letnik 2, številka 2, 2023

futura

ŠTUDENTSKA REVIJA FAKULTETE ZA UPRAVO

Prilagojena izdaja za netradicionalne skupine študentov

odgovorna urednica:
Nina Rems

Univerza v Ljubljani
Fakulteta za upravo

Revija FU-TURA (fu-tura@fu.uni-lj.si)
letnik II, številka 2, 2023
ISSN 2820-5138

Odgovorna urednica: Nina Rems
Področne urednice: Tamara Fiksl, Valinea Sušec, Klavdija Košec in Svetlana Brecelj
Izdajatelj: Univerza v Ljubljani, Fakulteta za upravo, Gosarjeva ulica 5, 1000 Ljubljana
Jezikovno svetovanje: doc. dr. Tadeja Rozman
Oblikovanje: Darja Remc

Pogostost izhajanja: 2x na leto
Format: digitalna izdaja (pdf) in tiskana izdaja
J ezik izdajanja: slovenski
Ključne besede: javna uprava, upravljanje, vladavina prava, sistem, javni interes, študenti
Razvid medijev MK RS: št. 2489

»Vsak dan ti ponuja prazno platno in novo barvico.«

Novo študijsko leto, nova številka strokovne študentske revije FU-TURA. Ta številka je prav posebna, saj je bila del sodelovanja študentskega RSF projekta za prilagoditev vsebin netradicionalnim skupinam študentov. V tej številki si lahko preberete članek v nemškem jeziku in dvojezični slovensko-italijanski intervju. Opis revije je za slepe zapisan v Braillovi pisavi, za gluhe in naglušne pa je v video posnetku tolmačen v znakovni jezik. Poleg običanje spletne verzije imamo na voljo še posebno izdajo, ki je prilagojena slabovidnim bralcem, dislektikom ter bralcem z motnjo pozornosti.
Pri FU-TURI menimo, da je treba branje naše revije omogočiti vsakomur, saj lahko v tej številki preberete zanimive strokovne članke na temo diskurza v sodobni družbi, zlorabe osebnih podatkov v digitalni dobi, pakta za stabilnost in rast EU ter stanja prekomerne razpoložljivosti zaposlenih za delo izven delovnega časa v zasebnem sektorju v obdobju covida-19. Poleg strokovnih člankov si lahko preberete tudi nekaj lahkotnejših vsebin, ki predstavljajo ter povzemajo študentsko (obštudijsko) dogajanje na Fakulteti za upravo, in sicer delovanje sveta FU v lanskem študijskem letu, aktivnosti na 13. Študentski konferenci, dogodke, ki jih organizirajo FUL Povezani, in še mnoge druge vsebine.
Kot vedno bomo seveda veseli vaših vsebinskih idej in predlogov za izboljšave, pišite nam po e-pošti na naslov fu-tura@fu.uni-lj.si.

Veliko užitka pri branju!

Področne urednice *Tamara Fiksl, Valinea Sušec, Klavdija Košec, Svetlana Brecelj* in odgovorna urednica *Nina Rems*.

Predstavitev revije FU-TURA v znakovnem jeziku

Revija FU-TURA, letnik II, številka II, je nastala v okviru projekta Študentske objave tekom vpetosti v študijski proces – pilotna implementacija prilagoditve vsebin z upoštevanjem specifik izbranih netradicionalnih skupin, ki je financiran v okviru internega razpisa Univerze v Ljubljani »Razvoj rešitev za vključevanje netradicionalnih skupin študentov v visokošolski študij«, vezano na ukrep RSF (tj. Razvojni steber financiranja 2021-2024) »Prilagajanje študijskih programov potrebam netradicionalnih skupin« (S.C.1.2).

kazalo

prilagojeno
za ADHD

Diskurz v sodobni družbi

Tadej Jezernik
tj0950@student.uni-lj.si

Tadej **Jeze**rnik je **štud**ent **1. letn**ika **magist**rskega **prog**rama **Up-ra**va - **upravl**janje **javn**ega **sekt**orja **n**a **Fakul**teti **z**a **upra**vo. **Jul**ija **20**23 **j**e **zaklj**učil **man**dat **predst**avnika **v Sve**tu **mla**dih **pr**i **evro**ps-ki **strat**egiji **z**a **alp**sko **reg**ijo (**EUSA**LP). **Zani**majo **g**a **zdravs**tvene **polit**ike, **razm**erje **me**d **mlad**imi, **upra**vo **i**n **poli**tiko **ter kako**vost **jav**nih **stori**tev.

06

povzetek

Kakšen **disk**urz **s**e **poja**vlja **v sodo**bni **druž**bi? **Ka**ko **ko**t **bodo**či **držav**ni **urad**niki **zna**mo **prepo**znati **posam**ezne **elem**ente **disk**urza **i**n **al**i **s**e **bo**mo **z disku**rzom **sreče**vali **tu**di **pr**i **svo**jem **del**u? **Kaj pravz**aprav **j**e **met**oda **krit**ične **anal**ize **disk**urza **i**n **ka**ko **j**o **interpr**etirati **v konte**kstu **šir**še **teor**ije **disku**rza, **te**r **ka**ko **k poj**avu **disk**urza **prist**opiti **celov**ito, **analit**ično, **pragma**tično? **V čla**nku **s**e **osredo**točamo **n**a **teoret**sko **predst**avitev **disk**urza **v druž**bi **i**n **posku**šamo **odgov**oriti **n**a **pr**ej **zastav**ljena **vpraš**anja. **Pojas**niti **želi**mo, **ka**ko **disk**urz **v dru**žbi **nast**aja, **ka**ko **s**e **reprod**ucira **i**n **ka**ko **lah**ko **z met**odo **krit**ične **anal**ize **disk**urza **prist**opimo **k bo**lj **analit**ičnemu **razmiš**ljanju **o te**m, **kaj disk**urz **z**a **dru**žbo **spl**oh **predst**avlja.

Ključne **bese**de: ***disk**urz, **krit**ična **anal**iza **disku**rza, **upra**vni **disk**urz, **upra**va.*

Diskurz v sodobni družbi

DISKURZ

V začetku našega članka želimo predstaviti teoretsko osnovo diskurza, ki temelji na filozofskem konceptu, ki so ga v svojih delih razvijali številni avtorji. Da bi lahko omenjeni koncept diskurza predstavili celovito in čim bolj objektivno, se bomo najprej osredotočili na golo definicijo diskurza. V različnih filozofskih obdobjih v pretekli osti je imel diskurz več definicij, saj so ga teoretiki in filozofi razlagali skozi različne, samosvoje teoretske poglede. Z analitično obravnavo diskurza skozi čas pa se je počasi med raziskovalci uveljavila definicija diskurza, ki jo je oblikoval francoski filozof Michael Foucault.

Foucault je diskurz opredeljeval v najširšem smislu, in sicer kot skupek situacij, učinkov, posledic, odzivov, interpretacij in konkretizacij posameznih izjav, ki jih izvajajo posamezniki v družbi. Pri Foucaultovem pojmovanju diskurza gre torej za nabor najširše množice prej naštetih elementov, ki pa vsak zase predstavlja pomemben delček mozaika, ki mu pravimo diskurzivna izjava (Dolar, 2010).

Vezovnik (str. 10-11) v svojem delu pojasnjuje, da lahko diskurz razumemo kot odnos do različnih družbenih subjektov, ki ga odraža posamezna izjava. Diskurza torej ne gre razumeti samo kot pojav, ki obstaja v nekem družbenem okolju, temveč ga lahko razumemo tudi kot odnos posamezne izjave oziroma posameznika, ki izjavo izjavi, do subjekta, ki ga izjava posredno in neposredno zadeva. Pri obeh izpostavljenih definicijah gre za najširše razumevanje diskurza, ki temelji na interpretiranju in razumevanju diskurzivnih izjav.

Diskurz se pojavlja v različnih družbenih okoljih in posledično vsebuje različne vsebinske elemente, ki temeljijo na skupnem cilju diskurzivne izjave. Danes tako poznamo več različnih vrst diskurza: upravni diskurz, politični diskurz, marketinški diskurz, vojaški diskurz, pravni diskurz itd. Vse navedene zvrsti diskurza pa nastajajo in se razvijajo zato, ker človek z izjavljanjem nenehno povezuje vsebino posameznih elementov z dogajanjem okoli sebe. Za glavni pokazatelj tega, za kakšen diskurz gre, lahko označimo kontekst, v katerem je posamez nikova izjava nastala, se udejanjila in povzročila posledico (Jagers & Walgrave, 2007).

Navedeno lahko pojasnimo tudi s posameznimi primeri. Politik, ki v okoliščinah politične kampanje poskuša motivirati in aktivirati svoje politične privržence, se poslužuje vrste diskurza, ki mu pravimo »politični diskurz«. Skozi politični diskurz želi politični akter uveljaviti svojo politično agendo, v našem primeru politični cilj – prepričati volivca, da glasuje zanj. S pomočjo političnega diskurza se torej poskuša vplivati na privržence in si zagotoviti zadostno podporo.

V državni upravi uradniki pri svojem delu uporabljajo upravni diskurz, kadar se sklicujejo na določene zakonske in podzakonske akte. Velikokrat pogovorno rečemo, da je državni uradnik (birokrat) govoril in uporabljal zelo birokratski jezik, ki smo ga težko razumeli. Navedeno izhaja prav iz upravnega diskurza, kjer uradnike enačimo z »birokrati«. V našem socialnem okolju ima omenjena beseda pogosto slabšalni prizvok, saj s tem označujemo posameznike, ali sisteme (birokracija), ki se ukvarjajo s kupom nepotrebnih predpisov in dokumentov.

V svetu marketinga pa smo kot potrošniki skoraj na vsakem koraku priča sugeriranju, da kupimo določene izdelke oziroma storitve. Tudi to na koncu predstavlja svojevrsten diskurz – marketinški diskurz.

UPRAVNI DISKURZ

Upravni diskurz je lahko sam po sebi predmet preučevanja in interpretiranja. Farmer (1999) opisuje, da za upravni diskurz velja visoka stopnja profesionalnosti in homogenosti. Upravni diskurz naj bi bil omejen glede na naloge in dolžnosti, ki so upravi predpisane v posameznih državi. Stil upravnega diskurza se bo po mnenju Farmerja še naprej razvijal in nadgrajeval ter v nekaterih državah postal zelo tehničen in emocionalno prazen. Čeprav naj bi državni uradniki (birokrati) svoje storitve v prihodnosti poskušali čim bolj približati uporabnikom (državljanom), se upravni diskurz sooča s težavo, ki pesti mnoge državne aparate – pretirano birokracijo. Upravni diskurz bo po besedah Farmerja v prihodnosti še naprej omejen na velikost »birokratizma« v posameznih državi, saj prav ta upravni diskurz največkrat definira.

Rosca (2013) dodaja, da na dojemanje upravnega diskurza vplivajo predvsem mediji, politiki in civilna družba. Vsi našteti pri svojem delu zelo velikokrat omenjajo delovanje državne uprave in opozarjajo na njene pomanjkljivosti. Tovrstne aktivnosti pri ljudeh puščajo posledice, saj začnejo državno upravo doje mati kot (ne)nujen aparat, ki je finančno izredno potraten, državljanke in državljani pa od aparata naj ne bi imeli ničesar, ker naj bi pri uradniškem delu šlo zgolj za »prelaganje papirjev« in ustvarjanje problemov.

Kljub zapletenosti državne uprave, ki se sooča s pretirano birokracijo, je upravni diskurz posebna vrsta diskurza, ki bi ga veljalo v prihodnosti raziskati tudi v Sloveniji. S tem bi pridobili posreden vpogled v razmere v Sloveniji. Z natančno analizo bi lahko tudi definirali upravni diskurz v Sloveniji in ga primerjali z drugimi državami, ki imajo podobne državne sisteme in se soočajo s podobnimi problemi kot Slovenija.

PRISTOPI K PREUČEVANJU DISKURZA

Omenili smo že, da je pri preučevanju diskurza in pri določanju vrste diskurza pomembno, da poskušamo diskurz interpretirati in opredeliti kontekst, v katerem je nastal. Oboje naredimo v procesu interpretacije in kontekstualizacije. Izjavo poskušamo interpretirati, pojasniti, kaj z njo sporočamo, nato pa vse skupaj postavimo v kontekst, kjer poskušamo čim bolj objektivno zajeti in definirati okoliščine, v katerih je diskurzivna izjava nastala. Na ta način se do diskurza opredelimo in ga razložimo. Poudariti želimo, da oba procesa ne predstavljata samostojne raziskovalne metode, s katero želimo raziskovati diskurz. Procesa interpretacije in kontekstualizacije sta del metode kritične analize diskurza.[1]

Ontološki pristop k razumevanju diskurza predstavlja pomembno iztočnico, ko govorimo o načinih preučevanja diskurza. Poudariti želimo, da diskurz ni vedno nekaj oprijemljivega, sploh če na diskurz gledamo skozi prizmo idealizma. Posamezniku se pojavljajo vprašanja, kako nekaj takšnega, kot je *disk*urz, ki vsebuje veliko abstraktnosti, sploh preučevati, razložiti in razumeti.

Erjavec in *Kovačič* (2007) utemeljujeta, da lahko z metodo kritične analize diskurza poskušamo analizirati diskurzivni subjekt ter interpretirati posamezno izjavo. Metoda kot takšna nam daje možnost, da poskušamo ugotoviti, kakšna izjava se je pojavila v določenem diskurzivnem prostoru, kakšne so njene jezikovne značilnosti in prvine, pa tudi kakšne elemente uporablja, da bi poskušala vplivati na slušatelja oziroma bralca izjave.

