Sodelavne večuporabniške spletne simulacije na področju poučevanja kibernetske varnosti

Saša Divjak
Fakulteta za računalništvo in informatiko, Večna pot 13, Ljubljana
sasa.divjak@fri.uni-lj.si

Izvleček

Prispevek je posvečen popestritvi predavanj s področja kibernetske varnosti in v bistvu predstavlja nadgradnjo kiberletov - računalniških simulacij s tega področja. Uvaja zamisel o večuporabniških spletnih aplikacijah, pri katerih v simulirani varovani objekt vstopajo napadalci in branilci vsak s svoje spletne strani. Izhodišče je znani pristop z rdečo in modro ekipo, ki raziskujeta varovani objekt s stališča njegove ranljivosti. Po pregledu nekaterih obstoječih rešitev opiše večuporabniško spletno aplikacijo, ki je sicer namenjena didaktiki, vsebuje pa tudi elemente poigritve.

Ključne besede: Kibernetska varnost, računalniške simulacije, poigritve, izobraževanje.

Collaborative, multi-user online simulations for teaching cybersecurity

Abstract

The paper is dedicated to enriching lectures in the field of cyber security and is basically an upgrade of cyberlets – computer simulations in this field. It introduces the idea of multi-user web applications, where attackers and defenders enter the simulated protected object, each from their own web page. The starting point is the well-known approach with the red and blue teams exploring the protected object from the point-of-view of its vulnerability. After reviewing a number of existing solutions, it describes a multi-user web application, which, although intended for didactics, also contains elements of gamification.

Keywords: Cyber security, computer simulations, gamifications, education

1 UVOD

Ker uporaba računalniških omrežij narašča, postaja kibernetska varnost vse bolj pomembna. To delo temelji na potrebi po testiranju orodij za situacijsko zavedanje oziroma za odkrivanje in analizo napadov na računalniška omrežja. Izvajanje poskusov s kibernetskimi napadi na resničnih računalniških sistemih, ki vsebujejo kritične podatke, je zelo nezaželeno. Ena od možnih alternativ je postavitev fizičnega računalniškega omrežja brez kritičnih podatkov in izvajanje kibernetskih napadov na omrežje ter zbiranje podatkov iz sistemov za zaznavanje vdorov. Druga možnost je ustvarjanje sintetičnih podatkov z uporabo simulacije. Ta prispevek je v bistvu nadaljevanje razprave, ki smo jo podali v članku »Popestritev predavanj o kibernetski varnosti z interaktivnimi računalniškimi simulacijami« [1], vendar je usmerjen v večuporabniške spletne simulacije, morda tudi v izobraževalne igre.

2 O DIDAKTIČNEM SMISLU VEČUPORABNIŠKIH SIMULACIJ

Večuporabniške simulacije imajo v didaktičnem smislu številne prednosti. Gre za interaktivna virtualna okolja, v katerih se udeleženci lahko učijo in pridobivajo izkušnje na simuliran način. Te simulacije se lahko uporabljajo v različnih izobraževalnih kontekstih, vključno z visokošolskim izobraževanjem, poklicnim

usposabljanjem, vojaškim izobraževanjem, poslovnimi treningi in drugimi področji.

Naštejmo nekaj prednosti večuporabniških simulacij v didaktičnem kontekstu:

- **Realistično učenje:** Večuporabniške simulacije posnemajo resnične situacije, kar omogoča udeležencem, da se naučijo in pridobivajo izkušnje na realističen način. To je zlasti pomembno pri poklicnem usposabljanju, kjer udeleženci lahko simulirajo naloge, ki jih bodo izvajali v svojem dejanskem poklicu.
- **Aktivno sodelovanje**: Udeleženci simulacije aktivno sodelujejo in se vključujejo v dogajanje. To spodbuja njihovo angažiranost, motivacijo in boljše razumevanje obravnavane tematike. Sodelovanje med udeleženci omogoča tudi interakcijo in izmenjavo znanja ter izkušenj med različnimi udeleženci.
- **Napake kot učna priložnost**: Simulacije omogočajo udeležencem, da se naučijo iz napak brez resničnih posledic. S tem se spodbuja refleksija, analiza in izboljšanje prihodnjega delovanja. Udeleženci lahko preizkušajo različne pristope, ocenjujejo rezultate in se učijo iz svojih napak.
- **Individualno prilagajanje:** Večuporabniške simulacije omogočajo prilagajanje glede na posameznikove potrebe in stopnjo znanja. Udeleženci lahko napredujejo v svojem tempu in se osredotočajo na specifične vidike, ki jih morajo izboljšati. To zagotavlja bolj poosebljeno izkušnjo učenja.
- **Timsko delo**: Simulacije spodbujajo timsko delo in sodelovanje med udeleženci. To je pomembno za razvoj komunikacijskih veščin, reševanje problemov in skupinsko odločanje. Udeleženci se naučijo, kako se učinkovito povezati in delovati skupaj v simuliranem okolju.
- **Prilagodljivost**: Simulacije omogočajo ponavljanje in eksperimentiranje v nadzorovanih pogojih. Udeleženci lahko preizkusijo različne scenarije, strategije in pristope ter preučijo njihove učinke. S tem se spodbuja kritično razmišljanje, raziskovanje in ustvarjalnost.
- **Globalni dostop**: Večuporabniške simulacije omogočajo učenje na daljavo in omogočajo udeležbo udeležencev iz različnih delov sveta. To odpira možnosti za mednarodno sodelovanje, izmenjavo idej in kulture ter bogati izkušnjo udeležencev.

Večuporabniške simulacije imajo velik potencial v didaktičnem okolju, saj spodbujajo interaktivno, realistično in sodelovalno učenje. Omogočajo udeležencem, da se aktivno vključujejo, pridobivajo izkušnje ter razvijajo ključne veščine in znanja na interaktiven način.

3 KIBERNETSKA VARNOST IN MODRA TER RDEČA EKIPA

V kontekstu kibernetske varnosti se izraza »modra ekipa« in »rdeča ekipa« nanašata na dve različni vrsti ekspertov, ki sodelujejo pri testiranju in izboljševanju varnostnih sistemov organizacij.

