„Kurk Lietuvai“ projektų vadovai
Justas Kidykas, Rūta Beinoriūtė ir Gabrielė Bilevičiūtė

Vilnius, 2020

Pasiūlymai dėl smulkaus ir vidutinio verslo kibernetinio saugumo brandos kėlimo Lietuvoje

Šie pasiūlymai yra „Kurk Lietuvai“ projekto „Smulkiojo ir vidutinio verslo įmonių kibernetinio saugumo sąmoningumo didinimas“ dalis, kurie parengti atsižvelgiant į atliktas situacijos Lietuvoje ir pasaulyje apžvalgas, užsienio šalių gerųjų praktikų analizę, atliktą smulkaus ir vidutinio verslo (toliau – SVV) įmonių apklausą ir interviu ciklą su kibernetinio saugumo (toliau – KS) ekspertais iš viešojo, privataus ir akademinio sektorių. Pasiūlymai bus pateikti Krašto apsaugos ministerijai (toliau – KAM) ir Nacionaliniam kibernetinio saugumo centrui (toliau – NKSC), tačiau šiame dokumente aprašomos rekomendacijos yra aktualios ir kitoms suinteresuotoms valstybinio sektoriaus institucijoms.

Pasiūlymai skirti išryškėjusioms aktualiausioms problemoms spręsti, kurios apima: SVV kibernetinio saugumo sąmoningumo ir žinių trūkumą, kibernetinio saugumo higienos kėlimą Lietuvoje, glaudesnį viešojo ir privataus sektoriaus bendradarbiavimą kibernetinio saugumo (toliau – KS) srityje. Rekomendacijos yra teikiamos atsižvelgiant į Nacionalinėje kibernetinio saugumo strategijoje iškeltus tikslus ir uždavinius.

Įgyvendinus pateiktus pasiūlymus, valstybė galėtų sustiprinti savo vaidmenį KS srityje, suteikiant bazines ugdomąsias priemones SVV įmonėms, kurios neturi pakankamai žinių ar sugebėjimų pasirūpinti savo KS. Norint užtikrinti mūsų šalies ekonomikos augimą ir stabilumą, svarbu rūpintis tuo, kad SVV įmonės netaptų lengvomis kibernetinių incidentų aukomis ir skatinti jas kelti savo atsparumo lygį. Efektyvios SVV įmonių kibernetinio saugumo sąmoningumo ugdymo priemonės leistų stiprinti Lietuvos verslo atsparumą kibernetinėms grėsmėms ir keltų bendrą šalies kibernetinio saugumo kultūrą.

Įvadas

Kibernetinės atakos jau ne pirmus metus atsiduria tarp dažniausiai vykdomų nusikaltimų. Nepaisant to, kad atakos prieš smulkaus ir vidutinio verslo (SVV) įmones gana retai pasiekia žiniasklaidos antraštes, daugiau nei pusė visų kibernetinių atakų pasaulyje yra nukreiptos prieš SVV įmones. „Ponemon“ instituto duomenimis, net **66 proc. smulkaus ir vidutinio verslo įmonių 2018 metais patyrė kibernetinius incidentus**[1].

2018 m. Nacionalinis kibernetinio saugumo centras (NKSC) Lietuvoje užregistravo 53 183 kibernetinius incidentus. Nors bendras atakų skaičius nežymiai mažėja, NKSC pažymi, kad užfiksuojama vis daugiau pažangesnių ir sunkiau aptinkamų atakų. Nacionalinės kibernetinio saugumo būklės atskaitoje yra teigiama, kad vien 2018 metais incidentų, susijusių su socialinės inžinerijos metodais, skaičius Lietuvoje išsaugo net 25 proc. Tokie incidentai yra ypač svarbūs verslo įmonėms, kurios tokiu būdu patiria veiklos sutrikimus bei finansinę žalą ar praranda konfidencialią informaciją. Ekspertų teigimu, **gerosios KS praktikos atsiranda skiriant didesnį dėmesį individualių žmonių sąmoningumo ir žinių ugdymui**. Tą pažymi ir Nacionalinė kibernetinio saugumo strategija, kurioje teigiama, kad nuo kibernetinių incidentų apsisaugoti negalima net ir taikant visas egzistuojančias technines KS priemones, todėl labai svarbu, jog viešojo ir privataus sektoriaus atstovai rūpintųsi savo darbuotojų kibernetinės kultūros kėlimu.

Projekto metu atlikta išsami temos analizė parodė, kad SVV pažeidžiamumas išlieka aukštas dėl penkių pagrindinių priežasčių:

- **Naudojamų KS priemonių trūkumo.** 2019 m. Lietuvos statistikos departamento atliktas įmonėse naudojamų e. saugos priemonių tyrimas parodė, kad vidutiniškai mažos įmonės (10 – 49 darbuotojai) 36 proc. mažiau nei didelės įmonės (250+ darbuotojai) naudojo bent vieną kibernetinio saugumo / e. saugos priemonę. SVV įmonės dažnai nežino kaip reikėtų apsisaugoti nuo kibernetinių atakų ir jaučiasi nepasiruošusios atremti kibernetines atakas. Mažų įmonių KS priemonės dažnai yra nepakankamos. Dažnu atveju, atakai jau įvykus, smulkesnės įmonės neturi užtektinai žmogiškųjų ir techninių išteklių incidento suvaldymui ir situacijos atstatymui.

- **KS grėsmių rizikų neįvertinimo.** Nepaisant augančių grėsmių, verslas vis dar vangiai žiūri į KS kaip svarbų komponentą jų verslo tęstinumui. Atlikta SVV apklausa parodė, kad beveik pusė SVV įmonių nemano, jog gali būti kibernetinio įvykio aukomis. Didelės kompanijos apsaugai nuo tokių įvykių skiria nemažai lėšų, todėl pagrindiniais taikiniais tampa mažos įmonės, kurios dažnai patampa tiltu į stambesnes įmones tiekimo grandies viršuje.

- **Skaitmeninio turto vertės nesuvokimo.** Įmonės nesuvokia savo turimo skaitmeninio turto, jo vertės ir to, kad prarastas informacinis turtas gali sukelti didelių neigiamų pasekmių jų verslui. Dėl kibernetinio įvykio sutrikusi įmonės ar / ir internetinio puslapio veikla gali padaryti daug žalos, kurią sunku įvertinti.

[1] Ponemon Institute, „*2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*“ (2019), https://www.keeper.io/hubfs/PDF/2019_Ponemon_Infographic.pdf.

- **Darbuotojų žinių trūkumo.** Dauguma kibernetinių atakų yra sėkmingos ne dėl netinkamo SVV įmonių techninio pasiruošimo, bet dėl jų darbuotojų nepakankamo KS sąmoningumo. Kompetentingų darbuotojų trūkumą kaip didžiausią riziką įmonės saugumui įvertino net 70 proc. „Ponemon“ instituto tyrime dalyvavusių IT saugos specialistų[2].

- **KS priemonių kainos ir kompleksiškumo.** Verslui dažnai yra labai sudėtinga ir neaišku kaip reikėtų tikslingai įsivertinti įsilaužimo žalą, ko pasekmėje, įmonėms yra sunku įvertinti investicijų į kibernetinio KS grąžą. Mažesnės įmonės dažnai nemato prasmės apmokyti visų darbuotojų arba nėra linkusios tam skirti papildomų kaštų. „Kurk Lietuvai“ apklausa parodė, kad mažiau nei pusė (43 %) įmonių teigė turinčios pakankamai žinių ir supratimo, reikalingo kibernetinio saugumo priemonių pasirinkimui.