(Mullet, 2018) opisuje, da gre pri kritični analizi diskurza za metodo, ki ima kvalitativen pristop. Z uporabo omenjene metode poskušamo torej razumevati, odkrivati, opisovati posamezne segmente diskurza, in sicer na način, da je naše raziskovanje usmerjenje induktivno. Sprašujemo se po kritičnih prvinah diskurza, kot so manipuliranje, vprašanje asimetrije moči, izkoriščanja, metaforičnega izražanja, neenakosti, prepričevanja itd. Preučevani vzorec pri uporabi metode kritične analize je po navadi majhen, podatke pa zbiramo predvsem na podlagi izrečenih oziroma napisanih izjav ali pa se poslužujemo zbiranja podatkov z intervjuji. Zaključek metode kritične analize diskurza je opisen, vsestranski in zajema tudi subjektivno mnenje raziskovalca, ki je pravi loma ločeno označeno od primarnega dela zaključka.

Ker kritična analiza diskurza velja za mehko metodo razisko vanja, nima strogo definiranih posameznih elementov oziroma faz raziskovanja. Kljub temu Mullet (str. 122) navaja posamezne segmente raziskovanja, ki so lahko razis kovalcu v pomoč. Prvi segment govori o tem, da je na začetku treba definirati, katero vrsto diskurza želimo preučiti, sledi zbiranje dokumentacije in posameznih izjav. Tretji in četrti segment raziskovanja temeljita na raziskovanju okoliščin diskurzivne izjave in na identifikaciji besedila. Sledi analitični pristop k diskurzivni analizi v smislu iskanja družbenih razmerij med posameznimi diskurzivnimi izjavami. Sprašujemo se torej po tem, kako je diskurzivna izjava vplivala oziroma poskušala vplivati na socialno okolje okoli nas. Na koncu sledi še interpretacija diskurzivne izjave glede na kontekst izjave in povezovanje diskur-

[1] *CDA – Critical Discourse Analysis*

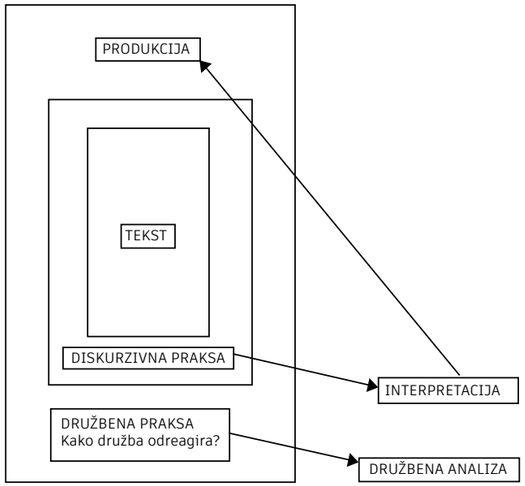
zivne izjave s profilom posameznika, ki je preučevano izjavo izjavil.

Če povzamemo: raziskovalec pri svojem delu uporablja pristop, s katerim tesno poveZuje socialno-družbeni kontekst situacije s procesom interpretacije diskurzivne izjave. Glavni cilj raziskovalca je torej poskušati odgovoriti na vprašanje, kako se je diskurzivna izjava oblikovala, kakšne so družbene okoliščine, v katerih je nastala, kakšne posledice je izjava povzročila in kako družba (socialno okolje) odreagira.

DISKURZIVNA PRAKSA

Pri naši obravnavi diskurza je potrebno omeniti še pojav diskurzivne prakse. Gre za družbeno (ne)nadzorovan pojav, ki ga Hardy (2001) izpostavlja kot ključnega za dosego cilјev diskurza. Skozi diskurzivno prakso posamezne izjave reproduciramo, družba pa na te diskurzivne izjave odreagira. Reakcija družbe ima lahko različne posledice, tako objektivne (za družbo) kot subjektivne (za posameznika).

Erjavec in Kovačič (2007, str. 49) izpostavljata, da družbeno analizo naredimo tako, da preučimo reakcijo družbe, ki jo je povzročila prej omenjena produkcija posameznih izjav. Proces sta tudi grafično predstavili, pri čemer pojasnjujeta, da je pomembno, da znamo analizirati posamezne konsekvence, ki so nastale zaradi diskurzivnega izvajanja.



Slika : Diskurzivna praksa
Vir: (Erjavec & Kovačič, 2007, str. 49)

SKLEPNA MISEL

S članom smo želeli predstaviti osnovne koncepte diskurza in pot do njegove uveljavitve. Prikazati smo želeli, kako diskurz nastaja, kateri so elementi, ki ga definirajo, in kako se diskurz v družbi pojavlja in razvija.

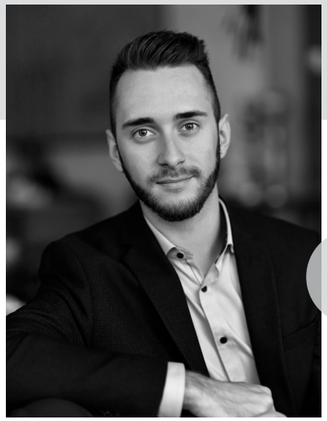
Razumevanje diskurza, njegove definicije in načina preučevanja pomembno prispeva k vposameznikovemu splošnemu in strokovnemu znanju ter k razumevanju procesov, ki se odvijajo v družbi. V družbi – ki je občutljiva na diskurzivne dražljaje in kjer pri prenosu sporočil in posameznih izjav igrajo veliko vlogo družabna omrežja, medijski portali in mediji na sploh – je potrebno poznati vzorce, ki kažejo na zlorabo diskurzivnega prostora v našem ožjem in širšem družbenem okolju. Kot diplomanti Fakultete za upravo, ki lahko svoje znanje unovčimo tako v javnem kot zasebnem sektorju, moramo znati prepoznati ključne elemente diskurza in na podlagi ponavljajočih se diskurzivnih vzorcev v našem okolju paziti na integriteto in objektivnost našega dela ter profila poklica, ki ga opravljamo. Kot strokovnjaki s svojega področja moramo znati svetovati in reševati zapletene upravne procese, ki imajo velikokrat odmevnejše posledice tudi v širši javnosti. Razumevanje uporabe metode kritične analize diskurza diplomantom daje prednost pri razumevanju in preprečevanju zlorab posameznikovega diskurzivnega okolja.

Od posameznika je odvisno, kako pozorno bo v svojem profesionalnem okolju obravnaval diskurz in prepoznaval njegove poglavitne značilnosti, kako kritičen bo do diskurzivnega vedenja in kako zelo občutljiv bo do posameznih diskurzivnih izjav. V zvezi z navedenim menim, da znanje o diskurzu predstavlja eno od ključnih prednosti posameznika, ki deluje in ustvarja v kolektivnem okolju. Neposredna aplikacija posameznikovega znanja v določeni situaciji pa je že kot takšna lahko predmet nadaljnjih analiz in sociоloških raziskav.

Viri in literatura

prilagojeno za
akromatopsijo

Od zlorab podatkov do njihove zaščite: uporabniška ozaveščenost kot ščit pred digitalnimi pastmi



Grega Rudolf, mag. upr. ved
gr.gregarudolf@gmail.com

Grega Rudolf je magister upravnih ved in doktorski študent na Pravni fakulteti Univerze v Ljubljani. Pri Informacijskem pooblaščencu je zaposlen na oddelku mednarodnega sodelovanja in nadzora. Tako v delovni praksi kot pri znanstvenem in strokovnem raziskovanju se ukvarja z vprašanji, povezanimi s pravicami glede zasebnosti in varstva osebnih podatkov, z vplivom umetne inteligence in drugih (novih) tehnologij na pravni položaj posameznikov ter z analizo demokratičnih varovalk pred oblastnimi posegi v pravice zasebnosti. Je tudi član Evropske zveze za umetno inteligenco, Informacijskega pooblaščenca pa zastopa v številnih ekspertnih skupinah na ravni Evropskega odbora za varstvo podatkov (za sodelovanje, tehnologijo, družbena omrežja, finančne zadeve, piškotke idr.).

povzetek

Digitalna doba, ki jo zaznamujejo hitri tehnološki preboji in rast količine podatkov, prinaša s seboj številne izzive glede zasebnosti, informacijske varnosti in varstva osebnih podatkov. Ti izzivi postanejo še posebej pereči, ko se soočamo z zlorabami tovrstnih podatkov, ki se lahko kažejo v obliki kraje ali izgube osebnih in drugih zaupnih informacij. V ospredju tega prispevka je raziskovanje tovrstnih zlorab, ki se pogosto izvajajo s tehniko socialnega inženiringa – metodami, kjer prevaranti manipulirajo z ljudmi, da bi pridobili dostop do njihovih podatkov ali do zaupnih informacij, do katerih imajo ti ljudje dostop. Socialni inženiring se tako pogosto izkaže kot učinkovit način za izvajanje prevar, saj izkorišča najbolj ranljiv del vsakega varnostnega sistema – človeka. Premisa tega prispevka in njegovo glavno raziskovalno vprašanje izhaja torej iz prepričanja, da je razumevanje človeških dejavnikov in človeškega vedenja ključno za preprečevanje takšnih zlorab. Poudarja, da je ozaveščanje posameznikov ne le pomemben, ampak osnovni steber varstva osebnih podatkov. Prav zato so prizadevanja za povečanje ozaveščenosti o teh vprašanjih nujno potrebna za zagotavljanje varstva osebnih podatkov in zasebnosti v digitalni dobi. V prispevku so tako orisane najpogostejše taktike socialnega inženiringa ter načini njihovega zaznavanja in preprečevanja. Dosedanje raziskave na tem področju kažejo zlasti to, da prevaranti sistematično izkoriščajo taktike nujnosti ali vzbujanja strahu, s čimer prisilijo tarče, da prevarantom omogočijo dostop do svojih podatkov. Hkrati je v pričujočem članku izpostavljeno, da je ključnega pomena, da posamezniki razvijejo zdravo stopnjo skeptičnosti do zahtev po nenavadnih osebnih ali drugih zaupnih informacijah, saj se lahko zahtevane informacije izkažejo za potencialne prevare socialnega inženiringa. Zgolj s celostnim in vseživljenjskim izobraževanjem in informiranjem posameznikov o pasteh in taktikah, ki jih uporabljajo prevaranti, se lahko poveča njihova odpornost in zmanjša možnost uspeha tovrstnih zlorab. Izpostavljeno je, da je potrebno kot učinkovito taktiko zmanjševanja tveganja za zlorabe vzpostaviti učinkovite pravne okvire in politike, ki bodo podpirali varstvo osebnih podatkov in informacijsko odpornost za zaščito sistemov.

Prispevek tega članka je v tem, da izpostavi pomen razumevanja človeških dejavnikov in uporabniške ozaveščenosti pri oblikovanju odpornosti proti zlorabam podatkov. Ugotovitve tega članka pa so ključne za vse deležnike, ki sodelujejo v oblikovanju in izvajanju varnostnih strategij – od informacijskih strokovnjakov, ki oblikujejo in skrbijo za tehnične protokole, do zakonodajalcev, ki oblikujejo pravne okvire, pa vse do posameznikov, ki so končni uporabniki teh sistemov. Za prihodnje raziskave na tem področju je potrebno zlasti poglobljeno preučevanje psiholoških, tehničnih in pravnih vidikov tega izziva. To vključuje raziskovanje psiholoških dejavnikov, ki vplivajo na vedenje posameznikov, razumevanje tehničnih vidikov varnosti informacijskih sistemov in proučevanje pravnih instrumentov, ki bi lahko prispevali k vzpostavitvi učinkovitejših preventivnih ukrepov. Zgolj celostni interdisciplinarni pristop bo omogočil boljše zaznavanje zlorab podatkov in hitrejši ter bolj uspešen odziv na njih.

Ključne besede: *varstvo osebnih podatkov, socialni inženiring, zlorabe podatkov, kibernetski kriminal, phishing.*

V današnji digitalni dobi posamezniki postajamo vse bolj odvisni od priročnosti in vseobsegajočih razsežnosti spletnih storitev, ki jih posamezniki vedno pogosteje uporabljamo tako rekoč za vse, od upravljanja s svojimi financami preko spletnih bank do povezovanja in mreženja s prijatelji preko družbenih omrežij. Vsa ta digitalna interakcija pa obenem pomeni, da se za potrebe delovanja teh storitev (pa naj si bo spletno bančništvo ali uporaba družbenega omrežja) obdeluje obilica naših osebnih podatkov, ki jih ponudniki teh storitev potrebujejo in jih s tem namenom (poleg svojih samostojnih ločenih namenov)[1] s pridom obdelujejo.

Ravno zaradi vedno večje prisotnosti ter uporabe spleta in digitalnih tehnologij nasploh pa smo posamezniki izpostavljeni vrsti tveganj, vključno s kibernetskimi napadi, krajami identitet in drugimi nevarnostmi zlorabe osebnih podatkov uporabnikov teh storitev ali drugih zaupnih informacij.

V dobi digitalne povezanosti kraja identitete izstopa kot ena izmed najbolj razširjenih in zaskrbljujočih groženj. Pri kraji identitete gre pri takem načinu zlorabe osebnih podatkov največkrat takrat, ko tretja oseba v imenu posameznika nedovoljeno in neavtorizirano ukrade in zlorabi posameznikove osebne podatke (bančne podatke, številko kartice, ime in priimek itd.) za namen svojega okoriščanja (največkrat finančnega) ali pa celo kot mehanizem izvajanja kaznivih dejanj pod krinko prisvojene »lažne« identitete (npr. v obliki inkriminacije druge osebe) (Arachchilage & Love, 2014).

