VšĮ Investuok Lietuvoje

Atviros Vyriausybės iniciatyvos

Lietuvos konkurencingumo didinimas kibernetinio saugumo industrijoje

Teminio tyrimo

Kokie yra Lietuvos konkurencingumo didinimo kibernetinio saugumo industrijoje iššūkiai ir galimybės?

ATASKAITA

Ieva Namavičiūtė

Vilnius

2018

Kuriame Lietuvos ateitį
2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Turinys

1. Santrumpos

KS – Kibernetinis saugumas

LR – Lietuvos Respublika
KAM – Krašto apsaugos ministerija
JK – Jungtinė Karalystė
JAV – Jungtinės Amerikos Valstijos

2. Įvadas

Valstybinės įstaigos, privačios įmonės ir individai vis daugiau dėmesio skiria kibernetiniam saugumui (KS) ir jo svarba neabejojama. Valstybės nacionaliniu lygmeniu rengia KS strategijas ir vis daugiau pinigų tam skiria biudžetuose. Didėjantys atakų skaičiai ir jų padariniai, žmonių neatsparumas kibernetinėms grėsmėms, įsigaliojantys nauji duomenų apsaugos reikalavimai ES lygmeniu ir didžiuliai finansiniai nuostoliai kuria vis didesnį kibernetinio saugumo specialistų poreikį.

Kibernetinio saugumo specialistų trūkumas jaučiamas visame pasaulyje. Prognozuojama, kad jau 2020 metais bus 3,5 milijonai laisvų darbo vietų kibernetinio saugumo srityje visame pasaulyje. Lietuva – ne išimtis. Remiantis asociacijos „Infobalt“ turimai duomenimis čia jau dabar jaučiamas aukštos kvalifikacijos specialistų trūkumas, o 2020 metais reikės 13300 IT specialistų iš kurių, bent 700 internetinio saugumo specialistai. „Investuok Lietuvoje“ duomenimis, šiuo metu Lietuvoje yra apie 100 sertifikuotų kibernetinio saugumo specialistų ir 229 studentai kibernetinio saugumo bakalauro ir magistro programose.

Užsienio investuotojai, kaip vieną svarbiausių kriterijų pasirenkant šalį įvardina talentus. Taigi siekiant, kad Lietuva taptų dar konkurencingesnė kibernetinio saugumo industrijoje ir pritrauktų tiesioginių užsienio investicijų šioje srityje, privalu investuoti į KS gebėjimų, atitinkančių rinkos poreikius, vystymą. Tačiau, KS specialistai yra svarbūs ne tik investicijoms pritraukti, bet ir kibernetinės erdvės bei valstybės saugumui užtikrinti.

Šio tyrimo tikslas – apžvelgti pasaulines KS tendencijas ir KS specialistų padėtį Lietuvoje. Taip pat išanalizuoti gerąsias užsienio šalių praktikas, siekiant atrasti efektyvių, Lietuvoje pritaikomų pavyzdžių.

Pirmąja tyrimo dalimi siekiama apžvelgti esamą situaciją pasaulyje: išsiaiškinti kokios vyrauja pasaulinės tendencijos KS srityje, koks yra KS specialistų poreikis bei reikalavimai jiems. **Antrąja tyrimo dalimi** siekiama išsiaiškinti kibernetinio saugumo specialistų padėtį Lietuvoje: išsiaiškinti kiek ir kokių KS specialistų turime šiuo metu bei kas ruošia juos ruošia, kokios mokymų galimybės. **Trečiąja tyrimo dalimi** siekiama išanalizuoti gerąsias užsienio praktikas ir išsiaiškinti, kaip kitos valstybės kovoja su KS specialistų trūkumų, kokių iniciatyvų imamasi, atrasti geriausias praktikas, kurios galėtų būti pritaikytos Lietuvoje.

2.1. Tyrimo pagrindimas

Kibernetinio saugumo svarba, investicijų pritraukimas ir specialistų, atitinkančių rinkos poreikius ruošimas pabrėžiami svarbiausiuose LR strateginiuose dokumentuose:

1. 17-osios LR Vyriausybės programa, patvirtinta 2016 m. gruodžio 13 d. Nr. XIII-82 nutarimu, teigia:

   197.16. Sukursime palankias sąlygas Lietuvos informacinių ir ryšių technologijų sektoriaus konkurencingumui vietinėje bei užsienio rinkose, skatinsime valstybės, verslo ir mokslo bendradarbiavimą, finansavimą skirsime vietinei ir tarptautinei rinkoms aktualių inovacijų kūrimui.

2. 17-osios LR Vyriausybės programos įgyvendinimo plane, patvirtinto 2017 m. kovo 13 d. Nr. 167 nutarimu, numatyti darbai:

   2.1.3. Darbas. Profesinio mokymo ir aukštojo mokslo studijų turinio ir metodų atnaujinimas, orientuojantis į konkurencingų XXI a. kompetencijų suteikimą.

   5.2.1. Darbas. Kibernetinių incidentų prevencija ir valdymo sistemos tobulinimas.

Savo projektu prisidėsiu prie aukščiau išvardytų prioritetų ir jiems pasiekti numatytų darbų įgyvendinimo.

Projektu siekiama padidinti Lietuvos konkurencingumą kibernetinio saugumo industrijoje, prisidedant prie tiesioginių užsienio investicijų pritraukimo ir šalies saugumo didinimo. „Kurk Lietuvai“ parengti pasiūlymai taps pagrindu tolesniam „Investuok Lietuvoje“, KAM ir kitų valstybės institucijų ir privataus sektoriaus, bei švietimo ir mokslo įstaigų tolesniam bendradarbiavimui KS švietimo ir valstybės saugumo srityse.

3. Dėstymas

3.1. Metodologija

Nagrinėjant Lietuvos konkurencingumo didinimo kibernetinio saugumo industrijoje galimybes ir iššūkius buvo pasitelkti trys analizės metodai.

Pirmiausiai analizuojamos **pasaulinės kibernetinio saugumo tendencijos ir specialistų poreikis**. Pasitelkiat pirminius ir antrinius šaltinius, buvo apžvelgtos pasaulinės tendencijos KS industrijoje, investicijų augimas, laisvų darbo vietų didėjimas ir specialistų trūkumas. Taip pat buvo apžvelgti populiariausi ir vertingiausi sertifikatai KS srityje pasaulyje.

Apžvelgus pasaulines tendencijas, buvo analizuojama **kibernetinio saugumo specialistų padėtis Lietuvoje**. Buvo siekiama išsiaiškinti kiek ir kokių specialistų kibernetinio saugumo srityje turime Lietuvoje, kokios švietimo įstaigos ruošia KS specialistus ir kokios yra sertifikavimo galimybės.

Trečiame tyrimo etape buvo atliekama **geruųjų užsienio šalių praktikų analizė**. Buvo siekiama išsiaiškinti, kokiais būdais kitos valstybės kovoja su specialistų trūkumais, apžvelgtos Nacionalinės kibernetinio saugumo strategijos ir privačios iniciatyvos.

3.2. Esamos situacijos analizė: pasaulinės kibernetinio saugumo tendencijos ir specialistų poreikis

Šioje analizėje buvo apžvelgta KS situacija pasaulyje ir nuostoliai patiriami po kibernetinių atakų, taip pat aptartos investicijos ir pardavimai KS produktų ir paslaugų. Detaliau pristatytos KS subindustrijos ir reikalavimai specialistams, bei apžvelgtas KS specialistų trūkumas pasaulyje. Pristatyti ir populiariausi ir reikšmingiausi KS sertifikatai (žr. priedą nr.1).

Analizė parodė, kad kibernetinio saugumo industrija sparčiai auga: kuriasi vis daugiau KS įmonių, investuojama vis daugiau pinigų į KS. Nuo 2005 metų KS paslaugų ir produktų pardavimai išaugo net 34 kartus, o investicijos į šias paslaugas ir produktus išaugo net 3 kartus nuo 2013 metų ir siekia beveik 8 milijardus. Tai yra dar viena sritis, kur kiekviena valstybė gali išsiskirti kurdama naujas KS įmones ir pritraukiant investicijas.

Analizės metu pastebėta, kad inovacijas KS srityje kuriančios valstybės susiduria su bendru iššūkiu – kibernetinio saugumo specialistų trūkumas. Prognozuojama, kad 2021 metais pasaulyje bus apie 3,5 milijonai laisvų darbo vietų KS srityje ir pagal atliktus tyrimus, net 68% organizacijų pripažįsta, jog jaučia šių specialistų poreikį. Pasaulyje didėjantis laisvų darbo vietų skaičius KS srityje, tik parodo, koks didelis yra specialistų poreikis ir kokiu sparčiu greičiu auga ši industrija.

Kibernetinio saugumo industrijoje yra išskiriamos dvi sritys – KS paslaugos ir KS produktai. Specialistams, yra keliami skirtingi reikalavai kiekvienoje šių sričių. Iš KS produktų kūrėjų reikalaujama kiek paprastesnių kvalifikacijų ir sertifikavimas dažniausiai nėra būtinas, tačiau paslaugų kūrėjams yra keliami aukšti reikalavimai. Bendrai kalbant, kibernetinio saugumo specialistams yra keliami aukšti reikalavimai ir pakankamas jų kiekis šalyje gali ne tik užtikrinti valstybės saugumą, bet ir pritraukti užsienio investicijas.

Pasaulyje yra nemažai įvairių KS srityje pripažįstamų sertifikatų, tačiau analizės metu buvo atrasti ir apžvelgti TOP 10 sertifikatų 2018 metams, kuriuos labiausiai vertina darbdaviai pasaulinėje rinkoje. Visiems sertifikatams gauti yra keliami skirtingi reikalavimai ir vien egzamino nepakanka. Dažniausiai reikalaujamas ir atitinkamas išsilavinimas ar darbo patirtis. Viena iš pasaulinių organizacijų sertifikatams ruošia specialistus ir Lietuvoje.

Analizė leidžia daryti išvadą, kad auganti KS industrija yra puiki galimybė kiekvienai šaliai kurti palankią terpę steigtis KS verslams. Atsižvelgiant į tai, koks yra KS specialistų trūkumas, investavimas į šių specialistų rengimą, gali būti puiki galimybė valstybei išsiskirti ir pritraukti užsienio investicijas, bei plėtoti KS klasterį šalyje. Kibernetinio saugumo užtikrinimas yra labai svarbus tiek valstybėms, tiek kiekvienai įstaigai. Todėl kiekviena valstybė turi į tai investuoti, ugdyti KS gebėjimus ir prisidėti prie saugios kibernetinės erdvės kūrimo.

3.3. Kibernetinio saugumo specialistų padėtis Lietuvoje

Išanalizavus pasaulines kibernetinio saugumo tendencijas buvo apžvelgiama ir KS specialistų padėtis Lietuvoje. Buvo svarbu detaliau apžvelgti Lietuvoje jau veikiančias KS įmones, specialistų kiekį ir jų trūkumą, bei mokslo, studijų ir sertifikavimo galimybes šalies viduje (žr. priedą nr.1).

Visų pirma, verta paminėti, kad ir Lietuvoje jau kuriasi KS įmonės ir jų šiuo metu šalyje yra 35. Kai kurios jų yra orientuotos į produktų arba paslaugų kūrimą, kai kurios konsultacines paslaugas teikiančios įmonės. Tai gi, KS verslo užuomazgų yra ir Lietuvoje, tačiau dauguma šių įmonių buvo sukurtos Lietuvoje, tikslingai šios srities įmonės iki šiol nebuvo pritraukiamos.

Analizė parodė, kad KS specialistai yra ypatingai svarbūs ir kiekvienai įmonei, nes po sėkmingų atakų patiriami nuostoliai yra milžiniški, kuriuos patiria ir Lietuvos įmonės. Šiuo metu Lietuvoje turime apie 100 sertifikuotų KS specialistų, apie 250 IT specialistų dirbančių KS įmonėse, 229 studentus, besimokančius KS specialybėse. Prognozuojama, kad iki 2020 metų Lietuvoje reikės papildomai iki 700 kibernetinio saugumo specialistų.

Lietuvoje, dar mokykloje vaikai yra mokomi kaip saugiai elgtis internete. Daugiausiai kalbama apie turinio atsirinkimą, o kibernetinė sauga nėra gausiai išskiriama. Siekiant pritraukti daugiau užsienio investicijų kibernetinio saugumo srityje reikia turėti pakankamai aukštos kvalifikacijos specialistų. Tačiau vien to nepakanka ir labai svarbu kelti bendrą visuomenės suvokimo lygį, kad žmonės taptų atsparesni vykstančioms atakoms ir incidentams. Talentus ugdyti reikia nuo mažų dienų, siekiant juos sudominti ir įtraukti, kad ateityje jie norėtų tapti KS specialistais.