Programos „Kurk Lietuvai“ rėmuose 2019 m. spalio mėn. – 2020 m. sausio mėn. buvo įgyvendinta viešoji konsultacija, kurios tikslas – išgirsti tikslinių auditorijų nuomonę, siekiant nustatyti Lietuvos SVV (darbuotojų skaičius iki 250) įmonių KS padėtį ir poreikius šioje srityje, išsiaiškinti ar Lietuvos situacija atspindi esmines KS sąmoningumo problemas pasaulyje bei identifikuoti potencialias SVV įmonių KS stiprinimo priemones, kurias galėtų kurti ar įgyvendinti valstybės institucijos:

- Suorganizuotas interviu ciklas su kibernetinio saugumo ekspertais. Nustatyta, kokiais būdais yra efektyviausia stiprinti SVV įmonių KS įgūdžius, įvertinta KS sąmoningumo ugdymo svarba, valstybės vaidmuo keliant verslo KS brandą, konsultuotasi dėl bazinio lygio KS informacinio vadovo SVV įmonėms, kurios dar netaiko jokio sistemingo požiūrio į KS ir tokio dokumento naudingumą.
- Internetinėje platformoje „e. pilietis“ paskelbta elektroninė apklausa, kurios metu nustatytos Lietuvos SVV įmonių KS spragos, įvertintas SVV įmonių KS sąmoningumo lygis ir KS sąmoningumo stiprinimo priemonių poreikis.

[2] Ponemon Institute, „*What CISOs Worry about in 2018*“ (2018), https://www.hcinnovationgroup.com/cybersecurity/news/13029693/what-are-cisos-worried-about-in-2018-data-breaches-and-the-human-factor-survey-finds.

1. Problema: SVV kibernetinio saugumo vadovo tęstinumas

Informacinio SVV kibernetinio saugumo vadovo (toliau – Vadovas) išleidimas yra tik pirmasis žingsnis siekiant didinti mažų ir vidutinių privataus sektorių atstovų KS brandą. KS ekspertų teigimu, siekiant užtikrinti Vadovo tolimesnę sklaidą ir naudojimą tarp SVV įmonių yra **būtina tęsti komunikacinę kampaniją siekiant palaikyti Vadovo žinomumą ir naudojimą**. Šiuo kibernetinio saugumo vadovu siekiama padėti SVV įmonių vadovams geriau suprasti kibernetinio saugumo iššūkius ir rizikas, su kuriomis verslas susiduria kiekvieną dieną, dalinantis bazinio lygio patarimais ir gerosiomis praktikomis, kurios leistų įmonėms didinti jų kibernetinį atsparumą. Taigi, yra svarbu užtikrinti šio Vadovo tęstinumą.

1.1. Pasiūlymas Nr. 1: Platinti Vadovą visuose su KS ir verslu susijusiuose dokumentuose bei platformose

- KAM / NKSC pranešimuose susijusiuose su KS grėsmėmis ir įvykiais aktualiais verslui rekomenduojama įtraukti nuorodą į Vadovo PDF dokumentą.
- Siūlytina paruošti NKSC socialinės medijos kanalų komunikacijos planą, kuriuo būtų užtikrintas reguliarus trumpų pranešimų, orientuotų į Vadovo skilčių reklamavimą, paleidimas.
- Rekomenduojama įtraukti RRT, LRVK ir IVPK į Vadovo sklaidos procesą: pakviesti juos įsidėti Vadovą į savo el. svetaines bei įtraukti Vadovą į partnerių komunikacijos kampanijas.
- Siūlytina KAM skirti lėšų užsakomiesiems straipsniams nacionalinėje ir regioninėje žiniasklaidoje.
- Skatinti bendradarbiavimą su savivaldybėmis ir įvairiomis verslo asociacijomis skleidžiant žinią apie Vadovo naudą verslui.
- Glaudinti bendradarbiavimą su INFOBALT kibernetinio saugumo grupės nariais ir kitomis KS ar IT paslaugas teikiančiomis įmonėmis siekiant, kad privataus sektoriaus atstovai prisidėtų prie Vadovo sklaidos, nukreiptų klientus į Vadovą.

1.2. Pasiūlymas Nr. 2: SVV kibernetinio saugumo Vadovo turinio peržiūra ir atnaujinimas kas metus

Siūlytina atsižvelgti į KS grėsmių tendencijas Lietuvoje bei pasaulyje ir pagal tai atnaujinti kai kurias rekomendacijas. Taip pat, atsiradus **naujesnių atvejų pavyzdžių (*case studies*)**, pirmenybę teikiant Lietuvoje įvykusiems atvejams, būtų naudinga juos įtraukti į Vadovą ir taip palaikyti jo aktualumą. Rekomenduojama apsvarstyti galimybę kurti daugiau edukacinio turinio ir apie kibernetines nusikalstamas veikas bei priminti priežastis, kodėl SVV yra parankus taikinys programišiams.

Be to, siūlytina į Vadovą **įtraukti gerųjų pavyzdžių, kaip Lietuvos įmonės tvarkosi su savo KS arba įtraukti įmonių vadovų atsiliepimus (*testimonials*) apie Vadovą**. KS ekspertų teigimu, daugiau teigiamų rezultatų KS sąmoningumo ugdymo srityje būtų sulaukta būtent akcentuojant ir viešinant geruosius, o ne bloguosius pavyzdžius, nes negatyvi informacija ir gąsdinimas gali sukelti atmetimo reakciją. Taip pat, ateityje būtų galima sukurti ir į Vadovą įtraukti atskirą KS politikos šabloną, kurį SVV įmonės galėtų panaudoti ir pritaikyti savo poreikiams.

Dar vienas rekomenduojamas sprendimas yra išversti Vadovą į anglų kalbą, kadangi tai leistų ne tik plačiau paskleisti žinią apie Lietuvos pastangas ugdyti SVV KS sąmoningumą, bet ir sudarytų sąlygas susipažinti su jo turiniu ir užsienio KS ekspertams bei taip dalintis gerosiomis praktikomis ir patarimais.

1.3. Pasiūlymas Nr. 3: Panaudoti Vadovo turinį kuriant naujas KS priemones

Dokumente įtrauktas turinys ir pasiūlymai gali būti dar kartą panaudojami kuriant papildomas rekomendacijas. Įvertinus interviu ciklo metu išsakytas KS ekspertų įžvalgas, siūlytina atsižvelgti į tai, kokia veikla užsiima verslas ir kokie kibernetiniai įvykiai yra tikėtini / aktualūs būtent tai veiklos sričiai. Pavyzdžiui, KS rekomendacijų rinkinys aptarnavimo veiklos sektoriui arba rekomendacijos, kaip elgtis įvykus tam tikram kibernetiniam įvykiui (pvz., kaip apsisaugoti nuo ir elgtis nukentėjus nuo *ransomware* atakos). Toks metodas didintų SVV KS svarbos supratimą. Kartu, rekomenduojama ruošti konkrečių paminėtų temų **išplėstines ir / ar labiau vizualines (kelių puslapių) atmintines**, pavyzdžiui: apie *asmeninių įrenginių naudojimo* (BYOD) politiką, socialinę inžineriją, debesiją, BDAR ir KS, ir pan.

