir įsibrovimų prevencijos sistemos, skirtos ištirti specifinius srautus (pvz., Ne IT protokolus), pasibaigiančius dar prie įrenginio, taip pat vis dažniau naudojamos aptikti nepageidaujamus įsibrovimus ir užkirsti kelią kenkėjiškam veikimui komunikacijos sluoksnyje.

Daiktų interneto kibernetinio saugumo principai saugios komunikacijos sluoksnyje:

3) **Initiate a connection to the cloud (užmegzti ryšį su debesiu)**

Kai tik ugniasienės prievadas atidaromas tinklui, jūs atidarote savo tinklą, realioms saugumo grėsmėms. Ugniasienės prievado atidarymas iš tikrųjų reikalingas tik tam, kad kažkas galėtų prisijungti prie paslaugos. Tačiau greičiausiai visi „field“ išoriniai įrenginiai nebus palaikomi tokiu pačiu saugumo laipsniu kaip „hosted“ programos, tokios kaip žiniatinklis / el. Paštas ar balso / vaizdo serveriai. Jie neturės administratoriaus pataisymo, perkonfigūravimo, testavimo ir stebėjimo programinės įrangos, kuri paprastai taikoma debesies servisui.

Dėl šios priežasties paprastai sunku prisijungti iš interneto į įrenginį. Įrenginys turi inicijuoti ryšį su debesiu, todėl neleis įeiti. Ryšys su debesiu taip pat gali palengvinti dvikryptį kanalą, tokiu būdu leisdamas IoT įrenginį valdyti nuotoliniu būdu.
aplinkybėmis.

4) **Messaging control (pranešimų ribojimas).**

Ryšiai su daiktų interneto įrenginiu nepriklausomai nuo to, ar jie vyksta į įrenginį, ar iš jo turėtų būti elgiamasi atsargiai. Pranešimais pagrįsti protokolai turi keletą ryškių pliusų, dėl kurių jie yra tinkami IoT įrenginiams, įskaitant dvigubo šifravimo, eilių sudarymo, filtravimo ir netgi dalijimosi su trečiosiomis šalimis galimybes. Tinkamai ženklinant, kiekvieną pranešimą galima tvarkyti laikantis atitinkamos saugumo politikos. Pvz., Galima apriboti prieigą prie pranešimų, kurie leidžia vykdyti „nuotolinio valdymo“ funkcijas, arba leisti „failų perkėlimą“ tik viena kryptimi arba dvigubai užšifruoti visus pranešimus, kuriuose yra kliento duomenų, kad jie būtų apsaugoti. Turint tokią infrastruktūrą tampa įmanoma kontroliuoti pranešimų srautą į norimą tikslą. Pranešimai ir su jais susijusi prieigos kontrolė yra labai galingas daiktų interneto komunikacijos sluoksnio įrankis.

C. Secure Cloud (Saugaus debesies sluoksnis)

Debesies sluoksnis nurodo programinės įrangos IoT sprendimo pagrindą, t.y. kai duomenys iš įrenginių yra paimami, analizuojami ir interpretuojami, kad būtų galima susidaryti įžvalgas ir atlikti veiksmus. Saugumas visada buvo pagrindinė diskusijų tema vertinant debesų ir sprendimų riziką. Tačiau daiktų interneto debesis yra laikomas pagrindiniu įmanomu plataus taikymo aspektu. Tikimasi, kad debesų paslaugų teikėjai pateiks saugias ir veiksmingas debesų paslaugas, o apsauga nuo didelių duomenų pažeidimų ar sprendimų netaps problema

Svarbios debesies saugos architektūros savybės:

- Slapta debesyje saugoma informacija turi būti užšifruota, kad būtų išvengta lengvo atakų poveikio, pvz., Kai trečioji šalis, turinti žemesnę saugos kontrolę, prieina prie jūsų duomenų. Taip pat naudinga patikrinti kitų debesų platformų ar trečiųjų šalių programas, kurios bando susisiekti su jūsų debesies paslaugomis, vientisumą, kad būtų apsaugota nuo kenksmingos veiklos. Skaitmeniniai sertifikatai gali atlikti svarbų vaidmenį nustatant ir autentifikuojant poreikius, reikalingus daiktų internetui. (IoT Analytics, 2019)

Daiktų interneto kibernetinio saugumo principai „Cloud“:

5) **Identifikacija, autentifikacija, šifravimas skirtas įrenginiams ne žmonėms**

Žmonės, kurie naudojasi debesijos paslaugomis, beveik visada naudoja slaptažodį. Kai kuriais atvejais gali būti taikomas dviejų faktorių autentifikavimas, pavyzdžiui, slaptažodžio ir

vienkartinio slaptažodžio generatoriaus. Slaptažodžiai yra priimtinas autentiškumo patvirtinimo būdas, kurį žmonės gali naudoti. Tačiau įrenginiai, naudodami debesies paslaugas, daug geriau tvarko skaitmeninius sertifikatus. Skaitmeniniuose sertifikatuose naudojama asimetrinė, šifravimu pagrįsta autentifikavimo sistema, skirta ne tik patvirtinti operaciją, bet ir užšifruoti kanalą iš įrenginio į debesį prieš autentifikuojant. Skaitmeninis sertifikatas taip pat gali suteikti kriptografinį identifikavimą, kurį labai sunku pasiekti naudojant tik vartotojo ID / slaptažodį. (George Cora, 2019)

D. Secure Lifestyle Management (Saugus gyvenimo ciklo valdymo sluoksnis):

Saugus gyvavimo ciklo valdymas susijęs su visa apimančiu sluoksniu, kuriame vykdomi nenutrūkstami procesai, reikalingi IoT sprendimo saugumui atnaujinti. Kitaip tariant tai suprojektuota sauga, kuri yra tik pirmas žingsnis į nuolatinio intelekto internete užtikrinimą. Kiti šio ciklo žingsniai yra politikos vykdymas, reguliarus auditas ir pardavėjo kontrolė.

Svarbios internetinės internetinės saugos funkcijos:

- Veiklos stebėjimas vaidina svarbų vaidmenį stebint, registruojant ir nustatant įtartiną veiklą. Internetiniams įrenginiams ir programoms reikia reguliarių saugos pataisų, kad jos būtų atnaujintos, sustiprintų atsparumą išpuoliams ir pašalintų galimus pažeidžiamumus. Saugus nuotolinis valdymas yra būtinas, ypač kai reikia prižiūrėti milijardus daiktų interneto prietaisų.

Daiktų interneto kibernetinio saugumo principai gyvavimo ciklo valdymo sluoksnyje:

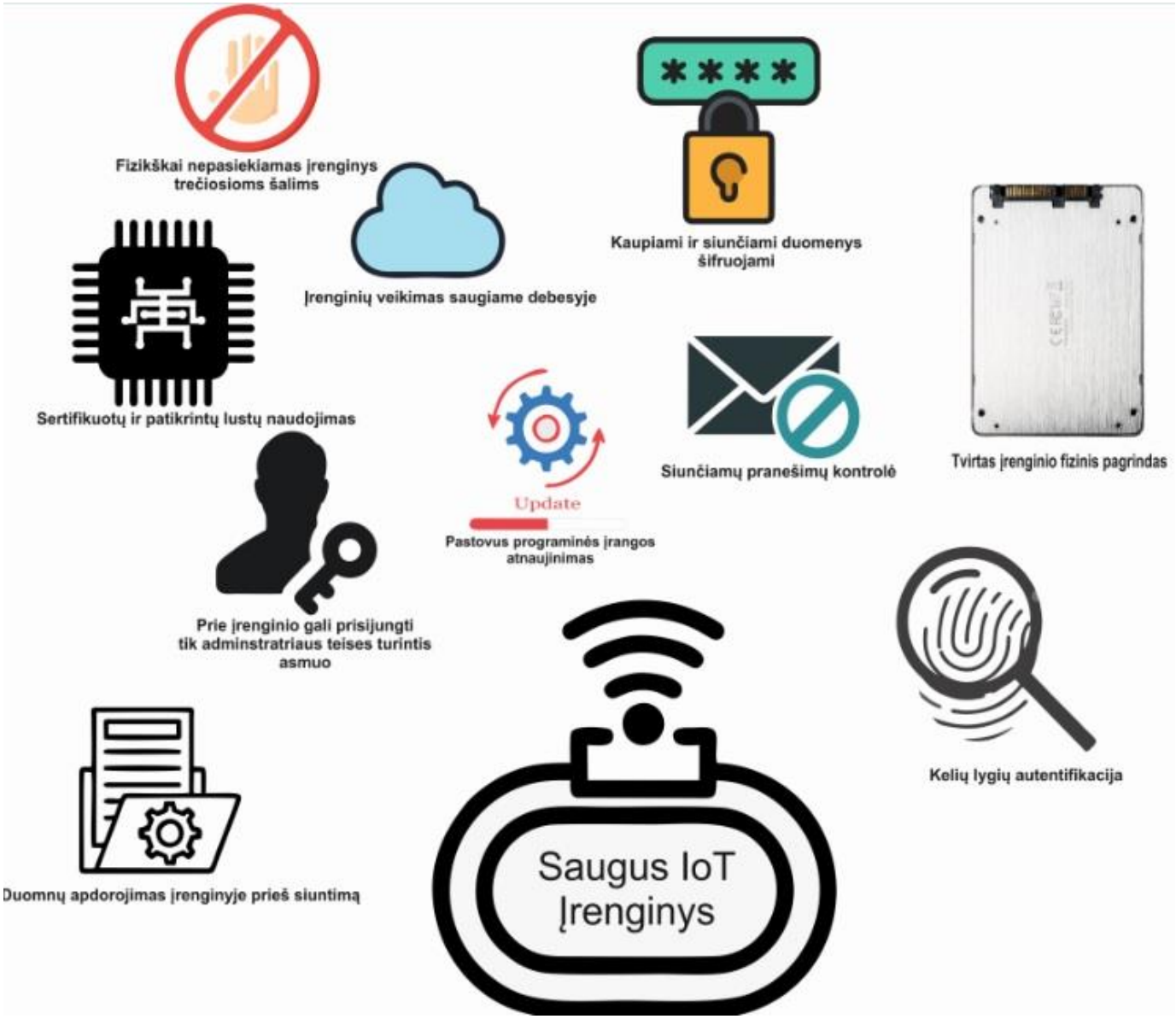
6) Nuotolinio valdymo ir atnaujinimų saugumas

