

## DRUŠTVENE VIJESTI

DGITM ČAKOVEC ORGANIZIRAO STRUČNI SEMINAR

# Informacijska sigurnost

Društvo građevinskih inženjera i tehničara Međimurja DGITM Čakovec je 9. veljače 2024. organiziralo stručni seminar na temu *Informacijska sigurnost*

Seminar je sastavni dio Programa stručnog usavršavanja DGITM-a za razdoblje od 1. siječnja 2023. do 31. prosinca 2024. godine. U glavnu se temu izvrsno uklopila i stručna tema "Inovacije i najnovija tehnološka dostignuća u graditeljstvu". Seminaru je prisustvovao 41 član Društva. I taj je put stručni seminar održan u Centru održivog razvoja. Radi se o znanstveno-istraživačkome centru koji se koristi za potrebe Međimurskoga veleučilišta u Čakovcu (MEV) i drugih znanstvenih subjekata. DGITM Čakovec već dugi niz godina uspješno surađuje s MEV-om.

Stručno predavanje u trajanju od četiri školska sata održali su stručnjaci iz tvrt-

ke *Baldinistudio d.o.o.* i Policijske uprave Međimurske.

U sklopu seminara "Inovacije i najnovija tehnološka dostignuća u graditeljstvu" predstavljene su dvije teme, i to "Pregled BIM alata u interakciji arhitekata i građevinskih inženjera" te "3D sken u BIM-u". Tvrtka *Baldinistudio d.o.o.* zastupnik je softvera namijenjenih građevinskoj, arhitektonskoj i strojarскоj industriji. Pored zastupništva jedna od njezinih glavnih djelatnosti jest edukacija i implementacija BIM načina rada u poslovanje građevinskih i arhitektonskih tvrtki. Misija im je omogućiti kvalitetnu i cjelovitu implementaciju BIM načina rada svim sudionicima građevinskih projekata koja

će se postići prodajom vrhunskih BIM softvera, sveobuhvatnim edukacijama i stalnom podrškom aktivnim korisnicima softvera. Zastupljeni su u Hrvatskoj, Sloveniji i Srbiji.

Stručno predavanje na tu temu održao je Ivan Derežič, mag. ing. aedif. U uvodu naveo je poražavajuće brojke u graditeljskome poslovanju. Naime, građevinski sektor u svijetu vrijedi otprilike 3,5 trilijuna dolara, a najmanje 20 posto navedenog iznosa nije iskoristivo jer je 10 posto materijala višak, 30 posto projekata se promijenilo, 40 posto vremena nije produktivno, 40 posto projekata premaši raspoloživi budžet i 90 posto projekata kasni. Sve su to posljedice neučinkovite komunikacije, planiranja i kolaboracije. Do prekoračenja troškova dolazi zbog loših informacija, nedostatka koordinacije te loše produktivnosti i gradnje. Prema tipovima projekata, prosječno prekoračenje troškova iznosi 11 posto kod mostova, 27 posto kod cesta, 30 posto kod željeznica, 39 posto kod zgrada, 56 posto kod zračnih luka, 68 posto kod brana i 149 posto kod tunela. Prednosti su BIM-a bolja komunikacija/kolaboracija između projektnih timova (smanjenje nepredviđenih promjena za 40 posto), ranije donošenje preciznih odluka o dizajnu (80 posto manje vremena potrebnog za izradu procjene troškova), smanjenje prepravaka kroz prepoznavanje "sudara" (smanjenja vrijednosti ugovora od 10 posto), smanjenje rasipanja materijala i ugljičnoga dioksida (točnost procjene unutar tri posto) i brža dostava projekata (sedam posto kraće trajanje projekta). Na predavanju predstavljena je interakcija softvera u području arhitekture, građevinarstva i strojarstva, i to softvera *Allplan*, *Lumion*, *Scia*, *Idea Statica* i *Geo5*. Na kraju predstavljen je Bimplus koji se koristi za projektni menadžment, upravljanje informacijama, praćenje promjena te za koordinaciju i suradnju sudionika u procesu gradnje.



Polaznici seminara o informacijskoj sigurnosti

## DRUŠTVENE VIJESTI

U drugome dijelu predavanja obrađena je tema "3D sken u BIM-u". Odmah na početku istaknuto je da je zabluda da se laserskim skeniranjem dobiva sve i da se radi o najmodernijoj i najmoćnijoj tehnologiji u službi projekatana. Uobičajeni koraci 3D skena jesu skeniranje, obrada skena, 3D model i BIM model. Međutim, potreban je nulti korak koji si projektanti često ne postavljaju, odnosno odgovor na pitanje zašto uopće skeniramo. Ukratko su predstavljeni softveri *Matterport cloud* i *Matterport stages*. Prvi se odnosi na skeniranje prostora te na naknadno precizno mjerenje svih elemenata, čime se štedi vrijeme i eliminiraju ponovni posjeti gradilištu. Drugi se odnosi na platformu za praćenje napretka izgradnje, čime se mogu usporediti pogledi na različite faze građevine u podijeljenome zaslonu. Tijekom gradnje može se podvući vremenska crta, a omogućen je i vrlo brz i jednostavan pristup sveobuhvatnoj tehničkoj dokumentaciji. Na kraju predavanja, u praktičnome dijelu prikazano je skeniranje prostorije u kojoj je održano predavanje.