Tokie dokumentai galėtų būti ruošiami tiesiogiai pasitelkiant jau turimų rekomendacijų sąrašą, jas išplečiant ir pritaikant konkretesnius pavyzdžius. Siūlytina, kad kiekvienas toks dokumentas įtrauktų nuorodą į Vadovą, kur įmonė ar kiti subjektai visada galėtų bendrai susipažinti su KS pradmenimis ir pasitikrinti savo KS žinias bei įmonės pasirengimą atremti kibernetines grėsmes. Tokius dokumentus galėtų ruošti tiek pati KAM ar NKSC, ar kartu su „e.saugumas“ ir IVPK komandomis bei kitomis suinteresuotomis institucijomis.

2. Problema: SVV ir bendrai privataus sektoriaus kibernetinio saugumo būklės stebėsena

Iki „Kurk Lietuvai“ projekto pradžios, Lietuvoje ypatingai trūko kiekybinių duomenų apie Lietuvos SVV įmonių KS situaciją. Vienintelis Lietuvos statistikos departamentas yra atlikęs įmonių naudojamų e. saugos priemonių apklausą. Tad, ši „Kurk Lietuvai“ komandos Krašto apsaugos ministerijoje vykdyta apklausa buvo pirmoji apklausa Lietuvoje, kuria buvo siekiama įvertinti įmonių vadovų požiūrį į KS, vertinant jų suvokimą apie jų pasirengimą atremti kibernetines grėsmes, investicijas skiriamas KS ir pan. Atsižvelgiant į tai, kad vykdant šią apklausą buvo sulaukta daug teigiamų komentarų apie tokios apklausos prasmingumą, siūlytina KAM / NKSC pakartotinai rengti įmonių KS sąmoningumo apklausas ne vien dėl KS būklės stebėsenos, bet ir dėl apklausos švietėjiškos paskirties.

2.1. Pasiūlymas Nr. 1: Vykdyti reguliarius SVV įmonių KS sąmoningumo tyrimus

Rekomenduojama **tęsti SVV įmonių KS sąmoningumo tyrimus bent kartą į dvejus metus**, kad būtų galima reguliariai vertinti SVV įmonių KS situaciją Lietuvoje. Siūlytina, kad kitas toks tyrimas būtų atliktas 2021 m. Šis apklausos formatas taip pat gali būti panaudojamas kaip vienas iš būdų įsivertinti Strategijoje paminėtų priemonių, skirtų viešojo bei mažų ir vidutinių privataus sektorių atstovų KS būklei gerinti, efektyvumą.

Siūlytina, kad apklausos klausimyno apimtis būtų kiek mažesnė nei „Kurk Lietuvai“ darytos apklausos (< 28 klausimai). Itin svarbu, kad būtų siekiama įtraukti reprezentatyvią respondentų imtį (> 1000 įmonių vadovų). Ateityje vykdomose apklausose rekomenduojama įtraukti klausimą „Ar esate susipažinę su SVV kibernetinio saugumo informaciniu vadovu?“, tokiu būdu būtų galima nustatyti Vadovo efektyvumą. **Siekiamybė, kad ≥ 5 % apklaustų įmonių būtų susipažinusios su šiuo Vadovu**.

Kiti apklausos / tyrimo KPI: **Sąmoningumo kriterijai**	**2019 m.** („Kurk Lietuvai“ vykdyta apklausa)	**Siekiama – 2021 m.**
Kibernetinio saugumo politiką įsivedusių įmonių dalis (proc.)	29 %	≥ 35 %
Rizikos vertinimą per pastaruosius 12 mėn. vykdžiusių įmonių dalis (proc.)	14 %	≥ 20 %
Įmonių organizavusių kibernetinio saugumo mokymus dalis (proc.)	26 %	≥ 30 %
Įmonių sutinkančių, kad yra pasiruošusios atremti kibernetines atakas dalis (proc.)	26 %	≥ 35 %
Įmonių sutinkančių, kad turi pakankamai žinių, reikalingų kibernetinio saugumo priemonių pasirinkimui, dalis (proc.)	43 %	≥ 55 %

Ateities tyrimai gali būti organizuojami kartu su Lietuvos statistikos departamentu bei konsultuojantis su INFOBALT kibernetinio saugumo grupės nariais dėl apklausos klausimyno atnaujinimo ar papildymo.

3. Problema: Viešojo sektoriaus siūlomų į verslą orientuotų KS priemonių trūkumas

Žinant, kad SVV įmonės sudaro 99,6 proc. visų Lietuvos įmonių ir sukuria daugiau nei du trečdalius šalies bendro vidaus produkto, SVV KS brandos klausimas atliepia ne tik ekonominio vystymosi ir stabilumo poreikius, bet ir daro tiesioginę įtaką bendrai šalies KS situacijai.

Esamoji analizė parodė, kad **viešojoje erdvėje pateikiama informacija apie KS yra gana fragmentiška ir nesusisteminta.** Jos yra daug, skirtingomis temomis, pritaikytos skirtingo žinių lygio auditorijoms, o įvairūs tarptautiniai standartai, tokie kaip ISO šeimos sertifikatai ar COBIT, dažnai yra sunkiai suprantami mažų įmonių vadovams arba per daug kompleksiški smulkaus verslo poreikiams. Dėl to, ekspertai pastebi akivaizdų vieno patikimo ir centralizuoto pirminio nesudėtingo informacinio šaltinio, kuris leistų ne IT specialistams geriau įsisavinti kibernetines rizikas ir KS priemonių svarbą, trūkumą. Vadovas dalinai užpildo šią informacinę spragą, tačiau siūlytina imtis tolimesnių iniciatyvų. Užsienio šalių praktika rodo, kad viešasis sektorius nelieka nuošalyje ir deda pastangas, kad kuo didesnė dalis įmonių turėtų bazinius KS standartus ir būtų paskatintos rūpintis savo kibernetiniu atsparumu.

3.1. Pasiūlymas Nr.1: Stiprinti valstybės vaidmenį KS srityje

Jungtinės Karalystės ir Belgijos šalių praktika rodo didėjančią paklausą iš verslo pusės, kad valstybinės institucijos teiktų **daugiau susistemintos ir lengvai prieinamos informacijos apie žingsnius ir gerąsias praktikas**, padedančias stiprinti įmonių KS. Be to, interviu ciklo metu, respondentai pabrėžė, kad valstybės vaidmuo šiame kontekste yra labai didelis, nes valstybė gali skatinti įvairias iniciatyvas, ji yra atsakinga už KS brandos kėlimą, todėl turėtų paruošti metodikas, nemokamai jomis dalintis bei organizuoti nemokamus kursus. Suprantama, kad tokių paslaugų pasiūla labai priklauso nuo jų efektyvumo bei turimų žmogiškųjų ir finansinių išteklių, dėl to siūlytina svarstyti galimybę didinti NKSC biudžeto dydį ar etatų kiekį, siekiant įgalinti NKSC ir pačią valstybę imtis didesnės švietėjiškos rolės KS srityje.