Modra ekipa predstavlja obrambno stran kibernetske varnosti. Naloga modre ekipe je odkrivanje ranljivosti in zagotavljanje varnosti omrežij, sistemov in podatkov organizacije. Delujejo znotraj organizacije in se osredotočajo na preprečevanje, zaznavanje in odzivanje na varnostne incidente. Modra ekipa izvaja redne varnostne preglede, izvaja penitracijska testiranja, vzdržuje in nadzira varnostne sisteme ter gradi obrambne strategije za zaščito organizacije pred napadi.

Glavni cilj modre ekipe je zagotoviti, da so varnostni sistemi organizacije učinkoviti, da so zaščiteni pred napadi ter da se organizacija hitro odzove na morebitne varnostne incidente. Prav tako si prizadevajo za stalno izboljšanje varnostnih mehanizmov.

Rdeča ekipa je zunanja skupina strokovnjakov za kibernetsko varnost, ki se ukvarja z izvajanjem napadov na organizacijo. Njihova naloga je simuliranje resničnih kibernetskih napadov, da bi preizkusili učinkovitost varnostnih sistemov organizacije. Rdeča ekipa uporablja različne taktike, tehnike in orodja, ki jih uporabljajo pravi napadalci, in s tem identificira morebitne ranljivosti, ki bi jih morala modra ekipa rešiti. Cilj rdeče ekipe ni povzročiti škodo, ampak pomagati organizaciji pri izboljšanju njihovega obrambnega sistema. Glavni namen rdeče ekipe je identifikacija morebitnih pomanjkljivosti v varnostnih sistemih organizacije ter pomoč pri izboljšanju kibernetske varnosti z razkrivanjem ranljivosti, testiranjem obrambnih mehanizmov ter s povečanjem zavedanja o varnostnih tveganjih med člani organizacije.

Skupno delovanje modre in rdeče ekipe je učinkovit pristop k izboljšanju kibernetske varnosti organizacije. Sodelovanje med obema ekipama omogoča odkrivanje ranljivosti, testiranje varnostnih postopkov ter izmenjavo znanja in izkušenj med obrambno

in napadalno stranjo, kar pripomore k celovitemu izboljšanju varnostnih sistemov organizacije.

Rdeča ekipa ima naslednje naloge pri izvajanju varnostnega preizkusa:

- **Posnemanje napadov:** Glavna naloga rdeče ekipe je izvajanje simuliranih kibernetskih napadov na organizacijo. To vključuje uporabo različnih taktik, tehnik in orodij, ki jih uporabljajo dejanski napadalci. Cilj je preizkusiti varnostne postopke organizacije in preveriti, kako dobro so pripravljeni na različne vrste napadov.
- **Identifikacija ranljivosti:** Rdeča ekipa išče ranljivosti v varnostnih sistemih organizacije. To vključuje iskanje pomanjkljivosti v omrežjih, aplikacijah, operacijskih sistemih, varnostnih politikah in drugih komponentah organizacije, ki bi lahko bile izkoriščene s strani napadalcev.
- **Preizkus sistema zaznavanja in odziva:** Rdeča ekipa preizkuša sposobnost organizacije za zaznavanje in odzivanje na varnostne incidente. S ciljanimi napadi preverja, ali organizacija učinkovito zazna napadalne dejavnosti, pravilno reagira na incidente ter izvaja ustrezne ukrepe za njihovo obvladovanje.
- **Poročanje o ugotovitvah:** Rdeča ekipa pripravi podrobno poročilo o ugotovitvah in priporočilih za organizacijo. V poročilu opisujejo identificirane ranljivosti, uspešnost napadov, ugotovljene pomanjkljivosti v varnostnih postopkih ter predlagane izboljšave za okrepitev kibernetske varnosti.
- **Sodelovanje z modro ekipo:** Rdeča ekipa sicer tesno sodeluje z modro ekipo organizacije. Skupaj analizirata ugotovitve, izmenjujeta informacije o varnostnih taktikah in strategijah ter skupaj oblikujeta načrte za izboljšanje varnostnih sistemov organizacije.

Modra ekipa v kibernetski varnosti izvaja naslednje naloge:

- **Zaščita in obramba:** Glavna naloga modre ekipe je zagotavljanje varnosti omrežij, sistemov in podatkov organizacije. Skrbi za vzpostavitev in vzdrževanje varnostnih mehanizmov ter politik, ki ščitijo organizacijo pred kibernetskimi napadi. To vključuje konfiguriranje požarnih pregrad, sistemov zaznavanja napadov, varnostnih protokolov in drugih varnostnih rešitev.
- **Zaznavanje in nadzor:** Modra ekipa spremlja omrežja in sisteme organizacije ter zaznava morebitne varnostne incidente. Uporablja različna orodja in tehnologije za zaznavanje nepravilnosti, sumljivega prometa ali napadov. Njena naloga je hitro prepoznati in analizirati morebitne varnostne grožnje ter ukrepati v skladu z ustreznimi postopki.
- **Preiskovanje varnostnih incidentov:** Ko se zgodi varnostni incident, modra ekipa prevzame vlogo preiskovalcev. Raziskujejo napade, ugotavljajo izvor in obseg vdora ter ocenjujejo škodo. Pomembno je, da modra ekipa razume, kako se je napad zgodil, ter sprejme ustrezne ukrepe za odpravo ranljivosti in preprečevanje podobnih incidentov v prihodnosti.
- **Izvajanje varnostnih pregledov:** Modra ekipa izvaja redne varnostne preglede in ocene organizacije. To vključuje ocenjevanje varnostnih politik, protokolov in postopkov ter izvajanje tehničnih pregledov omrežij, aplikacij in sistemov. Namen teh pregledov je identifikacija morebitnih ranljivosti, pomanjkljivosti ali nepravilnosti v varnostnih postopkih ter priprava načrtov za njihovo odpravo.
- **Usposabljanje in ozaveščanje:** Modra ekipa ima tudi nalogo izobraževanja zaposlenih v organizaciji glede varnostnih praks in postopkov. Organizira usposabljanja, delavnice in ozaveščevalne kampanje, s katerimi povečuje zavedanje o kibernetski varnosti med člani organizacije. S tem pomaga zmanjšati tveganje za napade, ki jih lahko povzročijo nevednost ali malomarnost zaposlenih.