Nuotolinis valdymas arba galimybė siųsti komandas įrenginiui per visą jo gyvavimo ciklą gali būti labai galinga savybė. Nuotolinis prietaiso valdymas yra būtinas, kai leidžiama atlikti nuotolinę diagnostiką, nustatyti naują konfigūraciją, atnaujinti klaidingą programinę įrangą, nuskaityti failus, iš naujo nustatyti mokymosi algoritmą nauju mokymosi duomenų rinkiniu, pridėti naują produkto funkciją ir dar daugiau. Raktas į saugų atnaujinimą ir nuotolinį valdymą užtikrina, kad įrenginys neleidžia prisijungti (žr. 3 principą), tačiau turi dvipusį ryšį, yra tinkamai apsaugotas (žr. 1 principą), kaip komunikacijos kanalą naudoja pranešimus (žr. 4 principą) ir yra tinkamai įgyvendintas. Galiausiai įrenginio programinė įranga veikia kaip serveris, nors ir tas, kuris bendrauja tik su debesiu ir neleidžia niekam prisijungti. Tačiau įdiegti nuotolinio valdymo programinę įrangą ir valdyti saugius atnaujinimus viso prietaiso gyvavimo ciklo metu yra sudėtinga. (George Cora, 2019)

Taigi, išnagrinėjus daiktų interneto kibernetinio saugumo įmonės „Ardexa“ vadovo George Cora išdėstytus principus kiekviename įrenginio gyvavimo sluoksnyje galima pastebėti, kad norint sukurti įrenginį neužtenka jog jis gerai veiktų bei atliktų savo funkcijas, tačiau ne ką mažiau darbo reikia įdėti kuriant jo saugumo architektūrą. Jeigu kiekvienas įrenginys būtų taip kruopščiai parengtas pagal šiuos išdėstytus saugumo principas ir būtų į juos atsižvelgiama, neabejotinai kibernetinių incidentų kiekis naudojantis daiktų interneto spragomis būtų ženkliai mažesnis. Žinoma, kiekvienas architektūrinis sprendimas turi savo kainą, dėl ko įrenginio kaina gali kilti, tačiau formuojant teigiamą įrenginių saugumo ugdymo politiką, žmonės taps supratingesni ir rinksis saugesnius ir patikrintus produktas už juos sumokėdami didesnę sumą pinigų vardan savo duomenų ir asmens saugumo.

3.3.1 Saugaus įrenginio modelis

Išnagrinėjus įvarius pavyzdžius pasaulyje, dažniausiai atakuojamus įrenginius ir kokiais būdais jie yra dažniausiai pažeidžiami susidarė bendrieji saugumo architektūros principai, kurie tinka daugeliui daiktų interneto įrenginių. Kuriais remiantis pradinėje gamybos stadijoje galima išvengti jau minėtų atakos tipų. Taigi, šiame skyriuje apibendrintai pavaizduoti įrenginio saugumo architektūros sprendimai, kurie buvo aprašyti 3.4. skyrelyje. (žr. 9 pav.)



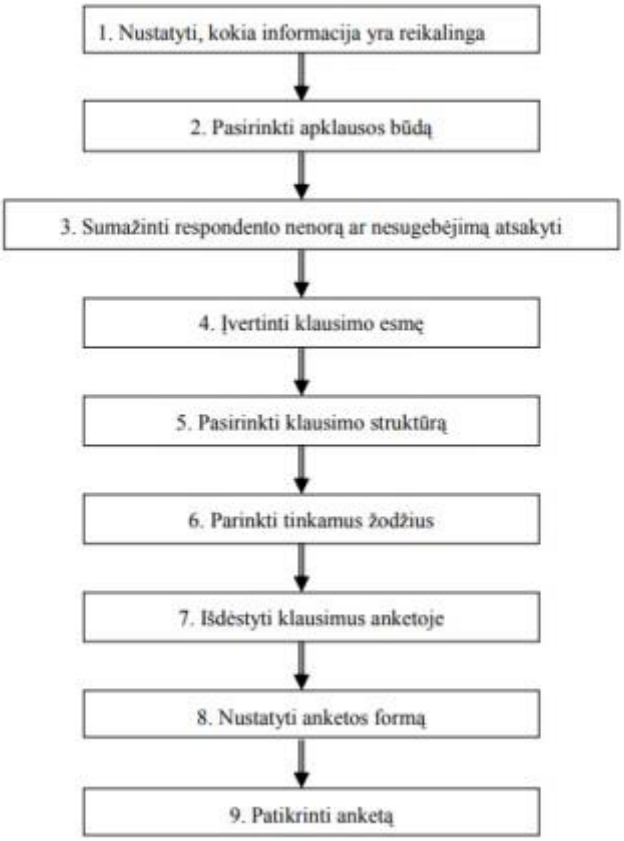
9 pav. Saugaus IoT įrenginio modelis. Sudarytas autoriaus pagal „Ardex“ vadovo George Core analizę.

1. Duomenų apdorojimas įrenginyje prieš siuntimą
2. Kelių lygių autentifikaciją. (pvz. slaptažodis, piršto anspaudo, veido nuskaitymas)
3. Tvirtas įrenginio fizinis korpusas. (pvz. metalinis pagrindas neleis sugadinti įrenginio lusto)
4. Prie įrenginio gali prisijungti tik administratoriaus teises turintis asmuo.
5. Pastovus programinės įrangos atnaujinimas.
6. Siunčiamų pranešimų kontrolė.
7. Sertifikuotų ir patikrintų lustų naudojimas.
8. Kaupiamų ir siunčiamų duomenų šifravimas.
9. Įrenginių veikimas debesijos tinkle.
10. Fiziškai nepasiekiamas įrenginys pašaliniams

4. KIBERNETINIO SAUGUMO UŽTIKRINIMAS ĮMONĖSE: DAIKTŲ INTERNETO ASPEKTAS. TYRIMAS

4.1Tyrimo metodologija

Tyrimui atlikti buvo pasirinktas kokybinis tyrimo metodas. Toks tyrimo metodas atskleidžia atskleidžia ne tik matomus ir racionaliai suvokiamus įvairių reakcijų bei vertinimų aspektus, tačiau ir giliau slypinčius požiūrius, motyvus, įsitikinimus bei vertybes. Tokia kokybinė analizė leidžia tikslingai modeliuoti esamą situaciją, sudaryti galimybes prognozuoti ateities poreikius ir numatyti būdus spręsti problemas (Rita Žukauskienė, 2008). Kaip teigia kokybinių tyrimų specialistai, šis būdas leidžia gauti iš atliekamo tyrimo tikslesnius bei daugiau naudos teikiančius rezultatus tiriant socialinėje aplinkoje vykstančius reiškinius. (Agnė Tonkūnaitė, 2012). Tyrimui atliki buvo sudaryta anketa ekspertams pagal Vytautą Dikčių. (žr. 10 pav.)



10 pav. Anketos sudarymo schema pagal Vytautą Dikčių, 2011.

Tinkamai suformuluoti, trumpi bei lengvai suprantami klausimai sukuria didesnes galimybes gauti tikslesnius ir naudingesnius tyrimo duomenis. Iš viso anketoje ekspertams reikėjo atsakyti į 7 klausimus. Abstraktiems ir apytikslių skaičių reikalaujantiems trims klausimams buvo pasirinkta testinio pabūdžio klausimai. O likusiems 4, kurie reikalavo ekspertų profesinių žinių – atviri. Klausimai suformuluoti trumpi ir aiškūs, nes kuo mažiau respondentui reikia pačiam rašyti, tuo labiau sukuriamas anonimiškumo išlaikymas, taip pat daug teksto ir bendrai didelė apklausos apimtis atbaido respondentus atskinėti arba atsakymai nesuteikia tyrimui naudos, parašyti atmestinai (Kardelis, 2002, p. 93-94).