Čeprav storilci tovrstnih kaznivih dejanj nenehno izboljšujejo svoje taktike prevar, pa so še vedno najpogostejše metode za pridobivanje osebnih in drugih zaupnih podatkov zlasti napadi, ki temeljijo na socialnem inženiringu. Gre za tehniko, ki s pomočjo psihološke manipulacije posameznika in posledično njegove prevare uspe pridobiti dostop do sistemov, ki vsebujejo podatke, dokumente ali druge informacije (kot na primer o bančnem računu), do katerih prevarant ne bi smel dostopati (Washo, 2021). Raziskave na področju socialnega inženiringa pričajo o tem, da njegovo razumevanje zahteva interdisciplinarni pristop, ki združuje informacijske, psihološke, sociološke in managementske vidike, kjer zgolj celosten pregled nad področji omogoča boljše obvladovanje tovrstnih tveganj pred zlorabami (Aleem et al., 2013; Washo, 2021).

Namen tega prispevka je na kratko orisati pasti in tveganja, s katerimi se srečujemo v digitalnem svetu, še posebej v luči kibernetskih napadov in kraje identitete skozi socialni inženiring, ki predstavlja eno izmed največjih tveganj informacijske varnosti danes (Airehrour et al., 2018; Montañez et al., 2020). Prikazani bodo zlasti načini pridobivanja osebnih in drugih zaupnih podatkov z metodami socialnega inženiringa, kot so napadi ribarjenja, virusi/trojanski konji/črvi, pharming napadi, smishing, vishing napadi itd. Članek bo vključeval pregled statističnih podatkov o pogostosti tovrstnih zlorab na ravni Slovenije in EU, zlasti na primeru napadov ribarjenja ter s ciljem osvetlitve preventivnih ukrepov, ki jih lahko posamezniki sprejmejo za zaščito svoje digitalne identitete. Upoštevaje navedeno, s prispevkom želimo ugotoviti, katere so najpogostejše taktike socialnega inženiringa, s katerimi prihaja do zlorabe osebnih in drugih zaupnih informacij, ter ali lahko ozaveščanje posameznikov predstavlja temelj za njihovo prepoznavanje in preprečevanje.

METODOLOGIJA

Osnovna metodologija tega prispevka je temeljila na pregledu literature ter opravljeni empirični analizi. Uvodoma je bila pregledana vrsta znanstvenih in strokovnih člankov, na podlagi katerih so bile zbrane in povzete različne tehnike socialnega inženiringa, ki prevladujejo v praksi. Pregled literature je tako služil kot osnova za razumevanje kompleksnih metod socialnega inženiringa, ki jih prevaranti uporabljajo pri poskusih vdora v osebne in druge občutljive podatke.

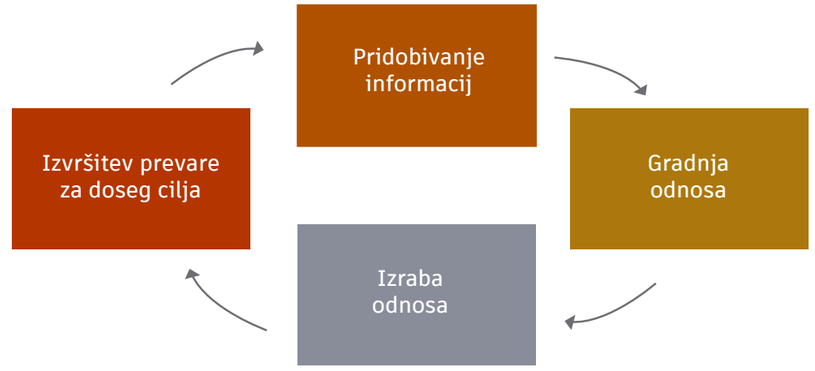
Na tej podlagi je bila izvedena tudi empirična analiza, s katero je bila ocenjena razširjenost poglavitnih kibernetskih napadov v zadnjem obdobju. Ta analiza je temeljila na poročilu "Threat Landscape 2022", ki ga je objavila ENISA – Agencija Evropske unije za kibernetsko varnost, iz katerega smo razbrali število incidentov s področja kibernetske varnosti v obdobju od julija 2021 do junija 2022. Za zagotovitev celovite in primerjalne perspektive so bili podatki agencije ENISA primerjani z ugotovitvami iz poročila Urada Vlade RS za informacijsko varnost za leto 2022. To poročilo je analiziralo incidente od januarja 2020 do decembra 2022, pri čemer je zbralo vpoglede dveh organizacij: SI-CERT – nacionalnega odzivnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij ter SIGOV-CERT – odzivnega centra za incidente v informacijskih sistemih organov državne uprave. Za boljše razumevanje časovne dinamike teh groženj je bila izvedena še analiza poročila SI-CERT iz leta 2022, ki je osvetlila trend incidentov ribarjenja v obdobju od leta 2008 do leta 2022.

Po pregledu literature in interpretaciji empiričnih podatkov so bila zbrana spoznanja sintetizirana in pripravljena je bila vrsta izvedljivih priporočil. Na podlagi opaženih trendov na področju tehnik socialnega inženiringa in empirične razširjenosti kibernetskih napadov tako članek predlaga vrsto orodij in metod, prilagojenih za odkrivanje in blaženje takšnih digitalnih pasti in groženj. Ta priporočila niso le odziv na trenutne grožnje, temveč so namenjena tudi predvidevanju in preprečevanju razvoja taktik socialnega inženiringa. Z združevanjem teoretičnega znanja z empiričnimi opažanji želi članek posameznike in organizacije opremiti z znanjem in orodji, potrebnimi za obrambo in boj proti nenehni grožnji napadov socialnega inženiringa.

DIGITALNE PASTI SKOZI TEHNIKE SOCIALNEGA INŽENIRINGA

Socialni inženiring se v najširšem smislu nanaša na strateško manipuliranje prevaranta s posamezniki, kjer prevarant skuša posameznike, ki so tarča take manipulacije, prisiliti k izvedbi določenih dejanj ali razkritju zaupnih informacij (lastnih ali drugih, npr. organizacijskih). Tehnike socialnega inženiringa so zasnovane predvsem na izkoriščanju človeške ranljivosti, pri čemer pogosto posameznika prisilijo ali zavedejo, da ogrozi lastne ali organizacijske interese. Tako ravnanje zajema vse od razkritja občutljivih podatkov, kot so gesla in bančni podatki, do izvedbe dejanj, ki lahko ogrozijo osebno varnost ali varnost organizacij. Bistvo socialnega inženiringa je predvsem v manipulatorjevi spretnosti k vzbujanju zaupanja, uporabi tehnik prevare ali izkoriščanju čustev in navad posameznika. Manipulatorji se pogosto izdajajo za zaupanja vredne osebe ali avtoritete, da bi dosegli želeni odziv posameznika. Končni cilj je namreč doseči, da ciljna oseba prostovoljno posreduje informacije ali izvede taka dejanja, ki bi se jim običajno izognila, če bi se zavedala manipulatorjevih resničnih namenov. Glavna skrb takih tehnik je zlasti v tem, da se lahko izognejo tudi najstrožjim tehničnim varnostnim ukrepom, saj so usmerjene na človeški dejavnik in človeška čustva. Socialni inženiring tako poudarja potrebo po multidisciplinarnem pristopu, ki vključuje dognanja psihologije, sociologije, menedžmenta in informatike, da bi učinkovito ublažili tovrstne grožnje (Chetioui et al., 2021; Kaushalya, 2018; Fan et al., 2017; Salahdine & Kaabouch, 2019).

Grafikon 1: Prikaz tipičnega cikla prevare
Vir: povzeto po Kaushalya et al., 2018 in Nohlberg in Kowalski, 2008



[1] *Marsikatera družbena omrežja ne obdelujejo osebnih podatkov posameznikov zgolj za delovanje družbenega omrežja, temveč dodatno (še) za svoje samostojne ločene namene – zlasti oglaševanje in s tem pridobivanje dobička. Sodobna marketinška praksa tako zahteva uporabo digitalnih tehnologij in podatkov o posameznikih, ki te tehnologije uporabljajo, za ustvarjanje (primarno svoje) dodane vrednosti (več o tem tem Appel et al., 2020; Stasti, 2019; Quach et al., 2022).*

Splošno sprejet okvir za prikaz tipičnega cikla prevare s pomočjo socialnega inženiringa vključuje štiri glavne faze. Na začetku se napadalec loti podrobnega in celovitega zbiranja informacij o tarči. Ta faza raziskovanja, ki se izvede pred kakršno koli neposredno interakcijo, postavi temelje za učinkovitejšo manipulacijo. V naslednji fazi je poudarek na vzpostavitvi odnosa s posameznikom, na podlagi katerega tarča prevare prične zaupati prevarantu. Na področju socialnega inženiringa je namreč zaupanje ključno orodje – kadar uporabnik verjame, da komunicira z zaupanja vrednim subjektom, je bolj verjetno, da mu bo razkril občutljive informacije, s čimer bo nezavedno ustregel ciljem prevaranta. Ko se odnos vzpostavi, prevarant s tarčo manipulira in od nje pridobi potrebne informacije. V zadnji fazi prevarant informacije, pridobljene v prejšnjih fazah, izkoristi, da doseže svoj končni cilj. Ta končni cilj pogosto vključuje nepooblaščen dostop, nadaljnjo manipulacijo, krajo osebnih podatkov, finančno korist in podobno, s čimer prevarant praviloma zaključi krog svoje prevare in začne prevaro pri drugi tarči (Mitnick, 2002).

V tem poglavju bomo na kratko predstavili različne tehnike, ki se uporabljajo pri socialnem inženiringu, kjer vsaka izmed teh uporablja edinstvene strategije za izkoriščanje človeških ali tehničnih ranljivosti in predstavlja različne grožnje za posameznika in njegove osebne podatke. Z razumevanjem teh tehnik lahko posameznik lažje zagotovi bolj trdno obrambo pred morebitnimi napadi socialnega inženiringa s strani prevarantov ter tako sam sebe in organizacijo zavaruje pred morebitno škodo.

Socialni inženiring, ki kot metoda prevare izkorišča zlasti človeško neprevidnost in zaupanje kot izogib zanesljivim varnostnim ukrepom, predstavlja zapleten izziv na področju kibernetske varnosti. Tovrstne taktike na splošno lahko razvrstimo v štiri kategorije: fizične, tehnične, socialne in na hibridne pristope. Vsaka kategorija vsebuje vrsto različnih tehnik socialnega inženiringa z edinstvenim pristopom delovanja. Vse pa stremijo k skupnemu cilju – vdoru v varnost sistema s pomočjo človeških ranljivosti (Fan et al., 2017; Informacijski pooblaščenec, 2009; Kaushalya et al., 2018; Salahdine & Kaabouch, 2019).

FIZIČNE METODE PREVAR

Fizične metode socialnega inženiringa so strategije, pri katerih prevarant za dostop do občutljivih podatkov uporablja fizične (vidne, realne, praktične) tehnike. Te metode izkoriščajo neposredno prisotnost posameznika in storilca, njegovo zaupanje ter pomanjkljivosti v varnostnih ukrepih – vse od neustreznega ravnanja z odpadnim materialom (npr. smeti) do nepozornosti posameznika. Največkrat gre torej za spodaj navedeni metodi:

1. Brskanje po smeteh (ang. Dumpster diving): Ta taktika izkorišča nepravilno ravnanje z občutljivimi odpadki in smetmi. Prevaranti s to tehniko največkrat prebirajo smeti posameznika ali organizacije in pri tem iščejo malomarno odvržene dokumente, s katerih bi izhajali podatki, ki lahko služijo njihovim zlonamernim ciljem. To vključuje natisnjena elektronska sporočila, interne zapiske ali celo ročno napisane beležke, ki vsebujejo številne zaupne informacije.

2. Vohunjenje čez ramo (ang. Shoulder surfing): Ta metoda vključuje bolj oseben, priložnostni pristop prevaranta. Pri njem prevarant na bližnji razdalji opazuje dejavnosti neke osebe, bodisi da nekomu gleda čez ramo in si ogleduje njegov računalniški zaslon bodisi prisluškuje zaupnim pogovorom. Namen uporabe te metode je zlasti pridobiti nepooblaščen dostop do občutljivih informacij, kot so kode dostopa, gesla ali celo podatke o bančnih karticah.

Te tehnike zlasti poudarjajo pomembno vlogo preventivnih ukrepov varnosti (tako posameznika kot organizacije), primarno predvsem ustreznega usposabljanja in ozaveščanja posameznikov. Preprečevanje poskusov tovrstnih prevar vključuje zlasti vidike varnega uničevanja občutljivih dokumentov, ustrezno varnost dokumentov, ki vsebujejo osebne podatke in ravnanje z njimi, spodbujanje previdnosti med zaposlenimi ter uveljavljanje strogega nadzora dostopa do kritičnih območij in infrastrukture (npr. omejitev dostopa do videonadzornega sistema zgolj nujno potrebnim posameznikom). Tehnike za preprečevanje prevar obsegajo tudi spoštovanje načel čiste mize in praznega zaslona. Ti dve načeli opozarjata na pomen varnega shranjevanja nosilcev podatkov (npr. USB ključev, dokumentov) stran od oči in dosega nepooblaščenih oseb. Nosilce podatkov je tako potrebno ustrezno pospravljati z delovnih miz, jih ustrezno shranjevati, zaklepati in zaščititi npr. s ključavnico ali z uporabo gesel. Posamezniki morajo poskrbeti, da je dostop do njihovih naprav in zaslonov, s katerih je možno razbrati zaupne in osebne podatke, prilagojen tako, da so te informacije vidne le uporabniku teh naprav in ne drugim nepooblaščenim osebam. Ko naprave, kot so prenosniki ali telefoni, niso v uporabi, pa je priporočljivo, da jih izklopimo ter dostop do podatkov v napravah ustrezno zaščitimo (npr. z nastavitvijo gesla za dostop do naprave) (Ministrstvo za javno upravo, 2010).