Apžvelgus studijų programas pastebėta, kad KS specialistus ruošia 5 universitetai Lietuvoje ir galima rinktis iš bakalauro ar magistro studijų. Šios programos yra naujos ir viso, kvalifikacinį laipsnį jose yra įgiję 33 studentai. Šių programų kokybė nėra ištirta, todėl nėra aišku, kokie specialistai išeina į rinką. Pasaulyje yra vertinami tarptautiniai KS saugumo sertifikatai, o Lietuvos aukštojo mokslo programos to nesiūlo. Tačiau, Lietuvoje yra įsikūrusi tarptautinė organizacija, kuri administruoja 4 globaliai pripažintas profesionalų sertifikatus IT audito, saugos, valdymo ir rizikos profesionalams. Taip pat, Lietuvoje yra įsikūrusios kelios įmonės, kurios teikia įvairius KS mokymus vartotojams ir įmonių darbuotojams. Yra sudaromos sąlygos su kibernetinėmis atakomis kovoti tikrovėje ir gauti realių praktinių žinių, kurių labiausiai ir reikia KS srityje.

Apibendrinant, Lietuvoje yra daug IT specialistų, tačiau KS specialistų skaičius nėra didelis. Specialistų trūkumas jaučiamas jau dabar, o po kelių metų jų reikės dar daugiau. Tad dabar yra puikus metas investuoti ir į visuomenės atsparumo kibernetinėms grėsmėms didinti, ir į aukštos kvalifikacijos specialistų ugdymą. Kadangi pasaulyje KS srityje specialistų trūksta milijonais, Lietuva galėtų pasinaudoti šiuo šansu ir sukurti pasiūlą, atitinkančia rinkos poreikius. Tokiu būdu Lietuva galėtų pritraukti įmones kuriančias KS produktus ar paslaugas globalioms rinkoms.

3.4. Užsienio šalių gerųjų praktikų analizė

Atliekant analizę buvo apžvelgiamos gerosios užsienio praktikos vystant KS talentus. Šios tyrimo dalies tikslas yra surasti gerų pavyzdžių, kurie veikia užsienyje siekiant išugdyti KS talentus, kurie galėtų būti pritaikyti Lietuvoje.

Atlikus pirminę informacijos paiešką ir apžvelgus įvairių valstybių pavyzdžius, detalesnei analizei buvo pasirinktos šios šalys: Jungtinė Karalystė (JK), Jungtinės Amerikos Valstijos (JAV), Lenkija ir Čekija (žr. priedą Nr.2). Šalių pasirinkimą nulėmė keli faktoriai: dvi valstybės pasirinktos, kaip pirmaujančios KS srityje ir dvi artimesnės Lietuvai savo istorinėmis ir ekonominėmis aplinkybėmis. JK ir JAV turi vienus didžiausius skaičius KS specialistų, tačiau jų trūkumas yra taip pat vienas didžiausių pasaulyje būtent šiose šalyse.

Atliekant užsienio praktikų analizę buvo apžvelgtos šių valstybių KS strategijos ir koks dėmesys jose tenka švietimui, buvo analizuojami įvairūs internetiniai šaltiniai ir duomenų bazės. Apibendrinus užsienio praktikų analizės rezultatus matomos šios tendencijos:

- Visos išnagrinėtos šalys rūpinasi KS ir tai atsispindi jų strategijose, bei kituose nacionaliniuose dokumentuose. Į kibernetinę saugą valstybės investuoja vis daugiau pinigų, ruošia KS strategijas ir kitus dokumentus, siekiant užtikrinti valstybės saugumą.

- Visos analizuotos valstybės KS pradėjo rūpintis skirtingais laikotarpiais, o pirmoji jų JAV, kuri pirmąją strategiją išleido dar 2003 metais. JAV ir UK yra žymiai toliau pažengę KS srityje, todėl visų šių strategijų tarpusavyje lyginti nereikėtų, tačiau visoms joms yra būdingi keli bruožai:
  - Ypatingas dėmesys skiriamas KS švietimui, visuomenės informavimui ir specialistų ruošimui;
  - Pabrėžiamas privataus sektoriaus, viešojo sektoriaus ir akademijos bendradarbiavimas įgyvendinant strateginius tikslus, kuris yra ypatingai svarbus norint pasiekti geresnių rezultatų;
  - Daugiausiai švietimo iniciatyvių inicijuoja Krašto apsaugos ministerijos, Nacionaliniai kibernetinio saugumo centrai ar kitos atitinkamos institucijos.

Užsienio praktikų analizė parodė, kad iš kiekvienos valstybės Lietuva galėtų pasimokyti ir gerąsias praktikas pritaikyti KS švietime ir talentų ugdyme. Nors JK kibernetine sauga rūpinasi ilgiau nei Lietuva, jų rengiamos iniciatyvos yra puikūs pavyzdžiai. Vienas tokių „CyberFirst“ programa, kurią iniciavo Kibernetinio saugumo centras bendradarbiaujant su privačiu sektoriumi. Ši programa įtraukia vaikus nuo 11 metų iki studentų. Programos metu rengiami įvairūs konkursai mergaitėms ir tai leidžia valstybei išsiskirti. JAV savo kibernetinės erdvės saugumu rūpinasi jau 15 metų ir per tą laiką rengė įvairias iniciatyvas. Viena tokių buvo pradėta 2013 metais, kai Valstybinis saugumo departamentas pradėjo iniciatyvą, kurios metu buvo sukurtas internetinis šaltinis, kur galima rasti visą informaciją apie mokymus, studijas, informavimo programas ir pan. KS srityje. Šaltinis prieinamas visiems ir skirtas įvairioms auditorijoms. Iš Lenkijos galime pasimokyti ryžtingumo. Ši šalis nusprendė, jog nori tapti KS industrijos lydere. Buvo atlikti tyrimai, kurių metu išryškėjo Lenkijos potencialas ir jie bandys ryžtingai to siekti. Tyrimo metu buvo numatyti tikslai, ką ir kaip riktų daryti, norint tapti lydere. Lietuva turi šansą neatsilikt ir imtis atitinkamų veiksmų, siekiant išsiskirti ir rasti savo pranašumus KS srityje. Čekijos KS strategijos veiksmų planas yra puikus pavyzdys, kurio uždavinius galima pritaikyti ir kuriant Lietuvos Nacionalinę kibernetinio saugumo strategiją.

Akivaizdu, kad KS švietimui, mokymams ir visuomenės informavimui privaloma skirti ypatingą dėmesį, norint tapti saugia ir sėkminga šalimi KS srityje. Užsienio praktikų analizė nurodė aiškų poreikį ir kryptis viešajai konsultacijai vykdyti.

4. Išvados

Atlikus esamos situacijos ir užsienio šalių praktikų analizę buvo prieita išvadų, kad Lietuva turi galimybę, koncentruotai dirbant kelti KS švietimo ir visuomenės sąmoningumo lygį, bei tapti dar konkurencingesne valstybe KS industrijoje. Matoma, kad Lietuvoje jau yra KS švietimo užuomazgų, nes yra net kelios studijų programos, bei privačių mokymų galimybės, tačiau tai nėra vykdoma nacionaliniu mastu. Studijų ir mokymų kokybė taip pat nėra aiški, kaip ir nėra aišku ar studentai išeinantys į rinką atitinka jos poreikius. Analizė parodė, kad stipriausios valstybės KS industrijoje, daug investuoja į švietimą ir specialistų ruošimą, tad šiuo pavyzdžiu galėtų sekti ir Lietuva. Mes, kaip valstybė turime puikų šansą susitelkti ir tapti išskirtine valstybe, turinti stiprius aukštos kvalifikacijos KS specialistus. Analizės metu nustatyta, kad yra būtinas viešojo sektoriaus, privataus sektoriaus ir akademijos bendradarbiavimas, siekiant ryškesnių rezultatų. Valstybė turėtų daugiau investuoti į KS švietimą ir talentų ugdymą, tokiu būdu ne tik pritraukiant užsienio investicijas, bet ir prisidedant prie bendros kibernetinės erdvės ir valstybės saugumo užtikrinimo.

Identifikavus pagrindines problemas, matome, kad šiuo metu svarbiausia sudaryti veiksmų planą valstybinių lygiu, įtraukiant viešojo ir privataus sektoriaus, bei akademijos atstovus, kaip būtų galima padidinti KS specialistų skaičių ir kokybę Lietuvoje. Pradėti reikėtų nuo mokyklų programų, universitetų programų peržiūrų, rinkos tyrimų ir galbūt informavimo kampanijų plačiajai visuomenei.

Išnagrinėjus problemą ir identifikavus galimus sprendimo būdus, išryškėjo poreikis rengti viešąją konsultaciją, kurios metu bus siekiama atsakyti į kilusius klausimus:

- Kokių specialistų reikia Lietuvoje;
- Koks yra KS specialistų poreikis viešajame sektoriuje;
- Kaip privatus sektorius pritraukia ir ruošia savo darbuotojus, bei su kokiais iššūkiais susiduria;
- Kokios kvalifikacijos ir įgūdžiai reikalingi užsienio investuotojams;
- Kaip vertinami diplomai ir įvairūs sertifikatai Lietuvoje bei užsienyje.

Siekiant atsakyti į šiuos klausimus, kilo poreikis rengti viešąją konsultaciją su KS įmonėmis veikiančiomis Lietuvoje, viešojo sektoriaus įstaigomis atsakingoms už KS, universitetais, užsienio įmonėmis, bei kitomis suinteresuotomis šalimis. Konsultacijos metu bus siekiama gauti atsakymus į iškilusius klausimus.

Suinteresuotos šalys: „Investuok Lietuvoje“, Krašto apsaugos ministerija, „Infobalt“, KS įmonės, universitetai, studentai, IT specialistai, Nacionalinis kibernetinio saugumo centras, Vidaus reikalų ministerija.

Numatomi konsultacijų tikslai: išsiaiškinti koks ir kokių KS specialistų poreikis yra privačiame ir viešajame sektoriuose, bei išsiaiškinti užsienio įmonių KS specialistų poreikį investuojant į kitas šalis. Identifikavus rinkos poreikius, bus konsultuojamasi su suinteresuotomis šalimis dėl atitinkamų veiksmų įgyvendinimo.

Viešajai konsultacijai rengti nuspręsta vykdyti interviu ciklą apklausiant KS įmones Lietuvoje ir viešojo sektoriaus atstovus, bei vykdant užsienio įmonių apklausa „Infosecurity“ parodos metu Londone. Rezultatai bus pristatomi VšĮ „Investuok Lietuvoje“ ir Krašto apsaugos ministerijai.

Siekiant užtikrinti konsultacijos kokybę, atsirenkant dalyvius bus konsultuojamasi su Krašto apsaugos ministerija, VšĮ „Investuok Lietuvoje“ ir nacionalinio informacinių ir ryšių technologijų sektoriaus asociacija „Infobalt“. Remiantis atlikto tyrimo duomenimis, prieš pradedant konsultacijas, bus parengta metodinė medžiaga ir pasiruošta konsultacijų metu gautos medžiagos sisteminimui ir analizavimui.

Konsultacijų rezultatai bus pristatomi VšĮ „Investuok Lietuvoje“ ir KAM ir pristatyti viešai visuomenei. Remiantis šiais rezultatais bus parengti pasiūlymai Nacionalinės kibernetinio saugumo strategijos tarpinstituciniam veiklų planui.