3.2. Pasiūlymas Nr.2: Nemokamų interaktyvių KS didinimą skatinančių priemonių kūrimas

Atsižvelgiant į Jungtinės Karalystės gerąją praktiką, rekomenduojama KAM bei NKSC kurti SVV skirtus nemokamus interaktyvius **mokomuosius testus / užduotis, kurie būtų pateikiami su skirtingais scenarijais:** įmonės vadovui, IT politikos sprendimus priimančiam žmogui, IT specialistui, komunikacijos specialistui, žmogiškųjų išteklių arba įmonės teisės specialistui. Tokios interaktyvios užduotys leistų SVV ugdyti savo darbuotojų KS / IT sugebėjimus, nustatyti sritis, kurias dar reikia toliau tobulinti bei įsivertinti, kiek veiksmingi yra įmonės KS ir reagavimo mechanizmai.

Kuriant tokią priemonę siūlytina atsižvelgti į Jungtinės Karalystės sukurtą nemokamą lengvai prieinamą internetinę priemonę *Exercise in a box*, kuri leidžia SVV įmonėms ir kitoms organizacijoms pasitikrinti, kaip įmonė elgtųsi kibernetinio įvykio atveju ir taip padeda stiprinti jų kibernetinį

atsparumą. Britų duomenimis, tokia jų paslauga per pastaruosius 12 mėn. pasinaudojo beveik 3 tūkstančiai įmonių, tai leidžia manyti, kad tokia priemonė būtų paklausi ir atneštų teigiamų rezultatų didinant KS sąmoningumą.

Rekomenduojama sukurti įsivertinimui skirtą **interaktyvų sąrašą (angl. *checklist*) / įrankį, kurį naudojant įmonė ar organizacija galėtų pasitikrinti kokias rekomenduojamas technines ir organizacines priemones yra įsidiegusi įmonė**. Suomijos ir Jungtinės Karalystės tyrimai atskleidžia, kad savarankiškas įsivertinimas yra veiksminga priemonė siekiant, kad įmonės keltų savo sąmoningumo lygį ir įsisavintų KS svarbą bei naudą. Siūlytina sukurti **interaktyvų ir automatizuotą įmonės KS įsivertinimo įrankį**, kuris užpildžius klausimyną nustatytų įmonės KS lygį ir sugeneruotų konkrečias rekomendacijas.

3.3. Pasiūlymas Nr.3: Paruošti įvadinį KS rizikos valdymo modelį skirtą įmonių vadovams

Siūlytina bendradarbiaujant su privačiu sektoriumi **paruošti įvadinį KS rizikos valdymo modelį** lietuvių kalba skirtą įmonių vadovams. KS ekspertų nuomone, ISO, COBIT ir kiti naudojami IT bei KS rizikų valdymo modeliai SVV yra per daug kompleksiški ir sunkiai įgyvendinami, jau nekalbant apie labai smulkias įmones, kurioms pirmasis žingsnis turėtų būti KS klausimo įtraukimas į verslo rizikų ir tęstinumo vertinimą. Taip pat, reikia įvertinti ir tai, kad toms įmonėms, kurios jau yra supratusios KS svarbą, didžiausias iššūkis išlieka būdai, kaip jos gali kokybiškai įsivertinti ir valdyti rizikas, dėl kurių įmonės galiausiai pasirenka neinvestuoti daugiau kaštų į KS priemones. Dėl to, siūlytina, kad vienas iš pirmųjų nemokamų priemonių būtų trumpas (iki 10 psl.) KS rizikų įsivertinimo proceso pradžiamokslis.

3.4. Pasiūlymas Nr.4: Reklamuoti jau esamas patikimas KS priemones

Viešojoje erdvėje, tiek Lietuvoje, tiek užsienyje yra sukurta nemažai naudingų nemokamų KS priemonių, kurių naudojimas prisidėtų prie SVV KS stiprinimo. Siūlytina NKSC sudaryti tokių **priemonių sąrašą ir viešai skelbti savo tinklalapyje** tam, kad ne tik SVV, bet ir kiekvienas žmogus žinotų apie tokių priemonių egzistavimą ir jų naudojimo patikimumą / saugumą. Dėl nuolat kintančių kibernetinių atakų, rekomenduojama tokį sąrašą reguliariai peržiūrėti ir atnaujinti.

Kitas esamų priemonių panaudojimo pavyzdys yra – „Prisijungusi Lietuva“ projektas, kurio metu buvo sukurta platforma su mokomąja medžiaga, kurią būtų galima toliau naudoti kuriant įvairų interaktyvų turinį, įskaitant ir medžiagą orientuotą į įmonių vadovus.

3.5. Pasiūlymas Nr.5: Didinti tarpsektorinį bendradarbiavimą KS tema

Efektyvus tarpsektorinis bendradarbiavimas sudarytų sąlygas naujų KS priemonių ir sėkmingų KS sąmoningumo ugdymo kampanijų kūrimui bei viešinimui, užtikrintų sklandų ir naudingą dalijimąsi gerosiomis praktikomis.

Siūlytina daugiau bendradarbiauti su akademiniu sektoriumi. Interviu ciklo respondentai pabrėžė **kibernetinių atakų imitavimu paremtų testavimų**, kai saugumo studentų komandos ar kokia nors KS įmonė simuliuoja kibernetines atakas, kurių metu bandoma pavogti įmonės tinkle esančius duomenis, **naudą**. Toks metodas leistų įmonėms tiesiogiai parodyti egzistuojančias jų KS spragas. Rekomenduojama KAM bei NKSC apsvarstyti dėl tokios praktikos įgyvendinimo glaudesnio bendradarbiavimo su Lietuvos akademiniu sektoriumi, kuris jau vykdo tokią praktiką, užmezgimą. Su įmonių sutikimu yra simuliuojama kibernetinė ataka, o vėliau įmonei yra pateikiama ataskaita ir rekomendacijos, taip pat galimi ir vėliau organizuojami mokymai tose KS srityse, kur įmonei sekasi

sunkiau. Šioje vietoje dar svarbu pabrėžti ir tai, kad šio bendradarbiavimo metu ypač daug naudos gautų ir studentai, kurie ne tik galėtų savo teorines žinias pritaikyti praktikoje, prisidėti prie Lietuvos verslo KS kėlimo, bet ir būtų labiau matomi darbo rinkoje.

Rekomenduojama **stiprinti Kibernetinio saugumo tarybos veiklą**, kurios susitikimai nėra periodiški ir jų potencialas nėra visapusiškai išnaudojamas. Siūlytina, kad Kibernetinio saugumo tarybos susirinkimai būtų reguliarūs. Tik dirbant kartu ir reguliariai akademinis, privatus ir valstybinis sektoriai gali užtikrinti sėkmingą KS sąmoningumo sklaidą ir didinti verslo pasirengimą ir atsparumą kibernetinėms grėsmėms.

KAM / NKSC tarpsektorinis bendradarbiavimas yra labai reikšmingas, nes jo metu galima skleisti svarbią informaciją apie KS grėsmes ir silpnąsias vietas, koordinuoti efektyvų incidentų valdymą ir stiprinti kritinės infrastruktūros atsparumą KS grėsmėms. Pavyzdžiui, KAM / NKSC glaudžiai bendradarbiaujant su savivaldybėmis, įvairiomis verslo asociacijomis ir verslo informacijos centrais būtų galima sėkmingai dalintis informacija KS tema ar / ir naujomis viešojo sektoriaus sukurtomis KS priemonėmis.