TEHNIČNE METODE PREVAR

Tehnične metode prevar se osredotočajo predvsem na uporabo tehnologije, pogosto spletnih orodij, s katerimi se posameznike ali organizacije zavede, da delijo občutljive podatke. Ta kategorija vključuje zlasti:

1. Ribarjenje (ang. phishing): Precej razširjen pristop, ki vključuje pošiljanje zavajajočih sporočil (pogosto e-poštnih ali SMS sporočil), v katerih se prevarant izdaja za zaupanja vredno osebo (npr. kot uradna oseba, zaposlena na banki, policist). Tovrstna sporočila pozivajo prejemnike, naj delijo svoje osebne podatke, kot so uporabniška imena, gesla ali podatki o bančnih karticah. Zaradi razširjenosti splošnih metod ribarjenja se navadno tovrstne metode izvajajo množično in so usmerjene na veliko skupino posameznikov brez večjega razlikovanja (npr. na večje število elektronskih naslovov, pridobljenih iz javno dostopnih ali drugih baz, do katerih imajo prevaranti dostop,[2] v zvezi s čimer bo umetna inteligenca prevarantom ustvarjanje takšnih sporočil še olajšala). Metoda ribarjenja tako ne izkorišča le posameznikovega pomanjkanja znanja, ampak tudi njegovo zaupanje v organe in druge organizacije (npr. banke, državne organe itd.) ter z njimi povezane digitalne platforme (Alkhalil et al., 2021; Binks, 2019).

2. Usmerjeno ribarjenje (ang. Spear-Phishing): Pri usmerjenem ribarjenju gre za izpopolnjeno različico splošnega ribarjenja, ki velja za usmerjeno na določene posameznike, skupine posameznikov ali organizacije. Prevaranti pogosto skrbno raziščejo ozadje svojih predvidenih tarč in prilagodijo svoja zavajajoča sporočila tako, da so videti bolj prepričljiva, s čimer povečajo možnost uspeha prevare.

3. Napad preko napajališča (ang. Waterholing): Gre za izredno natančen in ciljno usmerjen način socialnega inženiringa, kjer prevarant ugotavlja in targetira tista spletna mesta, ki jih uporabniki pogosto obiskujejo ali so verjetno zanimiva za določeno tarčo ali skupino. Prevaranti največkrat tako spletno stran ogrozijo na način, da nanjo vnesejo zlonamerno programsko opremo, katere cilj je okužiti tarčo, ko posameznik brska po teh kompromitiranih spletnih straneh (npr. naložitev zlonamernega piškotka na terminal posameznika). Zaradi prikritosti in selektivnosti napadov je to metodo pogosto težko predvideti in preprečiti, zato je zanj potrebna močna varnostna zaščita (tako na strani ponudnika spletne strani kot obiskovalcev) in redne sistemske revizije, da se takoj odkrijejo in odpravijo morebitne informacijske ranljivosti.

4. Trojanski konji, virusi in izsiljevalska programska oprema: Trojanski konji so zavajajoči programi, ki vsebujejo skrito zlonamerno kodo in napadalcem omogočajo nepooblaščen dostop do naprave posameznika. Virusi se razmnožujejo sami in okužijo datoteke ali sisteme ter povzročijo škodo, izgubo podatkov ali nepooblaščen dostop. V napadih z izsiljevalsko programsko opremo se uporablja zlonamerna programska oprema za šifriranje datotek ali zaklepanje sistemov, kjer prevarant za dešifriranje ali odklepanje zahteva plačilo. Ti napadi izkoriščajo ranljivosti, pogosto z uporabo in pomočjo socialnega inženiringa v kombinaciji z ranljivostjo programske/strojne opreme. Povzročijo lahko hude posledice, za zmanjšanje tveganj pa so potrebni proaktivni ukrepi, kot so posodobitve programske opreme, (dobra) varnostna programska oprema in ozaveščanje uporabnikov.

5. Nastavljanje vabe (ang. Baiting): Gre za tehniko, ki izkorišča človeško radovednost in pohlep. Vabljenje se lahko zgodi tako v fizičnem kot digitalnem svetu, kjer prevaranti pustijo določeno napravo (USB ključek, zgoščenko itd.), ki je okužena z zlonamerno programsko opremo, na mestih, kjer jih potencialne žrtve zlahka najdejo. Te naprave so lahko označene z vabljivimi nalepkami, ki vzbudijo

[2] *Več o številnih kršitvah varnosti in nezakonito objavljenih osebnih podatkih posameznikov z družbenih omrežij (npr. primer Facebook) zlasti Fuller, 2018 in Brown, 2020. Business Insider (2021) celo poroča o nezakoniti objavi več kot 533 milijonov telefonskih številk, imen in priimkov uporabnikov, njihovih lokacijskih podatkov in elektronskih naslovov uporabnikov družbenega omrežja Facebook.*

radovednost in spodbudijo posameznika, da jih uporabi ter posledično okuži svoj oz. organizacijski sistem. V digitalni obliki je lahko vaba v obliki brezplačnih prenosov okužene programske opreme ali vsebine, ki bi ciljno osebo zanimala. Ko žrtev sprejme vabo, se njen sistem okuži z vgrajeno zlonamerno programsko opremo, kar napadalcu omogoči dostop do njenih podatkov ali nadzor nad njenim sistemom. Učinkovitost vabe zlasti opozarja na pomen varnih spletnih praks, kot sta izogibanje nezaželenim prenosom in previdnost posameznikov pri izbiri fizičnih medijev, ki jih vstavljamo v svoje naprave.

6. Pharming napadi: Pri tovrstnih prevarah gre največkrat za krajo prometa s ciljnega spletnega mesta s preusmeritvijo na goljufivo spletno mesto prevaranta z namenom zbiranja občutljivih podatkov. Prevarant ta namen doseže z vdorom v sistem domenskih imen (DNS), ki skrbi za pretvorbo IP zapisa v spletni naslov. S preusmeritvijo uporabnikov na lažno spletno mesto jih prevarant zavede, da nanj vnesejo svoje osebne podatke, ki jih lahko nato uporabi v zlonamerne namene. Napadi Pharming za izvajanje goljufivih dejavnosti izkoriščajo slabosti v infrastrukturi DNS.

Tehnične metode tako predstavljajo močno orodje v naboru metod prevarantov, saj lahko hitro in dokaj učinkovito dosežejo veliko število posameznikov in povzročijo obsežno škodo. Ključnega pomena zato je, da posamezniki in organizacije dajo prednost ozaveščanju o varnosti na spletu ter varnem ravnanju s strojno in programsko opremo ter uvedbi ukrepov za zaščito pred tovrstnimi sofisticiranimi napadi.

SOCIALNE METODE PREVAR

Socialni pristopi izkoriščajo predvsem psihološke vidike človeškega vedenja z namenom, da tarče prevare prepričajo, da razkrijejo občutljive informacije. Te metode se pogosto osredotočajo na krepitev zaupanja med prevarantom in tarčo, izkoriščanje odnosa do avtoritete ali izrabljanje družbenih norm in vedenja.

1. Napadi pod pretvezo (ang. Pretexting): Gre za taktiko, ki vključuje ustvarjanje izmišljenega, vnaprej pripravljenega scenarija, ki tarčo prevare zavede, da razkrije določene občutljive informacije ali izvede določena dejanja (npr. omogoči dostop v zavarovan objekt). Prevaranti najprej svoje tarče preučijo in pripravijo prepričljive zgodbe, da bi jih prepričali, naj jim zaupajo. Pri tem se lahko izdajajo za uslužbence iz različnih poslovalnic organizacije ali se celo predstavljajo kot revizorji ali svetovalci. Napadi s pretvezo lahko potekajo po različnih kanalih, vključno s telefonskimi klici, e-pošto ali fizičnimi stiki. Cilj je izkoristiti zaupanje žrtve in jo prepričati, da jim posreduje zaupne informacije.

2. *»Nekaj za nekaj«* napad (lat. Quid pro quo): Napadi, ki temeljijo na preslepitvi, izkoriščajo psihološke ranljivosti posameznika, da bi tarčo take prevare prepričali v izpolnitev določene škodljive zahteve v zameno za določeno storitev. Pogost scenarij je na primer prevarant, ki se izdaja za predstavnika tehnične podpore in tarčo prepriča, da je njen računalnik okužen z virusom. Prevarant nato tarčo prepriča, da mu omogoči oddaljen dostop do svojega računalnika ali mu posreduje osebne podatke, da bi rešil domnevno težavo. Prevarant izkoristi skrb posameznika za varnost svoje naprave in domnevni (lažni) avtoriteti razkrije osebne podatke.

3. Povratni socialni inženiring (ang. reverse social engineering): Napadi s povratnim socialnim inženiringom so napredna taktika manipulacije, pri kateri se napadalec predstavi kot pomočnik ali reševalec konkretnega problema posameznika. Gre na primer za primer, ko se prevarant izdaja za vodstvenega delavca v podjetju ali delavca v oddelku za informatiko z namenom, da izkoristi zaupanje zaposlenih v tovrstne avtoritete. Prevarant pošlje posamezniku nujna elektronska sporočila, v katerih se pretvarja, da je prišlo do kršitve varnosti v sistemih, in zaposlenim naroči, naj spremenijo svoja gesla z uporabo posredovane povezave. Napadalec izkoristi zaupanje posameznikov v te vloge in zaposlene prelisiči, da razkrijejo svoje poverilnice za vstop v sistem.

4. Kraja prek preusmeritve (ang. Diversion theft): Tovrstna tehnika vključuje lažno preslepitev prevoznega ali kurirskega podjetja, da dostavi paket na drugo lokacijo, kot bi bilo potrebno. Prevarant pri tem uporabi različne taktike manipulacije z dostavnim osebjem, kot sta izdajanje za stranko ali zagotavljanje dovoljšne količine lažnih informacij, da ga prepriča, da odstopi od prvotnega načrta dostave. Ta napad zahteva skrbno načrtovanje, raziskovanje in izkoriščanje zaupanja dostavnega osebja. Cilj je preusmeriti dragocene pošiljke v korist in roke prevaranta.

5. Prepričevanje (ang. Persuasion): Pri tej taktiki prevarant skuša manipulirati s čustvi, željami ali ranljivostmi posameznika, da bi tako vplival na njegovo vedenje. Za razliko od taktike quid pro quo ali povratnega socialnega inženiringa prepričevanje ne vključuje neposredne izmenjave koristi ali pretvarjanja. Namesto tega lahko napadalec uporabi psihološke tehnike, kot so ustvarjanje občutka nujnosti, vzbujanje sočutja ali radovednosti tarče oziroma celo izkoriščanje njenega strahu. Prevarant se lahko na primer izdaja za predstavnika dobrodelne organizacije in žrtev prepriča, naj daruje, tako da vzbudi njeno sočutje za določen namen. Cilj prepričevanja je prepričati žrtev, da izpolni napadalčevo zahtevo ali prostovoljno razkrije občutljive informacije o sebi ali podjetju.

HIBRIDNE METODE PREVAR

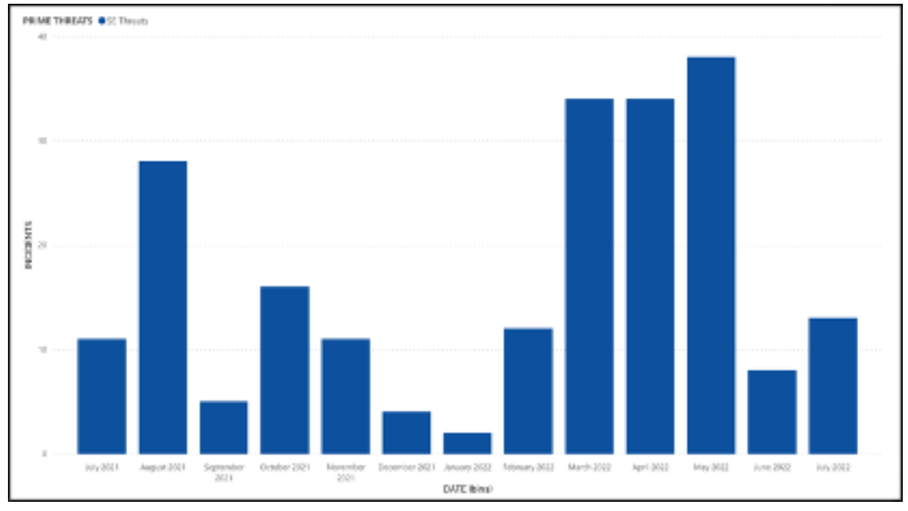
Hibridni pristopi združujejo različne mešane metode za hkratno izkoriščanje različnih šibkih točk posameznikov. Te pogosto kompleksne metode socialnega inženiringa so zasnovane tako, da manipulirajo s človeškimi in tehničnimi ranljivostmi za doseganje svojega cilja.