4 POMEN RAČUNALNIŠKIH SIMULACIJ

Obstaja več (ne vedno računalniških) simulacij, ki posnemajo sodelovanje med modro in rdečo ekipo ter pomagajo organizacijam izboljšati svoje varnostne postopke. Nekatere tovrstne simulacije so:

Portal ThreatGEN® Red vs. Blue [2] omogoča dostop do platforme za simulacijo kibernetske varnosti, tečajev na zahtevo, laboratorijev in scenarijev. Vsak tečaj je serija kratkih video lekcij, ki pokrivajo specifične koncepte kibernetske varnosti, ki se utrjujejo z laboratoriji in scenariji v obliki simulacije kibernetske varnosti in strateške igre. Učenci še izboljšajo svoje učenje z igranjem tekem proti računalniškemu nasprotniku ali na spletu proti drugim študentom ali kolegom. Organizacije lahko olajšajo dogodke s turnirskimi načini, lestvico najboljših in namiznimi načini vadbe. Študenti in dogodki, podatki, statistika

in zgodovinski trendi se spremljajo prek analitične nadzorne plošče in poročil.

Cobalt Strike [3] je komercialno orodje za testiranje penetracije, ki preizkuševalcem varnosti omogoča dostop do široke palete zmožnosti napada. Cobalt Strike se lahko uporablja za lažno predstavljanje in pridobitev nepooblaščenega dostopa do sistemov ter lahko posnema različne zlonamerne programske opreme in druge napredne taktike groženj.

Crisis Simulation podjetja Immersive Labs [4] je spletna aplikacija, ki v realnem času pelje branilce v kibernetske krize. Sistem izziva ekipe, da sprejmejo kritične odločitve, ko se ukvarjajo z nastajajočimi incidenti, kot so izbruhi izsiljevalske programske opreme, grožnje notranjih informacij, kršitve podatkov in napadi lažnega predstavljanja.

Capture the Flag (CTF) [5]: To je vrsta simulacije, pri kateri se modra ekipa bori proti rdeči ekipi v boju za nadzor nad določenimi viri ali sistemom. Modra ekipa poskuša zaščititi svoje vire, medtem ko rdeča ekipa izvaja napade in poskuša pridobiti dostop do teh virov. Tekmovanja tipa CTF (Capture the Flag) so priljubljena oblika simulacij, ki ponujajo realistične scenarije napadov in obrambe. Capture the Flag (CTF) v računalniški varnosti je vaja, pri kateri so »zastavice« na skrivaj skrite v namerno ranljivih programih ali spletnih mestih. Lahko je to v tekmovalne ali v izobraževalne namene. Tekmovalci kradejo zastave drugim tekmovalcem (CTF v slogu napada/obrambe) ali organizatorjem (izzivi v slogu nevarnosti).

OWASP WebGoat [6] je namerno nezanesljiva aplikacija, ki omogoča preizkušanje ranljivosti, ki se pogosto pojavljajo v javanskih aplikacijah, ki uporabljajo običajne in priljubljene odprtokodne komponente. Glavni cilj je preprost: ustvariti dejansko interaktivno učno okolje za varnost spletnih aplikacij. Med izvajanjem tega programa bo naš računalnik izjemno ranljiv za napade. Med uporabo tega programa moramo zato prekiniti povezavo z internetom in tako zmanjšati izpostavljenost.

OWASP Juice Shop [7] je sodobna nezanesljiva spletna aplikacija. Uporablja se lahko pri varnostnih usposabljanjih, demonstracijah ozaveščanja in kot poskusni zajček za varnostna orodja. Juice Shop zajema ranljivosti skupaj s številnimi drugimi varnostnimi pomanjkljivostmi, ki jih najdemo v resničnih aplikacijah.

CyberStart [8] je spletna platforma, namenjena učenju in razvijanju kibernetskih varnostnih veščin. Učencem nudi zanimivo izobraževanje o kibernetski varnosti s pomočjo praktičnega učenja v obliki igre. Rešujemo skrivnostne kibernetske zločine, odkrivamo nove primere in pridobivamo spretnosti s področja kibernetske varnosti, medtem ko se podajamo skozi razburljive zgodbe in napredujemo kot kibernetski agent. Z iskanjem zastavic pridobivamo točke, na voljo imamo namige.

Nekatere spletne večuporabniške simulacije omogočajo interaktivno sodelovanje med takoimenovano modro in rdečo ekipo prek spleta. Sodelujoči lahko rešujejo izzive, preizkušajo svoje veščine, odkrivajo ranljivosti in se učijo o kibernetski varnosti na praktičen način. Take simulacije ponujajo realistične okoliščine, v katerih modra in rdeča ekipa sodelujeta pri odkrivanju ranljivosti, preizkušanju varnostnih sistemov in izboljševanju skupnega delovanja. Uporaba takšnih simulacij je koristna pri pripravi organizacije na morebitne kibernetske napade in izboljšanju njihove obrambne strategije.

5 DIDAKTIČNE SIMULACIJE IN MODRA TER RDEČA EKIPA

Didaktične simulacije modre in rdeče ekipe so zelo koristne pri usposabljanju in ozaveščanju glede kibernetske varnosti. Omogočajo praktično učenje, razvijanje veščin prepoznavanja ranljivosti, odzivanja na incidente ter izboljšanje celotne obrambne strategije organizacije.

Take simulacije omogočajo udeležencem, da se vživijo v vloge modre in rdeče ekipe ter pridobijo praktične izkušnje in znanje.

Didaktične simulacije modre in rdeče ekipe pogosto vključujejo naslednje elemente:

- **Scenariji napadov:** Simulacije ponujajo realistične scenarije napadov, ki jih je treba reševati. To vključuje simulirane napade, kot so poskusi vdora v omrežja, izkoriščanje ranljivosti, socialno inženirstvo, napadi z zlonamerno kodo in podobno. Cilj je, da modra ekipa prepozna in prepreči napade, medtem ko rdeča ekipa poskuša izkoristiti ranljivosti in pridobiti neupravičen dostop.
- **Upravljanje incidentov:** Simulacije ponujajo priložnost za učenje upravljanja varnostnih incidentov. Udeleženci se učijo, kako identificirati, analizirati in odpraviti varnostne incidente, medtem ko delujejo v skladu s postopki modre ekipe. Hkrati se rdeča ekipa trudi izkoristiti ranljivosti in povzročiti varnostne incidente, ki jih je treba zaznati in obvladati.

