Revija za univerzalno odličnost / Journal of Universal Excellence, Članek / Article
December 2018, leto / year 7, številka / number 4, str. / pp. 334–346.

Odkrivanje potencialnih groženj za informacijski sistem

Andrej Dobrovoljc*
Fakulteta za organizacijske študije v Novem mestu, Ulica talcev 3,
8000 Novo mesto, Slovenija
andrej.dobrovoljc@3ad.si

Povzetek:
Raziskovalno vprašanje (RV): Ali nam lastnosti informacijskega sistema lahko pomagajo pri odkrivanju potencialnih bodočih groženj?
Namen: Z raziskavo želimo preveriti odnos običajnih uporabnikov in različnih skupin napadalcev do lastnosti informacijskega sistema. Ob tem se usmerjamo na merjenje pomembnosti lastnosti za posamezno populacijo.
Metoda: Izvedli smo kvantitativno raziskavo z uporabo vprašalnika. Opise informacijskih sistemov, ki so bili uporabljeni v vprašalniku, smo opredelili na podlagi razpoložljivih podatkov v spletu.
Rezultati: Potrdili smo domneve, da napadalci večinoma vrednotijo iste lastnosti informacijskega sistema drugače od običajnih uporabnikov. Praviloma napadalci v večini lastnosti prepoznajo večjo vrednost kot običajni uporabniki, in v nekaterih primerih so te razlike očitne. Razlike so tudi med napadalci. Rezultati so dobra osnova za nadaljnje raziskovanje, in sicer preverjanje h katerim elementom človeške grožnje prispevajo posamezne lastnosti.
Organizacija: Lastnosti informacijskega sistema, kjer med uporabniki in napadalci prihaja do očitnih razlik v vrednotenju, so lahko dober indikator tveganja. S prepoznavanjem takšnih lastnosti lahko izboljšamo odločanje pri oceni tveganja.
Družba: Z raziskavo želimo okrepiti prepričanje, da je pri zagotavljanju informacijske varnosti pomembno upoštevati vidik napadalca in že pred samim začetkom uporabe informacijske rešitve izdelati model bodočih človeških groženj.
Originalnost: Raziskava potrjuje idejo, da je potrebno pri oceni tveganja upoštevati vidik napadalca. Z eksperimentom smo pokazali, da napadalci večini lastnosti informacijskega sistema pripisujejo višjo uporabno vrednost kot običajni uporabniki.
Omejitve/nadaljnje raziskovanje: V raziskavo smo lahko vključili poznavalce informacijske varnosti, ne pa realnih napadalcev, ki so v resnici skrita populacija. Pri nadaljnjem raziskovanju želimo preveriti, kako lastnosti informacijskega sistema prispevajo k posameznim elementom človeške grožnje (motivaciji, prepoznavi priložnosti, preverjanju sposobnosti).

Ključne besede: grožnja, informacijski sistem, napadalec, ocena tveganj, informacijska varnost.

1 Uvod

Kljub številnim koristim, ki nam jih prinašajo sodobne informacijske rešitve, se vedno bolj zavedamo njihove občutljivosti na kakršnekoli motnje in nepravilnosti v njihovem delovanju. V ta okvir sodita tudi nepravilna uporaba in zloraba razpoložljivih funkcionalnosti informacijskega sistema (IS). Razsežnost problema razkrivajo številne raziskave s področja informacijske varnosti. Že v letu 2011 je bilo tako samo z uporabo družbenega inženiringa (angl. *social engineering attack*) napadenih kar 40 % organizacij po svetu, z različnih poslovnih področij in vseh velikosti. Organizacije in posamezniki so izpostavljeni tudi

* Korespondenčni avtor / Correspondence author

Prejeto: 15. november 2018; revidirano: 17. november 2018; sprejeto: 22. november 2018. /
Received: 15th November 2018; revised: 17th November 2018; accepted: 22rd November 2018

številnim naprednim tehnološkim napadom, ki jih napadalci lahko izvajajo na daljavo in anonimno preko svetovnega spleta (Dimensional Research, 2011, str. 1).