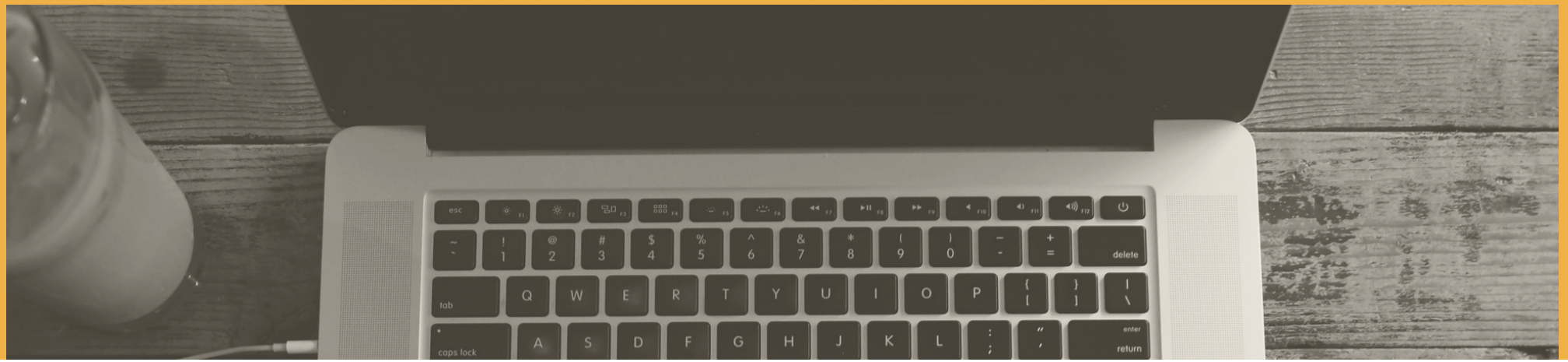
5. *Naudota literatūra/ šaltiniai*

http://www.taxpayer.net/national-security/cyberspending-database/
https://thebestvpn.com/cyber-security-statistics-2018/
https://lietuvosdiena.lrytas.lt/aktualijos/2017/09/29/news/dalia-grybauskaite-butina-isteigti-es-kibernetines-greitojo-reagavimo-pajegas-2748919/
https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#78c3320b4947
http://www.businessinsider.com/cybersecurity-startups-raked-in-76-billion-in-vc-money-in-2017-2018-1
https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg
http://cyberseek.org/pathway.html
https://www.csoonline.com/article/3235961/security/largest-cybersecurity-venture-capital-deals-in-2017.htmlhttps://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#46a657345163
https://thebestvpn.com/cyber-security-statistics-2018/
https://cybersecurityventures.com/jobs/
https://www.consultancy.uk/news/16068/majority-of-companies-now-hit-by-a-cybersecurity-skills-gap
https://www.csoonline.com/article/3116884/security/top-cyber-security-certifications-who-theyre-for-what-they-cost-and-which-you-need.html
https://www.knowledgenet.com/certifications/2018s-top-ten-cybersecurity-certifications/
https://certification.comptia.org/certifications?level=cybersecurity
https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html
https://www.isc2.org/#
http://www.isaca.org/CERTIFICATION/Pages/default.aspx
http://www.comptiastore.eu/product-p/pvcomptiacasp-euro.htm
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
https://www.consultancy.uk/news/16068/majority-of-companies-now-hit-by-a-cybersecurity-skills-gap

https://www.cyberfirst.ncsc.gov.uk/girlscompetition/
https://www.ncsc.gov.uk/new-talent
https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf
https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
https://www.csoonline.com/article/3258994/data-protection/cybersecurity-skills-shortage.html
https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf
https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies
https://niccs.us-cert.gov/about-niccs
https://stopthinkconnect.org/about
https://pl.asseco.com/en/news/poland-may-become-a-global-leader-in-the-cyber-security-sector-the-report-of-the-kosciuszko-institute-2482/
http://www.ik.org.pl/wp-content/themes/ik/report-img/security-through-innovation.pdf
https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSO_Poland_2017.pdf
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf
https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf
https://ccdcoe.org/sites/default/files/multimedia/pdf/The%20Czech%20Republic.%20A%20Case%20of%20a%20Comprehensive%20Approach%20toward%20Cyberspace_Lucie%20Kadlecov%C3%A1.pdf
http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_czechrepublic.pdf
VšĮ „Investuok Lietuvoje“ duomenys

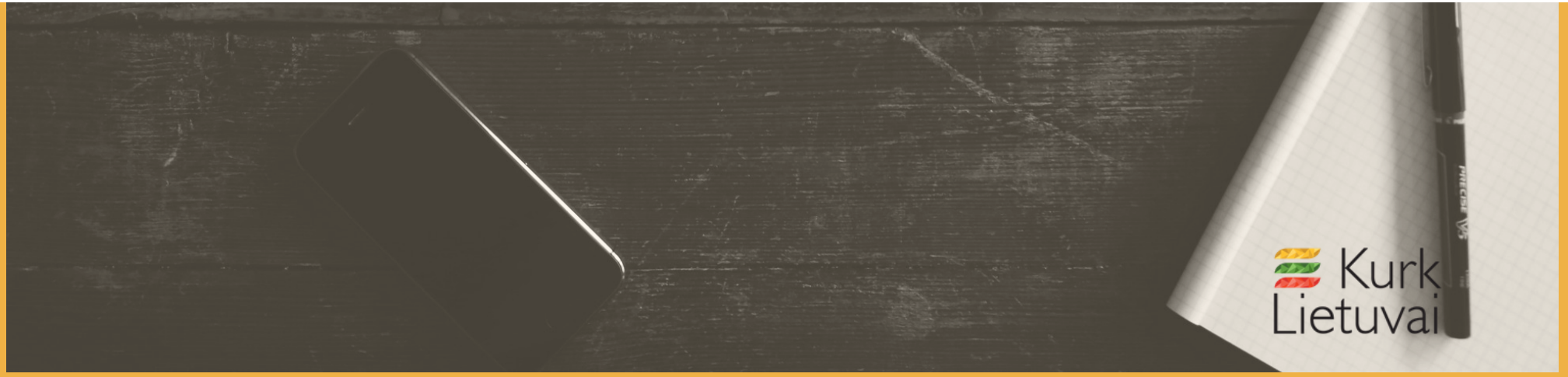
6. Priedai

1. Esamos situacijos analizė
2. Užsienio gerųjų praktikų analizė



Pasaulinių kibernetinio saugumo (KS) industrijos tendencijų ir KS specialistų padėties Lietuvoje apžvalga

IEVA NAMAVIČIŪTĖ



1. Pasaulinės tendencijos kibernetinio saugumo industrijoje

IEVA NAMAVIČIŪTĖ

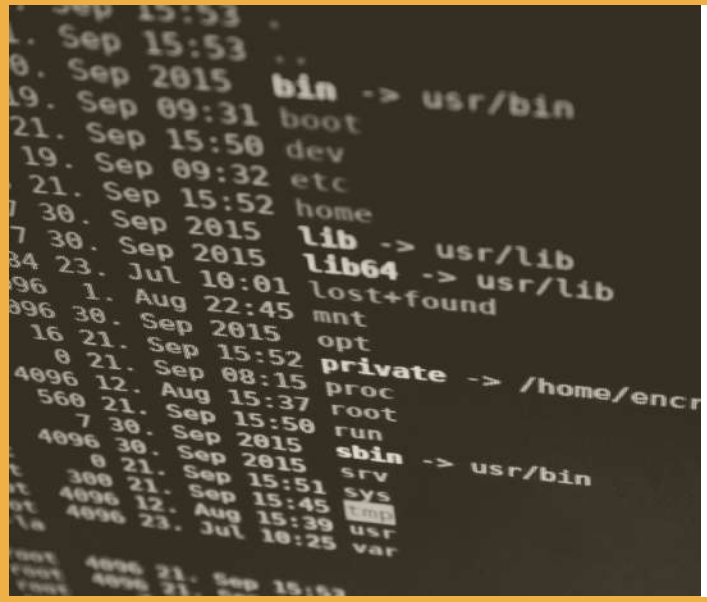
Kibernetinis saugumas

Kibernetinis saugumas (KS)– visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti (LR kibernetinio saugumo įstatymas).

Kurk Lietuvai

Apžvalga

Kibernetinių atakų skaičiui augant kiekvieną dieną, kibernetinio saugumo svarba nebeabejoja niekas. Kiekviena įstaiga, valstybė patiria vis daugiau nuostolių, tad valstybiniu mastu yra kuriamos strategijos, vis daugiau pinigų skiriama kibernetinio saugumo užtikrinimui ir valstybių biudžetuose. Štai pavyzdžiui JAV 2016 metais KS išleido 28 milijardus JAV dolerių ir tai viršija daugelio valstybių bendrus biudžetus 2017 metams.



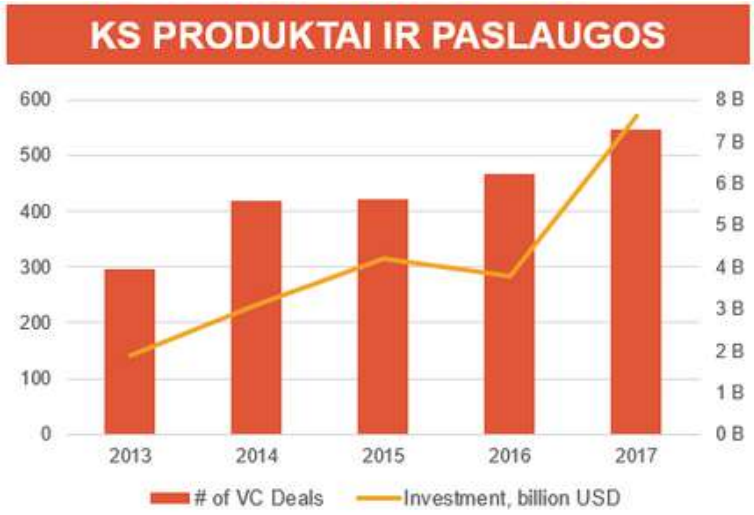
Finansiniai nuostoliai patiriami kibernetinių atakų metu yra šokiruojantys. Spėjama, kad vienas duomenų pažeidimas (įsilaužimas) vidutiniškai gali kainuoti apie 150 milijonų JAV dolerių 2020 metais. Numatoma, kad 2021 metais kibernetinės atakos kainuos apie 6 trilijonus JAV dolerių per metus. Europos Komisijos duomenimis, nesugebėjus atremti KS atakų ES ekonomika gali patirti iki 640 milijardų eurų nuostolį.

Kurk Lietuvai

Pardavimai

Įstaigoms vis daugiau dėmesio skiriant kibernetiniam saugumui atsiranda puiki terpė vystytis KS industrijai. Kuriasi vis daugiau KS startuolių, kurie teikia KS paslaugas arba kuria KS produktus. 2017 metais, kibernetinio saugumo produktų pardavimai siekė 3,5 milijardo JAV dolerių. Nuo 2005 metų šis skaičius paaugo net 34 kartus. Akivaizdu, kad šie skaičiai sparčiai augs ir toliau, nes siekiant apsaugoti savo įstaigas ir duomenis bus naudojama vis daugiau KS produktų.

Investicijos



Nuo 2013 metų investicijos į kibernetinio saugumo paslaugas ir produktus išaugo daugiau nei 3 kartus.

Kurk Lietuvai

Iššūkis - specialistų trūkumas visame pasaulyje

3,5 mln.

Prognozuojama, kad 2021 metais pasaulyje bus apie 3,5 milijonus naujų darbo vietų KS srityje.

3 x

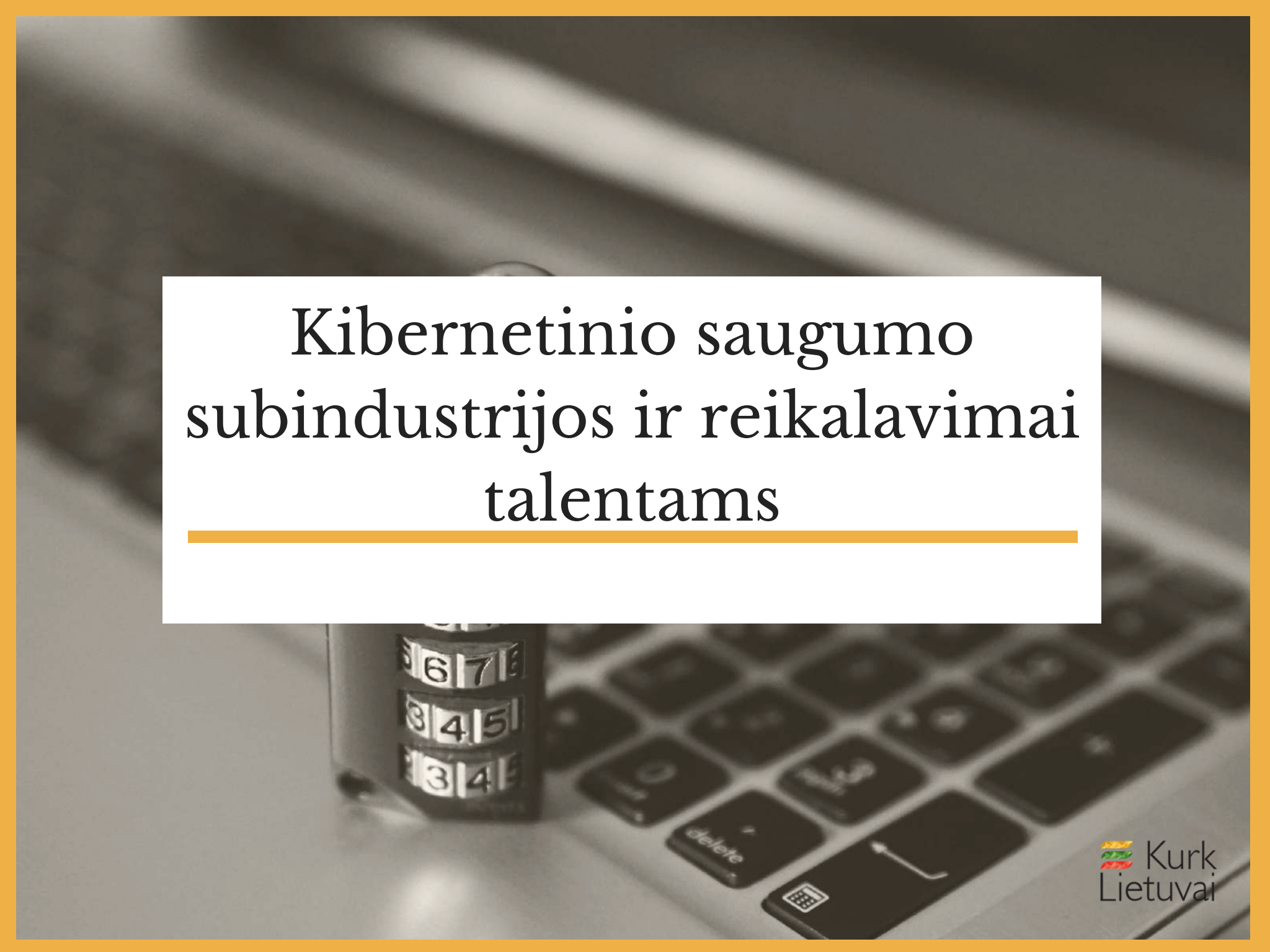
3 kartus daugiau naujų darbo vietų KS srityje lyginant su visu IRT sektoriumi.

