



Naujienlaiškis

2025 m. rugpjūtis

Apie kibernetinio saugumo mokymo programą

Dėl didėjančio kibernetinių grėsmių paplitimo ir didėjančios priklausomybės nuo skaitmeninių technologijų būtina įgyvendinti patikimą kibernetinio saugumo mokymo programą. Universitetų bendradarbiavimas yra puiki galimybė gerinti studijų kokybę, kurti inovatyvias studijų programas, praturtinti studentų patirtį. Norint pasiekti geriausių rezultatų, svarbu pasirinkti tinkamas metodikas ir strategijas. Kibernetinio saugumo skaitmeninei mokymo programai įgyvendinti naudosime hMOOC, federacinį švietimą ir iššūkiams pagrįstą mokymosi metodiką. Siūloma kibernetinio saugumo mokymo programa ketina supažindinti besimokančius su pagrindiniais dalykais: kibernetinio saugumo pagrindais, tapatybės ir prieigos valdymu, kibernetinėmis atakomis ir kibernetine gynyba bei kibernetinio saugumo valdymu. Trumpas susijusių kursų aprašymas ir kontekstualizavimas kibernetinio saugumo scenarijuose:

Kibernetinio saugumo pagrindai

Kibernetinis saugumas yra sudėtinga sritis, apimanti techninių ir teorinių sąvokų derinį. Kursas "Kibernetinio saugumo pagrindai" išsamiai apžvelgia kompiuterių ir informacijos saugumo problemas, pagrindines kibernetinio saugumo koncepcijas, principus, formalius saugumo modelius, informacinių technologijų saugumo techninės ir programinės įrangos metodus bei gebėjimų standartus ir ugdo gebėjimus juos taikyti. Jame aptariamos įvairios temos, įskaitant IT saugumo problemas, informacijos saugumo modelius, kriptografiją ir saugius informacijos kodavimo metodus, informacijos ir IT saugumo standartus ir specifikacijas, aparatinės įrangos saugumą, tapatybės valdymą, OS saugos mechanizmus ir failų sistemos saugumą. Kursas skirtas suteikti studentams žinių ir įgūdžių, kad jie galėtų spręsti besikeičiančius kibernetinio saugumo iššūkius, su kuriais šiandien susiduria organizacijos.

Tapatybės ir prieigos valdymas

Kursas "Tapatybės ir prieigos valdymas" yra pagrindinis kibernetinio saugumo mokymo programos komponentas, sprendžiantis didėjančią saugių ir efektyvių skaitmeninių tapatybių valdymo metodų poreikį šiuolaikinėse organizacijose. Šiame kurse pagrindinis dėmesys skiriamas principams, technologijoms ir praktikai, reikalingiems prieigai prie kritinio skaitmeninio turto apsaugoti, užtikrinant konfidencialumą, vientisumą ir prieinamumą. Studentai išnagrinės tapatybės valdymo gyvavimo ciklą, įskaitant tapatybės kūrimą, patikrinimą ir eksploatavimo nutraukimą, kartu su šiuolaikiniais prieigos kontrolės mechanizmais. Kursas pabrėžia tiek teorinius pagrindus, tiek praktinį pritaikymą.



Kibernetinės atakos ir kibernetinė gynyba

Kibernetinių atakų ir kibernetinės gynybos kursas suteikia išsamų supratimą apie kibernetines grėsmes ir gynybos priemones. Jis prasideda nuo įvado į įvairias kibernetines atakas ir grėsmes, paaiškinant "CyberKillChain" ir "MITRE ATT&CK" sistemą, skirtą priešininkų taktikai analizuoti. Kursas apima kenkėjiškų programų tipus ir gynybos koncepciją, pabrėžiant daugiasluoksnes saugumo strategijas. Studentai sužino apie kibernetinio saugumo standartus ir etiškus įsilaužimo metodus, įskaitant OWASP dešimt geriausių atakų ir įprastų pažeidžiamumų, tokių kaip SQL injekcija ir XSS. Kursas taip pat gilinasi į įsiskverbimo testavimą, raudonąją komandą, sukčiavimą kaip paslaugą ir "WiFi" saugumą. Be to, jis apima tinklo saugumą ir perimetro apsaugą, daugiausia dėmesio skiriant 2 lygmens saugumui, naujos kartos ugniasienėms (NGFW), IDS/IPS sistemoms ir VPN technologijoms, tokioms kaip IPSec ir OpenVPN. Nagrinėjami pagrindiniai sistemos registravimo ir stebėjimo aspektai grėsmėms aptikti, taip pat kibernetinio saugumo incidentų valdymo strategijos. Kursas baigiamas kibernetinių operacijų ir saugumo operacijų centrų (SOC) apžvalga, kartu su SIEM/SOAR sprendimais ir didėjančiu dirbtinio intelekto vaidmeniu kibernetiniame saugume, siekiant pagerinti grėsmių aptikimą ir automatizuotą reagavimą.

Kibernetinio saugumo valdymas

Šis kursas suteiks studentams kibernetinio saugumo valdymo principų apžvalgą. Dalyviai sužinos, kaip užtikrinti saugaus turto konfidencialumą, vientisumą ir prieinamumą, nustatyti saugumo rizikas, reikalavimus ir atsakomąsias priemones, mažinančias šią riziką ir įgyvendinti saugumo reikalavimus. Kursas pagrįstas nusistovėjusiu saugumo rizikos valdymo srities modeliu ir modeliu pagrįsto saugumo principais. Saugumo valdymas bus iliustruojamas taikant saugumo valdymo standartus ir modelius. Naudodamiesi iššūkiu pagrįsto mokymosi metodu, dalyviai nagrinės saugumo valdymo iššūkius verslo procesus atitinkančiose sistemose, išmaniojoje infrastruktūroje, paskirstytose sistemose, riziką suvokiančiose kriminalistikos sistemose ir saugiose tapatybės valdymo sistemose.

PROJEKTO KOORDINATORIUS



PROJEKTO PARTNERIAI



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

Kauno technologijos universitetas
Informatikos fakultetas

Studentų g. 50, Kaunas, Lietuva