Grožnje za IS se ne pojavijo na enkrat. Ponudniki novih informacijskih rešitev ob njihovem lansiranju na trg (npr. spletne aplikacije) upajo predvsem na hitro rast števila uporabnikov. Ob tem imajo pogosto v mislih le model uporabnikov, katerim so v osnovi namenjene podprte funkcionalnosti. Zaradi visokih stroškov razvoja pogosto zanemarijo modeliranje groženj oz. napadalcev (Steven, 2010, str. 83-84). Priljubljene informacijske rešitve pa sčasoma lahko postanejo zanimive različnim skupinam napadalcev. Njim je osnovni cilj zlorabiti sistem ali povzročiti škodo (Alhazmi, Malaiya, & Ray, 2007, str. 5; Frei, Schatzmann, Plattner, & Trammell, 2010, str. 3-4; Miller, 2007; Schneier, 2012). Sklepamo lahko torej, da se grožnje razvijejo postopoma. Razvijejo se v nekem daljšem časovnem obdobja kot posledica sprememb v okviru IS in njegovi okolici. Ugotovimo lahko torej, da se lastnostni IS skozi čas spreminjajo, to pa ima pomemben vpliv pri nastanku in oblikovanju groženj za IS.

Pri zagotavljanju informacijske varnosti v IS igrajo ključno vlogo ljudje (S. W. Smith, 2003, str. 75). Na nekatere vrste groženj se lahko pripravimo v naprej. Postopke, kako se zavarovati in ravnati v primeru naravnih nesreč (npr. poplava, potres, požar ipd.) ali v primeru odpovedi delov sistema, lahko načrtujemo, saj obstajajo že številne dobre prakse (Anderson, 2010; BSI, 2011). Po drugi strani pa ljudje predstavljamo tudi eno največjih in najbolj zahtevnih groženj. Arhitekti IS ob snovanju novih sistemov ponavadi skrbno upoštevajo vsa znana načela razvoja varnih informacijskih rešitev, a žal seznam teh načel nikoli ne more biti popoln (R. Smith, 2012, str. 25). Obnašanje ljudi je namreč nepredvidljivo. Razlikujemo se v zaznavanju groženj, kar nezadržno vodi v pojavljanje novih varnostnih incidentov (Workman, 2008, str. 463). S stalnim osveščanjem in usposabljanjem uporabnikov lahko omejimo naključne napake in izboljšamo prepozanavanje nekaterih znanih tipov groženj (Hall, Sarkani, & Mazzuchi, 2011, str. 155; Mann, 2008; S. W. Smith, 2003). Žal IS nikoli ne more biti popolnoma varen pred inovativnimi vsiljivci, ki sistem ogrožajo načrtno in premišljeno. Zato se sprašujemo, kako lahko predvidimo takšne bodoče grožnje.

Proaktivno zagotavljanje varnosti IS v prihodnosti, lahko temelji le na njegovih opisih in vizualizacijah v prihodnosti. Vprašanje je, kako dobro lahko na osnovi takšnih opisov prepoznamo bodoče grožnje. Predno poizkusimo odgovoriti na takšno vprašanje moramo dobro razumeti, kaj grožnja sploh je oz. kako jo lahko opredelimo.

Zlonamerna grožnja, ki jo predstavlja človek (napadalec), je sestavljena iz več komponent, in sicer: sposobnosti napadalca za izvedbo napada, priložnosti, ki mu jih nudi IS ter njegovo okolje in napadalčeve motivacije ter pričakovanega učinka zanj (Blyth & Kovacich, 2006; Pfleeger & Pfleeger, 2006, str. 23).

Informacijski sistem lahko opišemo z lastnostmi njegovih komponent, ki jih v osnovi sestavljajo strojna oprema (angl. *Hardware*), programska oprema (angl. *Software*), podatki, postopki in ljudje (Stair & Reynolds, 2013). Tako običajni uporabniki kot tudi napadalci

prepoznavajo IS preko njegovih lastnosti. V osnovi so vsem na voljo isti opisi IS. Postavlja se torej vprašanje, kje prihaja do razlik, ki prispevajo k oblikovanju groženj. Odgovor lahko iščemo v smeri podrobnega razumevanja posameznih komponent grožnje. Kljub vsemu želimo v prvem koraku preveriti, kakšne so razlike med posameznimi populacijami ljudi (običajni uporabniki, različne vrste napadalcev) v dojemanju pomembnosti posameznih lastnosti IS. Odgovor na to vprašanje nam lahko v nadaljevanju pomaga pri proučevanju posameznih komponent človeške grožnje ter nato pri oblikovanju metode za predvidevanje pojavljanja bodočih človeških groženj. Slednje je ključno pri pripravi ocene tveganj bodočega IS. Takšna metoda bi avtorju nove informacijske rešitve zagotovila ključne informacije pri odločanju o potrebni informacijski varnosti v prihodnosti, še preden bi rešitev lansiral na trg oz. še preden bi se pojavile grožnje.

