„Co-funded by the Prevention of and Fight against Crime Programme
of the European Union“

Lietuvoje sukurtas ir veikia nacionalinis kibernetinių nusikaltimų kompetencijų ir tyrimų centras

Dar 2013 m. suvienijus akademinės bendruomenės ir verslo pajėgumus Lietuvoje buvo įkurtas nacionalinis kibernetinių nusikaltimų kompetencijų ir tyrimų centras (L3CE), kuris tuo pačiu įsiliejo į tarptautinį nacionalinių kompetencijų centrų tinklą (2Centre). Šiuo metu tinklas vienija nacionalinius kompetencijų centrus, veikiančius daugelyje Europos Sąjungos (ES) šalių, ir suteikia prieigą šių šalių teisėtvarkos institucijoms prie tinklo išteklių – pareigūnų mokymo ir sertifikavimo programų, mokslininkų ir tyrėjų sukurtų programinių kriminalistikos įrankių, naujausių pasiekimų, panaudojant juos kibernetiniams nusikaltimams tirti. Tinklo veiklą koordinuoja ir palaiko mokslininkų programas visuomenės saugumui stiprinti kelios ES institucijos – Europolas, Jungtinis tyrimų centras, Europos kibernetinių nusikaltimų mokymų ir švietimo grupė (ECTEG) ir kt.

L3CE plėtrą parėmė Europos Komisija, finansuodama L3CE kūrimo projektą per Nusikaltimų prevencijos ir kovos su jais 2007–2013 m. programą (angl. *Prevention of and Fighting Against Crime Programme for 2007-2013, ISEC*), tikintis, kad centras taps kompetencijų vartais kovoje su kibernetiniais nusikaltėliais Lietuvoje ir Baltijos regione - centro turima informacija, metodikomis ir kitais įrankiais galėtų pasinaudoti Lietuvos ir užsienio teisėtvarkos atstovai.

L3CE projektas pratęsė pirminio – 2Centre projekto – idėją suburti ES nacionalinius kibernetinių nusikaltimų centrus į tvarų tinklą, kuris veiktų kaip tikrai globali bendradarbiavimo platforma. Kovojant su kibernetiniais nusikaltimais labai svarbus bendradarbiavimas tarp ES ir Lietuvos teisėsaugos ir kitų susijusių institucijų. Būtina išnaudoti nacionalinių valdžios institucijų, verslo ir akademinės bendruomenės pasiekimus, keistis žiniomis ir gerosiomis patirtimis, perimti kitų ES valstybių narių pasiekimus, vystyti naujas mokymo programas ir ugdyti naujas kompetencijas. Tokio centro atsiradimas yra savalaikis ir teisingas žingsnis Lietuvos teisėtvarkos ir mokslo glaudesnio bendradarbiavimo link.

Bendradarbiaujant su Lietuvos teisėsauga – Vilniaus apskrities Vyriausiuoju policijos komisariatu (toliau – VPK) – projekto metu buvo sukurtos dvi naujos mokymo programos, skirtos Lietuvos teisėsaugai: pirmoji programa – „Asmens tapatybės vagystės elektroninėje erdvėje. Teisiniai aspektai“ (pagrindinis rengėjas – Mykolo Romerio Universitetas) ir antroji – „Kriminalistiniai tyrimai virtualioje erdvėje ir paslėptų nusikaltimų pėdsakų aptikimas“ (pagrindinis rengėjas – Kauno Technologijų Universitetas). Pagal šias programas buvo apmokyta po 10 dėstytojų, kurie galės toliau apmokyti pareigūnus darbo vietoje arba vėliau organizuojant apmokymus. Tokia akademinės bendruomenės ir teisėsaugos bendra veikla leidžia ne tik geriau suprasti galutinio naudotojo poreikius, bet pasiūlyti labiausiai pritaikytus ir aktualiausius produktus.

Pirmoji programa skirta teisėtvarkos pareigūnams ir suteikia žinių apie asmens tapatybę bei asmens tapatybės nustatymą fizinėje ir elektroninėje erdvėje, įgalinančių suvokti galimą asmens tapatybės panaudojimą elektroninėje erdvėje, įskaitant neteisėtą kito asmens tapatybės panaudojimą elektroninėje erdvėje.

Antroji programa skirta teisėtvarkos atstovams, atliekantiems nusikaltimų tyrimus ir įvykių vietos tyrimus virtualioje ir debesų kompiuterijos aplinkoje.

Kitos dvi mokymo programos buvo perimtos iš užsienio partnerio – Dublino Universiteto Kibernetinio saugumo ir kibernetinių nusikaltimų tyrimų centro (Dublin College University Centre for Cyber Security and Cybercrime Investigation, toliau – UCD) – adaptuotos ir lokalizuotos Lietuvos sąlygomis. Toks kitose šalyse sukurtų pažangiausių mokymo programų adaptavimas leido sutaupyti laiko ir išteklių, nekuriant analogiškų programų.