68%

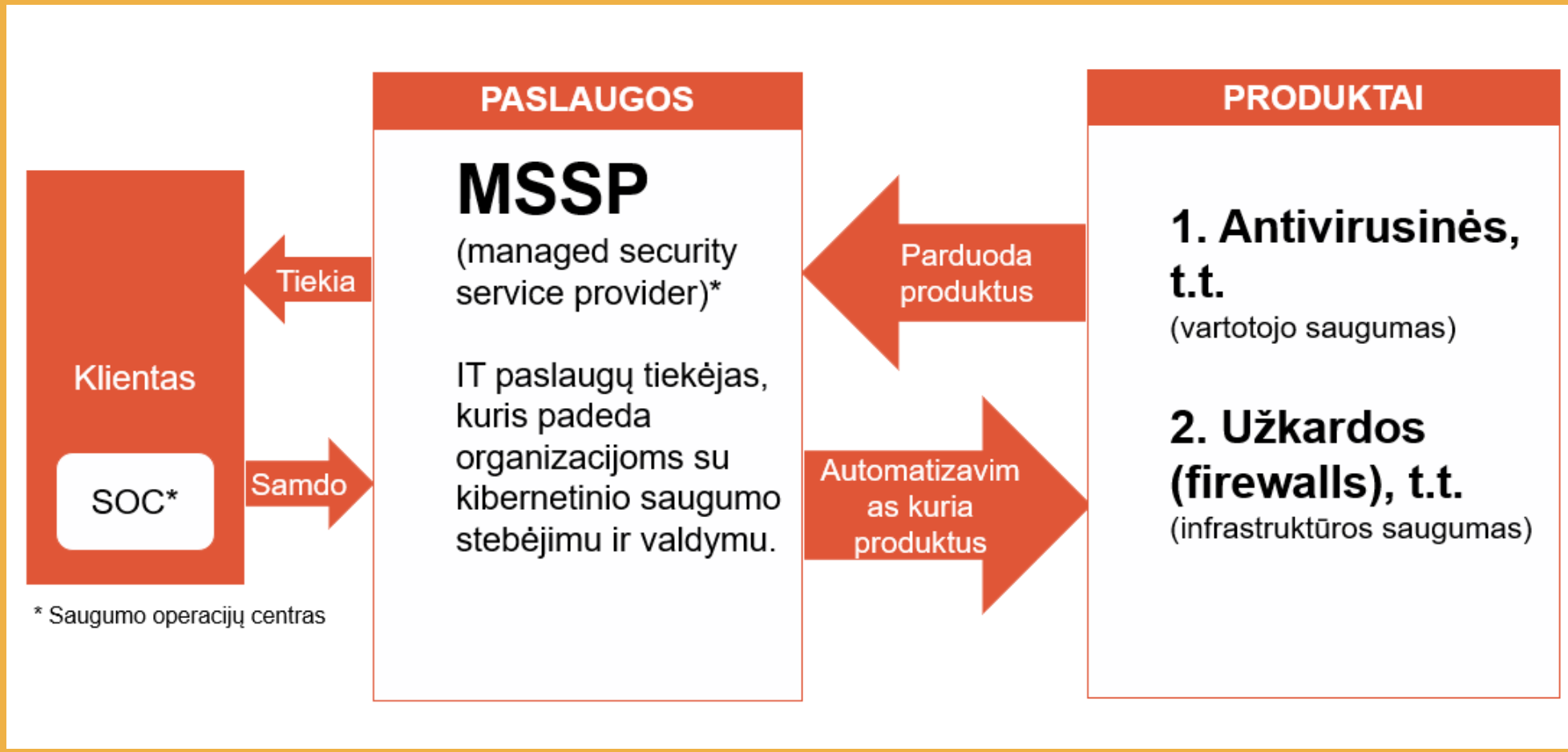
68% organizacijų visame pasaulyje jaučia KS specialistų poreikį.

Kurk Lietuvai

Kibernetinio saugumo subindustrijos ir reikalavimai talentams



Subindustrijos: KS paslaugos ir produktai



Kurk Lietuvai

KS paslaugos

Bendrieji reikalavimai

CISM - Sertifikuotas informacijos saugos vadovas
CISA - Sertifikuotas informacinių sistemų auditorius
CRISC - Sertifikuotas informacinių sistemų rizikos kontrolės specialistas
CISSP - Sertifikuotas informacinių sistemų saugos profesionalas

Specialūs reikalavimai

1 Pakopa	1-2 metų patirtis informacijos saugumo ir tinklų kūrimo srityje. **Sertifikatas:** nereikalaujamas
2 Pakopa	Mažiausiai 3 metų profesionali darbo patirtis reaguojant į informacinių sistemų saugumo incidentus. **Sertifikatas:** turi turėti bent 1
3 Pakopa	5 Metų kibernetinio saugumo analitiko ar inžinieriaus darbo patirtis. **Sertifikatas:** turi turėti bent 1

KS produktai

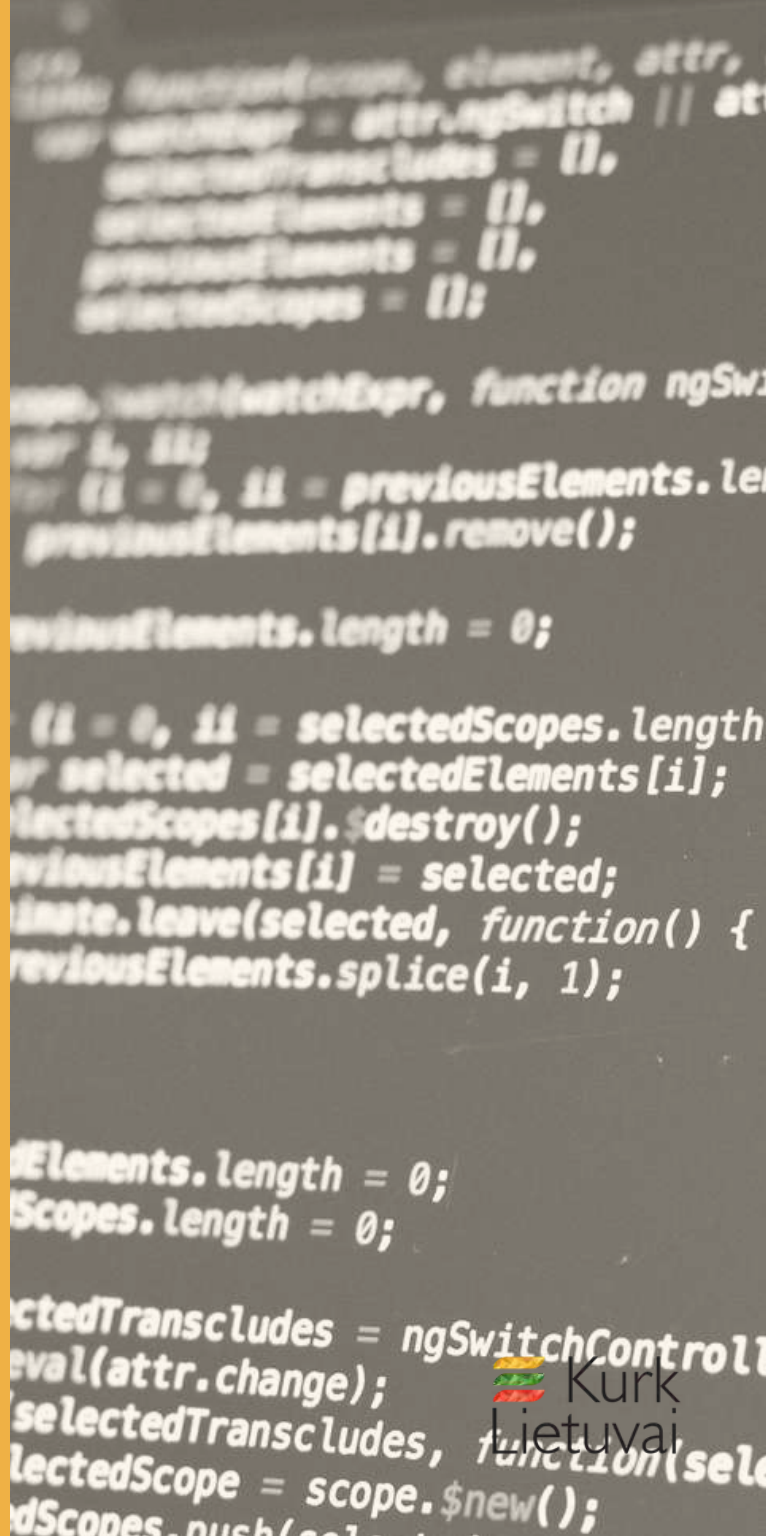
Bendrieji reikalavimai

Aukštesnio lygio programinės įrangos kūrimas:
C programavimo kalba
Atvirkštinė (reverse) inžinerija

Matematiniai įgūdžiai:
Kriptografija
Mašininis mokymasis

Saugumo mąstysena:
Tinklo protokolų detalios žinios

Dirbant su kibernetinio saugumo produktais ir jų kūrimu, specialių reikalavimų nustatyta nėra. Priklausomai nuo pozicijos yra reikalaujama atitinkama darbo metų patirtis ir įvairūs papildomi įgūdžiai. Tačiau, aukštesnėse pozicijose yra vertinamos papildomos kvalifikacijos ir sertifikatai.



Kibernetinio saugumo sertifikatai

Visame pasaulyje pripažįstamus sertifikatus siūlo: CompTIA, Cisco, EC-Council, ISACA, (ISC)2. ISACA turi skryių ir Lietuvoje, kuris vienija 130 įvairių IT specialistų. Šis skyrius administruoja 4 globaliai pripažintas sertifikacijas ir organizuoja egzaminus du kartus metuose. Kiekvienam iš sertifikatų yra keliami skirtingi reikalavimai ir dažnai tik išlaikyto egzamino nepakanka sertifikatui gauti.

Top 10 kibernetinio saugumo sertifikatų 2018 metams:

CompTIA Security+ - Sertifikuotas pradedantis saugumo specialistas
CompTIA CASP - CompTIA pažengęs saugos specialistas
CEH - Sertifikuotas etiškas hakeris
CCNA Security - Cisco sertifikuotas tinklų saugos jaunesnysis specialistas
CCNP Security - Cisco sertifikuotas tinklų saugos profesionalas
CISA - Sertifikuotas informacinių sistemų auditorius
CISM - Sertifikuotas informacijos saugos vadovas
CISSP - Sertifikuotas informacinių sistemų saugos profesionalas
CCSP - Sertifikuotas debesų sistemų profesionalas
CSSLP - Sertifikuotas programinės įrangos gyvavimo ciklo saugos profesionalas