2 Teoretična izhodišča

Lastnik informacijskega sistema je odgovoren, da zagotovi ustrezno informacijsko varnost skladno s potrebami in pričakovanji organizacije in posameznih skupin uporabnikov. Prvi korak pri zagotavljanju varnosti je priprava ocene tveganj za vse ključne komponente sistema (Gerber & von Solms, 2005, str. 17). Obstajajo številne metodologije, ki opisujejo, kako narediti takšno oceno tveganja. Med bolj znanimi lahko izpostavimo ISO27005, OCTAVE, NIST SP800-30, IT-Grundschutz, EBIOS, CRAMM, FRAPP, Mehari, CORAS idr. (Alberts & Dorofee, 2002; Braber, Hogganvik, & Lund, 2007; BSI, 2008; Dubois, Heymans, Mayer, & Matulevičius, 2010; ISO, 2011; Peltier, 2010; Stoneburner, Goguen, & Feringa, 2002; Syalim, Hori, & Sakurai, 2009). Nekatere izmed njih so sestavni del standardov ali pa jih le ti predlagajo. Njihova glavna pomanjkljivost je nesposobnost predvidevanja tveganj, ki se bodo morda pojavila v prihodnosti zaradi stalnih sprememb v okviru IS, njegovi okolici ali inovativnih idej in pristopov potencialnih napadalcev. Prav zaradi slednjega je zelo pomembno, da dobro razumemo tudi vidik napadalca (Evans & Heinbuch, 2004, str. 59-60; Whittaker & Ford, 2006, str. 69).

Sestavni del sodobnih pristopov pri oceni tveganj je opredelitev groženj (Bruce, 2011; BSI, 2011; Buc, Corbier, & Deronzier Eric, Jouas Jean-Philippe, Molines Gerard, 2009, str. 10; Ekelhart, Fenz, & Neubauer, 2009; IST-049, 2008; Peltier, 2010; Vidalis & Jones, 2005, str. 4). Prepoznavanje groženj in ocena potencialne škode sta težki nalogi (Rees & Allen, 2008). Pri prvem si lahko pomagamo z različnimi viri, kjer so opisane tipične grožnje za IS. Opise najdemo v raznih katalogih, kontrolnih seznamih in ontologijah (BSI, 2011; Fenz, Ekelhart, & Neubauer, 2011; Peltier, 2010).

Zanimiv pristop predstavljajo metode opisovanja groženj z atributi. Metodologija OCTAVE se na primer osredotoča na različne oblike informacijskega premoženja v okviru IS. Ob tem predlaga oblikovanje profilov groženj na osnovi več opisnih atributov (npr. vrsta premoženja, napadalec, motivacija, dostop, pričakovani izid ipd.). Kljub vsemu vrednost premoženja ocenjuje le z vidika notranjega uporabnika oz. organizacije, ob tem pa ne upošteva vidika napadalca (Alberts & Dorofee, 2002, str. 3).

Podjetje Intel je razvilo podoben pristop. Opredelili so knjižnico TAL (angl. Threat Agent Library) in v njenem okviru 22 tipičnih skupin napadalcev, ki se pojavljajo pri ogrožanju sodobnih IS. Opisani so z 8 opisnimi atributi (namen, dostop, izid, omejitve, viri, sposobnost, cilj in vidnost), preko katerih lahko prepoznamo njihove cilje in možne metode napada (Casey, 2007, str. 4; Casey, Koeberl, & Vishik, 2011, str. 2017-219). Tudi v tem primeru so opisi podani pretežno z vidika organizacije. Knjižnica TAL tako le delno razkrije vidik napadalca. Podobne omejitve najdemo tudi pri drugih podobnih pristopih opisovanja groženj (Evans & Heinbuch, 2004, str. 59; Vidalis & Jones, 2005, str. 5-6).

Napadalci cilje napada prepoznajo preko lastnosti IS. Ko prepoznajo cilj, poizkušajo med lastnostmi IS prepoznati priložnosti za izvedbo napada. Sočasno s spoznavanjem IS ves čas preverjajo tudi, kakšni so potrebni viri in znanja, da bi bili pri napadu lahko uspešni. Grožnja se torej oblikuje preko prepoznavanja IS.