Pirmoji adaptuota mokymo programa – „Įvadas į kriminalistinį tyrimą“ (angl. First responders) – skirta teisėsaugos pareigūnams, tiriantiems IT panaudojimą nusikalstamai veikai, tačiau nesantiems IT srities profesionalams, ir kuria siekiama supažindinti mokymų dalyvius su galimais piktnaudžiavimo technologijomis būdais, pateikti instrukcijas, kaip efektyviai reaguoti į nusikaltimus elektroninėje erdvėje bei pasiūlyti metodus, kaip tinkamai šiuos nusikaltimus tirti.

Antroji adaptuota mokymo programa – „Deepthought programinio kriminalistinio įrankio naudojimo mokymo programa“ (angl. *Deepthought*) – skirta teisėsaugos pareigūnams, dirbantiems įvykio ar kratos vietoje ir atliekantiems greitas peržiūras siekiant surinkti tik tuos duomenis, kurie potencialiai gali tapti įkalčiais, bei kibernetinių nusikaltimų tyrimų laboratorijos, kur paprastai atliekami itin didelės apimties kompiuterių kriminalistiniai tyrimai. Deepthought įrankiu siekiama sumažinti rankiniu būdu peržiūrimų failų skaičių, tokiu būdu, efektyvinant ribotų išteklių, kuriais disponuoja daugelio šalių teisėsauga, panaudojimą.

Pastaroji programa tapo sudėtine platesnės mokymo programos dalimi – „Išorinių laikmenų apžiūra“, kuri buvo sukurta ir pritaikyta teisėsaugos pareigūnams, atliekantiems išorinių laikmenų, galimai naudotų nusikalstamam IT naudojimui, apžiūrą. Šią programą parengė VPK kartu su UAB Ekonominės konsultacijos ir tyrimai. „Išorinių laikmenų apžiūros“ programa siekiama suteikti dalyviams žinių ir supratimą apie skaitmeninių pėdsakų rinkimo būdus ir įrankius, apie nuoseklius etapus ir kiekvieno etapo veiksmus, kaip tinkamai pasirengti ir vykdyti skaitmeninių pėdsakų rinkimą, kaip teisingai užfiksuoti ir dokumentuoti surinktus įkalčius, kad jie galėtų būti pripažįstami teisminiame procese.

Pagal abi adaptuotas mokymų programas buvo apmokyta po 10 dėstytojų, o vykdant *Deepthought* mokymus buvo akcentuotas praktinis mokymas, naudojant demonstracinį metodą (angl. *on-hands training*).

Projektas suteikė galimybę Lietuvos teisėsaugos pareigūnams susipažinti su Airijos kolegų patirtimi darbinio vizito į UCD (Airija) metu: buvo pristatyta ir stebėta veikla Airijos policijos kriminalinių nusikaltimų tyrimų padalinyje, Airijos Policijos padalinyje „Telecomms unit, Pheonix Park“, kuris yra atsakingas už mobiliųjų telefonų ir vaizdo įrašymo įrenginių kriminalistinius tyrimus, mobiliųjų įrenginių tyrimų laboratorijoje, visų vidinių sistemų stebėjimo padalinyje, Airijos policijos kompiuterių kriminalistinių tyrimų padalinyje. UCD taip pat pristatė turimas magistro studijas, skirtas policijos tyrėjams, bei pademonstravo sukurtus programinius įrankius, skirtus kibernetiniams nusikaltimams tirti. Iš pademonstruotų įrankių buvo atsirinkti 3 kriminalistiniai įrankiai tolesniam adaptavimui ir lokalizavimui Lietuvos sąlygomis.

Pirmasis įrankis – FiRST – skirtas ikiteisminio tyrimo tyrėjams, vykstantiems į įvykio ar kratos vietą ir vykdantiems įjungtų sistemų analizę, ypač jei įtariama, kad sistemose gali būti šifravimo ir disko trynimo programinė įranga, būta prisijungimų prie debesų kompiuterijos paslaugų tinklo, įjungtų virtualių mašinų ir pan.

Antrasis įrankis – Mighty Artefact Analyser (MAA) – tai tarpplatforminis grafine sąsaja grįstas įrankis, skirtas skirtingų artefaktų, rastų įtariamojo įrenginiuose, tikrinimui bei galintis greitai ir tiksliai atlikti įvairių

naudotojo artefaktų analizę bei pristatyti rezultatus naudotojui draugiška forma. MAA paprasta naudotis bet kokiam naudotojui nepriklausomai nuo turimos patirties. Unikali MAA savybė yra ta, kad pažengę naudotojai gali susikurti naujus ir pagal jų poreikius suformuotus papildinius.

Trečiasis įrankis – Deepthought – greitai aptinka grafinius failus, vaizdus, nuotraukas, filmus, video, internetinius pokalbius, elektroninio pašto laiškus, lankytus interneto puslapius, užšifruotus failus, virtualias mašinas pagal sukurtus raktinius žodžius bei generuoja paieškos rezultatų ataskaitą į atskirą įrodymų diską nepalikdamas pėdsakų įtariamojo įrenginyje.