Druga tema predavanja bila je "Informacijska sigurnost", o kojoj je govorio mr. sc. Miljenko Vrbanec, spec. krim. S obzirom na to da živimo u digitalnome društvu, informacijska tehnologija u globalnome svijetu postaje sve važnija i velik je potencijal za gospodarski rast, zapošljavanje, inovacije i poboljšanje kvalitete života građana. Međutim, radi se o dvije strane iste medalje, privatnosti i zaštiti. U današnje vrijeme internetska sigurnost više ne ovisi samo o tome kako mi, kao digitalni građani, upravljamo vlastitim sigurnosnim rizicima, već i o tome da svojim postupcima i ponašanjem ne izložimo druge opasnosti. Biti digitalni građanin znači naučiti kako zaštititi pristup svojim uređajima i pozorno postupati sa svime što može ugroziti privatnost i sigurnost nas ili drugih. Četrdeset posto vremena

koje provodimo budni provodimo na internetu, kojim se koristi 5,5 milijardi ljudi (64,4 posto svjetske populacije), a čak tri četvrtine svjetske populacije posjeduje mobitel. Više od polovine svjetskoga stanovništva koristi društvene mreže. Internetski napadi i internetski kriminal sve su češći i sofisticiraniji u cijeloj Europi. Taj će trend nastaviti rasti jer se očekuje da će 41 milijarda uređaja diljem svijeta do 2025. biti povezana s internetom. Kina je trenutno s 1,05 milijardi korisnika vodeća u svijetu po broju korisnika interneta, što čini više od 20 posto ukupnog broja korisnika interneta u svijetu. Oko 73,7 posto stanovništva Kine ima pristup internetu. Indija, druga najmnogoljudnija zemlja od 2023., drži drugo mjesto na listi sa 692 milijuna korisnika interneta, ali samo oko 48,7 posto indijskoga stanovništva ima pristup internetu, po čemu se nalazi ispod svjetskoga prosjeka. Zapravo, Indija s više od 730 milijuna ljudi koji nemaju pristup internetu ima najveći broj nepovezanih ljudi u svijetu.



Predavači i Izvršni odbor DGIT Međimurje

Internetski kriminal javlja se u raznim oblicima, a mnoga uobičajena kaznena djela lakše je počinuti preko interneta. Na

primjer, kriminalci mogu preuzeti kontrolu nad osobnim uređajima pomoću zlonamjernoga softvera, ukrasti ili kompromitirati osobne podatke i intelektualno vlasništvo kako bi počinili internetske prijevare. Trošak koji na svjetskoj razini uzrokuje internetski kriminal svake godine iznosi 5,5 bilijuna eura. Prijevare i kriptovorenja koja uključuju bezgotovinska plaćanja ozbiljna su prijetnja sigurnosti EU-a i donose znatne prihode organiziranome kriminalu. Takve vrste prijevara ujedno utječu na povjerenje potrošača u sigurnost digitalnih tehnologija. Društveni inženjering nastavlja rasti kao pokretač mnogih kibernetičkih kaznenih djela među kojima je krađa identiteta najučestaliji oblik. Kriminalci koriste društveni (socijalni) inženjering kako bi postigli ciljevi: dobivanje osobnih podataka, otimanje računara, krađa identiteta ili pokretanje nezakonitih plaćanja. Jedan jedini klik može biti dovoljan da ugrozi cijelu organizaciju. S obzirom na navedene opasnosti, predstavljeni su alati što poduzeti ako je računalo zaraženo zloćudnim računalnim programom. Napadi se mogu spriječiti sigurnosnim kopijama. Najbolje je napraviti dvije sigurnosne kopije, i to jednu koja je spremljena na oblak aplikaciji koja automatski radi sigurnosne kopije i drugu fizičku kopiju na prijenosni tvrdi disk, memorijski štapić (*USB stick*), dodatno prijenosno računalo i slično koje je nakon toga potrebno isključiti iz računala. Sigurnosne kopije također će biti korisne u slučaju da se slučajno izbrišu važne datoteke ili se naiđe na poteškoću pri korištenju tvrdog diska. Kvalitetan antivirusni softver služi za zaštitu sustava od *ransomware* zloćudnoga računalnog programa. Potrebno je i redovito ažurirati instalirane softvere na računalo. Bilo koji korisnički račun može biti ugrožen, a zloćudne poveznice mogu stići s korisničkih računa prijatelja na društvenim mrežama, kolega ili partnera u mrežnim

## DRUŠTVENE VIJESTI

videoigrama. Opće je poznato da nikada nije dobro otvarati priloge u e-porukama koje šalju nepoznati pošiljatelji. Internet-ski kriminalci često dijele lažne e-poruke koje su vrlo slične e-obavijestima internetskih trgovina, banaka, policije, suda ili porezne službe te na taj način mame primatelje da kliknu na zločudnu poveznicu i tako zločudnome softveru dopuste pristup u svoj sustav.

