# Nacionalna konferenca Informacijska varnost – odgovori na sodobne izzive

V prostorih Fakultete za varnostne vede Univerze v Mariboru je 20. januarja 2012 prvič potekala nacionalna konferenca z naslovom Informacijska varnost – odgovori na sodobne izzive. Namen konference je bil združiti različne poglede, znanja in mnenja strokovnjakov s področja informacijske varnosti. V središču pozornosti so bili različni pogledi reševanja problematik; vzpostavljanja, vzdrževanja in upravljanja informacijske varnosti v poslovnih sistemih ter problematik preiskovanja in odkrivanja kibernetske kriminalitete. Informacijska varnost je tema, ki se mora zasidrati v sodoben način življenja, zato je prav, da se z različnimi pogledi na tematiko predstavi njen celosten vidik. Konference so se udeležili strokovnjaki iz gospodarstva, javne uprave in posamezniki, ki se srečujejo s širšim področjem informacijske varnosti. Pomemben prispevek konferenci so prispevali tudi študenti, tako kot aktivni udeleženci s svojimi prispevki kot slušatelji. Tovrstni dogodki nudijo študentom spoznavanje novih pogledov, krepitev lastnih kompetenc ter možnost za spoznavanje strokovnjakov. Cilj konference je bil predstaviti sodobna spoznanja in raziskovalne ugotovitve s področja informacijske varnosti, prikazati pomembnost v realnem okolju, doprinos prakse k raziskovalno teoretičnemu ozadju in prenosa raziskovalnih znanj v prakso. Vsebina konference je prikazala učinke ustrezne ravni informacijske varnosti na delovanje organizacij in delo posameznikov ter spoznavanje z grožnjami v kibernetskem prostoru. Konferenca je bila organizirana v sklopu razvoja in promocije evropskega projekta »eSec« - evropskega varnostnega portala.

Udeležence konference je najprej nagovoril dekan Fakultete za varnostne vede Univerze v Mariboru, prof. dr. Gorazd Meško, ter glavni organizator konference dr. Igor Bernik, prodekan za pedagoško dejavnost in vodja katedre za informacijsko varnost na fakulteti. Dekan je poudaril pomen vseh segmentov varnosti v družbenem okolju in pomembnost razvoja informacijske varnosti, za kar se v veliki meri zavzemajo na fakulteti. Pomen raziskovanja področij varnosti je povezal z aplikativno vrednostjo, kar daje velik pomen pri povezovanju raziskovalnega področja na fakulteti z zunanjimi organizacijami in podjetji. V nadaljevanju otvoritvenih govorov je Igor Bernik povedal nekaj več o konferenci in mednarodnem projektu eSEC, zatem pa predal besedo plenarnim govornikom. Rančigaj in Lobnikar sta predstavila pomene vedenjskih vidikov pri zagotavljanju informacijske varnosti, Prašiček, Podbregar in Ivanuša pa pomen informacijske varnosti v procesu odločanja.

Po plenarnem delu so se začele delavnice, ki so predstavile praktične primere reševanja informacijsko varnostnih vprašanj in so potekala vzporedno s predavanji. Predstavile so ocenjevanje tveganj s sistemom neprekinjenega poslovanja (Netis

d.o.o.), iskanje revizijske sledi s programom Arbiter (Abakus d.o.o.) in z vprašanjem Ali lahko zaupamo CA-jem? preverile zgodbo o Diginotarju (Real Security d.o.o.).

V splošni sekciji so avtorji razpravljali in predstavili različne poglede na informacijsko varnost z vidika upravljanja, kazenskega prava, zasebnosti in ranljivosti kritične infrastrukture. Cvelbar je v prvem prispevku predstavil register tveganj kot nadzorno ploščo upravljanja informacijske varnosti. Register temelji na večletnem delu in zbiranju podatkov in služi kot osnova za upravljanje. Markelj in Zgaga sta obdelala vidike kazenskega prava pri uporabi mobilnih naprav in dostopanju do korporativnih podatkov. Ugotavljata, da raba mobilnih naprav lahko predstavlja nevarnosti za uporabnika in korporativna okolja ter prikažeta kazenske posledice morebitnih zlorab. Cunk je predstavil Slovensko informacijsko zasebnost ter kibernetsko kriminaliteto v letih 2000–2010, Kotnik pa grožnje in ranljivost kritične infrastrukture iz fizičnega in kibernetskega prostora.