1. Spremljanje iz ozadja (ang.Tailgating/Piggybacking): Prevarant s to tehniko išče nepooblaščen dostop do zavarovane lokacije s sledenjem osebi z ustreznimi pravicami dostopa. Tipičen scenarij lahko vključuje prevaranta, ki se izdaja za dostavljavca pošiljke in čaka pred zavarovano stavbo. Ko zaposleni pridobi dovoljenje dostopa in odpre vrata, prevarant vrata pridrži odprta in tako pridobi nepooblaščen dostop. Ta metoda izkorišča tako pomanjkljivosti fizičnega varovanja kot tudi človeško vljudnost oz. lahkomiselnost.

2. Telefonsko ribarjenje (ang. Vishing – voice phishing): Ta metoda vključuje goljufive telefonske klice, pri katerih se napadalec izdaja za legitimno organizacijo ali ponudnika določenih storitev. Cilj je prevarati tarčo, da pod pretvezo neke donosne priložnosti ali nujnega postopka za namene preverjanja preda svoje osebne podatke prevarantu. Napadalec lahko razkrite podatke uporabi za različne zlonamerne dejavnosti, kot je npr. kraja identitete ali pridobivanje poverilnic za dostop do drugih sistemov in podatkov. Ta metoda združuje tehnično izkoriščanje (zloraba telefonske storitve) in socialno manipulacijo (prepričevanje žrtve, da deli občutljive podatke).

POGOSTOST KIBERNETSKIH NAPADOV

Agencija Evropske unije za kibernetsko varnost (ENISA) kot strokovni center za kibernetsko varnost v Evropi na podlagi poročanja držav članic v svojem zadnjem poročilu iz leta 2022 opozarja na naraščajoči trend incidentov, ki so povezani s prevarami socialnega inženiringa. Naraščajoči trend sporočenih incidentov, povezanih s socialnim inženiringom, je možno razbrati iz grafikona.

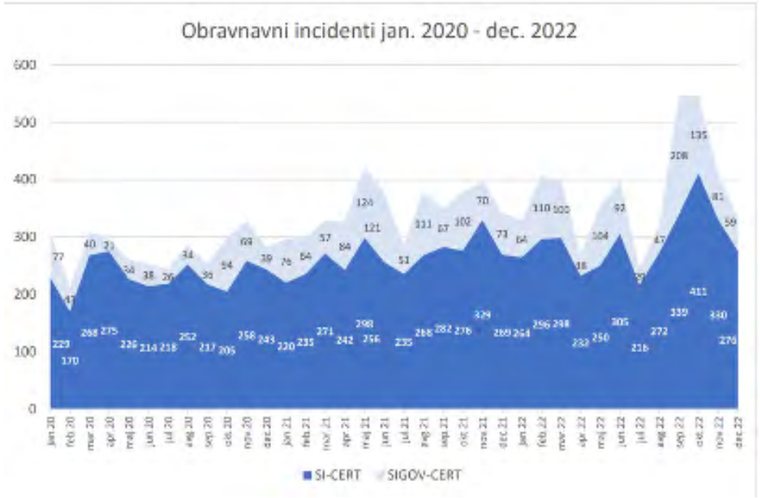


Grafikon 2: Časovni niz števila večjih incidentov, ki jih je opazila agencija ENISA (julij 2021–junij 2022)

Vir: ENISA, 2022 (str. 55)

Od zlorab podatkov do njihove zaščite: uporabniška ozaveščenost kot ščit pred digitalnimi pastmi

V letnem poročilu agencije ENISA za leto 2022 je navedeno, da je cilj socialnega inženiringa predvsem pridobitev nepooblaščenega dostopa do informacij ali storitev, kar pogosto vodi zlasti do finančnega dobička. Poročilo je razkrilo, da so bile v obdobju poročanja največkrat ravno finančne ustanove med tistimi, za katere so se prevaranti najpogosteje lažno izdajali. Poleg tega so se prevaranti lažno izdajali za velika tehnološka podjetja, kot so Microsoft, Apple in Google, ter skušali izkoriščati priljubljene storitve v oblaku in pretočne platforme.



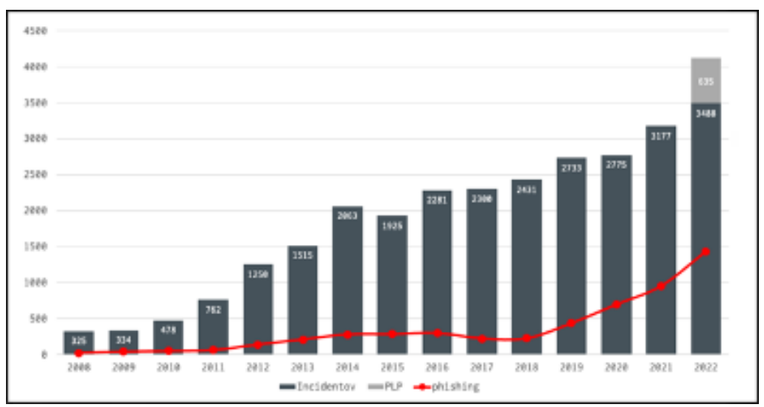
Grafikon 3: Časovni niz incidentov, ki so jih prejeli na SI-CERT in SIGOV-CERT (2020–2022)
Vir: Urad Vlade RS za informacijsko varnost, 2023 (str.5)

Poročilo je poudarilo tudi, da so prevaranti uspešno izkoriščali tudi pandemijo covida-19, v zvezi s katero prilagodili tehnike prevare in si olajšali svoje nezakonite dejavnosti.

Podoben trend naraščanja je moč opaziti tudi v polletnem poročilu Urada Vlade RS za informacijsko varnost (iz druge polovica leta 2022), iz katerega je razvidno, da je bilo samo v zadnjih dveh letih opaziti naraščanje prijavljenih incidentov kibernetskih napadov (a ne samo na podlagi socialnega inženiringa, temveč na splošno), prijavljenih tako na SI-CERT (Nacionalni odzivni center za kibernetsko varnost) kot tudi SIGOV-CERT (Odzivni center za incidente v informacijskih sistemih organov državne uprave).

Urad Vlade RS za informacijsko varnost v poročilu zlasti opaža, da se je število incidentov, ki so bili obravnavani v tretjem in četrtem četrtletju 2022, povečalo. Opažajo naraščanje števila incidentov, povezanih s tehnikami ribarjenja podatkov, ki postajajo vse bolj sofisticirani, ter naraščanje prevar na spletnih mestih. Zaznali so tudi skrb vzbujajočo rast števila poskusov prevar, v katerih se prevaranti izdajajo za organe pregona, finančne ustanove, ponudnike informacijskih storitev ali distribucijska podjetja.

Podoben porast, zlasti napadov ribarjenja, opaža v svojem pregledu za leto 2022 tudi SI-CERT, nacionalni odzivni center za kibernetsko varnost, ki koordinira razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. V letu 2022 je obravnaval kar 4123 incidentov, kar predstavlja več kot 30-odstotni porast v primerjavi z letom 2021. Za hiter odziv na omenjene incidente so na SI-CERT s septembrom 2022 uvedli tudi prvolinijsko pomoč (PLP) kot odziv na vprašanja in prijave, ki nimajo zahteve tehnične komponente. Ta služi kot mehanizem, ki bi razbremenil specializirani kader in analitike, da svoj čas posvečajo naprednejšim napadom in obravnavam ranljivosti (SI-CERT, 2023).



Grafikon 4: Časovni niz incidentov, ki so jih prejeli na SI-CERT (2008–2022)
Vir: SI-CERT (2023)

PREPOZNAVANJE DIGITALNIH PASTI IN NJIHOVO PREPREČEVANJE

Prevare prek socialnega inženiringa so po svoji zasnovi usmerjene na ranljivosti, ki so neločljivo povezane s človeškim vedenjem, zato je odkrivanje takšnih prevar lahko precejšen izziv tako za posameznike kot organizacije. Kljub temu lahko previdnost posameznikov in njihovo razumevanje indicov takšnih prevar pomagata pri zgodnjem odkrivanju in zmanjševanju tovrstnih groženj. Prepoznavanje vzorcev, ki pogosto spremljajo te vrste napadov, npr. uporaba taktik nujnosti ali vzbujanje strahu, nedosledna uporaba jezika, nenavadne zahteve in sumljiva komunikacija, je zatorej ključna za njihovo preprečevanje (Fan et al., 2017).

V hitro razvijajočem se digitalnem okolju se taktike in tehnike, ki jih uporabljajo prevaranti, nenehno spreminjajo, zaradi česar je ključnega pomena tudi, da so posamezniki ažurno seznanjeni z najnovejšimi trendi na teh področjih (Salahdine, 2019). Vsekakor ni dovolj, da se zanašamo zgolj na človeško pazljivost in ozaveščenost, temveč bi morali zlasti posameznike opolnomočiti, da informacijsko-komunikacijsko tehnologijo uporabljajo varno, ter obenem poskrbeti za uporabo orodij, katerih namen je odkrivanje in preprečevanju tovrstnih prevar.

V nadaljevanju zato v tabeli prikazujemo kratek pregled različnih orodij in tehnik za odkrivanje prevar socialnega inženiringa, od katerih vsaka zagotavlja ključne vpoglede v potencialne grožnje.

ORODJA/TEHNIKE ODKRIVANJA PREVAR	OBRAZLOŽITEV
Taktike nujnosti ali vzbujanje strahu	Prevaranti pogosto ustvarijo občutek nujnosti ali uporabijo taktike vzbujanja strahu, da bi tarče prisilili k takojšnjemu ukrepanju. Zaznavanje tovrstnih taktik naj vzbudi sum o prevari (Fan et a.l, 2017).
Sumljive zahteve	Zahteve po osebnih podatkih ali drugih zaupnih informacijah, ki se v danem trenutku posamezniku zdijo nenavadne, je treba obravnavati kot potencialne prevare socialnega inženiringa in biti do njih skeptičen (Fan et al., 2017).
Nedoslednosti ali slaba slovnica	Nedoslednosti v prejetih sporočilih, kot so pravopisne in slovnične napake ali nenavaden način izražanja, lahko kažejo na prevaro, saj pogosto izvirajo od oseb, ki jim jezik naslovnika ni materni jezik ali so svoja besedila prevedli s pomočjo spletnih prevajalnikov (Fan et al., 2017).
Nepričakovana ali nenavadna komunikacija	Nepričakovano sporočilo osebe, ki se predstavlja kot sodelavec, prijatelj ali ponudnik storitev, je lahko poskus prevare. Priporočljivo je, da ob primeru suma preverite njeno identiteto prek ločenega kanala, preden z njo delite zaupne informacije (Fan et al., 2017).
Nenavadni URL naslov ali domena	Prevaranti pogosto uporabljajo zavajajoče naslove URL ali domene, ki so zelo podobne legitimnim, da bi svoje tarče preslepili, da na teh straneh vpišejo in s prevarantom delijo svoje poverilnice. Ne pozabite preveriti URL spletnih mest ali povezav, ki so navedene v prejetih sporočilih (Fan et al., 2017).

ORODJA/TEHNIKE ODKRIVANJA PREVAR	OBRAZLOŽITEV
Prošnje za dostop do zaupnih podatkov	Bodite previdni pri zahtevah po osebnih ali drugih zaupnih podatkih, zlasti če prihajajo iz neznanih virov ali prek nezaželenih sporočil. Legitimne organizacije imajo običajno vzpostavljene varne kanale za zbiranje takšnih informacij (Fan et al., 2017).
Nadzor varnosti sistema	Z vzpostavitvijo zanesljivih (informacijskih) sistemov za nadzor nad varnostjo sistema lahko odkrijete in analizirate sumljive dejavnosti in morebitne poskuse prevar. To vključuje zlasti spremljanje omrežnega prometa, e-poštnih filtrov in sistemov za odkrivanje poskusov vdora (Salahdine & Kaabouch, 2019).
Analiza vedenja uporabnikov sistema	Z uporabo orodij za analizo vedenja uporabnikov lahko določite osnovne vzorce (predvidenega oz. zaželenega) vedenja posameznikov ali zaposlenih. Kakršna koli odstopanja ali anomalije od tovrstnih postavljenih vzorcev lahko kažejo na poskus prevare (Salahdine & Kaabouch, 2019).
Uporaba umetne inteligence	Z uporabo umetne inteligence, kot sta obdelava naravnega jezika in strojnega učenja, bi lahko sistemi umetne inteligence analizirali in interpretirali raznovrstno komunikacijo ter prepoznali vzorce in kazalnike taktik socialnega inženiringa. Algoritme umetne inteligence je mogoče usposobiti na velikih naborih podatkov o znanih prevarah socialnega inženiringa, kar jim omogoča učenje in prepoznavanje skupnih značilnosti in tehnik manipulacije, ki jih uporabljajo prevaranti (Lansley et al., 2019, str. 4–10). Umetna inteligenca lahko tudi simulira dejanske scenarije poskusov prevar in tako uporabnike z interaktivnim usposabljanjem opozarja, na kakšen način prepoznati in se odzvati na poskuse prevar. Ta interaktivni pristop k usposabljanju pomaga posameznikom razviti povečan občutek skepticizma in kritičnega razmišljanja, ko naletijo na sumljiva sporočila, kar zmanjša verjetnost, da postanejo žrtve tovrstnih napadov (Ansari et al., 2022).