CompTIA Certificates

ISACA Trust in, and value from, information systems

(ISC)2 International Standard for Information Security

CISCO

Kurk Lietuvai

Kibernetinio saugumo sertifikatai

TRUMPINYS	PILNAS PAVADINIMAS	KAS SUTEIKIA	APIBŪDINIMAS
CompTIA Security+	Sertifikuotas pradedantis saugumo specialistas	CompTIA	Pasaulyje pripažįstamas sertifikatas, patvirtinantis pagrindinius įgūdžius, reikalingus pagrindinėms saugumo funkcijoms atlikti ir pradėti karjerą IT saugumo srityje. Tai pirmas saugumo sertifikatas, kurį turėtų įgyti kiekvienas IT specialistas.
CompTIA CASP	CompTIA pažengęs saugos specialistas	CompTIA	Vienintelis praktikuojančiųjų (ne vadovaujančiųjų) sertifikavimas, pagrįstas veiklos rezultatais, skirtas pažengusiems kibernetinio saugumo specialistams. Tai idealus sertifikatas techniniams profesionalams, kurie nori likti ir gilintis į technologijas, o ne tik vadovauti procesams.
CEH	Sertifikuotas etiškas hakeris	EC-Council	Etiški hakeriai tampa vis populiaresni ir patvirtina paklausius „White-Hat" įsilaužimo įgūdžius. Šie hakeriai gali nustatyti sistemos pažeidžiamumą dar iki tol, kol juos atranda tie, kurie nori pavogti slaptus duomenis ir jautria informaciją. Jie taip pat moko kitus darbuotojus, kaip išvengti didelius nuostolius sukeliančių klaidų.
CCNA Security	Cisco sertifikuotas tinklų saugos jaunesnysis specialistas	Cisco	Šis sertifikatas patvirtina bendrojo lygio žinias ir įgūdžius, reikalingus Cisco tinklams apsaugoti. Su šiuo sertifikatu, tinklo specialistas gali pademonstruoti gebėjimus, reikalingus kuriant saugumo infrastruktūrą, atpažįstant grėsmes ir tinklų pažeidžiamumą, bei sušvelninant saugumo grėsmes.
CCNP Security	Cisco sertifikuotas tinklų saugos profesionalas	Cisco	Ši sertifikavimo programa yra priderinta specialiai Cisco tinklo saugumo inžinieriaus rolei. Šis žmogus atsakingas už maršrutizatorių saugumą, jungiklius, tinklų įrenginius ir prietaisus, taip pat pasirenkant, dislokuojant, palaikant ir šalinant užkardas, VPNS ir IDS / IPS sprendimais jų tinklo aplinkoje.
CISA	Sertifikuotas informacinių sistemų auditorius	ISACA	CISA sertifikavimas yra pasaulinis pripažinimas tiems, kas audituoja, stebi, ir vertina organizacijų informacines technologijas ir verslo sistemas. Tai profesinis laipsnis, suteikiamas itin didelę patirtį turintiems IS valdymo ir audito srities profesionalams.
CISM	Sertifikuotas informacijos saugos vadovas	ISACA	Sertifikatas skirtas informacijos saugos valdymo specialistams. Šis sertifikatas liudija, kad informacijos saugos specialistas turi patirties ir žinių, leidžiančių teikti tinkamas vadybos ir konsultavimo paslaugas. CISM apibrėžia pagrindines kompetencijas ir tarptautinius veiklos standartus, kuriuos privalo įvykdyti asmenys, atsakingi už informacijos saugos valdymą.
CISSP	Sertifikuotas informacinių sistemų saugos profesionalas	(ISC)2	Elitinė narystė kibernetinio saugumo lyderiams. Šis aukščiausio lygio sertifikatas iš (ISC) ² parodo gebėjimą projektuoti, konstruoti, įdiegti ir valdyti saugumo programą įmonės lygiu. CISSP yra visuotinai pripažįstamas dėl to, kad sertifikatą įgijęs žmogus turi pažangių žinių apie kibernetinį saugumą.
CCSP	Sertifikuotas debesų sistemų profesionalas	(ISC)2	Pasaulinis pažymėjimas, kuris reprezentuoja aukščiausio standarto debesų saugumo ekspertus. Įgijus šį sertifikatą reiškia, kad asmuo turi gilias žinias ir realią praktinę patirtį, susijusią su debesų saugumo architektūra, dizainu, operacijomis ir paslaugų instrumentavimu.
CSSLP	Sertifikuotas programinės įrangos gyvavimo ciklo saugos profesionalas	(ISC)2	Pasauliniu mastu pripažįstamas ir patvirtinantis aukšto lygio kompetencijas sertifikatas. Turint šį sertifikatą reiškia, jog asmuo turi tarptautiniu mastu pripažįstamą gebėjimą pritaikyti saugos procedūras kiekviename tinklo gyvavimo ciklo etape.

Kurk Lietuvai

Išvados

- Kibernetinio saugumo industrija sparčiai auga: kuriasi vis daugiau KS įmonių, investuojama vis daugiau pinigų į KS. Tai yra dar viena sritis, kur kiekviena valstybė gali išsiskirti.
- Pasaulyje didėjantis laisvų darbo vietų skaičius KS srityje, tik parodo, koks didelis yra specialistų poreikis ir kokiu sparčiu greičiu auga ši industrija.
- Kibernetinio saugumo specialistams yra keliami aukšti reikalavimai, tačiau pakankamas jų kiekis šalyje gali ne tik užtikrinti valstybės saugumą, bet ir pritraukti užsienio investicijas.
- Kibernetinio saugumo užtikrinimas yra labai svarbus tiek valstybėms, tiek kiekvienai įstaigai. Todėl kiekviena valstybė turi į tai investuoti, ugdyti KS gebėjimus ir prisidėti prie saugios kibernėtinės erdvės kūrimo.

Kurk Lietuvai

2. Kibernetinio saugumo specialistai Lietuvoje

IEVA NAMAVIČIŪTĖ

KS Lietuvoje

Kibernetinio saugumo srityje Lietuva nėra naujokė, o pastaraisiais metais KS skiriama vis daugiau dėmesio. 2014 metais čia įsigaliojo kibernetinio saugumo įstatymas, 2016 m. priimtas nutarimas dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, 2017 m. sukurtos kibernetinės greitojo reagavimo pajėgos, o 2018 metais bus patvirtinta ir Nacionalinė kibernetinio saugumo strategija. Lietuva gali didžiuotis tuo, kad nuo 2017 m. vadovauja PESCO (nuolatinis struktūrizuotas bendradarbiavimas) iniciatyvai sukurti Europines kibernetines greitojo reagavimo pajėgas.

Kurk Lietuvai

Lietuvos apžvalga

Remiantis Kibernetinio Saugumo ataskaitos duomenimis, 2017 metais Lietuvoje buvo užfiksuota 54950 kibernetinių incidentų tiek viešajame, tiek privačiame sektoriuje. Incidentų skaičius padidėjo nuo 2016 metų (49463) ir ši tendencija parodo koks iššūkis tenka Lietuvos kibernetiniam saugumui, viešajam ir privačiam sektoriams, bei piliečiams. Pastebima, jog esant tokioms tendencijoms, vis svarbiau ugdyti kibernetinio saugumo gebėjimus, kurti kompetencijas viešajame sektoriuje, planuoti ir siekti sumažinti KS grėsmių riziką. Svarbu paminėti, jog viena iš ryškiausių KS spragų yra vartotojų, įstaigų darbuotojų žinių ir dėmesio šiai temai trūkumas.

INFOBALT duomenimis Lietuvoje yra apie 31 500 IT specialistų iš kurių apie 10 000 yra programuotojai. IT studijos ir toliau išlieka vienos populiariausių šalyje ir jas renkasi vis daugiau studentų. Vaikai dar pradinėse klasėse mokosi programavimo ir šios tendencijos yra labai patrauklios užsienio investuotojams, kurie vis dažniau renkasi Lietuvą savo technologijų įmonėms steigti. KS produktų gamybos specialistams išskirtinių reikalavimų nėra, tad Lietuvoje esančių IT specialistų pasiūla galėtų būti labai patraukli investuotojams.

Kurk Lietuvai

Įmonių apžvalga

35 Tiek šiuo metu Lietuvoje yra įsikūrusių KS įmonių.

Šios įmonės skirstomos į tris pagrindines grupes:

- **Orientuotos į paslaugas:** daugiausiai saugumo operacijų centrai (SOC). Šiuo metu tokių Lietuvoje yra 13 ir daugiausiai veikia komerciniuose bankuose, telekomunikacijų kompanijose ir viešose įstaigose.
- **Orientuotos į produktus:** kompanijos, kurios specializuojasi R&D (moksliniai tyrimai ir plėtra), bei produktų vystimu (Antivirusinės, užkardos). Lietuvoje veikia 6 tokios įmonės, kurių pagrindinės buveinės yra kitose šalyse.
- **Konsultacinės:** šiuo metu veikia 16 įmonių, kurios teikia konsultavimo apie kibernetinius incidentus ir įvairių mokymų paslaugas. Yra ir keletas kompanijų, kurios specializuojasi į užsakomąją KS plėtrą.

Kurk Lietuvai

KS specialistų svarba

Pagal 2016 metų PWC (PricewaterhouseCoopers International Limited) duomenis apie 95% visų saugumo incidentų įvyksta dėl žmogiškos klaidos. Todėl bendras visuomenės švietimas, specialistų ugdymas, investavimas į įstaigų darbuotojų mokymus yra labai svarbus siekiant sumažinti kibernetinių atakų riziką, bei nuostolius ar draudimo išlaidas. Aukštos kvalifikacijos specialistai reikalingi ne tik saugumui užtikrinti, bet ir pritraukti užsienio investicijas. Vienas pagrindinių kriterijų, kodėl investuotojai renkasi tam tikrą šalį – talentai.

Kurk Lietuvai

KS specialistai ir jų trūkumas

~100 Sertifikuotų KS specialistų Lietuvoje

250 IT specialistų dirbančių KS įmonėse Lietuvoje

229 Studentų skaičius KS bakalauro ir magistro programose

700 Tiek KS specialistų papildomai reikės iki 2020m.

Kurk Lietuvai

KS talentų ugdymas

Kurk Lietuvai

Talentų auginimas

Siekiant pritraukti daugiau užsienio investicijų kibernetinio saugumo srityje reikia turėti pakankamai aukštos kvalifikacijos specialistų. Tačiau vien to nepakanka ir labai svarbu kelti bendrą visuomenės suvokimo lygį, kad žmonės taptų atsparesni vykstančioms atakoms ir incidentams. Talentus ugdyti reikia nuo mažų dienų, siekiant juos sudominti ir įtraukti, kad ateityje jie norėtų tapti KS specialistais. Šiuo metu mokyklose jau yra kalbama apie saugą internete ir yra vykdomi įvairūs projektai šia tema.

Bendrosios programos

Mokyklų bendrosiose programose yra nurodoma, kad moksleiviai turėtų mokėti saugiai elgtis internete, apsaugoti savo duomenis, saugiai naudotis socialinėmis medijomis. Dėl įsigaliojančio BDAR (GDPR) reglamento, mokytojams ir švietimo darbuotojams rengiami mokymai, kaip apsaugoti moksleivių duomenis. Taip pat, Švietimo informacinių technologijų centras vykdo saugesnio interneto projektą, kuriuo siekiama sukurti saugesnio interneto infrastruktūrą. Šis projektas labiau siekia mažinti patyčias internete, išmokyti atpažinti netinkamą turinį ir kaip su juo elgtis. Projekto tiksluose užsimenama ir apie duomenų saugumą, elgesį socialinėse medijose ir kitas grėsmes.

Studijų programos

STUDIJŲ PAKOPA	STUDIJŲ PROGRAMOS PAVADINIMAS	PRIIMTA STUDENTŲ IŠ VISO	STUDIJUOJA IŠ VISO	2017 M. SUTEIKTAS KVALIFIKACINIS LAIPSNIS ARBA (IR) PROFESINĖ KVALIFIKACIJA
Magistras	Informacijos ir informacinių technologijų sauga (KTU)	42	79	18
Magistras	Kibernetinio saugumo valdymas (MRU)	16	31	1
Magistras	Informacijos ir informacinių technologijų sauga (VGTU)	43	78	14
Bakalauras	Informacijos sistemos ir kibernetinė sauga (VU)	20	26	0
Bakalauras	Interneto inžinerija (KSU)	0	15	0

Kurk Lietuvai

KS kursai ir mokymai

Cyber Gym - pirmasis Šiaurės Europoje specialus nuotolinių kibernetinių saugumo pratybų centras. Šis mokymų centras išsiskiria savo koncepcija ir holistiniu požiūriu į kova su kibernetinėmis atakomis. Mokymų metu užtikrinama, kad visos organizacijos komandos būtų pasirengusios veiksmingai reaguoti į realybėje kylančias grėsmes.

„**Cyber Gym** ekspertai moko organizacijas tikėtis netikėto".

CYBERGYM

Code Academy
Programuok savo ateitį!

CodeAcademy – jau antrus metus IT specialistus ruošianti akademija. Ši akademija siūlo kursus pradedantiesiems, įvairias studijas pažengusiems , o šiuo metu nedirbantiems ir nesimokantiems kartu su Lietuvos darbo birža bei Europos Sąjunga – nemokamus pradedančiųjų kursus. Viena iš programų yra ir Kibernetinio saugumo programa.
CodeAcademy Kids - programavimo akademija 7 - 18 metų vaikams, kuria siekiama vaikus mokyti įdomiai ir inovatyviai.

Kurk Lietuvai

KS kursai ir mokymai

Kibernetinio saugumo akademija veikia nuo 2012 ir siekiama per praktinę pusę išmokyti IT specialistus apsaugoti organizacijos skaitmeninę informaciją IT tinklo infrastruktūrą ir web aplikacijas. Tikslas - greitai ir kokybiškai parengti kibernetinės erdvės saugumo specialistus, kurie naujus įgūdžius galės iš karto pritaikyti savo organizacijai saugoti. Rengiami įvairūs mokymai IT specialistams, įmonių vadomas ir darbuotojams.

CYBER SECURITY ACADEMY

CYBER SECURITY ACADEMY

Mokymų programos IT specialistams:

Kibernetinio saugumo pagrindai
Hack IT to Defend IT
Etiškasis hakeris-praktikas
Saugus programavimas
IT saugumo praktikas
Informacijos saugumo praktikas
Kibernetinio saugumo incidentų valdymas

Kurk Lietuvai

ISACA sertifikavimas

Asociacija ISACA Lietuva padeda specialistams siekti CISA, CISM, CGEIT, CRISC sertifikacijos, bei stengiasi užtikrinti ir kelti šalyje atliekamo IT audito ir saugos valdymo kokybę.