- **Sodelovanje in timsko delo:** Simulacije spodbujajo sodelovanje in timsko delo med udeleženci. Modra ekipa mora sodelovati in usklajevati svoje aktivnosti za učinkovito obrambo, medtem ko rdeča ekipa sodeluje pri izvajanju napadov. To poudarja pomen komunikacije, koordinacije in deljenja informacij med ekipami.
- **Analiza in izboljšave:** Po zaključku simulacije se izvede analiza rezultatov in izboljšav. Udeleženci se pogovorijo o ugotovitvah, ocenijo uspešnost modre ekipe pri preprečevanju napadov ter identificirajo možnosti izboljšav varnostnih postopkov. To pomaga pri učenju iz izkušenj ter pripravi na prihodnje izzive v kibernetski varnosti.

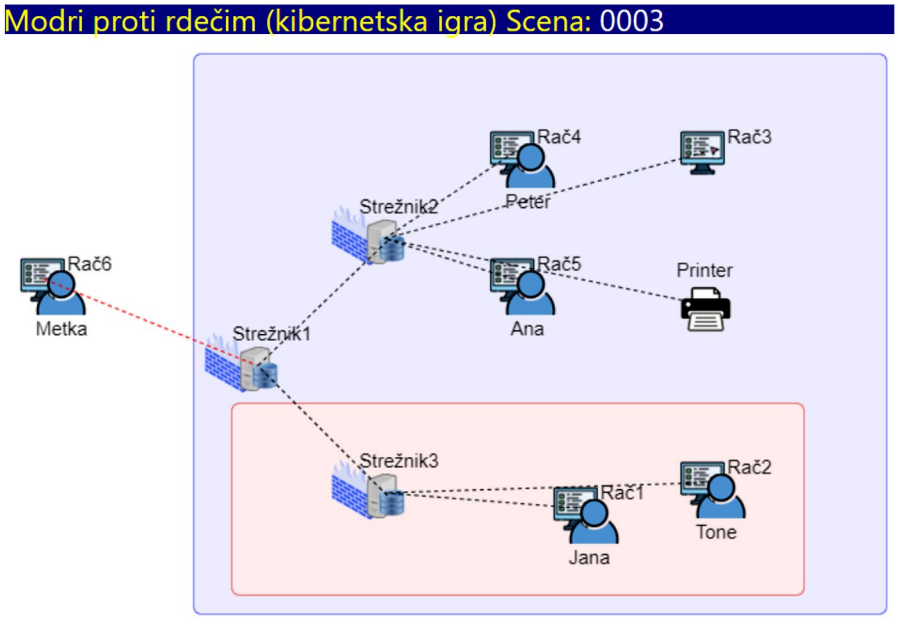
6 KIBERLETI IN SIMULACIJA MODRE IN RDEČE EKIPE

Kiberleti [9] so skupina računalniških simulacij s področja računalniške varnosti. Ime, deloma pa tudi programersko ozadje so dobili po analogiji s fizleti [10], ki so preproste simulacije na področju fizike. Ideja takih simulacij je konceptualno poučevanje znanosti, ki temelji na tem, da upoštevamo pri enostavnih (didaktično bolj razumljivih) primerih osnovne zakonitosti, kot sicer veljajo za resnične, kompleksne sisteme

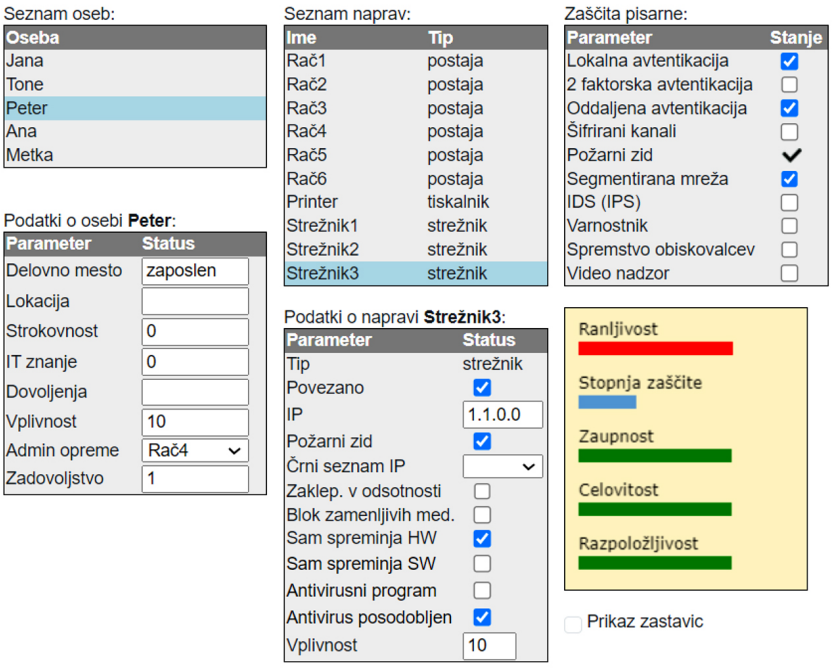
Simulacije tipično kažejo vnaprej konfigurirano mrežo strežnikov, delovnih postaj (uporabniških računalnikov, notesnikov ipd) in napadalcev. Delovne postaje med seboj komunicirajo s sporočili.

Posebnost strežnikov je, da na vsako prejeto sporočilo (zahtevek) pošljejo odgovor (izvedejo storitev, svoje sporočilo). Napadalci so tudi računalniki, ki pa le pošiljajo sporočila, ne morejo pa jih prejemati (so napadenim neznani). Računalniki se lahko okužijo, lahko jih tudi razkužimo in lahko jim dodajamo protivirusno zaščito. Računalnike lahko tudi vklapljamo (privzeto) ali izklapljamo. Mrežo lahko (tudi med potekom simulacije) poljubno širimo. Računalnike lahko izberemo s klikom miške in jih prestavljamo po zaslonu, morda zaradi boljšega pregleda.

Večina kiberletov so preproste računalniške simulacije, saj je njihov namen izobraževalni in vsaka taka simulacija ponazoruje predvsem določen koncept. Med bolj kompleksnimi simulacijami pa zasledimo večuporabniško spletno simulacijo »Modri proti rdečim«, ki je v bistvu spletna kibernetska igra. Scenarij predvideva uporabo simulacije v razredu tako, da predavatelj na svojem računalniku odpre sceno (objekt varovanja) in jo projicira na zaslon oziroma platno. Vsaka scena dobi svojo številčno kodo. Drugi udeleženci na svojih računalnikih poženejo vsak svojo spletno stran in (poleg svojega vzdevka) vpišejo kodo scene in se tako prijavijo v njej. Po dogovoru vstopajo v sceno kot člani modre ali rdeče ekipe.