Dobro je omogućiti opciju "prikaži ekstenziju datoteka" ili "show file extensions" u Windows postavkama računala. Datoteke s nastavcima .exe, .vbs i .scr treba izbjegavati. Prevaranti često koriste nekoliko nastavaka kako bi zločudnu datoteku prikazali kao video, fotografiju ili dokument (kao što je hot-chics.avi.exe ili doc.scr). Otkrije li se na uređaju nepoznati ili nekontrolirani proces, potrebno je odmah prekinuti internetsku ili drugu mrežnu vezu (kao što je kućni Wi-Fi) jer će to spriječiti daljnje širenje zaraze.

Sljedeće područje teme informacijske sigurnosti bilo je upravljanje zaporkama. Autentifikacija jest proces provjere identiteta osobe ili procesa (entiteta) čija je svrha potvrditi da je entitet upravo onaj za koji se izdaje. Posljednja je prepreka između korisnika i računala te široko rasprostranjena metoda. Autorizacija jest proces u kojemu se entitetu odobrava pristup resursima nakon što je uspješno završen proces autentifikacije. Činjenica je da zaporka nisu najbolji način autentifikacije zato što mogu biti relativno lako otkrivene, ukradene ili dijeljene među više korisnika, što rezultira zlouporabom. Cilj upravljanja zaporkama jest podići svijest korisnika, definirati razloge korištenja zaporki, opisati načine čuvanja zaporki te opisati alate koji služe za otkrivanje zaporki. Zanimljiv je podatak da je zaporka 123456 na vrhu rang-liste najčešćih zaporki u 2023. Vrijeme potrebno za "razbijanje" kraće je od sekunde, a koristila se čak 4 524 867 puta. Postoje dva



Polaznici seminara o informacijskoj sigurnosti

načina odabira zaporka, i to samostalni odabir i korištenje programskih proizvoda za generiranje zaporki. Pokazani su primjeri kakve bi zaporka trebalo izbjegavati te dane preporuke za "čvrste" zaporka. Osim softvera za generiranje zaporki postoje i softveri za čuvanje zaporki.

Na kraju se predavač osvrnuo na temu umjetne inteligencije (UI), odnosno prema engleskome akronimu AI (*Artificial Intelligence*). UI jest dio računalstva koji se bavi razvojem sposobnosti računala da obavljaju zadatke za koje je potreban neki oblik inteligencije. Osim toga UI označava svojstvo neživog sustava koji pokazuje inteligenciju, odnosno inteligentni sustav. Konkretno, UI omogućuje tehničkim sustavima oponašanje ljudskih aktivnosti, percipiranje okruženja i rješavanje problema. Primjeri primjene u svakodnevnome životu uključuju internetsku kupovinu i oglašavanje, digitalne osobne asistente i strojno prevođenje. U građevinarstvu su primjeri UI-a pametni domovi, gradovi i infrastruktura. UI može optimirati energetske učinkovitost i regulirati promet u pametnim gradovima. Ukratko, UI jest ključna tehnologija koja oblikuje našu sadašnjost i budućnost, omogućujući napredak u različitim područjima.

Kao odgovor na pitanje kako se zaštititi u digitalnome svijetu predstavljen je program i akcija "Web heroj" ("Ulovimo lika s weba koji tvoje € vreba"). Ta se akcija bavi raznim vrstama prijevara te time kako ih prepoznati te kako se uspješno zaštititi i unaprijediti svoju računalnu sigurnost. Pokazane su zamke i što poduzeti u slučaju internetskih prijevara (prijevara s računima, direktorska prijevarena, investicijska prijevarena, prijevare pri internetskoj kupnji, romantična prijevarena) te krađe identiteta (*phishing* mrežna krađa identiteta, krađa identiteta SMS-om, lažne stranice banaka i krađa identiteta pozivom).

Predavanje o informacijskoj sigurnosti uvijek je dobro ponoviti s vremenom na vrijeme jer premda mislimo da se nama to ne može dogoditi jer smo dobro poznati s mogućim prijevarama i zlouporabama, to se u ovim turbulentnim vremenima, u brzini ipak može nehotice dogoditi svakome. Samo mali trenutak nepažnje može dovesti do ozbiljnih posljedica. Bilo je to prvo stručno predavanje Društva u 2024. U nastavku godine slijede daljnji stručni seminari prema programu te jednostavna i višednevna stručna putovanja.

**Ratko Matotek, dipl.ing.grad.**