Nors kriminalistinių įrankių perėmimas yra greičiausias būdas apsirūpinti pažangiausiomis kriminalistinio tyrimo priemonėmis, ateityje kriminalistinio tyrimo programinius įrankius numatoma kurti ir Lietuvoje. Kauno technologijų universitete atlikto mokslinio tyrimo metu buvo sukurtas kriminalistinių nusikaltimų daiktų internete tyrimų metodas ir prototipas, kurių pagrindu bus galima sukurti naują tyrimo įrankį.

Užsienio partnerių patirtis buvo perimta ir kitoje srityje: iš Ispanijos S21SEC instituto, veikiančio kibernetinio saugumo srityje, buvo perimtos ir lokalizuotos 2 sertifikavimo programos – „Elektroninių objektų surinkimas“ ir „Windows artefaktai“.

Pirmoji sertifikavimo programa skirta ikiteisminį tyrimą atliekantiems pareigūnams, kurie savo veikloje susiduria su elektroniniu objektų surinkimu įvykio vietoje: pareigūnams, dalyvaujantiems įvykio vietos apžiūrose, kratose, poėmiuose ir operatyvinės grupės pareigūnams. Antroji sertifikavimo programa skirta populiariausios operacinės sistemos – Windows – artefaktų analizei kriminalistinėse laboratorijose ar policijos komisariatuose.

Pagal pirmą programą Lietuvos teisėsaugos pareigūnai ir specialistai mokėsi ir vėliau laikė egzaminus. Pilotiniai mokymai pagal sertifikavimo programą „Elektroninių objektų surinkimas“ vyko naudojant realios aplinkos simuliaciją, kuri leidžia ne tik įtvirtinti gautas žinias, bet ir įgauti praktinių įgūdžių bei vėliau išvengti klaidų.

Išlaikiusiems egzaminus pagal mokymo programas ir pirmąją sertifikavimo programą buvo išduoti sertifikatai, liudijantys, kad pareigūnai ir specialistai gavo būtinų žinių ir įgūdžių, todėl surinkti skaitmeniniai įkalčiai bus sunkiau ginčijami teisme. Iki šiol tai buvo viena iš spragų, kodėl kibernetinius nusikaltimus padarę asmenys kartais išsisukdavo nuo bausmės. Be to, apmokius pareigūnus ir specialistus pagal šias programas nusikaltimų elektroninėje erdvėje tyrimai bus atliekami daug greičiau.

Parengtos mokymo ir sertifikavimo programos turėtų tapti sudėtine teisėsaugos nacionalinės kompetencijų ugdymo sistemos dalimi. Numatoma, kad pagal šias programas būtų galima apmokyti virš 2000 pareigūnų ir specialistų visoje Lietuvoje. Geroji praktika adaptuojant ir lokalizuojant programas ir įrankius buvo pristatyta ir tarptautiniu mastu. Kartu su pasiūlymais, kaip tobulinti ES ir ES šalių teisėsaugos kompetencijų sistemą, ši praktika buvo pristatyta Europolo ECTEG metiniame susitikime bei Vokietijos kompetencijos centre, aktyviai veikiančio nacionalinės kompetencijų sistemos ir standartų kūrimo ES mastu, srityje.

Projekto metu sukurti produktai Lietuvos teisėsaugai yra prieinami prisijungus per L3CE internetinį portalą: bus galima susipažinti su mokymo ir sertifikavimo programomis, naujausiais įrankiais, skirtai nusikaltimų elektroninėje erdvėje tyrimui, mokslo tyrimų rezultatais bei tarptautinių renginių kibernetinių nusikaltimų ir kibernetinio saugumo bei prevencijos srityse tvarkaraščiu. Daugiau kaip metus veikiantis L3CE portalas

www.l3ce.eu pamažu tampa ne tik kompetencijos vartais Lietuvos teisėsaugai, bet ir tarptautinio bendradarbiavimo platforma ES, ES ir kitų šalių teisėsaugai.

Sukurtos programos ir įrankiai bus toliau tobulinami, keičiamasi su kitais kompetencijos centrais ir ES šalių teisėsauga, todėl ateityje kibernetinių nusikaltimų tyrimui skirtų priemonių pasiūla turėtų augti. Šią veiklą numato vykdyti L3CE. Parengta ilgalaikė ir vidutinės trukmės veiklos strategija ir veiklos modelis užtikrins stabilią ir tvarią centro veiklą.

L3CE projekto ir centro veikla per trumpą laiką sulaukė Europos Komisijos pripažinimo: 2015 m. buvo skirtas finansavimas šio projekto multiplikavimui ir jo išplėtimui ES mastu. Numatoma stiprinti analogiškų ES nacionalinių kompetencijos centrų bendradarbiavimą apjungiant jus į vieningą tinklą, kuriame būtų keičiamasi įvairiose ES šalyse parengtomis mokymo, sertifikavimo programomis, įrankiais, mokslo tyrimų pasiekimais ir gerąja praktika, kuriami bendri standartai, modeliai ES mastu, būtų vykdoma bendra veikla, diskutuojama ir siūlomi sprendimai naujoms grėsmėms suvaldyti bei problemoms spręsti.