3.6. Pasiūlymas Nr. 6: Surengti kibernetinio saugumo dirbtuves (angl. hackathon) KS priemonių kūrimui

2019 metais Lietuvoje įvyko pirmosios „ESET Lietuva“ organizuotos KS dirbtuvės, kuriose buvo kuriami KS sprendimai skirti verslui. Tokių dirbtuvių metu yra sudaromos itin palankios galimybės specialistams vienoje vietoje keistis gerosiomis praktikomis, mokytis vieniems iš kitų bei kurti naujus sprendimus. Kadangi Lietuvoje viešasis sektorius dar nėra rengęs tokių KS dirbtuvių, skirtų būtent verslui, siūlytina KAM kartu su NKSC pirmą kartą surengti tokio formato renginį. Tai ne tik stiprintų valstybės vaidmenį ir KAM įsitraukimą atliepiant KS temos aktualinimą verslo kontekste, bet ir sudarytų sąlygas naujų, mažai kaštų reikalaujančių, KS priemonių kūrimui. Į tokias dirbtuves rekomenduojama įtraukti ne tik IT specialistus, bet ir KS ekspertus iš visų sektorių – viešojo, akademinio ir privataus.

2019 metais vykusiose dirbtuvėse dalyvavo apie 80 IT specialistų, tai parodo, koks didelis yra susidomėjimas ir tokių dirbtuvių poreikis.

Reikšminga paminėti, kad „Kurk Lietuvai“ programos projekto KAM vykdyto interviu ciklo metu atstovai iš visų minėtų sektorių pritarė bendradarbiavimo būtinybei ir įžvelgė visapusę naudą.

3.7. Pasiūlymas Nr. 7: Tarptautinis bendradarbiavimas

Tiek ES šalyse, tiek už ES ribų, susiduriama su KS švietimo problemomis verslo tarpe, dėl to, rekomenduojama NKSC glaudinti bendradarbiavimą su kitų ES (ir ne ES šalių) kibernetinio saugumo centrais siekiant bendromis jėgomis kurti KS priemones bei dalintis gerosiomis patirtimis KS sąmoningumo kėlimo srityje. „Kurk Lietuvai“ projekto metu užmezgus kontaktą su Belgijos NKSC atstovais, buvo išreikštas noras dalintis gerosiomis KS sąmoningumo ugdymo praktikomis.

4. Problema: Sistemingų komunikacinių priemonių KS tema verslui trūkumas ir neefektyvumas

Komunikacija KS sąmoningumo didinime užima labai svarbią vietą, nes dažnai visuomenė nežino apie tam tikrų techninių KS priemonių egzistavimą, naujausias KS tendencijas, įvykius ir apskritai nesupranta KS svarbos šiandieniniame pasaulyje. Todėl, kibernetinėms atakoms tobulėjant ir nuolat kintant šiandien yra svarbu turėti **sistemingą komunikacijos planą ir išlaikyti aktyvų komunikacijos tęstinumą tam, kad visuomenė ir verslas būtų nuolatos šviečiami apie KS grėsmes.** Dauguma KS ekspertų akcentavo, kad trumpos informacinės kampanijos, tokios kaip „Sustiprink imunitetą“, dažnai turi tik trumpalaikį efektą, perpildo informacinę erdvę turiniu apie KS, o jų ilgalaikis efektas ir nauda yra sunkiai pamatuojami. Lietuvoje vis dar trūksta vieningo KS komunikacijos veiksmų plano, kuris užtikrintų KS informacinių kampanijų nuoseklumą, aktualumą bei skatintų ne tik tarpinstitucinį, bet ir tarpsektorinį bendradarbiavimą, nurodytų temų bei atsakomybių pasiskirstymą.

4.1. Pasiūlymas Nr.1: Viešinti daugiau informacijos apie įvykusius kibernetinius įvykius

KS ekspertai taip pat pabrėžė, kad būtų naudinga viešinti daugiau informacijos apie Lietuvoje ir užsienyje įvykusius kibernetinius įvykius. Rekomenduojama pateikti **mažiau teorijos ir daugiau praktinių pavyzdžių,** taip siekiant ugdyti įmones atitinkamai elgtis panašioje situacijose bei priversti susimąstyti apie KS svarbą ir galimus nuostolius pažeidimo atveju. Palyginimui, britų NKSC viešina savaitines KS apžvalgas apie naujai atsiradusias kibernetinių pažeidimų tendencijas ar atskleistas svarbias spragas dažnai naudojamose PĮ ar OS.

4.2. Pasiūlymas Nr.2: NKSC komunikacinių kanalų stiprinimas

Rinkodara per socialines medijas yra vienas iš universaliausių ir efektyviausių būdų, kuriais galima pasiekti tikslinę auditoriją ir didinti savo žinomumą. Didžioji dalis žmonių šiais laikais naudojasi socialinėmis medijomis ir jų skaičius vis didėja.

Rekomenduojama stiprinti NKSC *Facebook* paskyrą. Ši paskyra **gali būti išnaudojama parodant visuomenei suprantamą ir aktualią KS pusę. Tokiu būdu galima būtų kelti tiek pasitikėjimą NKSC, tiek visuomenės pasiekiamumą, o didėjant NKSC žinomumui verslo KS sąmoningumo lygis taip pat būtų didinamas**. Kiekvienas skelbiamas turinys socialinėse medijose yra puiki galimybė didinti NKSC svetainės žinomumą ir lankomumą.

Siekiant, kad rezultatai būtų kuo geresni, siūlytina NKSC *Facebook* paskyroje kurti tokį turinį, kuris įtrauktų žmones, būtų kuo kokybiškesnis ir vertingas, pavyzdžiui, atsižvelgti į KS aktualijas, skelbti KS patarimus, KS mitus ir faktus, apklausas vienu ar kitu klausimu, trumpus video ir kt. Be to, svarbu, kad paskyroje pranešimai būtų skelbiami aktyviai ir reguliariai, taip išlaikant auditorijos dėmesį ir susidomėjimą.

Reikšminga akcentuoti tai, kad pasitelkiant skirtingus socialinius tinklus galima pritraukti kuo įvairesnę auditoriją. Todėl siūlytina apsvarstyti ir NKSC *LinkedIn* paskyros sukūrimą. Ši profesinė platforma gali būti puikiai išnaudojama NKSC skleidžiant informaciją skirtą tikslinei auditorijai – verslui. Verta paminėti, kad pasitelkus šią platformą NKSC galėtų didinti savo žinomumą ne tik Lietuvoje, bet ir užsienyje. Socialinių medijų tinklai beveik nereikalauja jokių finansinių išteklių, daugiausia žmogiškųjų (laiko) išteklių, tačiau net **ir su minimaliais galima pasiekti labai reikšmingų rezultatų**. Dar vienas socialinių medijų privalumas yra tas, kad jos suteikia galimybę geriau pažinti auditoriją, taigi

NKSC turėtų progą susipažinti su tuo, kas labiausia KS srityje domina ne tik verslą, bet ir individualius asmenis, atsižvelgti kokios informacijos jiems reikėtų daugiau, o ką reikėtų patobulinti savo (NKSC) veikloje.