Slika 1: **Primer začetne scene simulacije »Modri proti rdečim«.**



Slika 2: **Prikaz lastnosti oseb in naprav v varovanem objektu.**

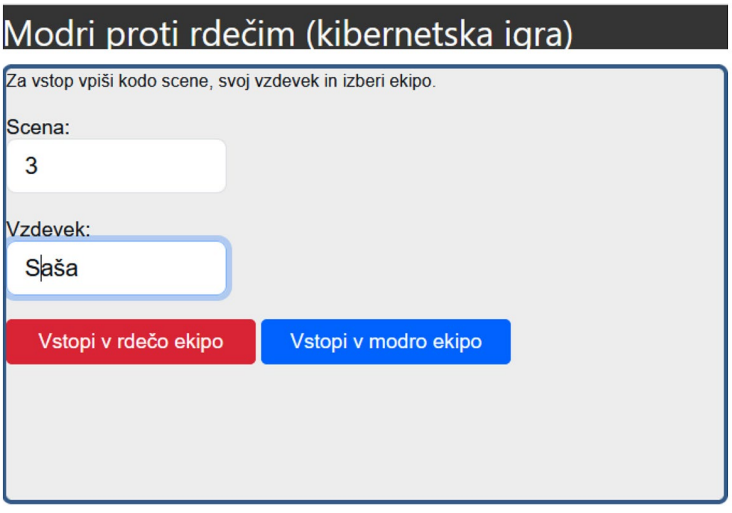
Spodnja slika prikazuje primer scene varovanega objekta, na začetku še brez članov modre in rdeče ekipe:

V varovanem objektu so že uvedli segmentirano notranjo mrežo in na strežnike namestili požarne pregrade. Ena od oseb dela »od doma«, na daljavo, niso pa še uvedli šifriranih komunikacijskih kanalov.

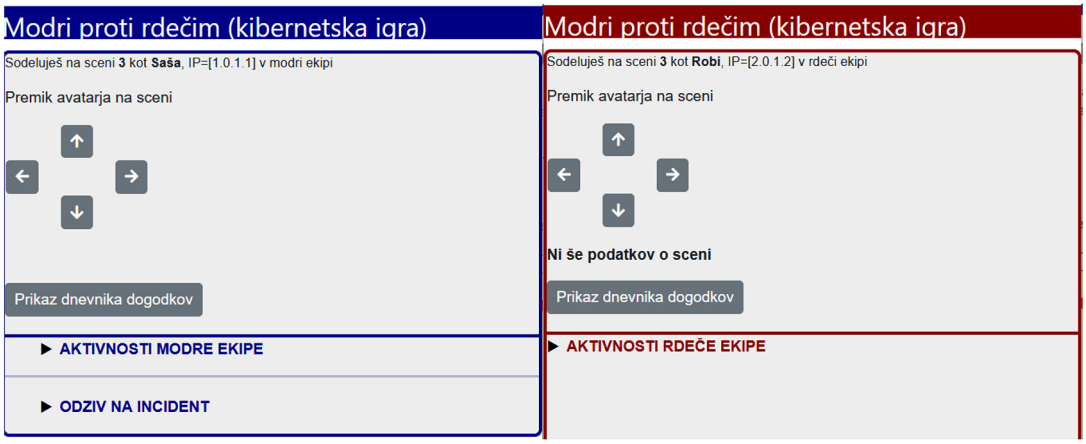
Na istem zaslonu (projiciranem na platno oziroma veliki zaslon) lahko spremljamo še karakteristike oseb in naprav v varovanem objektu in jih tudi lahko spreminjamo, Slika 2. kaže posnetek takega prikaza.

Nastavljanje teh lastnosti kot tudi varnostne politike v taki pisarni vplivajo na njeno ranljivost in stopnjo zaščite, po nastopu kakšnega varnostnega incidenta pa se primerno spreminja stopnja zaupnosti, celovitosti in razpoložljivosti.

Udeleženci simulacije (dijaki, študenti,..) vstopajo v sceno preko svojih računalnikov, lahko tudi tablic ali pametnih telefonov. Spodnje slike kažejo posnetek vstopne strani in posnetka strani člana modre oziroma rdeče ekipe.



Slika 3: **Vstopna stran za udeležence simulacije**



Slika 4: **Spletni strani udeležencev modre oziroma rdeče ekipe**

Vsak od udeležencev dobi na projicirani sceni svojo ikono - avatarja, ki jo lahko po sceni tudi premika s smernimi gumbi na svoji spletni strani. Bolj pomembno pa je, kaj vidi na svojem zaslonu.

Spodnja slika kaže sceno, v katero so vstopili 3 člani rdeče in 2 člana modre ekipe.

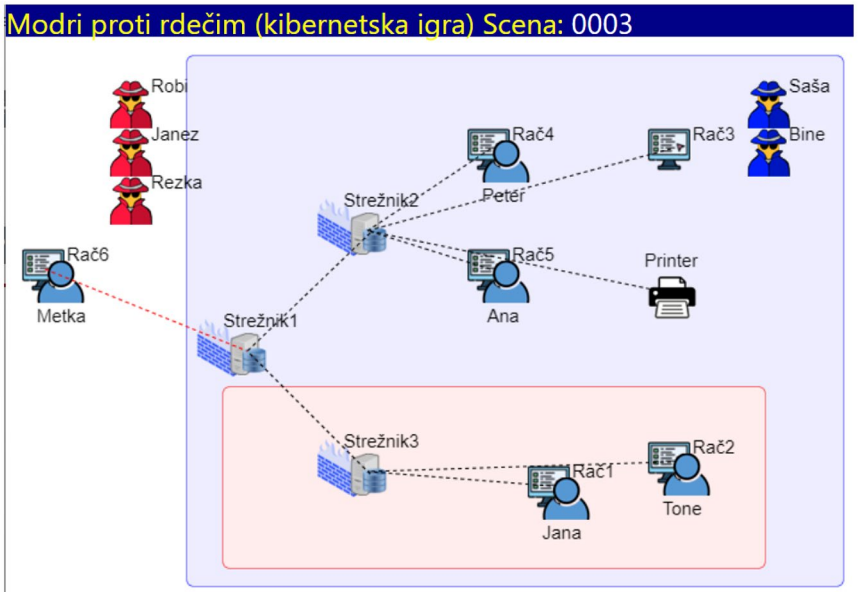
Člani rdeče ekipe so (vsaj v začetku) izven varovanega objekta, ki ga morajo najprej raziskati. Člani modre ekipe pa so že takoj znotraj varovanega objekta in so jim na voljo vse razpoložljive informacije. Seveda pa lahko vsak udeleženec s smernimi gumbi na svoji spletni strani poljubno premika svojega avatarja po prostoru. Člani rdeče ekipe lahko tako simulirajo fizični vdor v varovani prostor.