Anketos klausimai:

1. Kiek daiktų interneto įrenginių naudoja jūsų įmonė? (išskyrus kompiuterius)
2. Kiek vidutiniškai per metus patiriate bandymų įsilaužti į jūsų įmonės įrenginius?
3. Kokiems tikslams pasiekti dažniausiai atakuojami jūsų įmonės įrenginiai?
4. Kokie įrenginiai dažniausiai atakuojami?
5. Kokiais būdais dažniausiai bandoma įsilaužti? (atakų rūšys)
6. Kokias saugumo priemones naudojate kibernetinio saugumo užtikrinimui?
7. Įvertinkite nuo 1-10 jūsų įmonės darbuotojų pasiruošimą ir gebėjimą atpažinti kibernetinius incidentus?

Tyrimo tikslas – Apklausus ekspertus išsiaiškinti, kokios kibernetinio saugumo daiktų interneto aspekte tendencijos vyrauja e. versle

Tyrimo uždaviniai:

- Išsiaiškinti kiek plačiai naudojamas daiktų internetas įmonėse.
- Sužinoti, kokias atakas patiria įmonės.
- Išsiaiškinti koks tikslas vienija norinčius įsilaužti kibernetinius nusikaltėlius.
- Apibrėžti, įmonių gebėjimą apsaugoti įrenginius nuo kibernetinių incidentų.
- Įvertinti, įmonėse dirbančių darbuotojų išprusimą kibernetinio saugumo klausimu.

Tyrimo objektas – Kibernetinės atakos, daiktų interneto įrenginiai įmonėse.

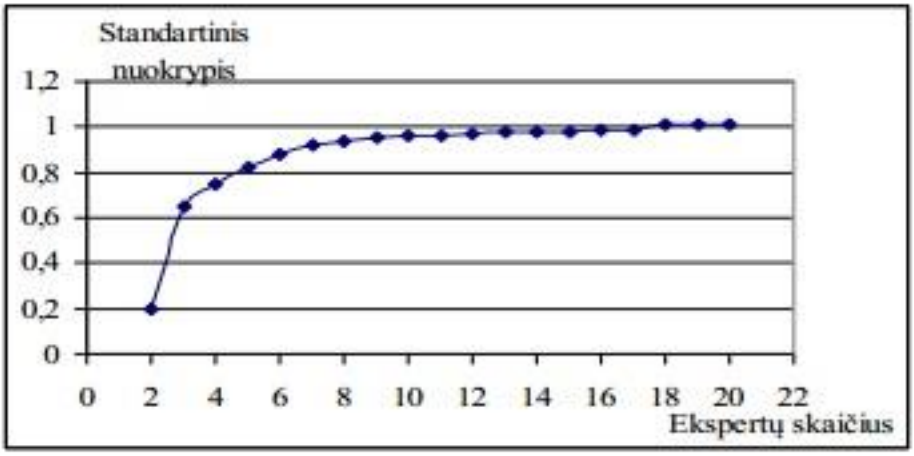
Tyrimo organizavimas

Tyrimas buvo pradėtas ir anketos išsiųstos 2019m. lapkričio 15d. ir užbaigtas (gauti paskutinieji atsakymai, bei jų patikslinimai) 2020m. Kovo 10d.

Tyrimas buvo atliekamas apklausiant įmonių, kurios plačiai naudoja išmaniuosius įrenginius ir didžiąją veikos dalį vykdo kibernetinėje erdvėje. Buvo apklausta 8 įmonių IT ekspertai:

1. UAB „Haltex“ IT sepcialistas.
2. AB „Telia“ IT tarptautinių projektų vadovė.
3. UAB „Kirptė“ IT skyrių aptarnaujantis įmonės „Atea“ specialistas
4. „Zenitach“ Vyresnysis programuotojas
5. „CSC Baltic“ programų testuotojas
6. „Danske Bank“ IT skyriaus specialistas
7. „Teltonika“ IoT group
8. „Western Union“ IT speacialistas

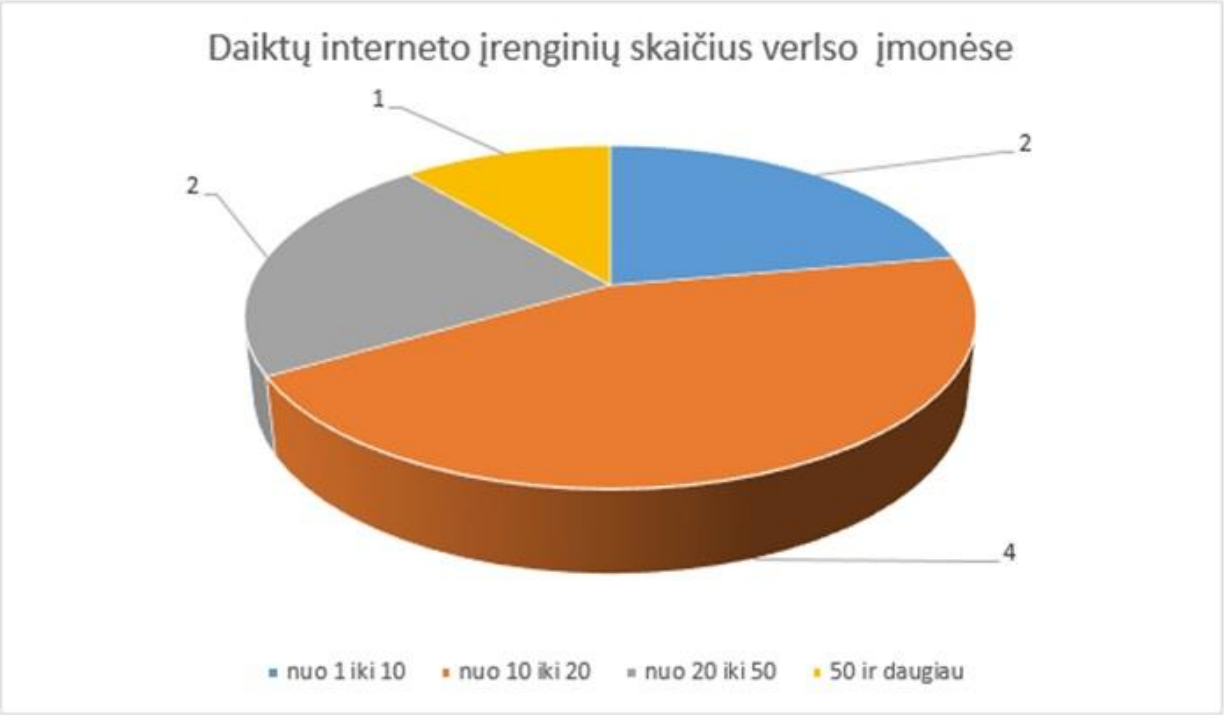
Tyrimui buvo pasirinkti 8 ekspertai atsižvelgiant į testų teoriją. Kurios teorija teigia, kad sprendimų patikimumą ir ekspertų skaičių sieja greitai gęstantis netiesinis ryšys (Baležentis, Žalimaitė, 2011). Kita plačiai naudojama teorija teigia, kad nedidelių ekspertų grupių atsakymų patikimumas nenusileidžia didelių grupių atsakymų tikslumui (Libby, Blashfield, 1978), ko rezultate matome, kad 8 ekspertų nuomonių pakanka atlikti kokybišką ir naudingą tyrimą. (žr. 11pav.)



11 pav. Ekspertų vertinimo nuokrypio priklausomybė nuo ekspertų skaičiaus. Šaltinis: pagal Žalimaitę ir Baležentį

4.2Tyrimo duomenų analizė

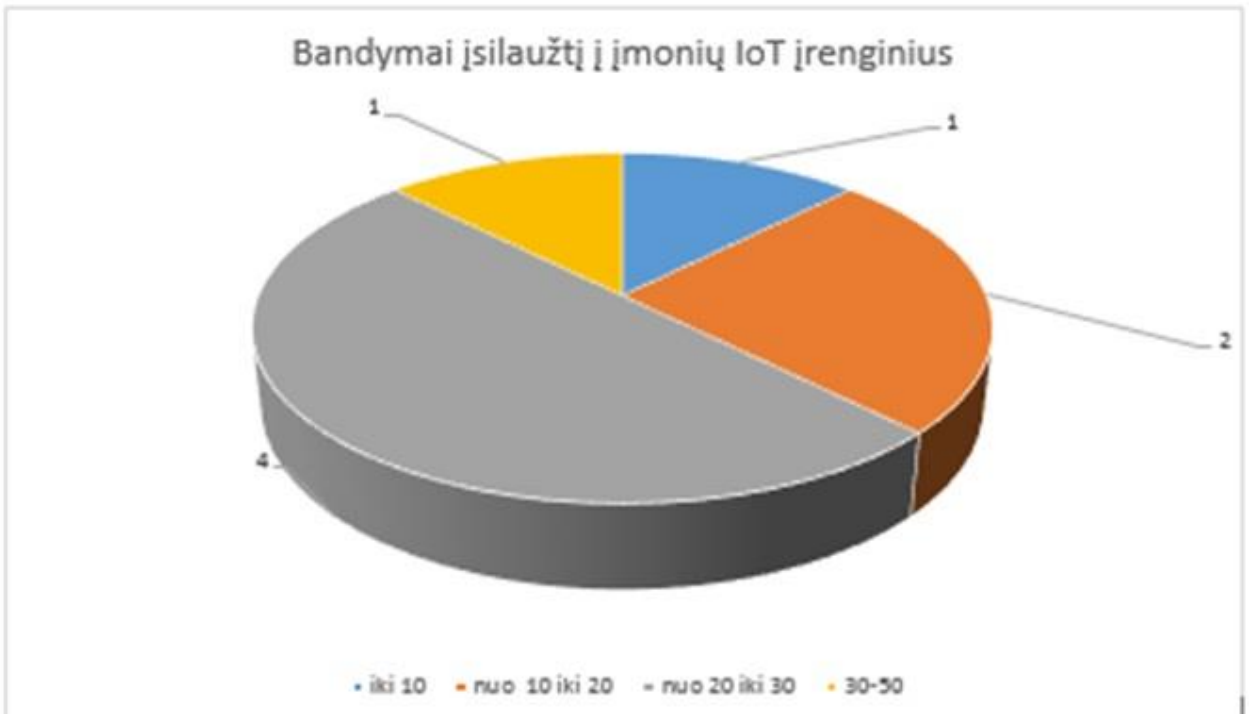
Iš pradžių buvo norima sužinoti, kiek daiktų interneto įrenginių yra įmonėje, kadangi šiomis dienomis kiekviename ofise apstu kompiuterių, todėl ekspertų buvo prašoma pateikti informacija apie įrenginius be personalinių ar nešiojamųjų kompiuterių. (žr. 12 pav.)