Iz tabele je razvidno, da je odkrivanje prevar socialnega inženiringa v veliki meri odvisno od sposobnosti zaznavanja nenavadnega ali sumljivega vedenja in anomalij. Poleg tega lahko uporaba napredne tehnologije, kot so sistemi za nadzor nad varnostjo in analiza vedenja uporabnikov, zagotovijo dodatno raven zaščite pred tovrstnimi grožnjami. Vedno se je treba namreč zavedati, da se prevare socialnega inženiringa nenehno spreminjajo, kar zahteva stalno pazljivost in aktualno razumevanje najnovejših tehnik, ki jih uporabljajo prevaranti.

V boju proti socialnemu inženiringu se kot najučinkovitejši pristop kaže ravno celostna obravnava in vzporedna uporaba raznovrstnih tehnik, kot so ozaveščanje, dobre prakse zaščite in varnosti ter stalna pozornost in skepticizem (Nohlberg & Kowalski, 2008; Kaushalya et al., 2018; Junger et al., 2017; Rajah et al., 2020).

Kot prva obrambna linija pred prevarami socialnega inženiringa velja zlasti spodbujanje ozaveščanja in usposabljanja posameznikov. Z rednimi usposabljanji lahko posameznike izobražujemo o grožnjah, načinih prepoznave in zmanjševanja tveganj, kar posameznikom omogoča, da sumljive dejavnosti prepoznajo in se nanje ustrezno odzovejo. Junger et al. (2017) opozarjajo, da učinek usposabljanj in kampanj za ozaveščanje posameznikov sčasoma slabi, kar kaže na potrebo po stalni pozornosti in previdnosti. Za zagotovitev dolgoročne zaščite pred razvijajočimi se grožnjami socialnega inženiringa je potrebno med drugim tudi ohraniti neprekinjen cikel izobraževanja in ozaveščanja posameznikov.

Od zlorab podatkov do njihove zaščite: uporabniška ozaveščenost kot ščit pred digitalnimi pastmi

Skepticizem do nenavadnih ali nepričakovanih sporočil in klicev prav tako predstavlja enega izmed pomembnih preventivnih ukrepov. Posamezniki morajo upoštevati in prakticirati tudi varne prakse ravnanja s podatki, kot tudi zagotavljati ustrezno varnost in kompleksnost svojih gesel in drugih poverilnic. Posamezniki bi morali za različne uporabniške račune uporabljati kompleksna in edinstvena gesla, za zagotavljanje dodatne ravni varnosti pa bi bilo treba, kadar je to mogoče, uporabljati dvofaktorsko avtentikacijo (Dastane, 2020). S tem je mogoče preprečiti nepooblaščen dostop do podatkov, četudi prevarantu uspe pridobiti dostop do naših gesel.

Zaključimo lahko, da so večplasten pristop, ki vključuje stalno in celostno izobraževanje, preverjanje in previdnost pri sumljivi komunikaciji, močne metode avtentikacije in gesel ter stalna pozornost temelji učinkovitega varstva pred napadi socialnega inženiringa, s čimer se zagotavlja trdno varstvo osebnih in drugih zaupnih podatkov posameznika ali organizacij.

SKLEPNO

Jedro varstva osebnih podatkov v veliki meri temelji na ozaveščanju in izobraževanju, ki posameznike opolnomoči z znanjem za varno krmarjenje po digitalnem okolju. Spodbujanj in opozarjanje na sumljive dejavnosti ter gojenje skeptične miselnosti posameznikom omogoča, da prevzamejo nadzor nad zagotavljanjem varnosti osebnih in drugih zaupnih podatkov, kar učinkovito zmanjša tveganje nepooblaščenega dostopa ali zlorabe. Ob nenehnem razvoju kibernetskih groženj sta torej izobraževanje in ozaveščanje temeljna stebra varstva osebnih podatkov, ki prispevata k varnejšemu digitalnemu ekosistemu.

Socialni inženiring je v svojem temelju vdor v človeški um. Kljub napredku tehnoloških varnostnih ukrepov pa ta oblika prevare ostaja pereč problem v digitalnem vsakdanu, saj za razliko od tehnologije človeških možganov ni moč posodabljati ali popravljati njihovih napak. Za ublažitev vpliva tovrstnih prevar se kot najučinkovitejši pristop zdi zlasti spodbujanje ozaveščenosti posameznikov o tovrstnih grožnjah z obsežnim izobraževanjem tako zaposlenih kot že mladih v okviru izobraževalnega sistema in s sprejemom večplastne strategije. Ta naj vključuje predvsem okrepitev politike dostopa po principu: kar je ustrezno, relevantno in omejeno zgolj na to, kar je potrebno in nujno. Ključnega pomena je torej zavedanje, da je socialni inženiring podoben igri, pri čemer mora biti cilj ustvariti čim več ovir za prevaranta, da z igro konča, saj s tem iz igre odstranimo element zabave in prevarante spodbudimo k iskanju drugih tarč ali celo prenehanju igranja te igre.

Viri in literatura

Italiano

prilagojeno za **slabovidnost**

Mlada, uspešna in nadarjena

Intervju s podjetnico Michelle Rizzo iz bližnjega zamejstva, ki ima v lasti največji kozmetični salon na italijanskem Krasu

Svetlana Brecelj

Mlada, uspešna in nadarjena. Rada ima šport, točneje ples, povrh vsega pa je julija postala mama fantku Christianu. To je skoraj štiriindvajsetletna Michelle Rizzo, ki ima trenutno v lasti največji kozmetični salon na italijanskem Krasu, znan kot Michelle estetica. V Sesljanu pri Trstu jo poznajo kot mlado podjetnico in uspešno business woman. »Vedno sem imela rada račune in delo računovodje. Zelo sem natančna in odločna, kar se pozna v mojem poklicu. Preciznost je moja dobra kakovost in odlika, saj če v svetu kozmetike nisi natančen, ti bo težje delati. Ta lastnost pozitivno vpliva na vse plati mojega vsakdanjega življenja, tako doma kot v službi ali pri drugih dejavnostih.«

Michelle Rizzo ha studiato in Italia prima presso le scuole con lingua d'insegnamento slovena e poi ha continuato gli studi alla IAL di Trieste, dove si è diplomata con profitto specializzandosi in estetica: "Dopo il diploma ho lavorato al centro benessere Avalon in Borgo Grotta Gigante all'inizio come tirocinante, poi come dipendente. Purtroppo, in seguito ci avevano fatto richiesta di aprire la propria partita IVA e dopo essermi consultata con il mio commercialista, ho constatato che per motivi economici per me era meglio avviare un'attività in proprio che lavorare presso qualcuno. Così all'età di diciott'anni ho deciso di aprire il mio primo centro estetico a casa mia e cioè a Ternova presso Trieste. All'inizio il mio salone consisteva di una sola stanza al piano terra, mentre al primo piano c'era il mio appartamento. Prima della pandemia avevo lavorato saltuariamente anche a Sistiana presso un salone da parrucchiera, dove avevo il mio sportello estetico. Però dopo il Covid quel rapporto lavorativo si era interrotto. Tramite i social network avevo acquisito tante nuove clienti, perciò avevo bisogno di aiuto, cioè di nuove collaboratrici ma anche di un centro più grande. Per questo motivo ho trasferito la mia attività in questo centro nuovo a Sistiana presso Trieste."

Michelle Rizzo se je šolala v Italiji, najprej na šolah s slovenskim učnim jezikom, nato pa se je vpisala na italijansko kozmetično šolo IAL v Trstu, kjer je uspešno zaključila študij kozmetike. »Po diplomi sem nekaj let delala v kozmetičnem centru Avalon v Briščkih pri Trstu. Najprej sem bila praktikantka, nato pa so me tam zaposlili. Žal so v tem centru zahtevali, naj si odpremo svoj espe. Po pogovoru z računovodjo sem se odločila, da se mi ekonomsko bolj splača odpreti svojo dejavnost, kot pa da sem nekje zaposlena. Pri osemnajstih letih sem torej odprla svoj prvi salon v domačih prostorih, torej v Trnovci pri Trstu. Najprej sem imela le eno sobo, saj je bilo na vrhu stanovanje, v pritličju pa salon. Pred pandemijo sem občasno delala pri frizerki v Sesljanu, kjer

Na fotografiji: Michelle Rizzo, lastnica salona Michelle estetica pri delu

sem imela najet prostor za opravljanje kozmetičnih storite. Po covidu-19 pa se je najino sodelovanje prekinilo. Preko družbenih omrežij sem pridobila veliko novih strank in sem potrebovala pomoč, torej nove sodelavke ter večji salon. Zaradi tega se je moja dejavnost letos preselila v nove prostore v Sesljan pri Trstu.«

Leto 2023 je zanjo obdobje velikih sprememb, presenečenj in novih izzivov. Seveda pa se za uspehom skriva veliko dela in truda. Največja težava so v tej dejavnosti seveda dokumenti, torej organizacija kritja stroškov, urejanja tretmajev, terminov, plač ipd. V Italiji namreč ni enostavno odpreti kozmetičnega salona, ker ima vsaka občina svoja pravila. »Danes imam več kot 1400 stalnih strank, poleg njih pa v salon zahajajo še druge stranke, ki niso fiksne. To so na primer razni turisti, najpogosteje iz bližnje Avstrije. Družbena omrežja so bistveno pripomogla k širjenju moje dejavnosti. Najpogosteje uporabljam Instagram, tudi Facebook in WhatsApp sta ključnega pomena za pridobitev strank,« navaja Michelle Rizzo.

Zanimalo nas je, ali se v kozmetični šoli res naučiš vsega, kar je za ta poklic pomembno znati. »V šoli te naučijo osnovna pravila za delo v svetu kozmetike. Potrebno je veliko prakse, ki jo pridobiš z izkušnjo. K sreči so mi bivše sodelavke in moja mama veliko pomagale. Sodelavke so mi iz osebne izkušnje svetovale, kaj naj kupim za svoj salon in kaj se mi ne splača, mama pa me je spremljala pri nakupih. Tudi če ni poznala sveta kozmetike, se je vseeno bolj spoznala na račune in stroške kot jaz, ki sem bila takrat zelo neizkušena. Tudi na lepotnih sejmih sem dobila nekaj novih nasvetov, saj so mi tam prisotne firme predstavile svoje izdelke in različne storitve. Tudi preko spleta in e-pošte prejemam reklame za kozmetiko. V tem poklicu moraš sam spoznati, kateri izdelki ti ustrezajo, kateri pa ne. Tudi organizacija delovnega urnika je pomembna: včasih sem delala več kot 12 ur na dan in sem bila zmeraj na razpolago svojim strankam, danes pa si postavljam nekaj več meja med delom in prostim časom. Poleg tega, da sem lastnica salona, sem tudi neke vrste Jolly, saj znam opravljati vse in tako grem tja, kjer me sodelavci potrebujejo.«

Eravamo curiosi di sapere se la scuola di cosmetologia fornisca veramente tutto il sapere necessario perquesto mestiere: »Alla scuola per estetiste si imparano le basi di questo mestiere, il resto lo acquisisci con tanta esperienza lavorativa. Fortunatamente ho avuto l'aiuto delle mie ex colleghe e di mia madre. Le mie colleghe hanno saputo consigliarmi su quali prodotti scegliere o cosa non mi conveniva, mentre la mia mamma mi ha accompagnato negli acquisti. Anche se non conosceva il mondo della cosmetica aveva senz'altro più esperienza di me nella gestione delle spese dato che all'epoca ero ancora molto inesperta. Molto utili mi sono state anche le varie fiere di cosmetologia durante le quali ho incontrato i rappresentanti di varie aziende che mi hanno presentato i loro prodotti e servizi di estetica. Tramite internet e posta elettronica ricevo tutt'ora la pubblicità dei prodotti per l'estetica e ho imparato a valutare da sola quali scegliere. Anche l'organizzazione dell'orario di lavoro è molto importante: se all'inizio della mia carriera ho lavorato anche per più di 12 ore al giorno ed ero sempre a disposizione, adesso mi sono posta dei limiti e cerco di prendermi del tempo libero per me stessa. Inoltre, essendo la proprietaria del mio salone ho anche il ruolo di Jolly, perchè so fare tutto e così posso aiutare dove c'è bisogno.«

Podjetnica ugotavlja, da v primerjavi s prejšnjim delo v novem salonu poteka na bolj utečen način, saj imajo njeni novi sodelavci veliko izkušenj zaradi dolgoletnega sodelovanja v drugih salonih, zato zelo dobro poznajo realnost kozmetičnega dela, medtem ko je prej delo potekalo na družinski način. Seveda pa je ponosna tudi na svoje tri sodelavke, ki so z njo delale že v salonu v Trnovci. Letos se je ekipi lepotnega salona pridružila še Michellina mama, ki je ob službi v vrtcu tu prevzela vlogo blagajničarke in tajnice. V prejšnjih mesecih so se skupini pridružile še vajenke iz kozmetične šole, ki so v salonu Michelle estetica opravile obvezno obštudijsko prakso. Ker se je njena dejavnost še dodatno povečala, je morala mlada podjetnica Michelle večkrat zamenjati računo-

vodjo: »V zadnjih letih sem zamenjala štiri računovodje. Danes je ena izmed mojih strank končno prevzela to funkcijo in me je veliko naučila o računih ter o drugih finančnih zadevah.«

Koronavirus je imel na večino podjetij in dejavnosti negativen vpliv, tako s finančnih kot organizacijskih vidikov. »Covid-19 je bistveno vplival na moje delo. Res je, da sem takrat končno pridobila nekaj časa zase, lahko bolj skrbela za svojo osebno nego in uredila stvari, ki sem jih prej zaradi službe postavljala na drugo mesto. Imela sem tudi več časa za svojo družino in za svoje bližnje. Bolj kot sama pa so bile moje stranke zelo prestrašene. Nekatere bolj pogumne so mi predlagale, da bi prišle v moj salon preko stranskih poti, seveda pa teh predlogov nisem sprejela. Obvezno nošenje mask, razkuževanje rok in drugi predpisi mi gotovo niso olajšali dela. Tudi z ekonomskega vidika je moja dejavnost nastradala. Res je, da nam je država nudila nekaj sredstev za kritje stroškov, a je bila vsota zelo nizka in ni krila vsega. Takrat sem še vedno plačevala najemnino za svoj prostor pri frizerki, zato so bili stroški visoki.« Kozmetičarka Michelle pa je vseeno prosti čas med pandemijo dobro izkoristila v druge namene: »Med karanteno sem dokončala peti letnik kozmetične šole, ki je pogoj, da lahko postaneš profesor kozmetike, torej lahko poučuješ na raznih tečajih in šolah na omenjenem področju. Po treh letih študija kozmetike v Italiji postaneš navaden kozmetičar, po štirih lahko odpreš svoj espe, po petih pa postaneš pedagog na tem področju. V dneh zaprtja sem torej pisala končno seminarsko nalogo. Poleg tega pa sem v večernih urah po aplikaciji Zoom vodila tečaj plesa, saj sem poleg kozmetičarke tudi šolana plesalka. Več kot 27 deklet in gospa se je udeležilo omenjenega tečaja plesa.«

Salon Michelle estetica se danes ponaša s 170 kvadratnimi metri prostora: razdeljen je na osem sobic in nudi razne tipe masaž, pedikuro, manikuro, solarij, epilacijo, prehrambene nasvete, permanentne tatuje za obrvi in vse, kar si lahko za svojo osebno nego zaželimo.