Posamezni člani rdeče in modre ekipe izbirajo med aktivnostmi., kot prikazujeta spodnji sliki.

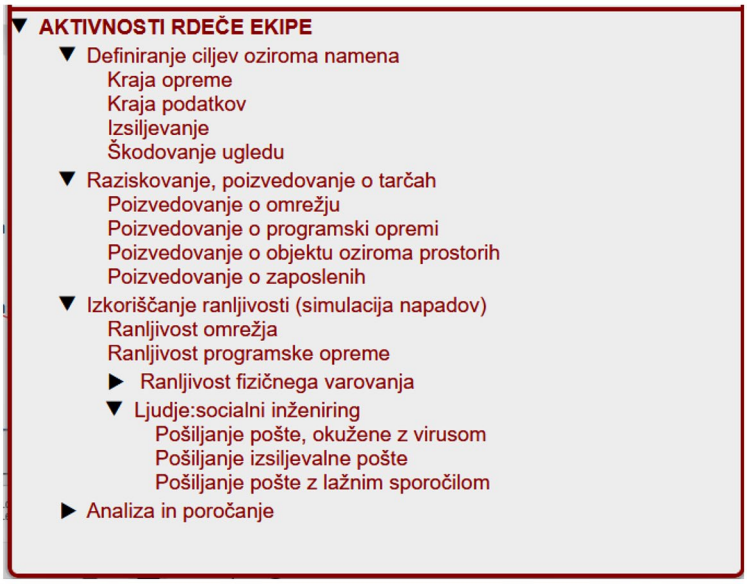
Člani rdeče ekipe morajo najprej opraviti poizvedbo oziroma raziskovanje o napadanem objektu. Šele nato začnejo izkoriščati ranljivosti in sprožajo različne napade.

Člani modre ekipe pa lahko vzpostavljajo različne obrambne mehanizme, v primeru ugotovitve incidenta pa lahko najprej opravijo forenzično raziskavo, nato pa izbirajo ukrepe za odpravo težav.

Tako člani rdeče kot člani modre ekipe lahko preklopijo na prikaz dnevnika svojih aktivnosti oziroma dogodkov. Spodnja slika na primer kaže v takem dnevniku, da je član rdeče ekipe najprej opravil poi-



Slika 5: **Scena z avatarji članov modre oziroma rdeče ekipe**

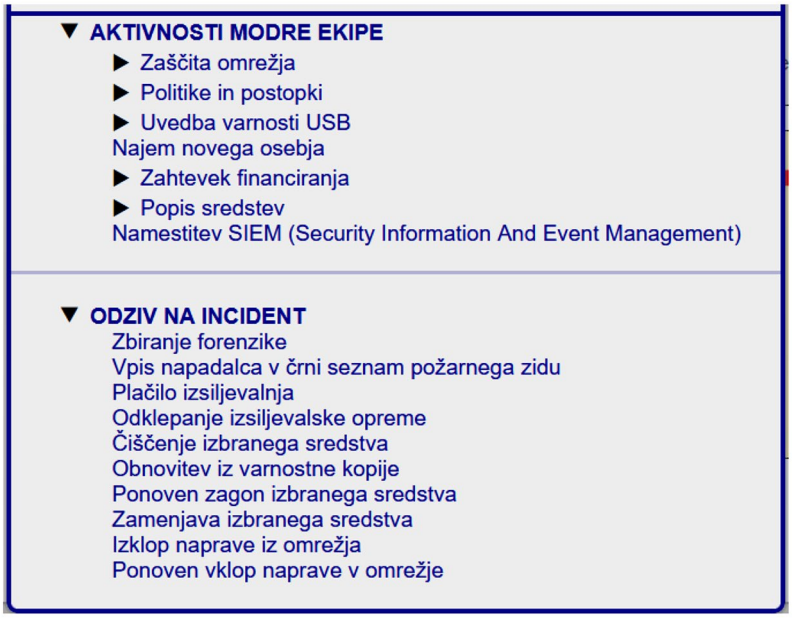


Slika 6: **Izbiranje aktivnosti člana rdeče ekipe**

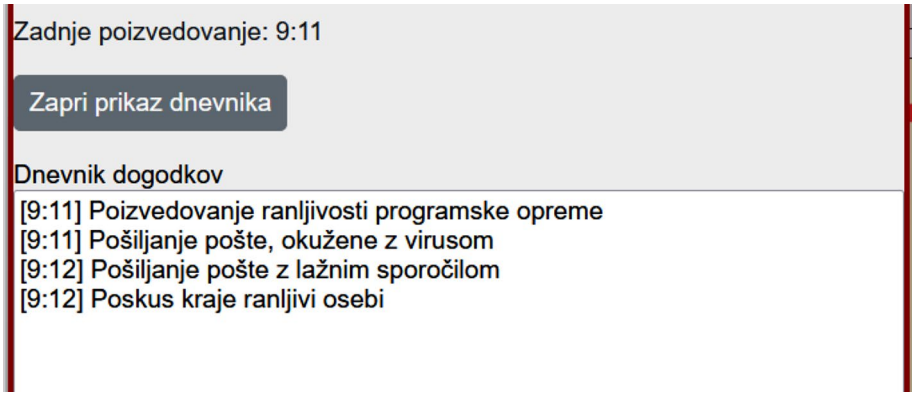
zvedovanje ranljivosti, nato pa poslal pošto, okuženo z virusom, in pošto z lažnim sporočilom. Končno mu je uspel tudi fizični vdor v objekt s ciljem kraje podatkov ali opreme.

Član modre ekipe pa je najprej opravil forenzično raziskavo in rezultate pogledal v svojem dnevniku dogodkov, kot to kaže spodnja slika:

Iz dnevnika lahko ugotovi, kateri IP je pošiljal komu sporočila z virusom ali lažna sporočila in kdaj je bil zaznan poskus fizičnega vdora. Slednje lahko ugotovi le, če je bil kot varnostni ukrep nameščen varnostnik ali pa je bil uveden video nadzor objekta. Forenzična raziskava tudi omogoči vpis napadalca v črni seznam v požarne zidove varovanega objekta.