12 pav. Daiktų interneto įrenginių skaičius tirtose verslo įmonėse.

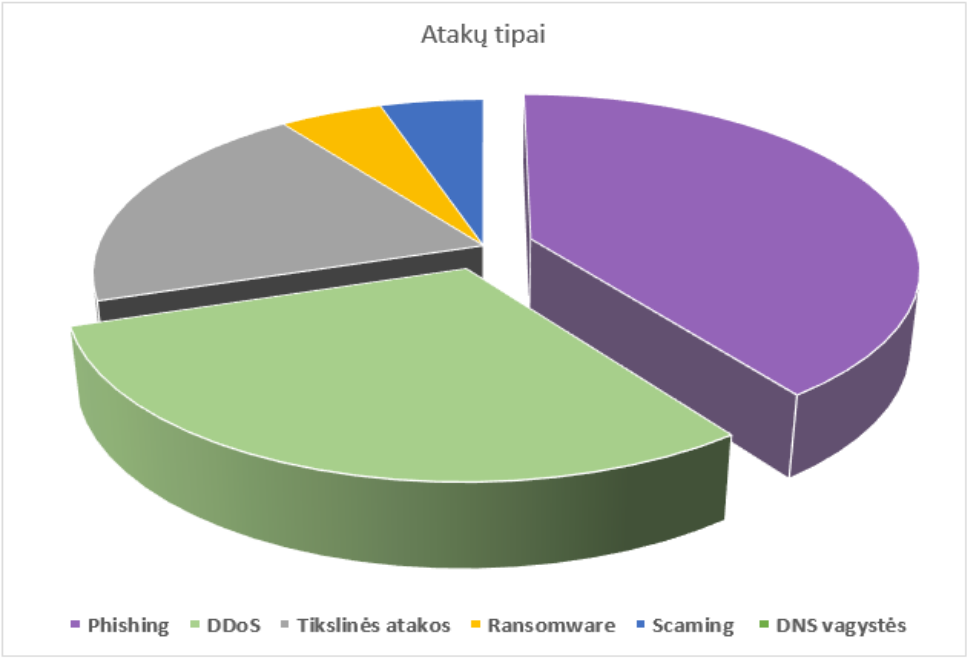
Matome, kad pusė apklaustųjų ekspertų, teigia, jog jų įmonės naudoja nuo 10 iki 20 daiktų interneto prietaisų. Viena gamybinė įmonė pasisakė naudojanti daugiau kaip 50 daiktų interneto įrenginių, kaip pats ekspertas minėjo, tai yra pramonės šakos išmanieji jutikliai, kurie teikia informaciją apie procesus.

Taigi, matome, kad laikui bėgant daiktų interneto įrenginių daugėja ir pas Lietuvoje esančius verslo subjektus. Todėl kitas klausimas buvo pateiktas norint sužinoti, kiek įmonės per metus patiria įsilaužimų arba bent jau bandymų įsilaužti. (žr. 13 pav.)



13 pav. Bandymai įsilaužti į įmonių IoT įrenginius

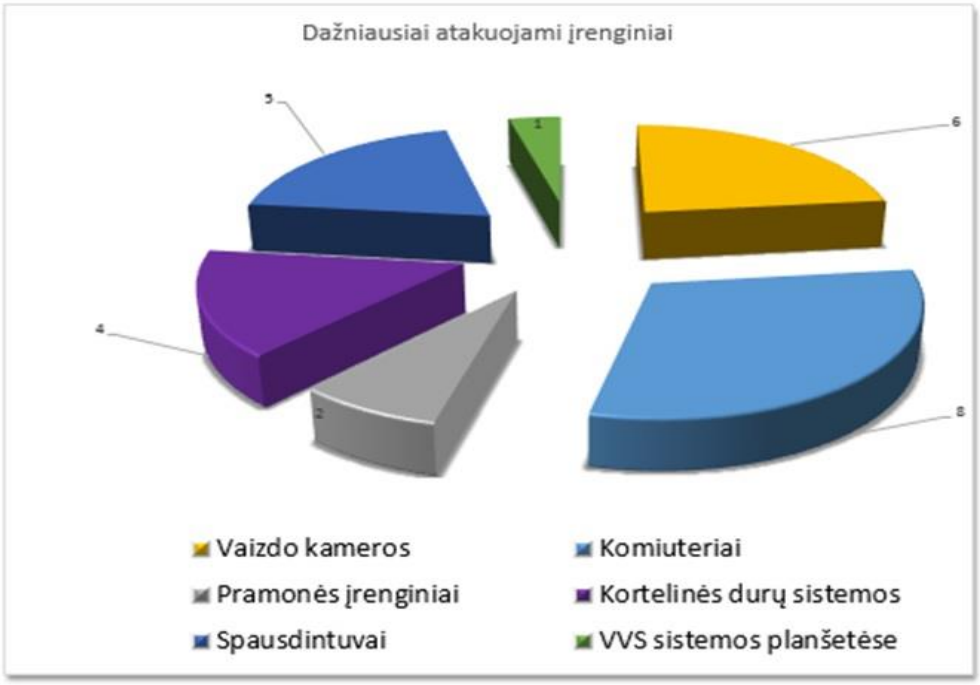
Matome, kad per metus įmonių įrenginiai daugiausiai 4 iš 8 ekspertai paminėjo, jog kenčia nuo įsilaužimų arba bent jau bandymų jiems pakenkti apie 20-30 per metus. Daugelis ekspertų, teigė, kad tai sudaro daugiau realūs bandymai pažeisti sistemas, neskaitant kaip daugelis vadina kasdieninių „phishing“ atakų į darbinius el. paštus ir panašiai. Todėl būtent kitas klausimas ir buvo – kokiais dažniausiai atakų tipais bandoma rasti kelius į IoT įrenginių sistemas. (žr. 14 pav.)



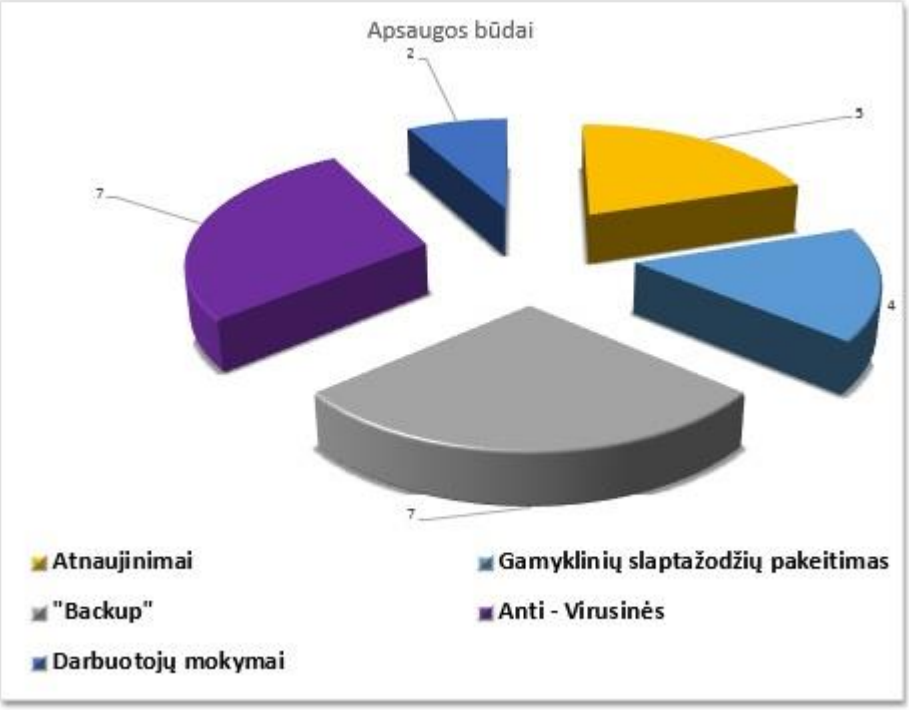
14 pav. Dažniausiai naudojami atakų tipai įmonėse.