Oggi il centro estetico di Michelle supera i 170 metri quadri, è composto da otto stanze ed offre vari servizi, come la manicure e la pedicure, il solarium, la depilazione con laser estetico, consulenze dietologiche, laminazione ciglia e sopracciglia... Tutto ciò che una persona può desiderare per il proprio benessere.

prilagojeno za **slabovidnost**

Analiza tujih praks:
revije prilagojene netradicionalnim skupinam študentov

Valinea Sušec

V zadnjih letih je mogoče opaziti pomemben poudarek na prepoznavanju individualnih značilnosti in potreb študentov v izobraževalnih ustanovah, vključno z njihovimi različnimi interesi, učnimi slogi, s kulturnimi ozadji, z jezikom in drugimi svojevrstnimi razlikami. Izobraževalne ustanove se zdaj zavzemajo za ustvarjanje enakovrednih pogojev in podpore za vse študente, ne glede na njihove razlike. Posebno pozornost namenjajo tudi netradicionalnim skupinam študentov, kot so posamezniki s posebnimi potrebami, z različnimi jezikovnimi in kulturnimi ozadji ter različnimi učnimi slogi. Cilj je zagotoviti enake možnosti dostopa do izobraževalnih materialov in programov za vse študente (Müller & Hofmann, 2021).

Tuje univerze so v ospredju pri uvajanju inovativnih pristopov, kot so tiskanje akademskih revij v Braillovi pisavi za slabovidne študente, vključno s taktilnimi grafikami za boljše razumevanje kompleksnih vizualnih informacij. Prav tako ponujajo zvočne transkripcije člankov v revijah za študente z okvaro vida ali tiste, ki imajo raje slušno razumevanje. Nekatere univerze uvajajo tudi podkaste, ki vsebujejo povzetke člankov iz revij, da bi informacije postale dostopnejše za študente s posebnimi potrebami. Univerze se zavedajo potrebe po vizualnih prilagoditvah za študente z okvaro vida in uporabljajo tehnologije, kot so bralniki zaslona in orodja za povečevanje besedila. Dodatno omogočajo alternativne opise fotografij in podnapisov, da bi študentom z okvaro vida omogočili dostop do vizualnih elementov v revijah. Spletne revije se prav tako trudijo za večjo dostopnost, vključno z alternativnimi besedilnimi opisi za slike, visokokontrastnimi različicami za študente z okvaro vida ter s podnapisi ali transkripcijami za videoposnetke in zvočne vsebine za gluhe ali naglušne študente. Poleg tega oblikujejo svojo vsebino z mislijo na dostopnost, uporabljajo dostopne barve in pisave ter se izogibajo motečim funkcijam, kot so utripajoča ali premikajoča se vsebina (Lazarus, et al., 2022).

Vir: Freepik

Vse te prakse odražajo zavezanost izobraževalnih ustanov in spletnih revij k ustvarjanju vključujočega učnega okolja, ki zadovoljuje različne potrebe študentov, vključno s tistimi s posebnimi potrebami (Informa Group, 2021).

V nadaljevanju je predstavljenih pet primerov tujih Univerz, ki so uvedle prilagoditve za t. i. netradicionalne skupine študentov. Med te spadajo: Kalifornijska univerza Berkeley, Univerza v Torontu v Kanadi, Univerza v Cambridgeu v Združenem kraljestvu, Univerza Stanford v Združenih drža-

Vir: Freepik

vah Amerike in Univerza v Melbournu v Avstraliji.

Kalifornijska univerza Berkeley je uvedla revijo »The Berkeley Inclusive Research Journal« (BIRJ), ki je prilagojena študentom s posebnimi potrebami, zlasti tistim z okvarami vida. Revija se osredotoča na objavljanje znanstvenih člankov in raziskav s poudarkom na inkluzivnosti in študijah o invalidnosti. Za študente z okvaro vida so uvedli prilagoditve, vključno s tiskanjem Braillove različice revije. Univerza sodeluje z univerzitetnim programom za študente invalide (DSP) in s strokovnjaki za podporno tehnologijo, da bi zagotovili dostopnost in različne formate za študente, vključno z velikim tiskom in elektronskim besedilom. Namen revije BIRJ je spodbujanje vključevanja in dejavnega sodelovanja študentov s posebnimi potrebami v akademskem okolju, kar prispeva k bolj vključujoči in raznoliki znanstveni skupnosti na univerzi. Pri tem se uporabljajo različne informacijske in komunikacijske tehnologije, vključno s programsko opremo za branje zaslona in tiskalniki Braillove pisave. Spletna platforma revije je zasnovana za dostopnost, upoštevajoč standarde in smernice za spletno dostopnost. Revija BIRJ je tako pomembna platforma za spodbujanje inkluzivnosti in raziskav na tem področju na univerzi Berkeley (Keavney, 2022).

Univerza v Torontu je uvedla revijo »The Inclusivity Review« (TIR),

Vir: Freepik

namenjeno študentom z različnimi invalidnostmi, z osredotočenostjo na teme inkluzivnosti, raznolikosti in študij invalidnosti. Za zagotavljanje dostopnosti revije za študente z okvarami vida tesno sodelujejo z uradom za storitve za invalide in s centrom za prilagojeno tehnologijo. Revijo prilagajajo v različne formate, kot so Braillova pisava, veliki tisk in elektronsko besedilo. Spletno različico oblikujejo z upoštevanjem smernic za dostopnost, vključno z alternativnimi besedilnimi opisi za slike, kar olajša uporabo bralnikov zaslona. Univerza dejavno uporablja informacijske in komunikacijske tehnologije (IKT) za podporo dostopnosti. Uporabljajo orodja za digitalno dostopnost, optimizirajo spletno mesto za združljivost z bralniki zaslona ter omogočajo dostop do programske opreme za podporno tehnologijo, kot so bralniki zaslona, orodja za povečevanje in pretvorbo besedila v govor. Za pretvorbo vsebine v alternativne formate uporabljajo specializirane orodja ali programsko opremo za pretvorbo dokumentov. Z revijo TIR Univerza v Torontu spodbuja vključujoče akademsko okolje in promovira prispevke študentov z invalidnostmi v znanstveni skupnosti (University of Toronto, 2019).

Univerza v Cambridgeu v Združenem kraljestvu je ustanovila revijo z naslovom »Access Journal«, ki se osredotoča predvsem na dostopnost in vključenost študentov invalidov. Cilj revije Access Journal je zagotoviti platformo za študente, raziskovalce in akademike, da objavijo svoje delo, pri čemer je zagotovljen dostop za širok krog invalidov. Revija pokriva različna področja in spodbuja prispevke, ki obravnavajo pravice invalidov, vključujoče izobraževanje, podporno tehnologijo in druge sorodne teme. Da bi bila revija dostopna, Univerza v Cambridgeu sodeluje s svojim centrom za pomoč invalidom ter strokovnjaki s področja dostopnosti in podporne tehnologije. Ponujajo več oblik, vključno z Braillovo pisavo, velikim tiskom in elektronskimi besedilnimi različicami člankov v reviji. Poleg tega uporabljajo najboljše prakse za digitalno dostopnost in zagotavljajo, da je spletna različica revije združljiva z bralniki zaslona, ima ustrezno strukturo naslovov in alternativno besedilo za slike. Z revijo Access Journal želi Univerza v Cambridgeu spodbujati vključujočo in podporno akademsko skupnost, ki ceni prispevke in perspektive študentov invalidov. Revija ima pomembno vlogo pri spodbujanju ozaveščenosti, razumevanja in raziskav na področju študij o invalidnosti, hkrati zagotavlja, da so informacije dostopne vsem posameznikom (Dolmage, 2017).
Univerza Stanford v ZDA je uvedla revijo »The Inclusive Scholar«,

namenjeno promociji vključevanja in dostopnosti za študente invalide v akademskem okolju. Revija je multidisciplinarna in se osredotoča na objavljanje raziskav, esejev in ustvarjalnih del, ki obravnavajo pravice invalidov, dostopnost in vključenost. Univerza sodeluje s svojim Uradom za dostopno izobraževanje (OAE) ter strokovnjaki za podporno tehnologijo in standarde dostopnosti. Za zagotavljanje dostopnosti revije so na voljo alternativne oblike, vključno z Braillovo pisavo za slabovidne študente, elektronskim besedilom in možnostjo velikega tiska. Spletna platforma revije je zasnovana z mislijo na dostopnost, upoštevajoč smernice spletne dostopnosti, kot so ustrezne strukture naslovov in alternativno besedilo za slike, kar olajša uporabo bralnikov zaslona. Publikacija »The Inclusive Scholar« dejavno spodbuja sodelovanje študentov invalidov v akademskem raziskovanju in diskurzu ter služi kot platforma za izmenjavo njihovih pogledov. Univerza Stanford z uporabo informacijskih in komunikacijskih tehnologij (IKT) omogoča študentom dostop do podporne tehnologije, kot so bralniki zaslona, programska oprema za pretvorbo besedila v govor in orodja za povečevanje, ki jim pomagajo pri uporabi vsebine revije (Easop, 2022).

Univerza v Melbournu v Avstraliji je uvedla revijo z naslovom »Diversity and Inclusion in Research and Education« (DIRE), ki se osredotoča na spodbujanje dostopnosti in vključevanja študentov invalidov. Revija DIRE objavlja raziskovalne članke, eseje in znanstvena dela, ki obravnavajo teme, povezane z raznolikostjo, vključevanjem in s študijami o invalidnosti na področju raziskovanja in izobraževanja. Revija si prizadeva ozaveščati o izzivih, s katerimi se srečujejo študenti invalidi, in raziskovati inovativne pristope k spodbujanju vključujočega učnega okolja. Za zagotavljanje dostopnosti Univerza v Melbournu sodeluje s svojo Enoto za stike z invalidi (DLU) ter strokovnjaki s področja dostopnosti in vključujočega oblikovanja. Ti zagotavljajo različne prilagoditve revije, vključno z različicami člankov v Braillovi pisavi za študente z okvarami vida. Poleg tega ponujajo alternativne formate, kot sta veliki tisk in elektronsko besedilo, da bi zadovoljili različne potrebe po dostopnosti.

Revija DIRE Univerze v Melbournu služi kot platforma za predstavitev prispevkov in pogledov študentov invalidov ter ustvarja vključujoč prostor za dialog in izmenjavo idej. S spodbujanjem dostopnosti in vključenosti v raziskovanje in izobraževanje revija prispeva k pravičnejšemu akademskemu okolju, ki ceni raznolikost in edinstvene perspektive vseh študentov (Studying in Australia, 2023).

Uvedba prilagojenih znanstvenih revij za študente s posebnimi potrebami predstavlja proaktivne ukrepe izobraževalnih ustanov za zagotovitev enakega dostopa do znanstvenih vsebin vsem študentom. Uporaba različnih informacijskih in komunikacijskih tehnologij, kot so programska oprema za podporno tehnologijo, orodja za digitalno dostopnost, sodelovalne platforme in orodja za pretvorbo dokumentov, omogoča univerzam, da zagotovijo alternativne formate in povečajo dostopnost svojih revij. Te pobude ne koristijo le študentom s posebnimi potrebami, temveč prispevajo tudi k oblikovanju bolj vključujočih akademskih okolij, ki cenijo raznolikost ter spodbujajo širše razumevanje dostopnosti in vključenosti v raziskave in izobraževanje. Glavna prednost se odraža v povečani dostopnosti, saj prilagoditve revij zagotavljajo enakopraven dostop do vsebine. S ponujanjem alternativnih formatov, kot so Braillova pisava, veliki tisk ali elektronsko besedilo, se omogoča slabovidnim študentom samostojno branje člankov v revijah. Takšna dostopnost omogoča netradicionalnim skupinam študentov, da se dejavno vključujejo v akademsko razpravo, dostopajo do znanja ter prispevajo svoje raziskave in ideje. Prilagojene revije prispevajo k ustvarjanju podpornega in vključujočega akademskega okolja, spodbujajo sodelovanje, dialog in izmenjavo idej med študenti, profesorji in raziskovalci.