Slika 7: **Izbiranje aktivnosti člana modre ekipe**



Slika 8: **Primer dnevnika dogodkov oziroma aktivnosti danega člana rdeče ekipe**

V simulacijo lahko vpletemo tudi koncept zavzema zastavic (Capture the flag), kakršno srečujemo tudi v tekmovanjih iz kibernetske varnosti. Tako bi lahko simulirali krajo podatkov ali opreme.

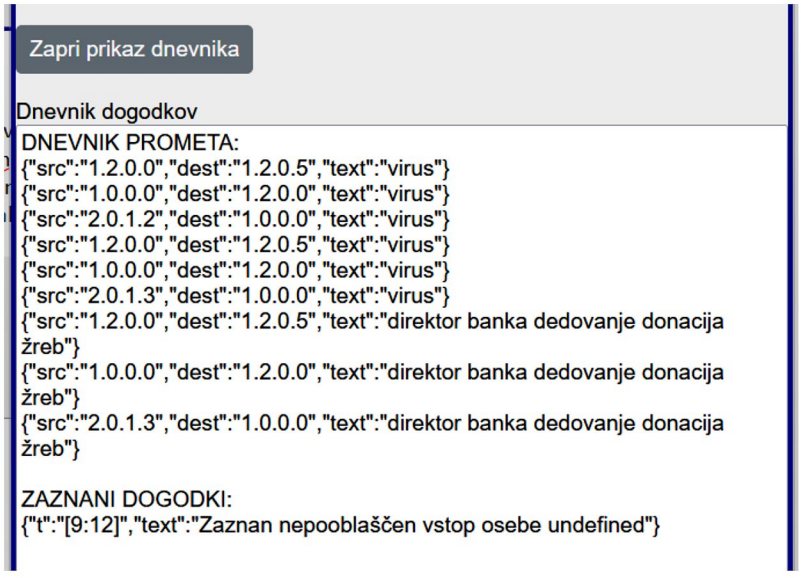
Slika10 prikazuje sceno z varovanim objektom in zastavice pri posamernih objektih.

Komentar: Modra ekipa je vzpostavila video nadzor, nastavila varnostnika, segmentirala interno omrežje in namestila požarne zidove na strežnike in tako izboljšala zaščito varovanega objekta.

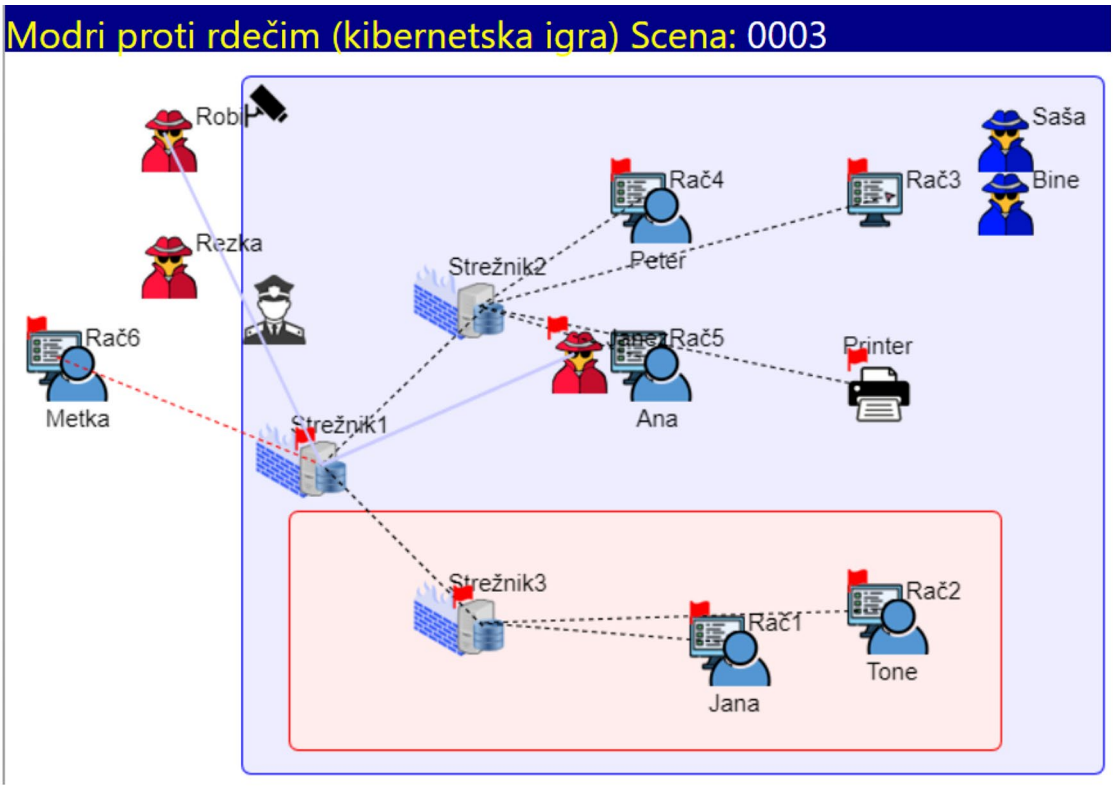
Vendar je kljub temu prišlo do kraje zastavice, ki jo je z enega obiskanega računalnika vzel nepridiprav (član rdeče ekipe) in tako simuliral krajo podatkov ali (dela) opreme. Morda sta bila uvedba video nadzora scene ali namestitev varnostnika prepozna. Seveda lahko do kraje pride tudi ob prisotnosti video nadzora in varnostnika, a bi v tem primeru modra ekipa imela na voljo vsaj forenzične podatke.

7 PROGRAMERSKO OZADJE SIMULACIJE

Ker je obravnavana simulacija večuporabniška, teče na strežnem računalniku strežni program, napisan v Javi. Tako simulacija scene kot simulacija članov obeh ekip je pisana v JavaScript, medsebojna komu-



Slika 9: **Primer dnevnika dogodkov danega člana modre ekipe**



Slika 10:**Scena z varovanim objektom, avatarji in zastavice pri posamernih objektih**

nikacija pa poteka preko WebSockets. Celotna aplikacija je tako kot ostali kiberleti pisana odprtokodno in brezplačno z licenco »CopyLeft«. To pomeni, da je na voljo komurkoli in brez kakršnihkoli omejitev.