Ši diagrama tik dar kartą patvirtina, jau minėtą ekspertų „phishing“ metodą, kai dažniausiai darbuotojams kasdien dideliais kiekiais siuntinėjami el. pašto laiškai su kenksmingomis programomis arba melaginga informacija, taip ieškant kelių į tolimesnes įmonių sistemas, šį metodą paminėjo visi be išimties 8 įmonių ekspertai. Ne ką mažiau atsiliko „DDoS“ metodas, kuris būdingas įmonėms naudojančioms daug daiktų interneto jutiklių. Ekspertai taip pat išskiria vieningą nuomonę, kad kartais net patys nesupranta dėl kokios priežasties į IoT įrenginius kaip vaizdo kameros ar išmaniosios durų spynos kenkėjai siunčia didelius kiekius duomenų taip sutrikdydamos jų veiklą. Taip pat nemažai paminėjo tikslines atakas. Vienas ekspertas, žinoma, paprašęs anonimiškumo pasidalino 2019m. gruodžio mėnesį patirta kolkas jų įmonei skaudžiausia kibernetine ataka, kurios rezultate įmonė deklaravo – 250 000 eurų nuostolį. Kai užpuolikai ilgą laiką vykdę įmonės veiklos stebėseną, išanalizavo vieną iš nuolatinių žaliavų tiekėjų, prisidengdami jų vardu iš banko sąskaitos sugebėjo padaryti pavedimus į savo sąskaitas Kinijoje. Smulkesnių detalių, kur buvo įmonėje buvo padaryta saugumo spraga ekspertas neatskleidžia, tačiau dalinasi savo patirtimi ir skatina saugoti kiekvieną savo įrenginį, ypatingai jeigu jis susijęs su įmonės svarbiais ištekliais. Būtent ši įmonės paminėjo, kad procesams valdyti naudoja daugiau kaip 50 daiktų interneto jutiklių sujungtų tinkle, todėl atakos galimi keliai analizuojami iki šiol.

Toliau nagrinėti esamą situaciją įmonėse buvo užduoti klausimai kokie dažniausiai įrenginiai patiria kibernetines atakas (žr. 15 pav.) ir kokių priemonių imasi apsaugoti savo įrenginius bei duomenis. (žr. 16 pav.)



15 pav. Dažniausiai kibernetines atakas patiriantys įrenginiai



16 pav. Įmonių apsisaugojimo būdai nuo kibernetinių incidentų.

Žinoma, prie dažniausiai atakuojamų įrenginių negalima nepriskirti ir kompiuterių, kuriuos kaip įrankį vykdyti kibernetines atakas paminėjo visi 8 apklaustieji ekspertai. Tačiau vis daugiau integruojant daiktų interneto įrenginius į verslą didžioji dauguma patiria atakas ne tik kompiuteriams bet ir kaip rodo apklausa – dažnai vaizdo kameros, išmaniosios įėjimo sistemos, kiek mažiau paprasti biuro įrengimai kaip spausdintuvai ir taip pat buvo paminėtas vienas incidentas su VVS (verslo valdymo sistema). Darbuotojams darbą lengvina gamybinėje įmonėje sudėti išmanieji jutikliai, kurie rodo įvairius gaminio parametrus ir būseną, jie tarpusavyje sujungti su verslo valdymo sistema, todėl užpuolikams atvėrė kelius į sistemos duomenų bazę patekti išmanieji jutikliai, kurių dėl didelio kiekio apsauga nebuvo pasirūpinta ir naudojo gamyklinius slaptažodžius. Didžiosios daugumos ekspertų atsakymuose vyrauja vaizdo kamerų atsakymas. Šie ekspertų atsakymai patvirtina didžiąją dalį naujausios daiktų interneto tendencijos, kad vaizdo stebėjimo kameros tampa populiariu užpuolikų taikiniu, nes kaupia naudingų asmeninių duomenų ir verslo veiklos paslapčių vienoje vietoje.

Nagrinėjant, apsaugos būdus (žr. 16 pav.) buvo tikimasi iš ekspertų didesnio atsakymų kiekio, kas rodo jog įmonės naudoja ir patikrintus ir gana patikimus būdus kaip – nuolatiniai įrenginių atnaujinimai ir legalios programinės įrangos naudojimas. Taip pat sveikintinas įmonių požiūris į atsargines kopijas

„backup“, kurias paminėjo 7 iš 8 apklaustųjų. Verta paminėti, kad tik 2 įmonės iš 8 paminėjo nuolatinį darbuotojų ugdymą kibernetinio saugumo klausimais kaip apsisaugojimo būdų nuo kibernetinių atakų. Nors paprašyti atsakyti į paskutinįjį klausimą ir įvertinti savo darbuotojų pasiruošimą atpažinti ir reaguoti į kibernetinius incidentus, įmonių vidutinis įvertinimas buvo – 7. Kas kiek sukelia abejonių atsakymo tikrumu, nes atsižvelgiant į tyrimo dalį, kurioje buvo klausima apie apsisaugojimo būdus, tik 2 įmonės suprato ir paminėjo darbuotojų mokymų svarbą.

Tyrimo išvados:

- Tyrimas parodė, kad verslas jau ir Lietuvoje naudoja vis daugiau išmaniųjų daiktų interneto įrenginių neskaitant kompiuterių.
- Pastebėta tendencija, kad kurios įmonės pasisakė turinčios daugiau daiktų interneto prietaisų (nuo 20 iki 50 ir daugiau), patiria dažniau kibernetines atakas įmonėje.
- Tyrimas patvirtino šalių analizėje pateiktą statistiką, kad kibernetinių atakų pradžios taškas yra „phising“ metodas, vėliau vykdant rimtesnio pobūdžio atakas kaip „Ransomware“ ir taip pat daiktų interneto įrenginių darbui sutrikdyti naudojamas vienas paprasčiausių bet kartu ir veiksmingiausių „DDoS“ atakų tipas.
- Daugiausiai bandoma sutrikdyti ir gauti informacijos iš vaizdo stebėjimo kamerų, o daugiausiai žalos padaroma atakuojant pramonės gamyklose sumontuotus išmaniuosius jutiklius.
- Taip pat tyrimas atskleidė, kad vis dar daugėja kibernetinių nusikaltėlių, kurie neturi konkretaus tikslo atakuoti įrenginius, tiesiog tai daro ir sukelia problemas sutrikdydami išmaniųjų įrenginių darbą.
- Tyrimas parodė, vis dar gana silpną verslo įmonių požiūrį į darbuotojų rengimą ir mokymus kibernetinio saugumo klausimas ypač naudojant daiktų internetą. Įmonės daugiau naudoja patikrintus ir senesnius apsaugos metodus kaip – antivirusinės sistemos, įrangos atnaujinimai. Tačiau savo darbuotojus kaip pasiruošusius priimti kibernetines atakas parengtas prieš išmaniuosius įrenginius vertina maždaug 7 balais iš 10, kas atsižvelgus į kitus tyrimo kriterijus kelia šiek tiek abejonių.

IŠVADOS

1. Kibernetinio saugumo ir daiktų interneto sąvokos gana plačiai ir aiškiai išnagrinėtos bei aprašytos. Daiktų internetas dažnai minimas kaip technologinis atradimas ir daugiau kalbama koks jis naudingas nei kokias problemas gali atnešti. Todėl įrenginius plačiai pradėjus naudoti versle atsirado daugybė naujų kibernetinių atakų, kas rodo prastą verslo vykdomą IoT įrenginių saugos politiką bei verčia keisti ir kurti naujus saugumo reikalavimus.
2. Išanalizavus didžiųjų pasaulio valstybių: JAV, Kinijos ir Vokietijos kibernetinio saugumo padėtį galima teigti, kad daugiausiai kibernetinių atakų patiria technologiškai labiausiai pažengusios šalys ir naudojančios naująsias daiktų interneto įrenginių technologijas. JAV pirmauja tiek pagal patiriamų atakų skaičių, tiek pagal nuostolius patirtus dėl kibernetinių atakų, toliau rikiuojasi Japonija, JK, Vokietija, Kinija. Pagrindinė problema – didžiosios verslo įmonės naudoja daug daiktų interneto įrenginių, kurie yra lengvai pažeidžiami, nes gaminant juos nėra griežtų saugumo reikalavimų ir atsižvelgiamą daugiau į kiekybė ir pigią kainą nei į saugumą. Išnagrinėjus situaciją Lietuvoje pastebėta, kad daiktų internetas versle jau gana plačiai naudojamas ir taip pat atneša naujas saugumo problemas įmonėms. Pagrindinės priežastys: prastas kibernetinio saugumo švietimas, naudojami nepatikrinti ir dažnai saugumo reikalavimų neatitinkantys daiktų interneto prietaisai verslo sektoriuose, neatliekami įrenginių diegimo mokymai pvz.: įrenginiuose paliekami numatytieji slaptažodžiai.
3. Remiantis tyrimo rezultatais galima teigti, kad jau ir Lietuvos versle daiktų internetas yra gana plačiai naudojamas, o gamybinės įmonės juos skaičiuoja jau ne vienomis dešimtimis. Lietuvoje kaip ir kitose pasaulio valstybėse vyrauja panaši atakų tendencija – užpuolikai naudojasi daiktų interneto įrenginių spragomis, kaip savo atakos pradžios taškais, kurie leidžia nuvesti juos į tinkle esančius kitus įrenginius, kurie saugo svarbius ir konfidencialius duomenis. Asmens duomenys, verslo, gamybos paslaptys – pagrindiniai nusikaltėlių taikiniai. Todėl daiktų interneto įtaka verslo saugumui kelia naujus reikalavimus bei verčia keisti požiūrį tiek į įrenginių, tiek į svarbių duomenų apsaugos galimybes ir esamą lygį.
4. Remiantis atliktomis analizėmis ir tyrimo rezultatais galima teigti, kad pagrindinė verslo kibernetinio saugumo problema yra naudojami nesaugūs daiktų interneto įrenginiai, kurių saugumu mažai rūpinamasi ir pasitikima gamintojo saugumo lygiu bei silpna darbuotojų kibernetinio saugumo svarbos samprata nes tik 2 iš 8 ekspertų paminėjo darbuotojų kibernetinio saugumo mokymus kaip prevenciją nuo atakų. Todėl, kaip rodo atliktas tyrimo rezultatai, vis dar populiarios duomenų vagystės vadinamuoju „phishing“ metodu dažniausiai paremtos naivių darbuotojų patiklumu.
5. Remiantis tyrimu, galima teigti, kad verslo įmonės pernelyg pasitiki standartinėmis bei įrenginių gamyklinėmis saugumo priemonėmis, kaip antivirusinės sistemos ir įrangos atnaujinimai.