ISACA administruoja 4 globaliai pripažintas profesionalų certifikacijas IT audito, saugos, valdymo ir rizikos profesionalams.

Taip pat ISACA turi COBIT5 Produkto certifikacijas, bei kibernetinės saugos CSX sertifikacijas.

CISA, CISM, CGEIT ir CRISC sertifikacijų reikalavimai:

Išlaikytas egzaminas
Darbo patirtis
Profesinės etikos kodekso laikymasis
Nuolatinio lavinimosi programos (CPE) reikalavimų laikymasis
Atitiktis atitinkamiems standartams

ISACA®
Trust in, and value from, information systems

Kurk Lietuvai

Išvados

- Dėl savo veiklų ir progreso, Lietuva jau yra žinoma kibernetinio saugumo industrijoje ir tai padės ateityje pritraukti užsienio investicijas. Tačiau vis didėjantis kibernetinių atakų skaičius atskleidžia pagrindinę problemą – visuomenė nėra atspari atakoms ir didžiausius nuostolius lemia būtent žmogiškosios klaidos.
- Lietuvoje yra daug IT specialistų, tačiau KS specialistų skaičius nėra didelis. Specialistų trūkumas jaučiamas jau dabar, o po kelių metų jų reikės dar daugiau. Tad dabar yra puikus metas investuoti ir į visuomenės atsparumo kibernetinėms grėsmėms didinti, ir į aukštos kvalifikacijos specialistų ugdymą. Kadangi pasaulyje KS srityje specialistų trūksta milijonais, Lietuva galėtų pasinaudoti šiuo šansu ir sukurti pasiūlą, atitinkančia rinkos poreikius.
- Apie saugumą internete mokoma jau nuo pradinių klasių, yra specialūs projektai, tačiau kibernetiniam saugumui daug dėmesio dar nėra skiriama. Universitetuose jau yra keletas programų tiek bakalauro, tiek magistro studijoms KS srityje. Pasaulyje yra vertinami tarptautiniai KS saugumo sertifikatai, o Lietuvos aukštojo mokslo programos to nesiūlo.

Kurk Lietuvai

Išvados

- Lietuvoje yra įsikūrusios kelios įmonės, kurios teikia įvairius KS mokymus vartotojams ir įmonių darbuotojams. Yra sudaromos sąlygos su kibernetinėmis atakomis kovoti tikrovėje ir gauti realių praktinių žinių, kurių labiausiai ir reikia KS srityje.
- Apibendrinant, kibernetinio saugumo industrija yra labai jauna ir dabar yra puikus metas į tai investuoti ir siekti išsiskirti iš kitų šalių regione ar Europoje. Pakankamas KS specialistų kiekis prisidės ne tik prie investicijų pritraukimo, bet ir didins valstybės saugumą.

Kurk Lietuvai

Šaltiniai

- http://www.taxpayer.net/national-security/cyberspending-database/
- https://thebestvpn.com/cyber-security-statistics-2018/
- https://lietuvosdiena.lrytas.lt/aktualijos/2017/09/29/news/dalia-grybauskaite-butina-isteigti-es-kibernetines-greitojo-reagavimo-pajegas-2748919/
- https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#78c3320b4947
- http://www.businessinsider.com/cybersecurity-startups-raked-in-76-billion-in-vc-money-in-2017-2018-1
- https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg
- http://cyberseek.org/pathway.html
- https://www.csoonline.com/article/3235961/security/largest-cybersecurity-venture-capital-deals-in-2017.htmlhttps://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#46a657345163
- https://thebestvpn.com/cyber-security-statistics-2018/
- https://cybersecurityventures.com/jobs/
- https://www.consultancy.uk/news/16068/majority-of-companies-now-hit-by-a-cybersecurity-skills-gap
- https://www.csoonline.com/article/3116884/security/top-cyber-security-certifications-who-theyre-for-what-they-cost-and-which-you-need.html
- https://www.knowledgenet.com/certifications/2018s-top-ten-cybersecurity-certifications/
- https://certification.comptia.org/certifications?level=cybersecurity
- https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html
- https://www.isc2.org/#
- http://www.isaca.org/CERTIFICATION/Pages/default.aspx
- http://www.comptiastore.eu/product-p/pvcomptiacasp-euro.htm

Šaltiniai

https://www.nksc.lt/doc/NKSC_ataskaita_2017_[lt].pdf
http://bakalauras.lamabpo.lt/bendro-priemimo-rezultatai/2017-m/#4
https://www.infobalt.lt/lt/naujienos/i/940
https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf
https://www.smm.lt/uploads/documents/svietimas/ugdymo-programos/vidurinis-ugdymas/IT_7_priedas.pdf
https://www.codeacademy.lt/musu-siulomi-kursai/
https://www.telia.lt/verslui/cybergym
https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee
http://www.consilium.europa.eu/lt/press/press-releases/2018/03/06/defence-cooperation-council-adopts-an-implementation-roadmap-for-the-permanent-structured-cooperation-pesco/
https://www.draugiskasinternetas.lt/lt/adult/pasinaudokite
https://www.cybersecurityacademy.lt/kibernetinio-saugumo-mokymai
http://www.isaca.org/chapters1/Lithuania/sertifikacija/Pages/default.aspx
"Investuok Lietuvoje" duomenys

Kontaktai

IEVA NAMAVIČIŪTĖ

ieva.namaviciute@kurklt.lt
ieva.namaviciute@investlithuania.com
+37060941313

Kurk Lietuvai

Investuok Lietuvoje

UŽSIENIO GERŲJŲ PRAKTIKŲ ANALIZĖ

IEVA NAMAVIČIŪTĖ

Kurk Lietuvai

ĮVADAS

Prognozuojama, kad 2021 metais pasaulyje bus apie 3,5 milijonus naujų darbo vietų kibernetinio saugumo (KS) srityje, o šiuo metu net 68% organizacijų visame pasaulyje jaučia KS specialistų poreikį. KS specialistų trūksta ir Lietuvoje, tad šia analize buvo siekiama išsiaiškinti, kaip su tuo kovoja kitos valstybės ir kokias gerąsias praktikas galima pritaikyti Lietuvoje.

Analizei pasirinktos keturios šalys: Jungtinė Karalystė (JK), Jungtinės Amerikos Valstijos (JAV), Lenkija ir Čekija. JK ir JAV yra vienos pažangiausių KS industrijoje, o Lenkija ir Čekija yra panašesnės savo istorinėmis aplinkybėmis į Lietuvą, todėl buvo pasirinkta apžvelgti ir jų padėtį.

Kurk Lietuvai

JUNGTINĖ KARALYSTĖ

Jungtinė Karalystė (JK) yra vienas iš gerųjų pavyzdžių KS industrijoje. Šalyje natūraliai buvo palanku steigti KS verslus, nes čia yra vieni didžiausių finansų ir IT sektoriai. Kuriant pirmąją KS strategiją, dar 2011 metais, JK numatė, kad nori būti rinkos lyderiais ir užtikrinti ne tik piliečių ir valstybės saugumą, bet ir sudaryti palankias sąlygas KS verslams plėstis. Dabar Jungtinėje karalystėje yra didžiausia KS įmonių koncentracija Europoje.

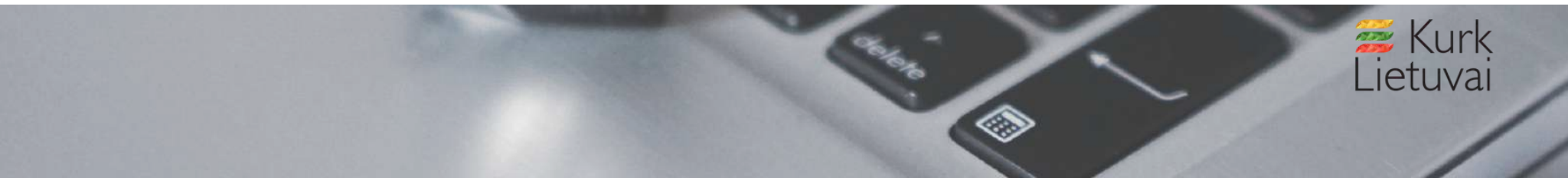
Nepaisant to, kad JK yra trečia pasaulyje pagal KS talentų skaičių, čia jaučiamas ir vienas didžiausias jų trūkumas. Valstybė tai pastebėjo dar prieš kelerius metus ir ėmėsi įvairių iniciatyvų KS specialistų gebėjimų vystymui.

Kurk Lietuvai

JK KIBERNETINIO SAUGUMO STRATEGIJA 2011 - 2015M.

Pirmoji kibernetinio saugumo (KS) strategija Jungtinėje karalystėje (JK) buvo išleista dar 2011 metais. Ši strategija turėjo aiškia viziją 2015 metams, suskirstytą į 4 pagrindinius tikslus:

- Kovoti su kibernetiniu nusikalstamumu ir būti viena saugiausių vietų pasaulyje kurtis verslams elektroninėje erdvėje;
- Būti atsparesnei kibernetinėms atakoms ir sugebėti geriau apsaugoti valstybės interesus elektroninėje erdvėje;
- Padėti suformuoti atvirą, stabilią ir gyvybingą kibernetinę erdvę, kuria JK visuomenė gali saugiai naudotis ir kuri remia atviras visuomenes;
- Turėti bendrąsias žinias, įgūdžius ir gebėjimus, kurių reikia norint paremti visus JK kibernetinio saugumo tikslus.



Kurk Lietuvai

JK KIBERNETINIO SAUGUMO STRATEGIJA 2016 - 2021M.

Šiam laikotarpiui savo biudžete JK skirs 1,9 milijardų svarų kibernetiniam saugumui užtikrinti tiek didelėse įmonėse, tiek apsaugoti kiekvieną individą.

Šiai strategijai įgyvendinti yra nustatyti trys pagrindiniai tikslai:

- APGINTI - JK turi tinkamų priemonių apginti šalį nuo kylančių kibernetinių grėsmių, veiksmingai reaguoti į incidentus, siekiant užtikrinti JK tinklų, duomenų ir sistemų saugumą. Piliečiai, įmonės ir viešasis sektorius turi žinių ir gebėjimų apginti patys save.
- SULAIKYTI - JK bus pasiruošusi atremti visų tipų agresijas kibernetinėje erdvėje. Taip pat aptiks, supras, tirs ir apribos priešiškus veiksmus, kurių bus imamasi prieš juos, o nusikaltėliai bus persekiojami ir patraukiami baudžiamojon atsakomybėn. Turės priemonių imtis agresyvių veiksmų kibernetinėje erdvėje, jei nuspręs tai daryti.
- VYSTYTI - JK turi novatorišką, augančią KS industriją, paremtą pasauliniais moksliniais tyrimais ir vystymu. Jie turi savarankiškai išsilaikančią talentų augimo sistemą, kuri suteikia įgūdžius, atitinkančius nacionalinius rinkos ir viešojo sektoriaus poreikius. Pažangiausios analizės ir patirtis padės JK įveikti ateities grėsmes ir iššūkius.

KS GEBĖJIMŲ STIPRINIMAS

- JK valdžia suprato, kad jiems reikia daugiau talentingų ir kvalifikuotų KS specialistų, todėl naujojoje strategijoje ypatingas dėmesys skiriamas KS gebėjimų vystymui ir stiprinimui.
- Valstybė nori paruošti ilgalaikę KS įgūdžių strategiją, tačiau norint padaryti didelį poveikį yra būtinas privataus sektoriaus, viešojo sektoriaus, akademijos ir švietimo įstaigų bendradarbiavimas.

Pagrindiniai tikslai:
- užtikrinti ilgalaikį tiekimą geriausių KS talentų užaugintų šalyje, tuo pat metu investuojant į trumpalaikius sprendimus KS talentų trūkumui mažinti.
- nustatyti ilgalaikį, koordinuotą (valstybės, industrijos ir akademijos) veiksmų planą, reikalingą siekiant išugdyti kompetentingus KS specialistus, kurie atitinka reikalavimus ir sertifikaciją dirbti saugiai ir konfidencialiai.
- bus sumažintas KS gebėjimų trūkumas gynyboje. Bus siekiama pritraukti KS specialistus į valstybines įstaigas šalies saugumui užtikrinti.

KS GEBĖJIMŲ STIPRINIMAS

Strategijoje numatoma imtis šių priemonių KS švietimui ir ugdymui stiprinti:

- Bus sukurta programa mokykloms, kuri bus didelis žingsnis į priekį KS specialistų ugdyme. Programa bus skirta talentingiems 14 - 18 metų vaikams veiklas vykdant pamokų metu, popamokinėse veiklose bendraujant su ekspertais ir mentoriais, įvairių projektų metu ir vasaros mokyklose.
- Įkurtas fondas darbo jėgos perkvalifikavimui, turinčiai potencialo KS profesijoje.
- Identifikuojamos ir remiamos kokybiškos KS bakalauro ir magistro studijos, nustatomos ir užpildamos trūkstamos specialistų sritys, pripažįstant universitetų svarbą KS gebėjimų ugdymo procese.
- Remiamos mokytojų akreditacijos profesiniam tobulinimui KS srityje.
- Vystoma kibernetinio saugumo profesija, siekiant oficialaus Karališkojo pripažinimo iki 2021 metų.
- Kuriama Kibernetinės Gynybos Akademija, kaip kompetencijų centras KS mokymams ir pratyboms.
- Vystomos bendradarbiavimo galimybės tarp valstybės, kariuomenės, industrijos ir akademijos, KS švietime ir ugdyme.

