



Naujienlaiškis

2026 m. rugpjūtis

Iššūkiais grįsti mokymosi scenarijai studijoms laboratorijoje ir integravimui į studijų programą

Iššūkiais grįstas mokymasis (CYBERCHALLENGE) suteikia veiksmingą ir efektyvią mokymosi sistemą, sprendžiant realaus pasaulio iššūkius. Ją gali naudoti visi mokyklos suinteresuotieji asmenys, siekdami plėtoti strateginį planavimą, susieti dabartinę praktiką, stiprinti atsakomybę ir suasmeninimą bei ugdyti visą gyvenimą besimokančius asmenis. Užuo konkuravęs su kitais metodais, jis siekia užmegzti ryšius ir padėti visoms suinteresuotosioms šalims kartu kurti mokymosi patirtį.

Bendrasis CYBERCHALLENGE tikslas – padidinti skaitmeninio turinio, technologijų ir praktikų prieinamumą, sukuriant kibernetinio saugumo mokymo programą, įskaitant federalinę kibernetinio saugumo laboratoriją, pagrįstą įrankių smėlio dėže ir naudojant CBL metodiką.

Vienas iš pagrindinių projekto tikslų – skatinti novatoriškas mokymosi ir mokymo praktikas, siekiant sustiprinti studentų motyvaciją, kritinį mąstymą ir problemų sprendimo įgūdžius. Šia prasme projektas taip pat apima kai kurių CBL scenarijų įtraukimą į sukurtas mokymo programas.

CBL universitetinėse studijose yra ne tik dar vienas mokymo metodas – tai studijų filosofijos pokytis – nuo teorinių žinių kaupimo prie realių rezultatų kūrimo.

CBL yra neatsiejama studijų modulio dalis, studijų procesas transformuojamas iš „klausymo ir užduočių atlikimo“ į „tyrimą, sprendimą ir įgyvendinimą“. CBL integracija studijų modulį paverčia ne statišku žinių rinkiniu, o dinamiška ekosistema. Magistro lygmenyje toks modelis yra itin efektyvus, nes imituoja realią profesinę aplinką, kurioje ekspertas turi ne tik „žinoti“, bet ir „veikti“ susidūręs su neapibrėžtumu. Sukurtas studijų modulio modelis su CBL integracija rodo, kaip kiekviena dalis viena kitą papildo.

Vienas iš pagrindinių projekto tikslų – skatinti novatoriškas mokymosi ir mokymo praktikas, siekiant sustiprinti studentų motyvaciją, kritinį mąstymą ir problemų sprendimo įgūdžius. Šia prasme projektas taip pat apima keletą CBL scenarijų įtraukimą į sukurtas mokymo programas.

Projekto įgyvendinimo metu buvo sukurti keturi CBL scenarijai, po vieną kiekvienam moduliui: Kibernetinio saugumo pagrindai, Tapatybės ir prieigos valdymas, Kibernetinės atakos ir kibernetinė gynyba bei Kibernetinio saugumo valdymas.

Kibernetinio saugumo pagrindai: išmaniųjų namų sistemų saugumas

Didžioji idėja: išmaniųjų namų sistemų saugumas.

Pagrindinis iššūkis (specifinė problema): išmaniųjų namų sistemų saugumo problemos dažnai susijusios su ryšio protokolų saugumo trūkumais. Protokolo lygmens saugumo trūkumai dažnai yra sistemingesni ir sunkiai ištaisomi neprofesionalui.

Prijungti namai siūlo patogumą, bet taip pat kelia didelę saugumo riziką. Kaip galime sukurti sistemas, kurios išliktų saugios net ir užpuolikui įgavus prieigą prie vidinio tinklo?

Tapatybės ir prieigos valdymas

Didžioji idėja: į iššūkius orientuotas projekto pasiūlymas: „Saugi prieiga ir tapatybė federalinėje ekosistemoje“.