Dauguma rūpinasi daugiau kompiuterių saugumo, pamiršdami kitus prie tinklo prijungtus daiktų interneto įrenginius. Tačiau ekspertai paminėjo naudojantys ir patikimus bei patikrintus apsaugos būdus kaip nuolatinės duomenų kopijos, įrenginių apsaugojimas saugiais ne gamykliniais slaptažodžiais.

6. Atsižvelgiant į kibernetinio saugumo specialistų įžvalgas bei ekspertų pateiktus tyrimo rezultatus galima išskirti pagrindiniu daiktų interneto apsaugojimo būdus versle:
    I. Diegti kokybiškus daiktų interneto įrenginius iš oficialių tiekėjų, patikrinti kokius saugumo reikalavimus atitinka įrenginys, jei trūksta apsaugos, papildomai jį apsaugoti pvz.: naudojant kelių lygių autentifikaciją, pranešimų siuntimo kontrolę.
    II. Vienas iš svarbiausių svarbių verslo duomenų apsaugojimo būdas – duomenų kopijos.
    III. Daiktų interneto prietaisus diegti atskirame tinkle, kuriame nebūtų įrenginių saugančių svarbius duomenis,
    IV. Vykdyti nuolatinius darbuotojų kibernetinio saugumo mokymus, bei mokyti kaip reikia elgtis su daiktais esančiais tinkle.
    V. IT specialistams įvertinti tinklo struktūrą bei įmonių tinkluose izoliuoti tam tikrus išorinius ir tinklo galimai pažeidžiamus prievadus.
    VI. Nepasitikėti tik visiems žinomomis ir bazinėmis apsaugos sistemomis kaip antivirusinės ir įrangos atnaujinimai.
    VII. Suteikti kiekvienam įmonės darbuotojui spec. Teises, kuriomis galėtų pasiekti ir valdyti tik jiems reikalingus įrenginius bei informaciją tinkle.
    VIII. Įmonėms, kurios daiktų interneto pagalba perduoda didelį kiekį svarbių duomenų, apdoroti juos savo sistemoje ir siųsti tinkle užšifruotus ir jau apdorotos, suspaustus duomenis.

REKOMENDACIJOS

- Siūlytina priimti ES šalims bendrus saugumo reikalavimus daiktų interneto prietaisų gamintojams bei vartotojams. Nes šiuo metu vyrauja daugiau kainos ir kiekybės principas nei įrenginio kokybės ir saugumo.
- Verslo subjektams svarbu suburti stiprią IT komandą atsižvelgiant į esamą įrenginių kiekį įmonėje, kad kiekvienas įrenginys būtų stebėsenoje. Taip pat turėti žmonės, kurie nuolatos mokytų ir supažindintų su naujovėmis, suskirstytų atsakomybes įmonės darbuotojams.
- Vykdyti mokymus ne tik vidinėje darbo aplinkoje, bet ir tarptautiniuose mokymuose, seminaruose, kad darbuotojai patys mokėtų reaguoti į pažeidžiamumus ir juos atskirtų.
- Periodiškai atlikti daiktų interneto įrenginių saugumo inventorizaciją, stebėti atsinaujinančią technologijų rinką, senus ir nesaugius įrenginius nesant galimybei jų atnaujinti, pakeisti juos kitais. Diegiant naują daiktų interneto tinklo architektūrą įmonėje galima pasikviesti į pagalbą pasaulinio lygio organizacijų kaip „Fireeye“ „McAfee“ „Eset“ saugumo specialistus, kurie pravestų mokymus bei padėtų sukurti saugų tinklą įrenginiams veikti.
- Įmonės IT infrastruktūrą suskirstyti į administravimo lygius, kad darbuotojai turėtų prieigą tik prie tų įrenginių ir informacijos su kuriais reikia tiesiogiai dirbti.
- Prieš siunčiant apdoroti daiktų interneto prietaisais siunčiamus duomenis vietiniame tinkle ir siųsti toliau šifruotus.
- Svarbius duomenis laikyti keliose atskirose talpyklose.
- Geriausiai naudoti vieno gamintojo daiktų interneto įrenginius, dėl geresnio tarpusavio sujungiamumo.
- Prieš įsigyjant įrenginius konsultuotis su gamintoju dėl prietaisų kokybės, saugumo garantijų užtikrinimo, įrangos atnaujinimo galimybių.
- Verslui turinčiam didelį kiekį daiktų interneto jutiklių, kurie reguliuoja gamybos srautus ir vidiniu procesus sukurti atskirą uždarą tinklą apsaugotą keliais autentifikacijos būdais.

LITERATŪROS SĄRAŠAS

1. Audronė Mikalauskienė, Zenonas Brazaitis, Informacinių sistemų sauga, 2010
2. Von Solms. Compiuter & security, 2006
3. Kardelis K. Mokslinių tyrimų metodologija ir metodai. Kaunas, 2002.
4. Vytautas Dikčius. Anketos sudarymo principai, Vilnius, 2011.
5. Parker, Donn, Computer Security Managment, 1981.
6. Rimvydas Savukynas, Virginijus Marcinkevičius „Daiktų interneto objektų identifikavimo metodų palyginimas“, 2017.
7. E. Kazanavičius „Kaunui įsitraukus į daiktų interneto tinklą – kokios galimybės atsiveria verslui?“ https://kauno.diena.lt/naujienos/kaunas/miesto-pulsas/kaunui-isitraukus-i-daiktu-interneto-tinkla-kokios-galimybes-atsiveria-verslui-911195
8. Forbes. 42 More Cybersecurity Predictions for 2020. https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/#1ed921794a56
9. Deadline. Cyber atack report: „Cyber Attack Was “Malicious”; Homeland Security Monitoring As Twitter & Netflix Come Back Online“ https://deadline.com/2016/10/twitter-netflix-cyber-attack-1201840510/
10. Code Academy, 2017. http://www.Codeacademy.com/
11. Kaspersky Lab. (2015). Spam & Phishing in Q2 2015. https://securelist.com/files/2015/08/KL_Q2_2015_SPAM_REPORT_ENG.pdf/
12. Lithuanian Cybercrime Center of Excellence for Training, Research & Education report. Gyvenimo daiktų internete ypatumai, 2016. < http://www.l3ce.eu/straipsnis/gyvenimo-daiktu-internete-ypatumai-skaitmenines-teises/>
13. IoT World Today, 2016. https://www.iotworldtoday.com/2016/07/27/10-most-vulnerable-iot-security-targets/
14. IoT World Today. „IoT Managed Services Mature, Despite Measured Enterprise Adoption“, 2020. https://www.iotworldtoday.com/2020/03/13/iot-managed-services-mature-despite-measured-iot-enterprise-adoption/
15. USA Department of Security. The department of Defense Cyber Strategy, April 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