Atsižvelgiant į gerąsias užsienio šalių praktikas bei į tai, kad kas antras SVV įmonių vadovas atsakė, kad patraukliausias būdas žinioms apie KS stiprinti jiems būtų informacija internetiniuose puslapiuose, o tarp labai smulkių įmonių netgi išskirtas, kaip pats patraukliausias komunikacijos kanalas, rekomenduojama apsvarstyti **atskiros skilties, skirtos būtent verslui, sukūrimą NKSC puslapyje**. Tokia skiltis leistų dar greičiau SVV rasti visą reikiamą informaciją vienoje vietoje. Šioje skiltyje būtų efektyvu patalpinti ir Vadovą. Taip pat, atsižvelgiant į KS ekspertų nuomonę, siūlytina tokią skiltį padaryti **kuo labiau draugišką vartotojui (*user-friendly*) – patrauklūs dizaino sprendimai, aiški bei susisteminta informacija**, interaktyvios užduotys, mokomoji video medžiaga, dažniausiai užduodami klausimai, KS stiprinimo priemonės, skirtos verslui ir kt. Dar svarbu atkreipti dėmesį į tai, kad šiuo metu ne tik SVV, bet ir plačiajai visuomenei trūksta informacijos apie tai kam pranešti įvykus kibernetiniam įvykiui. Siūlytina KS SVV skiltyje NKSC puslapyje pateikti informaciją ne tik apie tai kam pranešti apie įvykusį kibernetinį incidentą, bet ir kokios procedūros laukia pranešus.

Dėl šių išvardintų priežasčių, rekomenduojama **plėtoti NKSC viešąją komunikaciją**, siekiant, kad sustiprėtų NKSC žinomumas ir NKSC taptų pagrindiniu verslo informacijos apie KS šaltiniu.

4.3. Pasiūlymas Nr.3: Komunikacinių priemonių rinkiniai skirti SVV įmonių vadovams

Interviu ciklo metu KS atstovai ir ekspertai iš visų sektorių akcentavo tai, kad ugdant KS sąmoningumą yra būtina, jog kibernetinio saugumo svarbą suprastų įmonių vadovai, nes jie ne tik formuoja įmonių politikas, gali turėti įtakos darbuotojų KS žinių lygio kėlimui, bet ir skirsto įmonės finansinius išteklius. Atsižvelgiant į tai ir į gerąją belgų praktiką, rekomenduojama KAM bei NKSC sukurti **komunikacinių priemonių rinkinį skirtą SVV įmonių vadovams didinti KS sąmoningumą įmonės viduje**. Pavyzdžiui, belgai tokiame priemonių rinkinyje pateikia el. laiškų šablonus, skirtus siuntimui įmonės darbuotojams, trumpas skaidres su pastabomis pranešėjui, plakatus bei trumpus veiksmų planus įmonės vadovui su patarimais, kaip surengti tokią kampaniją. Taip pat, siūlytina rengti reguliarius seminarus, konferencijas, skirtus būtent SVV įmonių vadovams.

Atliktos viešosios konsultacijos (apklausų ir interviu ciklo) gauti rezultatai rodo, kad dažnai SVV įmonėms IT ir saugumas yra sinonimai ir yra tikimasi, kad IT paslaugų teikėjai taip pat atliks ir nemokamą IT paslaugų palaikymą / atnaujinimus. Neretai sudaromos sutartys su IT paslaugų teikėjais (ar el. svetainių kūrėjais) būna vienkartinės, taip IT paslaugų teikėjas atsitikus kibernetiniam įvykiui nėra įpareigotas padėti / konsultuoti įmonę. Be to, SVV įmonių vadovams trūksta supratimo kokia yra IT sprendimų atnaujinimų svarba KS ir kokių pasekmių kibernetinio įvykio atveju galima tikėtis. Siūlytina parengti komunikacines **žinutes su paprastais patarimais į kokius svarbiausius aspektus SVV turėtų atsižvelgti sudarant sutartis su IT paslaugų teikėjais** ir kodėl yra svarbu rūpintis nuolatiniais IT atnaujinimais bei peržiūra. Rengiant tokias žinutes svarbu turėti omenyje, kad SVV vadovų IT žinios ne visada yra aukšto lygio, taigi tokie patarimai būtų labai naudingi.

4.4. Pasiūlymas Nr.4: Sukurti KS standartų laikymąsi skatinančių priemonių

Analizuoti užsienio šalių geriųjų praktikų atvejai rodo, kad valstybės beveik nemato naudos iš privalomų KS reikalavimų. Rekomenduojama, kad Lietuvoje KS standartai būtų skatinami, o ne privalomai taikomi. Tai turi būti **siekiamybė, kurios link galėtų eiti įmonės, įvertinusios KS priemonių naudą, jų**

investicijų grąžą ir galimą kibernetinių įvykių ne tik momentinę žalą, bet ir ilgalaikėje perspektyvoje kylančias grėsmes jų verslui. Moksliniai tyrimai rodo, kad geryjų praktikų pavydžiai bei konkurencingumo skatinimas yra geriausia priemonė siekiant, kad daugiau įmonių diegtųsi KS priemones. Reikšminga atsižvelgti į tai, kad įrodymas įmonių vadovams, jog KS standartai turi tiesioginės naudos verslo reputacijai laikomas vienu iš didžiausių paveikiųjų veiksnių[3]. Projekto konsultacijų su ekspertais metu, kaip viena iš galimų paskatinimo priemonių buvo pasiūlytas KS standarto įtraukimas į „Verslo žinių" dienraščio projekto „Gazelės" atrankos kriterijų sąrašą. Šis apdovanojimas yra pripažįstamas ir tarptautinėje rinkoje bei yra patikimo verslo įrodymas, taigi norėdamos jį gauti SVV įmonės būtų suinteresuotos taikyti tam tikrus KS standartus. Rekomenduojama apsvarstyti ir kitų galimų papildomų skatinimo priemonių SVV įmonėms kūrimą.

4.5. Pasiūlymas Nr.5: Įsitraukti į European Cybersecurity Month informacinę kampaniją

Siūlytina kartu su kitomis valstybinėmis institucijomis (LRVK, RRT, ŠMSM, Lietuvos Policija) dalyvauti ENISA koordinuojamoje *European Cybersecurity Month* informacinėje kampanijoje. RRT jau yra dalyvavusi šioje kampanijoje, tačiau čia galima įžvelgti platesnį potencialą NKSC ir kitoms institucijoms kelti visuomenės KS žinių lygį. Tai kartu leistų optimizuoti institucijų laiko ir išteklių eikvojimą, kadangi bendra kampanijos tematika, dalis grafinio turinio ir veiklų idėjų būtų siūlomos ENISA iniciatyva. Tuo pačiu, Lietuvos specialistai irgi turėtų įtakos formuojant KS žinutę Europiniu mastu. Be to, mokomoji medžiaga galėtų būti lengvai pritaikyta tolesniam naudojimui lietuvių kalba.

[3] Barton, K. A., Tejay, J., Lane, M., & Terrell, S,. (2016) "Information System Security Commitment: A Study of External Influences on Senior Management." *Computers & Security* 59: 9-25. Print.

5. Problema: KS į(si)vertinimo mechanizmo trūkumas Lietuvoje

Gerosios užsienio šalių praktikos rodo didėjančią vyriausybės remiamų KS (neprivalomų) standartų sertifikavimo paslaugų paklausą ir pasiūlą. Tokios **KS sertifikavimo sistemos ne tik didina klientų pasitikėjimą verslu, jo paslaugomis, bet ir skatina konkurencingumą tarp įmonių, aukštesnių standartų siekimo bei svarbiausia kelia bendrą verslo KS lygį**.