Sukurti ir įdiegti federalinę autentifikavimo ir prieigos kontrolės sistemą, kuri apjungia privatumą užtikrinantį tapatybės valdymą (naudojant patikrinamus kredencialus ir decentralizuotus tapatybės principus) su smulkiais prieigos kontrolės mechanizmais (RBAC, ABAC ir OAuth 2.0 delegavimas).



CYBERCHALLENGE - Challenges Solving in Cybersecurity Study Program No. 2024-1-LT01-KA220-HED-000252504

Studentai turi imituoti realaus pasaulio aplinką, pvz., skaitmeninių paslaugų platformą (pvz., e. valdžios, sveikatos priežiūros ar universiteto sistemą), kuriai reikalingas saugus, privatumą užtikrinantis tapatybės tvarkymas ir politika pagrįsta prieigos kontrolė.

Pagrindinis iššūkis (specifinė problema): Kaip sukurti sistemą, kuri įgalintų saugią prieigą ir privatumą išsaugantį tapatybės patvirtinimą keliose paslaugose, naudojant federalinį autentifikavimą (SSO) ir deleguotąjį autorizavimą (OAuth 2.0), kartu įgyvendinant dinaminės prieigos kontrolės (RBAC/ABAC) politiką?

Pagrindinės subproblemos:

- Saugus skaitmeninių tapatybių ir prisijungimo duomenų valdymas.
- Vartotojų privatumo išsaugojimas ir duomenų atskleidimo sumažinimas.
- Suderinamo prisijungimo diegimas naudojant patikrinamus prisijungimo duomenis (suderintas su eIDAS).
- Prieigos kontrolės principų taikymas (mažiausios privilegijos, pareigų atskyrimas).
- Autorizacijos užtikrinimas naudojant OAuth 2.0 taikymo sritis ir žetonus.

Kibernetinės atakos ir kibernetinė gynyba

Didžioji idėja: partnerių įmonės infrastruktūros tobulinimas imituojant įvairių tipų atakas.

Pagrindinis iššūkis (specifinė problema): Transilvanijos universitetas, vykdydamas savo kibernetinio saugumo magistro programą ir būdamas vienas iš Braşov CyberHub steigėjų, bendradarbiauja su įvairiomis institucijomis ir įmonėmis, siekdamas stiprinti ir skatinti kibernetinį saugumą tarp visų suinteresuotųjų šalių. Remdamiesi šia partnerystės sutartimi, „Cyberchallenge“ studentai gali dalyvauti saugumo vertinimuose:

1 tema. Įmonės atsparumo sukčiavimo atakoms patikrinimas.

2 tema. Įstaigos tinklo patikrinimas dėl žinomų pažeidžiamumų.

3 tema. Žiniatinklio programų saugumo vertinimas.

Kibernetinio saugumo valdymas

Didžioji idėja: saugumo rizikos valdymas išmaniojoje infrastruktūroje, ypač paspirtukų pavėžėjimo sistemoje.

Pagrindinis iššūkis (specifinė problema): saugumo rizikos valdymo problemos pavėžėjimo sistemose yra susijusios su sistemos projektavimu, įskaitant įvesties patvirtinimą ir pateikimą, API piktnaudžiavimą, saugumo funkcijas, laiko ir būsenos valdymą, klaidų tvarkymą, kodo kokybę ir panašius klausimus. Sistemos komponentų sujungimas ir išmaniosios infrastruktūros kūrimas yra sudėtinga veikla, kuri gali sukelti saugumo riziką. Iššūkis yra numatyti šias rizikas prieš diegiant sistemą, jas įvertinti, sistemingai pagrįsti ir įdiegti jų sprendimo priemones.

PROJECT COORDINATOR



PROJECT PARTNERS



<https://www.cyberchallenge-erasmus.eu/>

Kaunas University of Technology
Faculty of Informatics

Studentu str. 50, Kaunas, Lithuania