8 RAZPRAVA

Predstavljena simulacija ni prava računalniška igra, saj je v običajnem scenariju modre in rdeče ekipe mišljeno, da imata skupni cilj - ugotavljanje ranljivosti varovanega objekta in njeno zmanjševanje. Zato naj bi rdeča ekipa o ugotovljenih ranljivostih vsaj na koncu poročala in o tem obvestila tudi modro ekipo. Podano večuporabniško spletno aplikacijo bi lahko dopolnili s sodobnimi komunikacijskimi metodami, morda v obliki klepetalnice. Ne nazadnje taka aplikacija temelji na enakih ali podobnih tehnologijah, v našem primeru WebSockets. Po drugi strani pa zasledimo elemente igre - skrivanje in pobiranje zastavic. V smislu poigritve bi lahko bolj upoštevali element reakcijskega časa, potrebnega za odzive na incidente. Ne nazadnje bi lahko upoštevali tudi nasprotujoče si dejavnike, kar bi vodilo v iskanje kompromisov pri odločanju. Na primer, marsikatera uvedba varnostnih mehanizmov tudi nekaj stane (namestitev dodatne opreme, zaposlitev dodatnega osebja,..) in tako zmanjšuje finančno uspešnost organizacije. Aplikacija ponuja možnost tudi dodatne nadgradnje, na primer z uvedbo filtriranja prejemane pošte glede na njeno vsebino, torej izločanja neželene pošte (spam). Poigritveno atraktivnost aplikacije pa bi lahko povečali z uvedbo 3D prikaza scene, kakršno zasledimo oziroma lahko vklopimo pri kiberletu »Varnost v pisarni«.

Podana spletna aplikacija je prvenstveno mišljena za uporabo v razredu oziroma predavalnici, saj za pogled na sceno (varovani objekt) uporabljamo projekcijo predavatelja na platno ali večji zaslon. Predvideva torej prisotnost vseh udeležencev v istem prostoru. Vendar bi lahko aplikacijo uporabljali tudi videokonferenčno (na primer z uporabo Zoom) tako, da bi predavatelj svoj zaslon delil tudi ostalim udeležencem.

9 ZAKLJUČKI

Osnovna naloga te simulacije je didaktični prikaz koncepta rdeče in modre ekipe in je namenjena, tako kot drugi kiberleti, predvsem popestritvi pouka. V razliko od ostalih simulacij pa je bolj kompleksna in

se poraja vprašanje, kje je konec didaktike in vodila »KISS« (Keep it small and simple). Program se da še bolj nadgrajevati, a lahko postane prekompleksen za uporabo pri predavanjih. Glede na to, da so vsi kiberleti in tudi ta večuporabniška aplikacija odprtokodni, pa lahko predstavlja izhodišče za raziskovalno in razvojno delo morda boljših študentov pri spreminjanju, izboljševanju in morda celo nadgrajevanju v skladu z lastnimi zamislimi. Tudi pri takem ustvarjalnem delu se učimo.

LITERATURA

[1] Jain, N. & Sharma, L. S. (2016). An Ontology based on the Methodology Proposed by Ushold and King. *International Journal of Synthetic Emotions (IJSE)*, *7*(1), 13-26.

[1] S.Divjak, Popestritev predavanj o kibernetski varnosti z interaktivnimi računalniškimi simulacijami, *Uporabna informatika, Letn. 31 Št. 1 (2023)*

[2] ThreatGEN® Red vs. Blue, *https://threatgen.com/, zadnji dostop 24. 6. 2023*

[3] Cobalt Strike: *https://www.cobaltstrike.com/, zadnji dostop 24. 6. 2023*

[4] Immersive Labs-CrisisSimulator, *https://www.immersivelabs.com/platform/cyber-crisis-simulator/, zadnji dostop 6. 7. 2023*

[5] Capture the Flag (CTF): The game for developers to learn information security, *https://nulab.com/learn/software-development/capture-the-flag-ctf-game-developers-learn-information-security/, zadnji dostop 26.6.2023*

[6] OWASP WebGoat, *https://owasp.org/www-project-webgoat/, zadnji dostop 4. 7. 2023*

[7] OWASP Juice Shop, *https://owasp.org/www-project-juice-shop/, zadnji dostop 4. 7. 2023*

[8] CyberStart, *https://cyberstart.com/, zadnji dostop 6. 7. 2023*

[9] Kibernetski napadi, *http://sasa.musiclab.si/KIBERLETI/, zadnji dostop 30. 9. 2023*

[10] Fizika s fizleti, *http://sasa.musiclab.si/fizleti/, zadnji dostop 6. 7. 2023*

▪

Saša Divjak je zaslužni profesor Univerze v Ljubljani, Fakultete za računalništvo in informatiko. Bil je vodja Odseka za avtomatiko, robotiko in biokibernetiko in kasneje načelnik Oddelka za elektroniko na Ins titutu Jo žef Stefan, pomočnik direktorja Iskre Delte, prodekan za raziskovalno delo na Fakulteti za elektrotehniko in računalništvo, prodekan za raziskovalno delo na Fakulteti za računalništvo in informatiko, dekan na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, gostujoči profesor na Fakulteti za informatiko Univerze v Vidmu, Predstojnik Katedre za programsko opremo na Fakulteti za računalništvo in informatiko v Ljubljani. Predsednik Slovenske sekcije IEEE. Predstojnik Laboratorija za računalniško grafiko in multimedije na Fakulteti za računalništvo in informatiko, odgovoren za več projektov s področja multimedijskih tehnologij, Predsednik računalniške sekcije v sklopu slovenskega društva IEEE, član Izvršnega odbor ACM Slovenija, član Izvršnega odbora Slovenskega društva INFORMATIKA, Urednik revije Uporabna informatika, Senior member IEEE. Predsednik mednarodnega združenja CoLoS (Conceptual learning of Science). Predsednik generalne skupščine mednarodnega združenja HSci (Hands on Science), član predsed stva in predsednik Evropske akademije znanosti (www.eurasc.org). Nosilec več projektov, predvsem s področja simulacije in avtomatizacije različnih tehnoloških procesov. Koavtor programske opreme prvih slovenskih robotov, sodelavec na italijanskem izobraževalnem projektu »Tovarne prihodnosti«. Nosilec več domačih in mednarodnih projektov s področja multimedijskih tehnologij v izobraževanju.