„Kurk Lietuvai“ programos projekto KAM atliktos SVV įmonių apklausos rezultatai rodo, jog 37 proc. SVV įmonių vadovų sutinka, kad KS įvertinimo sertifikatas atneštų naudos jų įmonei. Net 78 proc. SVV įmonių įžvelgiančių tokio sertifikato naudą sutiktų mokėti už tokią paslaugą. Apklausoje sertifikatas buvo apibrėžtas kaip „viešas liudijimas ar / ir dokumentas parodantis, kad įmonės kibernetinio saugumo lygis yra įvertintas ir ji yra įsidiegusi tam tikrą standartą atitinkančias kibernetinio saugumo priemones.“

Interviu ciklo **metu KS ekspertai taip pat teigiamai įvertino KS sertifikato naudą Lietuvos verslui ir sutiko**, kad sertifikatas atneštų teigiamų rezultatų. Pasak ekspertų, **sertifikato reikalavimo įvedimas į viešųjų pirkimų konkursinę dalį** ženkliai prisidėtų prie KS situacijos keitimo Lietuvoje. Be to, interviu ciklo metu KS atstovai pabrėžė, kad sertifikatas gali būti tik viena iš organizacinių priemonių, tačiau vien tik jo neužteks. Siekiant, jog sertifikatas ne tik veiktų, bet ir duotų teigiamų rezultatų reikia taikyti ir stiprinti visas KS priemones.

Sektinas pavyzdys galėtų būti Jungtinės Karalystės Vyriausybės remiama KS į(si)vertinimo programa *Cyber Essentials*. Tai – 2014 metais sukurta nacionalinė programa, kurios tikslas yra kelti JK kibernetinio saugumo subjektų bazinį KS lygį bei skatinti informacinio saugumo gerąsias praktikas. Ši iniciatyva buvo sukurta orientuojantis būtent į smulkesnį šalies verslą (bet pritaikoma ir kitiems), supratus, kad kitos britų NKSC teikiamos priemonės ar kiti saugumo kontrolės priemonių standartai (kaip ISO 27001) dažnu atveju yra per sudėtingi ir sunkiai pritaikomi mažesnėms įmonėms, kurios neturi finansinių resursų ar reikalingų žinių leidžiančių įgyvendinti atitinkamas priemones.

Dėl šių priežasčių, *Cyber Essentials* standartas buvo rengiamas atsižvelgiant į tai kokie yra dažniausiai pasitaikantys kibernetiniai incidentai ir kokios yra bazinės priemonės leidžiančios stiprinti įmonių atsparumą. Be to, kaip ir kitos į SVV orientuotos sąmoningumo ugdymo priemonės, siekiama, kad KS **standartas, kaip paskatų mechanizmas**, taip pat paragintų įmones imtis ir tolimesnių KS priemonių bei keistų jų KS kultūrą.

Cyber Essentials KS kontrolės priemonės buvo pasirinktos atsižvelgiant į dažniausiai įvykstančių įsilaužimų rizikos scenarijų ir pagal tai parenkant bazinio lygio KS sprendimus siekiant, kad įmonė būtų tikra, jog ji imasi atitinkamų saugumo priemonių. Norint išsaugoti kitų smulkaus verslo prioritetų pusiausvyrą, pasirinktos kontrolės priemonės atneštų apčiuopiamos naudos verslui ir sumažintų žalą kibernetinio incidento atveju. Pasirinktos sritys yra[4]:

- Saugios interneto prieigos sukūrimas ir ugniasienių diegimas;
- Saugi prietaisų konfigūracija;
- Saugi prieigos kontrolė;
- Apsauga nuo kenkėjiškų programų;
- Automatinis pataisų taikymas.

[4] https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure

Kaip veikia sertifikavimo procesas?

Britų NKSC patvirtino ir prižiūri[5] penkias akreditavimo įstaigas, kurios yra atsakingos už jų sertifikuojančių įstaigų tinklą. Programos įkūrimo pradžioje buvo parinktos penkios skirtingos akreditavimo įstaigos siekiant užtikrinti sąžiningą konkurencingumą šioje srityje. Tačiau nuo 2020 m. balandžio, akreditavimo įstaigos statusas bus paliktas tik vienai įstaigai – *IASME Consortium*, tokiu būdu siekiant užtikrinti vertinimo nuoseklumą tarp visų sertifikavimo įstaigų. Šiuo metu, *IASME Consortium* vienija daugiau nei 150 skirtingų įstaigų teikiančių sertifikavimo paslaugas[6].

Įmonė norinti pradėti sertifikato įsigijimo procesą:

1) Per akreditavimo įstaigą susisiekia su sertifikuojančia įstaiga;
2) Nusprendžia ar įmonė nori sertifikuoti visą IT infrastruktūrą (įskaitant visus asmeninius ir mobilius įmonės įrenginius bei debesijos ar interneto aplikacijų paslaugas teikiančių įmonių atitikimą) ar tik jos dalį;
3) Užpildo sertifikuojančios įstaigos pateiktą 50-ties klausimų ilgio įsivertinimo klausimyną[7], kuris yra sudarytas atsižvelgiant į aukščiau paminėtas penkias kibernetinio saugumo kontrolės sritis. Kadangi klausimyne yra pateikiami visi minimalūs reikalavimai, įmonė turi tris mėnesius užpildyti klausimyną t.y. tris mėnesius įgyvendinti reikiamas kibernetinio saugumo priemones.
4) Sertifikuojanti įstaiga peržiūri ir įvertina klausimyną, pateikia išvadas ir tolimesnes rekomendacijas, jei reikia, akredituojančiai įstaigai;
5) Sertifikuojanti įstaiga atlieka papildomą nuotolinį spragų patikrinimą (*vulnerability scan*) įsitikinant, kad laikomasi iškeltų kontrolės mechanizmų ir kad nėra jokių praleistų spragų;
6) Įmonės siekiančios įgyti aukštesnio lygio *Cyber Essentials Plus* sertifikatą taip pat turi suorganizuoti papildomus įvertinimus vietoje, siekiant užtikrinti, kad nėra jokių vidinių spragų įmonės IT infrastruktūroje. Šis papildomas įvertinimas apima dalies darbuotojų įrenginių, serverių, maršrutizatorių ar kitų priėjimą prie interneto turinčių įrenginių patikrą. Tam tikrais atvejais, atliekami ir papildomi patikrinimai;
7) Akreditavimo įstaiga įvertina sertifikavimo įmonės išvadas ir išduoda sertifikatą. Jei įmonės KS priemonės neatitinka reikalavimų, jai yra pateikiamos rekomendacijos dėl kontrolės priemonių įgyvendinimo;
8) Gavus patvirtinimą, įmonė gauna sertifikatą (ženklą), kurį gali viešinti savo puslapyje bei įmonės oficialiuose dokumentuose. Įmonė taip pat įtraukiama į viešai skelbiamą *Cyber Essentials* sertifikatą įgijusių įmonių ir organizacijų sąrašą[8];
9) Pagal naują tvarką, sertifikatas galios vienerius metus, po kurio įmonė turės vėl įrodyti ar yra laikomasi nustatytų kibernetinio saugumo reikalavimų;

Paprasto *Cyber Essentials* sertifikato įgijimo kainą – 300 (+ PVM) svarų. O *Cyber Essentials Plus* sertifikatas kainuoja tarp vieno ir trijų tūkstančių (+ PVM) svarų, priklausomai nuo įmonės dydžio ir IT infrastruktūros kompleksiškumo.