16. National Security Strategy. (2015). Cooperative Cyber Defense Centre of Excellence: Cyber Security Strategy Documents. USA. https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf
17. National Cyber Security Strategies. (2012). Enisa. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper.
18. LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS, 2014 m. gruodžio 11 d. Nr. XII-1428, Vilnius. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee.
19. Konvencija dėl elektroninių nusikaltimų. 2001 m. Lapkričio 23 d. Teisės aktų registras. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=.
20. Rekomendacijos Lietuvos Respublikos Kibernetinio saugumo įstatymui. dr. Darius Štitilis dr. Paulius Pakutinskas dr. Marius Laurinaitis Inga Malinauskaitė-van de Castel, Kovas 2017, Vilnius. https://repository.mruni.eu/bitstream/handle/007/14643/Rekomendacijos_Kibernetinio_saugumo_istatymui(galutinis).pdf?sequence=1.
21. Konvencija dėl elektroninių nusikaltimų. 2001 m. Lapkričio 23 d. Teisės aktų registras. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=.
22. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymo Nr. IX-1132 1, 2, 3 ir 7 straipsnių pakeitimo įstatymas. 2014. Teisės aktų registras. https://www.e-tar.lt/portal/lt/legalAct/332e48b059ed11e487eff7b424bd0f08.
23. Laima Zalieckaitė, Raimundas Žilinskas. Daiktų interneto technologijos taikymo versle nauda ir rizika, 2015 Vilnius. http://www.zurnalai.vu.lt/informacijos-mokslai/article/view/9223.
24. Štitilis, D., Laurinaitis, M. (2009). Tapatybės vagystė elektroninėje erdvėje. Informacijos mokslai. P. 240-247. http://www.zurnalai.vu.lt/informacijos-mokslai/article/download/3231/2348
25. BDI. Cybersecurity: The backbone of a successful digital transformation, 2020. https://english.bdi.eu/article/news/cybersecurity/
26. Kauno diena. „Daiktų internetas ir dirbtinis intelektas padės parinkti gydymą“, 2016. https://kauno.diena.lt/naujienos/ivairenybes/mokslas-ir-it/daiktu-internetas-ir-dirbtinis-intelektas-pades-parinkti-gydyma-746243
27. „Kibernetinių nusikaltimų aukso amžius“. Eset, 2019.

https://www.eset.com/lt/apie/naujienos/straipsniai/ivykiai/saugumo-specialistas-dabar-kibernetiniu-nusikaltimu-aukso-amzius/

28. Cyber Security Insiders, 2019. https://www.cybersecurity-insiders.com/germany-strengthens-its-nations-cybersecurity-with-a-new-military-unit/
29. „Did your company encounter incidents concerning data theft, corporate espionage or sabotage during the last two years?“, Statista, 2020. https://www.statista.com/statistics/429724/cyber-attacks-directed-at-companies-germany/
30. „Reguliarių kibernetinių atakų taikinys – Vokietijos farmacijos kompanija“. Lrt, 2019. https://www.lrt.lt/naujienos/verslas/4/954971/reguliariu-kibernetiniu-ataku-taikinys-vokietijos-farmacijos-kompanija
31. „Kibernetinis saugumas prasideda nuo suvokimo“. Verslo žinio, 2019. https://www.vz.lt/verslo-valdymas/2019/11/15/kibernetinis-saugumas-prasideda-nuo-suvokimo
32. Gabrielė Bilevičiūtė, Justas Kidykas, Rūta Beinoriūtė. Kibernetinio saugumo tendencijos Lietuvoje ir pasaulyje. Smulkiojo ir vidutinio verslo situacija, 2019. http://kurklt.lt/wp-content/uploads/2019/10/Esama-situacija-su-VK.pdf?fbclid=IwAR0fRdHz1AlynqSTOUYMWKKteJGJ3P9Zjj36RhjsjuUpBTv79UBE7P7GDgU
33. Bendrais duomenų apsaugos reglamentas. (BDAR) https://gdpr.lt/
34. Duomenų apsaugos tarnyba. (DAT) https://dat.lt/
35. „BDAR reikalavimai. 10 žingsnių, kuriuos privalu žinoti.“ Be1st agency, 2019. https://www.be1st.agency/bdar-reikalavimai-10-zingsniu-kuriuos-privalu-zinoti/
36. NACIONALINĖ KIBERNETINIO SAUGUMO STRATEGIJA PATVIRTINTA Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818
37. „Asmens duomenų saugumo pažeidimai: skaičius ženkliai išaugo“. Teisinė rizika, 2019. https://teisinerizika.lt/2019/07/15/asmens-duomenu-saugumo-pazeidimai/
38. „Kibernetinis ir duomenų saugumas – svarbiausias prioritetas finansinių paslaugų rinkoje“. Teisė Pro, 2019. http://www.teise.pro/index.php/2019/11/15/kibernetinis-ir-duomenu-saugumas-svarbiausias-prioritetas-finansiniu-paslaugu-rinkoje/
39. „Kibernetinis saugumas 2018-aisiais: tendencijos ir didžiausi pavojai“. CodeAcademy, 2018. https://www.codeacademy.lt/kibernetinis-saugumas-2018-aisiais-tendencijos-ir-didziausi-pavojai/

40. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (Tekstas svarbus EEE)
41. LR Kibernetinio saugumo įstatymas. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee
42. „IoT Cyber Security for Cloud and Lifecycle Management“. IoT Analytics, 2017. https://iot-analytics.com/understanding-iot-cyber-security-part-2/
43. „Industry 4.0 Adoption 2020 – who is ahead?“. IoT Analytics, 2020. https://iot-analytics.com/industry-4-0-adoption-2020-who-is-ahead/
44. „Data Privacy Law in China: Comparison with the EU and U.S. Approaches“. Emmanuel Pernot, 2020. https://epernot.com/data-privacy-law-china-comparison-europe-usa/
45. „Cybersecurity Law of the People's Republic of China“. Iapp, 2017. https://iapp.org/resources/article/cybersecurity-law-of-the-peoples-republic-of-china-english-translation/
46. Štitilis, D., Paškauskas, Ž. (2007). Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. Socialinės technologijos. 2(92); p. 37–45.
47. Konvencija dėl elektroninių nusikaltimų. 2001 m. Lapkričio 23 d. Teisės aktų registras. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=228195&p_query=&p_tr2=.
48. Wired report. WannaCry ransomware: what is it and how to protect yourself, 22 May, 2017. http://www.wired.co.uk/article/wannacry-ransomware-virus-patch.
49. Štitilis, D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. Socialinės technologijos. 3(1), p. 189–207. http://www.mruni.eu/lt/mokslo_darbai/st/paskutinis_numeris/dwn.php?id=351638.
50. Trys ketvirtadaliai interneto naudotojų neatpažįsta grėsmių (2015-10-15). Lrytas.lt. http://it.lrytas.lt/ismanyk/trys-ketvirtadaliai-interneto-naudotoju-neatpazista-gresmiu.html
51. Asmens duomenys versle: Kaip sumažinti kibernetinių atakų pasekmes, 2017. http://www.vz.lt/informacines-technologijos-telekomunikacijos/2017/05/30/asmens-duomenys-versle-kaip-sumazinti-kibernetiniu-ataku-pasekmes

52. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymo Nr. IX-1132 1, 2, 3 ir 7 traipsnių pakeitimo įstatymas. 2014. Teisės aktų registras. https://www.e-tar.lt/portal/lt/legalAct/332e48b059ed11e487eff7b424bd0f08.

53. „Cyber attacks and IT security management in 2025“. Cyber security radar, 2018. https://www.radarservices.com/resources/study2025/

54. „Pavojingiausias ginklas interneto istorijoje, kuris dar neiššovė“. Telia, 2019. https://www.telia.lt/pranesimai-spaudai/didziausias-uztaisytas-ginklas-interneto-istorijoje-kuris-dar-neissove

55. „Top 10 most notorious cyber attacks in history“. Arnnet, 2018. https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

56. „What Are the Most Common Cyber Attacks?“. Cisco, 2019. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks

57. „Traditional endpoint solutions are just that. Traditional.“. Cisco, 2019. https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/best-antivirus-strategy.html

58. „Now live: IoT Network for Germany“. Telekom, 2020. https://www.telekom.com/en/media/media-information/archive/now-live-iot-network-for-germany-574364

SANTRAUKA LIETUVIŲ KALBA

Magistro baigiamojo darbo tikslas – Remiantis pasirinktų pasaulio šalių, ekspertų nuomone, bei atliktu kokybiniu tyrimu, pateikti pagrindines daiktų interneto įrenginių keliamas problemas kibernetiniam saugumui verslo įmonėse, pateikti pasiūlymų kaip jas išspręsti.

Šiandieninės technologijos ir elektroninio verslo plėtra verčia tobulėti ir modernizuotis net tradicinį verslą, o daiktų interneto įrenginiai padeda tai įgyvendinti bei palengvinti procesus. Daiktų internetas tai naujausiomis technologijomis paremti išmanieji įrenginiai esantys tinkle, kurie pagreitina ir palengvina verslo procesus, tačiau jiems sparčiai daugėjant vis daugiau įrenginių yra lengvai pažeidžiami ir nesaugūs, kas atveria naujus galimybes kibernetiniams nusikaltėliams pakenkti ir pasipelnyti iš verslo. Daiktų interneto ir saugumo sąsajos mažai išanalizuotos ir aprašytos. Magistro darbe, išanalizavus esamą teorinę medžiagą, kibernetinio saugumo ekspertų pastebėjimus, bei atlikus pasirinktų pasaulio šalių analizę bus pateiktos išvados kaip daiktų internetas pakeitė verslą bei jo kibernetinį saugumą.