Kurk Lietuvai

JK SĖKMINGŲ INICIATYVŲ PAVYZDŽIAI

KIBERNETINIO SAUGUMO GEBĖJIMŲ NEATIDĖLIOTINO POVEIKIO FONDAS:

- Tikslas - didinti JK sparčiai augančio kibernetinio saugumo sektoriaus darbuotojų įvairovę ir skaičių.
- Fondas teiks skatinimo priemones įvairioms organizacijoms kurti, išplėsti arba perorientuoti kibernetinio saugumo mokymo iniciatyvas.
- Fondas atviras tokioms organizacijoms kaip mokymų teikėjai ir labdaros organizacijos, kurios gali parodyti, kad jų iniciatyvos yra naudingos įvairiems darbdaviams.

CyberFirst PROGRAMA

- Šia programa siekiama paruošti naująją KS kartą ir ją inicijavo Nacionalinis kibernetinio saugumo centras.
- Rengiami trumpi kursai skirti supažindinti 11 - 17 metų vaikus su KS pasauliu. Kursai vykdomi skirtinguose miestuose, skirtingoms amžiaus grupėms ir dažniausiai trunka 5 dienas. Kursai nemokami JK moksleiviams ir vyksta vasaros atostogų metu.
- Suteikiamos stipendijos (iki 4000 svarų metams) ir apmokoma darbo praktika studentams įgyti KS įgūdžių.
- Rengiamos varžybos mergaitėms, siekiant įkvėpti ir užauginti naują, sėkmingų KS specialisčių kartą.

JUNGTINĖS AMERIKOS VALSTIJOS

Jungtinės Amerikos Valstijos (JAV) yra dar vienas puikus pavyzdys kibernetinio saugumo srityje. Kibernetiniu saugumu jie susirūpino dar 2003 metais, kuomet buvo išleista pirmoji Nacionalinė kibernetinio saugumo strategija. Nuo to laiko į KS valstybė investavo vis daugiau pinigų ir 2018 metais KS skirta net 14 milijardų JAV dolerių.

JAV yra didžiausia KS įmonių koncentracija visame pasaulyje. Šalis turi ir vieną didžiausią kiekį KS specialistų (antra pasaulyje), tačiau jau dabar yra jaučiamas didžiulis trūkumas specialistų ir šiuo metu yra apie 350 000 laisvų darbo vietų KS srityje. KS specialistų trūkumas išlieka vienu didžiausių iššūkių ir JAV.

Kurk Lietuvai

JAV KIBERNETINIO SAUGUMO STRATEGIJA 2003M.

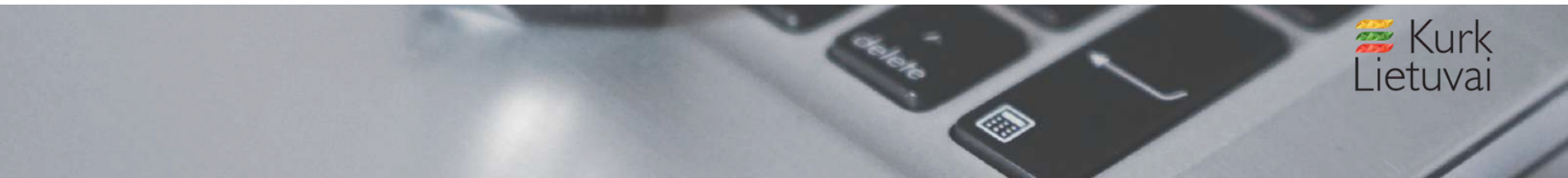
Pirmoji kibernetinio saugumo strategija JAV buvo paruošta 2003 metais. Ši strategija turėjo 3 strateginius tikslus ir buvo išskirti 5 prioritetai šiems tikslams pasiekti:

TIKSLAI:

- Kibernetinių atakų prieš valstybines kritines infrastruktūras prevencija;
- Sumažinti nacionalinį pažeidžiamumą kibernetinių atakų atveju;
- Sumažinti kibernetinių atakų žalą ir atsistatymo po jų laiką.

PRIORITETAI:

- Valstybinių kompiuterių sistemų ir tinklų apsauga;
- Greito reagavimo sistemos kūrimas;
- Grėsmių ir pažeidžiamumo mažinimo programos sukūrimas;
- Inicijuoti kibernetinio saugumo informavimo ir mokymo programą;
- Išvystyti tarptautinio bendradarbiavimo sistemą.



Kurk Lietuvai

KS GEBĖJIMŲ STIPRINIMAS

- Supratus, kokia yra KS svarba, pirmojoje strategijoje ypatingas dėmesys buvo skiriamas visuomenės švietimui ir KS talentų ruošimui. Todėl vienu iš svarbiausių prioritetų tapo KS informavimo ir mokymų programos kūrimas.

Pagrindiniai šio prioriteto įgyvendinimo veiksmai:
- Skatinti išsamią nacionalinę sąmoningumo kėlimo programą, kad visi amerikiečiai, įmonės, darbo jėga ir visi gyventojai būtų įgalinti patys apsaugoti savo kibernetinę erdvę;
- Skatinti tinkamas mokymo ir švietimo programas, skirtas valstybės kibernetinio saugumo poreikiams paremti;
- Padidinti jau egzistuojančių valstybinių KS mokymų programų efektyvumą;
- Skatinti privataus sektoriaus paramą koordinuotoms, plačiai pripažintoms, profesionalioms KS sertifikacijoms.

- Nacionalinė kibernetinės erdvės saugumo sąmoningumo skatinimo ir mokymų programa pakels KS sąmoningumo lygį įmonėse, valstybinėse agentūrose, universitetuose ir visos valstybės kompiuterių naudotojų tarpe. Joje taip pat bus nagrinėjamas apmokytų ir patvirtintų kibernetinio saugumo specialistų trūkumas.

JAV KIBERNETINIO SAUGUMO STRATEGIJA 2015M.

Nuo 2003 metų JAV buvo leidžiami įstatymai dėl kibernetinės erdvės saugumo, peržiūrimos strategijos ir rengiami kiti dokumentai. Paskutinė strategija buvo patvirtinta 2015 metais JAV valstybinio saugumo departamento.

Buvo numatyti 5 strateginiai tikslai:

- Sukurti ir išlaikyti pasiruošusią armiją ir sugebėjimus vykdyti KS operacijas;
- Apsaugoti Saugumo departamento informacinius tinklus, duomenis, ir sumažinti rizikas jų atliekamoms misijoms;
- Būti pasiruošus apginti šalį ir jos interesus nuo didžiules pasekmes turinčių kibernetinių atakų;
- Sukurti ir išlaikyti veiksmingas kibernetikos variacijas ir suplanuoti kaip jomis pasinaudoti siekiant sukontroliuoti konfliktų vystymąsi;
- Sukurti ir išlaikyti tvirtus tarptautinius bendradarbiavimus ir ryšius siekiant sunaikinti bendras grėsmes ir padidinti tarptautinį saugumą ir tvarumą.

JAV SĖKMINGŲ INICIATYVŲ PAVYZDŽIAI

- 2013 metais Valstybinis saugumo departamentas pradėjo Valstybinę iniciatyvą kibernetinio saugumo karjerai ir studijoms.
- Tai internetinis šaltinis apie karjerą KS srityje, švietimą, studijas ir mokymų galimybes. Visa reikalinga informacija patogiai pateikiama vienoje vietoje.

- Vizija: suteikti tautai įrankius ir išteklius, siekiant užtikrinti, kad visa darbo jėga būtų tinkamai apmokoma KS srityje.
- Misija: Būti pagrindiniu šaltiniu/ centru kibernetinio saugumo švietimui, karjerai ir mokymams.

Pagrindinės auditorijos:
- Valstybės tarnautojai
- Žmogiškojo kapitalo vadovai
- Visuomenė
- KS vadovai
- Politikos formuotojai
- Studentai
- Valstybinės, teritorinės ir vietinės valdžios
- Tėvai
- Mokytojai/ dėstytojai ir pan.
- Moterys ir įvairios mažumos

STOP.THINK.CONNECT.

- Sustok. Pagalvok. Junkis. (STOP.THINK.CONNECT.) - tai pasaulinė internetinė informavimo apie kibernetinę saugą kampanija, skirta padėti visiems skaitmeniniams piliečiams būti saugesniems ir saugiau naudotis internetu.
- Ši žinutė buvo sukurta precedento neturinčios privačių bendrovių, pelno nesiekiančių ir vyriausybinių organizacijų, koalicija, kuriai lyderiavo JAV Nacionalinė kibernetinio saugumo bendrija.

Šia kampanija siekiama:
- Padidinti ir sustiprinti KS sąmoningumo lygį, įtraukiant susijusias rizikas ir grėsmes, bei siūlyti sprendimus augančiam kibernetiniam saugumui;
- Pranešti visuomenei apie metodus ir strategijas, kaip išlikti patiems, šeimos nariams ir bendrijai saugesniems internetinėje erdvėje;
- Keisti Amerikos visuomenės suvokimą apie KS: nuo vengimo kažko nežinomo iki pripažinimo bendros atsakomybės;
- Įtraukti visuomenę, privatų sektorių ir valstybines bei vietos valdžios institucijas į šalies pastangas pagerinti kibernetinį saugumą;
- Padidinti suinteresuotų šalių ir bendruomenės pagrindu įkurtų organizacijų skaičių, kurios užsiima visuomenės švietimu apie kibernetinį saugumą ir apie tai, ką žmonės gali padaryti, kad apsisaugotų internetinėje erdvėje.

LENKIJA

Lenkija – tai šalis, kuri suprato, kad turi šansą tapti lydere kibernetinio saugumo industrijoje. 2017 metais buvo atliktas tyrimas ir paviešinta publikacija, kuri išryškino Lenkijos potencialą ir remiantis autorių nuomone, KS produktų ir paslaugų sektorius gali tapti viena svarbiausių Lenkijos ekonomikos dalių.

Lenkijos informacinių ir komunikacinių technologijų (IRT) vertė 2016 metais siekė 8,5 milijardus JAV dolerių ir tai yra viena iš priežasčių, kodėl KS sektorius gali sparčiai vystytis šalyje. Taip pat, Lenkijos universitetai kasmet išleidžia apie 30 000 ICT studentų, o Lenkijos programuotojai yra trečioje vietoje pasaulyje.

Nepaisant užsibrėžtų tikslų, Lenkijoje taip pat jaučiamas IT specialistų ir KS specialistų trūkumas.

Kurk Lietuvai

,,KOSCIUSZKO'' INSTITUTO PUBLIKACIJA

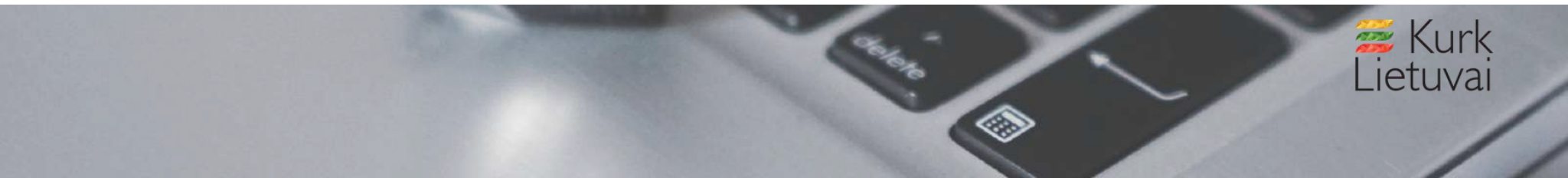
2017 metais keli mokslininkai atliko tyrimą, kaip Lenkija galėtų išnaudoti savo potencialą ir tapti kibernetinio saugumo industrijos lydere. Norint, kad taip nutiktų, buvo nustatyti veiksmai, kurių Lenkija turėtų imtis nedelsiant.

TIKSLAI:

- Vystyti privataus ir viešojo sektoriaus bendradarbiavimo mechanizmus;
- Vystyti karinės pramonės bendradarbiavimo mechanizmus;
- Sukurti tvirtą mokslinių tyrimų ir plėtros programą;
- Vystyti skirtingų rinkų plėtrą.

KELETAS VEIKSMŲ, KURIŲ TURĖTŲ BŪTI IMAMASI:

- Adaptuoti jau veikiančius privataus ir viešojo sektoriaus bendradarbiavimo mechanizmus, įtraukiant į KS orientuotus projektus;
- Kurti ilgalaikes kariuomenės ir nacionalinių IRT įmonių partnerystes;
- Skirti paramas moksliniams tyrimams;
- Padėti nacionalinėms kompanijoms patekti į užsienio rinkas rengiant ir įgyvendinant ilgalaikę PR strategiją, reklamuojant Lenkiją kaip KS kompetencijų centrą.