[5] Kartą į metus vykstančiu auditu.
[6] https://iasme.co.uk/certification-bodies/
[7] https://iasme.co.uk/wp-content/uploads/2019/06/Cyber-Essentials-only-Question-Booklet-v11a.pdf https://cyberessentials.org/system/resources/W1siZiIsIjIwMTkvMDEvMTYvMTRfMjIfNTlfMjAzX0NSRVNUX0N5YmVyX0Vzc2VudGlhbHNfUXVlc3Rpb25uYWlyZV92My4zX3dlYnNpdGVfdmVyc2lvbi5wZGYiXV0/CREST%20Cyber%20Essentials%20Questionnaire%20v3.3_website%20version.pdf
[8] https://www.cyberessentials.ncsc.gov.uk/cert-search/

Requirement:	Cyber Essentials	Cyber Essentials PLUS
Define Scope	✓	✓
Complete Questionnaire	✓	✓
External Verification	✓	✓
External Vulnerability Assessment	✓	✓
Malware Exposure Assessment		✓
Internal Vulnerability Assessment		✓
Workstation Build Assessment		✓
Mobile Device Assessment		✓

Nauda verslui:

- *Atsparumas* – įmonės įsidiegusios *Cyber Essentials* tapo visiškai pasirengusios atremti 80 proc. bendrųjų ir dažniausiai sutinkamų KS grėsmių, o net 99 proc. įmonių teigia esančios geriau pasiruošusios atremti bet kokią ataką[9];
- *Reputacija* – sertifikatas parodo verslo partneriams, klientams, tiekėjams ir kitoms reguliavimo institucijoms, kad įmonė rimtai vertina KS ir savo klientų apsaugą;
- *Konkurencingumas* – sertifikatas suteikia konkurencinį pranašumą ieškant naujų verslo partnerių ir investuotojų, palyginant su įmonėmis neturinčiomis KS sertifikato;
- *Prieiga prie viešųjų pirkimų* – viešuose pirkimuose, susijusiose su piliečių jautrios ir konfidencialios informacijos tvarkymu, įmonėms yra privaloma turėti *Cyber Essentials* sertifikatą (tais atvejis, kai tai yra JK gynybos ministerijos viešasis pirkimas – privalomas *Cyber Essentials Plus* sertifikatas). Didėja ir įmonių skaičius, kurios reikalauja tiekimo grandies įmones atitikti *Cyber Essentials* ar kitus KS / informacinės saugos standartus[10];
- *Draudimo įmokų sumažėjimas* – draudimo agentūros ar brokeriai palankiau vertina įmones įgijusias *Cyber Essentials* sertifikatus.

Nauda valstybei:

- **Keliama verslo subjektų KS branda** ir kultūra bei stiprinamas privataus verslo subjektų kibernetinis atsparumas;
- Užtikrinimas, kad kuo didesnė dalis verslo ir organizacijų turi pasiekę bent **minimalius KS reikalavimu**s;
- Stiprinamas **valstybės ir privataus verslo bendradarbiavimas** KS srityje;
- Plėtojama KS sertifikavimo niša rinkoje, ir taip **kuriama pridėtinė vertė šalies ekonomikai**.
- Per PVM ir kitus mokesčius, į valstybės biudžetą yra atnešama daugiau lėšų.
- Didesnė konkurencija versle stiprina šalies ekonomiką ir jos konkurencingumą regioniniame kontekste.

[9] https://eprints.lancs.ac.uk/id/eprint/74598/4/SCC_2015_02_CS_Controls_Effectiveness.pdf
[10] https://digitalisationworld.com/news/35022/hp-strengthens-uk-public-sector-supply-chain

Iki 2019 m. vasaros, *Cyber Essentials* sertifikatai buvo išduoti daugiau nei 30,000 įmonių ir organizacijų, o per paskutinį veiklos periodą (nuo 2018 m. rugsėjo iki 2019 m. rugsėjo) buvo išduota daugiau nei 14,000 sertifikatų. *Cyber Essentials* sertifikatai yra taip pat išduodami Airijoje ir Italijoje, tačiau pačios sertifikavimo programos yra kuruojamos ne valstybinių institucijų, o privačių akreditavimo įstaigų.

5.1. Pasiūlymas Nr.1: Sertifikato galimybių studija ir įgyvendinimo veiksmų plano sukūrimas

Rekomenduojama KAM inicijuoti šią diskusiją Kibernetinio saugumo tarybos formate. Sertifikato kūrimo idėja būtina pristatyti ir aptarti su **privačiomis KS ir IT paslaugas teikiančiomis įmonėmis, kurios būtų esminės partnerės vystant šią iniciatyvą**. Suradus bendrų sąlyčio taškų (tiek strategiškai, tiek finansiškai), būtų galima detaliau plėtoti sertifikavimo programos steigimo idėją. Svarstytina megzti glaudesnį kontaktą su INFOBALT kibernetinės saugumo grupės nariais ir kitomis IT priežiūros ar IT sistemų sertifikavimo paslaugas teikiančiomis įmonėmis, kurios galėtų vėlesnėje stadijoje būti pilotinės partnerės kuriant sertifikavimo sistemą ir rengiant bazinio lygio KS reikalavimus.

Siekiant išsiaiškinti tokios iniciatyvos pritaikymą ir galimą naudą valstybei, būtina užsakyti galimybių studiją įvertinančią bazinio lygio kibernetinio saugumo sertifikato potencialą Lietuvoje. Ji turėtų įtraukti ne tik ekonominės naudos ir naštos analizę, bet ir vertinimą, ar Lietuvos verslo subjektų (ypač SVV) kibernetinio saugumo (bei verslo) branda yra pakankama, kad būtų galima užtikrinti sertifikavimo programos sėkmę. Jei bus matoma, kad nėra pakankamai palaikymo sertifikavimo idėjai ar atnešamos naudos supratimo, ši iniciatyva turėtų būti nukelta keleriems metams į priekį.

Taip pat, rekomenduojama šia tema **užmegzti bendradarbiavimą su kitų šalių nacionaliniais kibernetinio saugumo centrais ar kitomis sertifikavimo įstaigomis**, kurios sėkmingai yra įdiegusios verslo subjekto sertifikavimo programą.

Atlikus galimybių studiją ir esant teigiamoms išvadoms, siūlytina sudaryti veiksmų planą, kurio įgyvendinimas sudarytų sąlygas sertifikavimo sistemos veikimui. Kartu, verta apsvarstyti iš anksto užmegzti kontaktą ir kurti įmonių tinklą, kurios galėtų būti pirmosios išbandančios sertifikavimo procesą. Panašiai, kaip vyko „Baltosios bangos“ kampanija, šios įmonės galėtų **skatinti savo KS besirūpinančio, socialiai atsakingo ir inovatyvaus verslo kultūrą** ir taip prisidėti prie bendros KS brandos kėlimo nacionaliniu mastu.