Darbe taikyta mokslinės literatūros analizė kibernetinio saugumo ir daiktų interneto sąvokoms apibendrinti. Buvo pasirinkti ir išnagrinėti keturių pasaulio šalių statistiniai duomenys, kaip kiekvienoje daiktų internetas paveikė kibernetinio saugumo situaciją, kokias problemas iškėlė verslui, pateikti praktiniai pavyzdžiai. Remiantis šia šalių analize buvo išsiaiškinta ir pateikta pagrindinės daiktų interneto spragos ir konkretūs atvejai paveikę kibernetinio saugumo situaciją, bei kokių priemonių buvo imtasi. Taip pat buvo atliktas kokybinis nuomonių tyrimas, kuriame buvo apklausti 8 įmonių saugos specialistai. Tyrimu buvo siekta išsiaiškinti kaip plačiai Lietuvos įmonėse naudojamas daiktų internetas, kokios saugumo spragos vyrauja, kokiais būdais bandoma įsilaužti į įmonių sistemas, kokie daiktų interneto įrenginiai dažniausiai atakuojami ir taip pat sužinoti koks darbuotojų požiūris į kibernetines atakas daiktų interneto aspekte. Problemoms apibendrinti ir išspręsti sudarytas išvadų ir rekomendacijų sąrašas.

Darbą sudaro 4 dalys. Pirmoje darbo dalyje išanalizuotos daiktų interneto ir kibernetinio saugumo sąvokos, bei įtaka verslui. Antroje dalyje buvo analizuojamos 4 pasirinktos pasaulio šalys: JAV, Kinija, Vokietija ir Lietuva. Buvo nagrinėjami konkretūs pavyzdžiai bei daiktų interneto plėtros problemos. Trečioje dalyje buvo nagrinėjamos daiktų interneto keliamos problemos kibernetiniam saugumui ir atskiriems sektoriams, remiantis analize buvo sudarytas saugaus įrenginio modelis. Ketvirtoje dalyje nagrinėjamas kokybinis tyrimas, kuriuo buvo norima išsiaiškinti pagrindines apklaustų įmonių kibernetinio saugumo problemas, kurias sukelia daiktų interneto įrenginiai ir kaip jie visa tai sprendžia.

SANTRAUKA ANGLŲ KALBA

The aim of the master's thesis - Based on the probable main issues raised by the world's countries, experts, performers and high-quality researchers on the Internet of Things devices, when cyber security is specific to businesses, presenting how to find out.

Today’s technology and e-business development will be improved and modernized. The Internet of Things is the best of all electronic devices that are upgraded and make the business process easier, and some of the new devices are easy to assimilate and secure. The interfaces between the Internet of Things and security are poorly analyzed and described. In the master's thesis, after analyzing the existing theoretical material, the observations of cyber security experts, as well as the selection of performers, the analysis of the world's countries will be prepared as a version of the Internet of Things package and its cyber security.

The analysis of the scientific literature is applied in the work to summarize the concepts of cyber security and the Internet of Things. Statistics from four countries around the world on how the Internet of Things has affected the cyber security situation, what problems it has posed to business have been selected and analyzed, and practical examples have been provided. Based on this country analysis, the main gaps in the Internet of Things and the specific cases that affected the cyber security situation were identified and presented, as well as the measures taken. A qualitative opinion poll was also conducted, in which safety specialists from 8 companies were interviewed. The aim of the study was to find out how widely used the Internet of Things in Lithuanian companies, what security vulnerabilities prevail, in what ways attempts are made to hack into corporate systems, which IoT devices are most often attacked and also to find out employees' attitudes towards cyber attacks. A list of conclusions and recommendations has been compiled to summarize and solve the problems.

The work consists of 4 parts. The first part of the work analyzes the concepts of the Internet of Things and cyber security, as well as the impact on business. In the second part, was selected 4 countries of the world were analyzed: the USA, China, Germany and Lithuania. Specific examples and problems of the development of the Internet of Things were examined. In the third part, the issues posed by the Internet of Things for cyber security and individual sectors were examined, and a model of a secure device was developed based on the analysis. The fourth part examines a qualitative study that sought to elucidate the main cyber security issues of the companies surveyed caused by IoT devices and how they address all of this.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Magistro baigiamajame darbe susipažinus su kibernetinio saugumo ir daiktų interneto teorine medžiaga, buvo pateikta tarpusavio priklausomybė ir įtaka verslo saugumui diegianti daiktų interneto įrenginiu. Išanalizavus pasirinktų šalių pavyzdžius, kibernetinio saugumo ekspertų nuomonę apie pagrindines daiktų interneto architektūros problemas taip pat atlikus kokybinį tyrimą buvo išsiaiškintos pagrindinės daiktų interneto keliamos problemos kibernetiniam saugumui bei galimi jų sprendimo būdai ir priemonės. Pirmoje dalyje nagrinėjami teoriniai aspektai bei kaip daiktų interneto atsiradimas pakeitė saugumo situaciją versle. Antroje – analizuojami JAV, Kinijos, Vokietijos, Lietuvos šalių pavyzdžiai, esama situacija, daiktų interneto diegimo tendencijos. Trečioji dalis skirta išnagrinėti kodėl daiktų internetas nesaugus naudoti ir kas tai lemia, kokie žingsniai norint tinkamai apsaugoti.

Pagrindiniai žodžiai: daiktų internetas, e. verslas, kibernetinis saugumas, kibernetinės atakos, daiktų interneto apsauga, kibernetinės atakos.

In the master degree after knowing theoretical material of cyber security and the Internet of Things, the interdependence and influence on the security of the business implementing the Internet of Things device was presented in the master 's thesis. After analyzing the examples of selected countries, the opinion of cyber security experts on the main problems of the Internet of Things architecture, as well as a qualitative study, the main problems of the Internet of Things for cyber security and possible solutions and tools were clarified. The first part examines the theoretical aspects and how the emergence of the Internet of Things has changed the security situation in business. The second part analyzes the examples of the USA, China, Germany, and Lithuania, the current situation, and the tendencies of the Internet of Things. The third part is devoted to examining why the Internet of Things is unsafe to use and what determines it, what steps to take to protect it properly.

Key words: Internet of Things, e. business, cyber security, cyber attacks, IoT protection, cyber attacks.

PRIEDAI

Priedas 1. Tyrime naudota anketa

Laba diena, gerbiamas (-oji) eksperte. Aš, Mykolo Romerio universiteto Kibernetinio saugumo valdymo magistro studijų studentas, atlieku tyrimą „Kibernetinio saugumo užtikrinimas įmonėse: daiktų interneto aspektas".

Pereinant prie e. verslo, jį modernizuojant daiktų internto įrenginiais atsiranda grėsmė kibernetiniam saugumui, dėl netinkamo įrenginių apsaugojimo būdų. Šio tyrimo tikslas - pasitelkiant ekspertų žinias, išsiaiškinti kibernetinių atakų rūšis, apsisaugojimo būdus, ar tinkamai yra apsaugoti įrenginiai įmonėse, išnagrinėti konkrečius pavyzdžius.

Šio tyrimo metu surinkta informacija bus pateikta tik apibendrinta forma. Šioje anketoje Jūsų pateikti duomenys viešai nebus skelbiami. Maloniai prašome Jūsų atsakyti į pateiktus klausimus.

Pažymėkite atsakymus apibraukdami/ pabraukdami tinkamą (-us) variantą (-us).

Anketos su atsakytais klausimais lauksiu el. paštu: ***deividas.am@gmail.com***

1. Kiek daiktų interneto įrenginių naudoja jūsų įmonė? (išskyrus kompiuterius)
   a) iki 10
   b) 10-20
   c) 20-50
   d) 50 ir daugiau

2. Kiek vidutiniškai per metus patiriate bandymų įsilaužti į jūsų įmonės įrenginius?

   a) iki 10
   b) 10-20
   c) 20-30
   d) 30-50

3. Kokiems tikslams pasiekti dažniausiai atakuojami įrenginiai?

_____

_____

_____

_____

4. Kokie įrenginiai tampa dažniausiu atakų taikiniu?

_____

_____

_____

_____

5. Kokiais būdais dažniausiai bandoma įsilaužti? (atakų rūšys) (***DNS vagystės***, ***Duomenų vagystė („phishing“)***, ***Inframe“ injekcija, Tikslinės atakos***, ***„SQLi“ ir t.t)***

_____

_____

_____

_____

6. Kaip apsaugojate savo įrenginius ir daiktus nuo kibernetinių atakų? Per kuriuos įrenginius bandoma Įsilaužti dažniausiai?

_____

_____

7. Įvertinkite nuo 1-10 jūsų įmonės darbuotojų pasiruošimą ir gebėjimą atpažinti kibernetinius incidentus?

_____

_____

Dėkojame už jūsų atsakymus ir sugaištą laiką!

Forma patvirtinta

Mykolo Romerio universiteto

Senato 2016 m. gegužės 9 d. nutarimu Nr. 1SN-44

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020 - 04 - 16
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

_____**Ekonomikos ir verslo fakultetas, kibernetinio saugumo valdymas**_____
(fakulteto / instituto, programos pavadinimas)

Studentas (-ė) **Deividas Ambrulevičius**__ _____
_____,
(vardas, pavardė)

patvirtinu, kad šis **magistro baigiamasis darbas**:

„**Kibernetinės grėsmės ir kibernetinio saugumo užtikrinimas įmonėse: daiktų interneto aspektas“**

_____:
(*baigiamojo darbo pavadinimas*)

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 nurodymais.

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

_____ **Deividas Ambrulevičius**
(parašas) *(vardas, pavardė)*