V sklopu predstavitve prispevkov se je po kratkem premoru sekcija razdelila na dve tematsko različni področji. Prva je bila tematsko obarvana z informacijsko varnostjo in kriminaliteto, medtem ko je bila druga sekcija tematsko usmerjena v informacijsko varnost v poslovanju.

V prvem sklopu predavanj so se avtorji svojih prispevkov dotaknili problema kriminalitete v kibernetskem prostoru in potrebi po večji ozaveščenosti. Nevedno oziroma nespametno ravnanje v kibernetskem prostoru, po prepričanju vseh avtorjev, uporabnike lahko pripelje v nezavidljiv položaj. Tako sta Bernik in Prislan predstavila upravljanje varnostnih tveganj pri rabi mobilnih naprav, Markelj pa poglede informacijske varnosti na storitve računalništva v oblaku. Potokar je predstavil uporabo razširjenega modela za oceno tveganja s pomočjo računalniškega programa DEXi, Gracer nevarnost skimminga in zlorab v Sloveniji, Prešeren je predstavil varnostne vrzeli v sistemu prenosa podatkov SSL/TLS, hekerske vdore in zaščito v Oracle zbirke podatkov pa Oblak. Sekcijo sta zaokrožila Božič s predavanjem »S sistemom neprekinjenega poslovanja do zmanjševanja tveganj« in Žurga z »Mehanizmi za overjanje dostopa do informacijskega sistema«.

V drugem sklopu predavanj so avtorji informacijsko varnost povezovali z dogajanji v poslovnem procesu. V veliki meri so izpostavili potrebo po izobraževanju uporabnikov. Informacijska tehnologija, po prepričanju avtorjev, tako uporabnikom kot organizacijam ponuja številne poslovne priložnosti. Istočasno pa predstavlja tudi številne pasti, v smislu informacijskih groženj, med katere sodijo tudi odtujitev podatkov in vdor v kriptiran prenos podatkov. Zupanova je predstavila zahteve za varovanje e-bančnih storitev in izzive varovanja, Rusova organizirano kriminaliteto v kibernetskem prostoru, Zormanova je nadaljevala s problematiko preiskovanja otroške pornografije na spletu, Košnik in Frangež pa sta predstavila ukrepe za zmanjšanje izpostavljenosti otrok s prispevkom »Blokiranje spletnih strani kot ukrep boja proti razširjanju posnetkov spolne zlorabe otrok«. Drugi del sklopa pa so napolnili z vsebinami o vlogi in pomenu informacijske varnosti na trgu konkurenčnosti sodobne družbe, ki jih je predstavila Mrzdovnikova, Kralj je predstavil varnostno politiko informacijskega sistema, zasebnost osebnih podatkov sta predstavila Repovž in Bernik, na podlagi zasebnosti pa je Breznik prikazal izpostavljenost tveganjem pri uporabi medmrežja.

V zaključku so sledila še tri predavanja s tematsko povezavo informacijske varnosti in njene prisotnosti oziroma odsotnosti v zdravstvu. Tako je Orel pregledal priporočilni standard SUVI in dopolnitve za področje varnosti v zdravstveni informatiki, Marcelan in Bernik sta ugotavljala stopnjo varnosti in zagotavljanje zasebnosti bolnišničnih podatkov o pacientih, Trdina pa je predstavil oceno varnostno informacijskih tveganj na primeru bolnišnice Golnik.

Da je potreba po tovrstnih konferencah velika, je pokazalo okvirno sto slušateljev. Očitno so varnostni izzivi v informatiki veliki, predstavljene teme pa so bile aktualne in skrbno predstavljene. V naslednjih letih pričakujemo stopnjevanje sodelovanja med teoretičnimi izhodišči, ki jih razvijamo na fakulteti in prenos v prakso in obratno ter internacionalizacijo konference. Prepričani smo, da bodo predstavljeni rezultati pripomogli k boljšemu razumevanju predstavljene problematike.

Organizatorji konference vabijo zainteresirane, da pregledajo zbornik konference, ki se nahaja na naslovu www.fvv.uni-mb.si/KonferencaIV/zbornik.html, in v koledarju označijo datum naslednje, ki se bo odvijala 5. oktobra 2012. Vabljeni.

*Blaž Markelj, Igor Bernik*