Viri in literatura

prilagojeno za
slabovidnost

FU potuje na Dunaj in v Bratislavo

Valinea Sušec

Grafična podoba dogodka Ekskurzija na Dunaj in v Bratislavo

FUL Povezani in Študentski svet Fakultete za upravo v sodelovanju s Fakulteto za upravo je za vse upravnice in upravnike organiziral strokovno ekskurzijo na Dunaj in v Bratislavo. Ekskurzija je potekala od 21. do 23. aprila 2023.

V zgodnjih jutranjih urah smo se v petek, 21. aprila 2023, študenti Fakultete za upravo odpravili na pot proti Dunaju, potem pa še na pot proti Bratislavi. Raziskovanje Dunaja je potekalo en dan, dva dneva pa smo imeli namenjena za raziskovanje Bratislave. Na pot smo se odpravili preko Avstrije do Dunaja, kamor smo prispeli v dopoldanskih urah.

Slika: Veleposlaništvo RS na Dunaju

Mesto Dunaj slovi po svoji zgodovinski pomembnosti, izjemni arhitekturi, bogati glasbeni tradiciji, muzejih in umetnosti.

Imeli smo priložnost ogleda Veleposlaništva Republike Slovenije na Dunaju, kjer so nam zaposleni predstavili organizacijo in delovanje veleposlaništva, v katerem opravljajo delo. Predstavili so nam možnost opravljanja študijske prakse, če bi imeli študentje zanimanje za opravljanje tovrstnega dela. Poudarek je bil na njihovem organizacijskem, konzularnem in internem delovanju. Predstavljena so bila aktual-

na dogajanja in naloge, ki jih opravljajo in učinkovito rešujejo.

Zatem smo se odpravili v mestno jedro, kjer smo si ogledali parlament, državno opero, muzejsko četrt in druge bogate palače, značilne za mesto Dunaj. Sladkosnedci so si privoščili znano 'Sacher' tortico in druge številne dobrote, ki jih ponuja mesto Dunaj. Sledil je prosti čas za samostojno raziskovanje mesta in zbor pri zbirni točki, kjer nas je čakal avtobus. Navdušeni smo bili nad turističnim vodenjem, saj smo imeli tudi čas zase, poleg tega pa smo vodenje izkoristili za ogled znamenitosti mesta. Vožnja z avtobusom po Dunaju nam je omogočila ogled znamenitosti, kjer nam je vodič sproti pripovedoval, kje se nahajamo, in na kratko predstavljal zgodovino znamenitosti, mimo katerih smo se peljali.

Zatem smo se v večernih urah odpravili v Bratislavo in se nastanili v hotelu. Po napornem dnevu je sledilo druženje in prosti čas.
Naslednji dan smo se po zajtrku odpravili v center Bratislave in se ustavili pred Mozartovo palačo, videli pa smo tudi sedež Academie Istropolitane, kjer je danes narodna univerzitetna knjižnica. Ogled smo nadaljevali z Martinovo katedralo, v kateri so kronali Marijo Terezijo, ter se podali proti glavnemu trgu, kjer smo imeli možnost samostojnega raziskovanja mesta. Po ogledu mesta smo

Slika: Parlament na Dunaju

se popoldan odpravili proti pokrajini Malih Karpatov, ki je znana predvsem po vinorodni pokrajini in okusnih vinih. Odšli smo si ogledat eno izmed vinskih kleti, kjer so nam na kratko predstavili zgodovino in značilnosti slovaških vin. Imeli smo degustacijo petih vin, značilnih za Bratislavo. Omogočen nam je bil tudi nakup vina, ki nas je najbolj prepričal po svojem specifičnem okusu. Ko smo končali z obiskom vinske kleti, smo se odpravili nazaj v hotel. Zvečer smo izkoristili čas za ogled nočnega dogajanja v Bratislavi, nekateri bolj utrujeni pa so si ta čas privoščili za počitek.

Slika: Sacherjeva torta

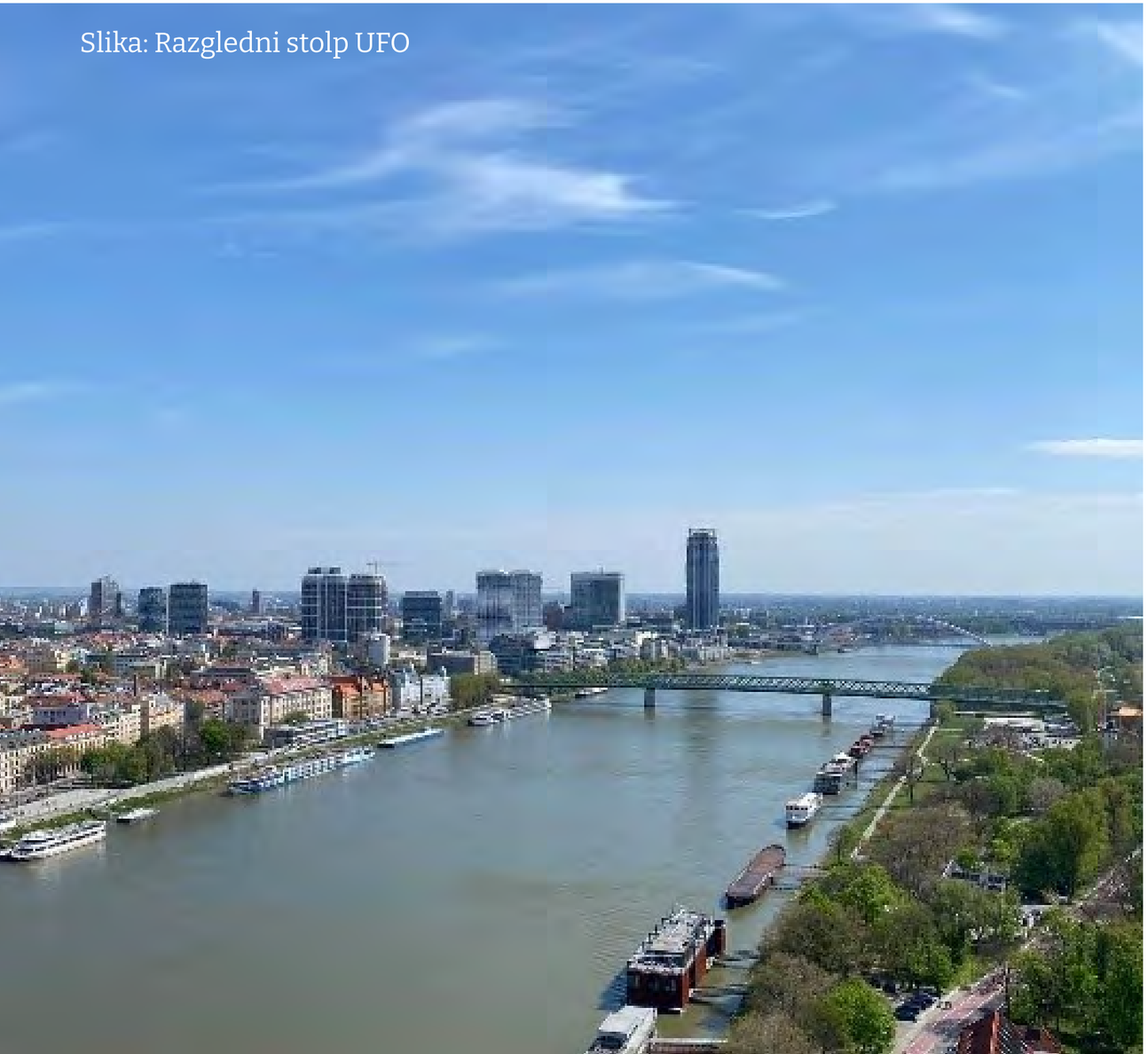
Slika: Starbucks v Bratislavi

Slika: Palača Hofburg na Dunaju

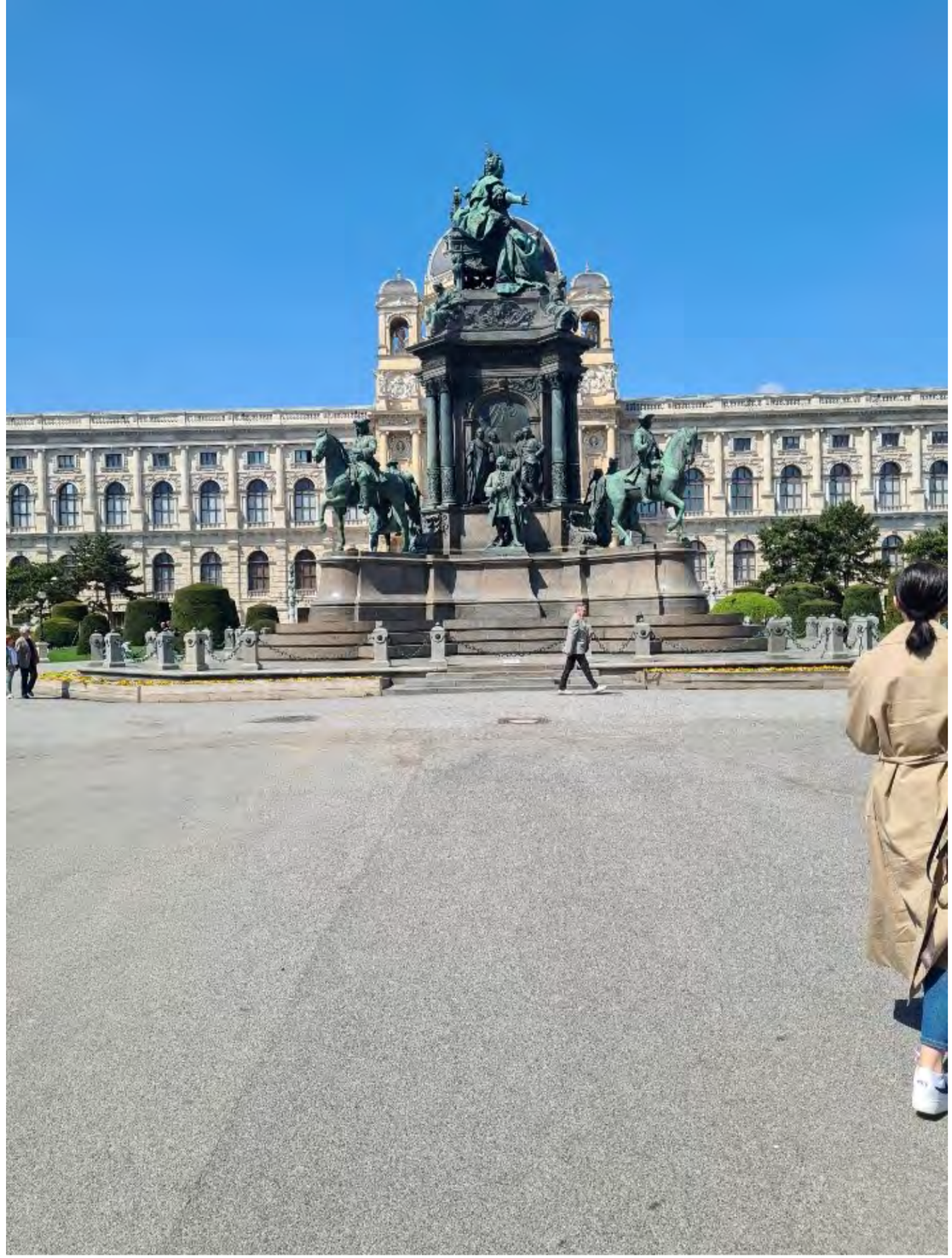
Naslednji dan v Bratislavi smo se povzpeli na vrh mostu SNP (Bridge of the Slovak National Uprising), kjer se nahaja eden najelegantnejših pogledov s fantastično panoramo na prestolnico. Znameniti stolp UFO, ki ponuja razgled na mesto, velja za enega najvišjih stolpov na svetu. V samo 45 sekundah smo se z dvigalom povzpeli na višino 95 metrov, kjer nam je razgled nudil čudovit pogled na Bratislavo. Po ogledu stolpa smo imeli prosti čas za obisk mesta, popoldan pa smo se že odpravili nazaj na avtobus, se poslovili od Bratislave in se odpravili na vožnjo proti Sloveniji, nazaj proti domu. V Slovenijo smo prispeli 23. aprila 2023 v poznih večernih urah.

V Študentski organizaciji Fakultete za upravo smo zadovoljni s potekom in izvedbo ekskurzije. Ekskurzije se je udeležilo 45 študentov, od katerih smo prejeli pozitivne odzive na izvedbo in potek izleta.

Želimo si še več podobnih dogodkov, druženja in medsebojnega sodelovanja, ki nas je pripeljalo do uspešno izvedene ekskurzije. Obisk Dunaja in Bratislave bomo še dolgo ohranili v spominu. Bilo je kratko, toda sladko. Posebej se zahvaljujemo Fakulteti za upravo za vso pomoč in podporo pri organizaciji ekskurzije. Bilo je nepozabno, hkrati pa smo pridobili nova prijateljstva oz. poznanstva, ki nas še bolj povezujejo. Veselimo se že naslednje organizirane ekskurzije.



Slika: Razgledni stolp UFO



Slika: Dunaj, umetnostnozgodovinski muzej