Kurk Lietuvai

LENKIJOS KIBERNETINIO SAUGUMO STRATEGIJA 2017 - 2022M.

- Iki šiol Lenkijoje buvo išleisti du strateginiai dokumentai (2013m ir 2016m.) skirti KS užtikrinti, o 2017 metais buvo paruošta pirmoji Nacionalinė kibernetinio saugumo strategija.

Pagrindiniai strategijos tikslai:

Padidinti pajėgumus nacionaliniu lygmeniu koordinuojamiems veiksmams, siekiant užkirsti kelią, aptikti, kovoti ir sumažinti poveikį atakų, kurios kelią pavojų IT sistemoms, gyvybiškai svarbioms valstybės veikimui;
Sustiprinti pajėgumus kovai su kibernetinėmis atakomis;
Didinti nacionalinį potencialą ir kompetenciją kibernetinio saugumo srityje;
Kurti stiprią Lenkijos tarptautinę poziciją KS srityje.

KS GEBĖJIMŲ VYSTYMAS

Strategijoje išskirti ir keli uždaviniai KS švietimui ir talentų ugdymui:

- Ugdyti kompetencijas atitinkamų sričių darbuotojų, kurie yra susiję su kibernetinės erdvės saugumu.

- Bus sukurtas ir įgyvendintas akademinio švietimo ir profesinio tobulėjimo sistemos modelis, kuris užtikrins tinkamą esamų ir būsimų darbuotojų kvalifikaciją;
- Aukštojo mokslo institucijos bus skatinamos kurti tarpdisciplinines specialybes, įtraukiant tokias kaip informacijos saugumo vadybą, asmeninių duomenų apsaugojimą, intelektinės nuosavybės apsaugojimą internete ir pan.;
- Rengiami mokymai darbuotojams, kurių darbas susijęs su kibernetinės erdvės saugumo užtikrinimu;
- Siekiant išlaikyti kvalifikuotus darbuotojus viešajame sektoriuje bus siūlomos paskatos, bei sukurta valstybinė paskatų programa;
- Už tokios programos įgyvendinimą bus atsakinga Skaitmeninių reikalų ministerija;
- Siekiant optimizuoti žmogiškuosius išteklius KS srityje, bus sukurtas valdymo modelis tokiems resursams suvaldyti.

Kurk Lietuvai

KS GEBĖJIMŲ VYSTYMAS

- Sukurti sąlygas piliečiams saugiai naudotis kibernetine erdve.

  - Švietimas KS srityje turėtų prasidėti nuo mažų dienų. Saugus kibernetinės erdvės naudojimas užims pagrindinę dalį mokyklų programose;
  - Planuojama pradėti kursus IT mokytojams atnaujinti jų žinias ir atlikti atitinkamus pokyčius programose, kurios ruošia šios srities mokytojus;
  - Lygiagrečiai, bendradarbiaujant su NVO ir akademiniais centrais, valstybės administracija imsis sisteminių veiksmų, siekiant pakelti visuomenės sąmoningumo lygį ir supratimą apie grėsmes kibernetinėje erdvėje;
  - Bus pradėtos socialinės kampanijos skirtos skirtingoms žmonių grupėms pasiekti (vaikai, tėvai, vyresnio amžiaus žmonės ir pan.);
  - Valstybės administracija parems kritinės infrastruktūros ir skaitmeninių paslaugų tiekėjų veiksmus, kurių bus imamasi visuomenės informavimui ir švietimui. Tikslas - vartotojams suteikti žinias, kad jie suprastų apie kibernetines grėsmes ir kaip nuo jų apsisaugoti.

ČEKIJA

Čekija savo valstybės kibernetiniu saugumu susirūpino dar 2011 metais, kuomet buvo išleista primoji KS strategija. Tačiau iki pat 2013 metų, kuomet įvyko didžiausia kibernetinė ataka šalyje, trukusi kelias dienas, aktyvių veiksmų nebuvo imtasi. Valstybė suprato, kad jie turi gerinti savo KS būklę.

Ši šalis neišsiskiria savo duomenimis iš kitų vidurio Europos šalių, tačiau laiku pastebėjo KS švietimo svarbą ir tam ypatingą dėmesį skiria savo dabartinėje KS strategijoje.

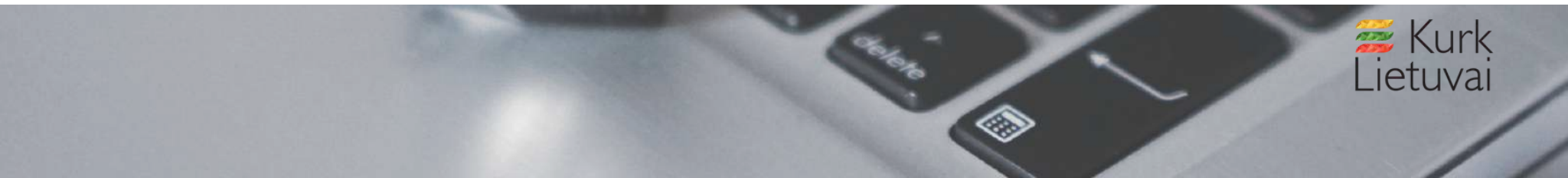
Kurk Lietuvai

ČEKIJOS KS STRATEGIJA 2015 - 2020M.

Čekija pirmąją savo KS strategiją išleido dar 2011 metais, tačiau rimtesnių veiksmų dėl KS buvo imtasi tik po 2013 metų. Šiuo metu Čekija turi naująją KS strategiją, kuri buvo patvirtinta 2015 metais ir yra skirta 5 metų laikotarpiui.

TIKSLAI:

- Svarbių struktūrų, procesų ir bendradarbiavimo efektyvinimas ir tobulinimas, siekiant užtikrinti KS saugumą;
- Aktyvus tarptautinis bendradarbiavimas;
- Nacionalinių kritinės infrastruktūros ir svarbios informacijos sistemų apsaugojimas;
- Bendradarbiavimas su privačiu sektoriumi;
- Moksliniai tyrimai/ Vartotojų pasitikėjimas;
- Švietimas, informavimo didinimas ir informacinės visuomenės vystymas;
- Remti Čekijos policijos pajėgumus tiriant ir pateikiant kaltinimus dėl kibernetinių atakų;
- KS teisinės sistemos tobulinimas. Dalyvavimas kuriant ir įgyvendinant Europinius ir tarptautinius reglamentus.



Kurk Lietuvai

KS STRATEGIJOS VEIKSMŲ PLANAS

Buvo numatytos konkrečios užduotys, kurių bus imamasi siekiant įgyvendinti penktąjį tikslą:
- Švietimas, informavimo didinimas ir informacinės visuomenės vystymas.

- Remti įvairias iniciatyvas ir visuomenės švietimo kampanijas; organizuoti konferencijos ir dirbtuves plačiajai auditorijai (vartotojams);
- Sukurti elektroninę mokymosi platformą plačiosios visuomenės ir ekspertų bendruomenės švietimui;
- Modernizuoti pradinių ir vidurinių mokyklų mokymų programas;
- Paruošti metodologiją ir medžiagą mokykloms, kad būtų lengviau įtraukti KS problemas į mokyklines programas;
- Paruošti užtektinai metodinės medžiagos mokytojams ir vykdyti mokymus KS srityje;
- Kartu su universitetais remti ir skatinti studentų talentą KS srityje;
- Suteikti galimybę studentams atlikti praktikas KS srityje Čekijoje arba užsienyje;
- Bendradarbiauti su universitetais ir kolegijomis kuriant naujas KS studijų programas ir jas įtraukiant į naujas mokymų programas;
- Institucionalizuoti kitas studijų programas, suteikiant sertifikatą baigus šias studijų programas;
- Padidinti švietimo kokybę KS srityje, taikant naujausius mokymo metodus.

APIBENDRINIMAS 1

- Kibernetinio saugumo svarba neabejoja niekas ir visos apžvelgtos valstybės juo anksčiau ar vėliau pradėjo rūpintis. Į kibernetinę saugą valstybės investuoja vis daugiau pinigų, ruošia KS strategijas ir kitus dokumentus, siekiant užtikrinti valstybės saugumą.
- Visos analizuotos valstybės KS pradėjo rūpintis skirtingais laikotarpiais ir tokios kaip JK ir JAV yra žymiai toliau pažengę KS srityje, todėl visų šių strategijų tarpusavyje lyginti nereikėtų, tačiau visoms joms yra būdingi keli bruožai:
  - Ypatingas dėmesys skiriamas KS švietimui, visuomenės informavimui ir specialistų ruošimui;
  - Pabrėžiamas privataus sektoriaus, viešojo sektoriaus ir akademijos bendradarbiavimas, kuris yra ypatingai svarbus norint pasiekti geresnių rezultatų;
  - Daugiausiai švietimo iniciatyvų inicijuoja Krašto apsaugos ministerijos arba Nacionaliniai kibernetinio saugumo centrai ar atitinkamos institucijos.

Kurk Lietuvai

APIBENDRINIMAS 2

Iš kiekvienos valstybės yra dalykų, kurių Lietuva galėtų pasimokyti ir geruosius pavyzdžius atitinkamai pritaikyti praktikoje.

- Nors JK kibernetine sauga rūpinasi ilgiau nei Lietuva, jų rengiamos iniciatyvos yra puikūs pavyzdžiai. Vienas tokių CYBER FIRST programa, kurią iniciavo Kibernetinio saugumo centras bendradarbiaujant su privačiu sektoriumi. Ši programa įtraukia vaikus nuo 11 metų iki studentų. Programos metu rengiami įvairūs konkursai mergaitėms ir tai leidžia valstybei išsiskirti.
- JAV savo kibernetinės erdvės saugumu rūpinasi jau 15 metų ir per tą laiką rengė įvairias iniciatyvas. Viena tokių buvo pradėta 2013 metais, kai Valstybinis saugumo departamentas pradėjo iniciatyvą, kurios metu buvo sukurtas internetinis šaltinis, kur galima rasti visą informaciją apie mokymus, studijas, informavimo programas ir pan. KS srityje. Šaltinis prieinamas visiems ir skirtas įvairioms auditorijoms.

Kurk Lietuvai

APIBENDRINIMAS 3

- Iš Lenkijos galime pasimokyti ryžtingumo. Ši šalis nusprendė, jog nori tapti KS industrijos lydere. Buvo atlikti tyrimai, kurių metu išryškėjo Lenkijos potencialas ir jie bandys ryžtingai to siekti. Tyrimo metu buvo numatyti tikslai, ką ir kaip riktų daryti, norint tapti lydere. Lietuva turi šansą neatsilikt ir imtis atitinkamų veiksmų, siekiant išsiskirti ir rasti savo pranašumus KS srityje.
- Čekijos KS strategijos veiksmų planas yra puikus pavyzdys, kurio uždavinius galima pritaikyti ir kuriant Lietuvos Nacionalinę kibernetinio saugumo strategiją. Akivaizdu, kad KS švietimui, mokymams ir visuomenės informavimui privaloma skirti ypatingą dėmesį, norint tapti saugia ir sėkminga šalimi KS srityje.

Kurk Lietuvai

Kibernetinės grėsmės gali būti įveikiamos technologijų pagalba, tačiau viskas priklauso nuo žmonių. Mes privalome investuoti į ateities profesionalų kartas, kurie pratęs šią kovą.

Matthew Rosenquist, 2015

Kurk Lietuvai

ŠALTINIAI

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
- https://www.consultancy.uk/news/16068/majority-of-companies-now-hit-by-a-cybersecurity-skills-gap
- https://www.cyberfirst.ncsc.gov.uk/girlscompetition/
- https://www.ncsc.gov.uk/new-talent
- https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf
- https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
- https://www.csoonline.com/article/3258994/data-protection/cybersecurity-skills-shortage.html
- https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf
- https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies
- https://niccs.us-cert.gov/about-niccs
- https://stopthinkconnect.org/about
- https://pl.asseco.com/en/news/poland-may-become-a-global-leader-in-the-cyber-security-sector-the-report-of-the-kosciuszko-institute-2482/
- http://www.ik.org.pl/wp-content/themes/ik/report-img/security-through-innovation.pdf
- https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSO_Poland_2017.pdf
- https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf
- https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Kurk Lietuvai

ŠALTINIAI

- https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf
- https://ccdcoe.org/sites/default/files/multimedia/pdf/The%20Czech%20Republic.%20A%20Case%20of%20a%20Comprehensive%20Approach%20toward%20Cyberspace_Lucie%20Kadlecov%C3%A1.pdf
- http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_czechrepublic.pdf

Kurk Lietuvai

KONTAKTAI

IEVA NAMAVIČIŪTĖ

ieva.namaviciute@kurklt.lt
ieva.namaviciute@investlithuania.com
+37060941313

Kurk Lietuvai

Investuok Lietuvoje