Dojemanje posameznih lastnosti IS se lahko močno razlikuje med posamezniki. Poleg tega posamezno lastnost lahko povezujemo z različnimi nameni in načini uporabe. Domnevamo, da napadalci v določenih lastnostih IS prepoznajo povsem nekaj drugega kot običajni uporabniki.

Pogosto se omenja, da je pogled s strani napadalca pomemben pri zagotavljanju varnosti IS. Namen običajnega uporabnika je uporabljati funkcionalnosti na način, kot je v osnovi načrtovano. Po drugi strani je namen napadalca zlorabiti sistem, zato se ob tem ne omejuje na običajen način njegove uporabe. Postavimo se lahko v vlogo potencialnega napadalca in z različnimi metodami poizkušamo poiskati čim več možnih napadov (angl. *Attack Trees*) ali potencialnih groženj (angl. Threat Trees) (Mauw & Oostdijk, 2006, str. 3).Ugotovimo lahko, da se inovativnim napadalcem odpirajo širše možnosti »uporabe« sistema kot običajnim uporabnikom. Zato je postalo pomembno razmišljati tudi o tem, česa programska oprema ne bo delala, in ne zgolj, katere funkcionalnosti bo imela (Whittaker & Ford, 2006, str. 70). V tem smislu so pomembne prav vse lastnosti IS, pomembno pa je tudi, h katerim komponentam grožnje prispevajo: h krepitvi motivacije napadalca, odpiranju priložnosti za napad ali zgolj preverjanju napadalčevih lastnih sposobnosti za izvedbo napada.

Domnevamo, da ista lastnost IS lahko predstavlja za različne posameznike drugačno vrednost in v nekaterih primerih je ta razlika lahko očitna. Za namen naše raziskave bomo predpostavili, da obstaja med posamezniki »značilna razlika« v dojemanju pomembnosti posameznih lastnosti IS takrat, ko se vrednosti v povprečju razlikujejo za vsaj 20 %. Prepogosto opazujemo IS samo z vidika običajnega uporabnika in posledično spregledamo takšne razlike v pomembnosti lastnosti. Zato postavljamo naslednjo hipotezo:

H1. V povprečju so nekatere lastnosti IS manj pomembne navadnim uporabnikom kot napadalcem. V nekaterih primerih so razlike v pomembnosti značilne.

Tudi vsi napadalci ne razmišljajo enako. Neka tipična skupina napadalcev ima lahko povsem drugačne cilje od preostalih napadalcev. Omenjeno domnevo lahko preverimo s testiranjem naslednje hipoteze:

H2. Različne skupine napadalcev v povprečju vrednotijo iste lastnosti IS različno.

Pri uporabi sistema je običajen uporabnik več ali manj osredotočen le na vsakdanje delo, ki obsega rutinsko izvajanje znanih funkcionalnosti. Po drugi strani se napadalec precej bolj poglobljeno ukvarja s sistemom, saj mora odkriti karkoli uporabnega za dosego svojega cilja. Da bi odkril čim več možnosti za izvedbo napada, mora dobiti natančno sliko o sistemu. V tem pogledu mora preveriti precej več lastnosti IS kot navaden uporabnik. Napadalec se torej ukvarja tudi s proučevanjem lastnosti, ki so večini navadnih uporabnikov nepomembne ali vsaj nezanimive. V raziskavi predpostavljamo, da je neka lastnost IS za izbrano populacijo pomembna, če jo populacija v povprečju vrednoti z več od 50 % njene maksimalne možne vrenosti. Zato postavljamo naslednjo hipotezo:

H3. Napadalci več lastnosti IS prepoznajo za pomembne kot običajni uporabniki.

Z raziskavo želimo torej preveriti, kako velike razlike obstajajo v dojemanju pomembnosti posameznih lastnosti IS med različnimi populacijami, česar iz obstoječih raziskav ni mogoče ugotoviti. Velika razlika v pomembnosti lastnosti je namreč lahko dober indikator varnostnega tveganja. V kasnejših raziskavah nam bodo ti odgovori v pomoč pri prepoznavanju posameznih komponent človeške grožnje.

3 Metoda

V raziskavi merimo pomembnost lastnosti IS za različne tipe uporabnikov. Merjenje smo izvedli nad opisi istega IS v različnih časovnih obdobjih, in sicer za sistem iz oddaljene preteklosti in današji sistem. Vsak sistem je opisan z naborom lastnosti. Ob tem smo predpostavili, da je oddaljena preteklost čas, v katerem posamezne lastnosti doživijo očitne kakovostne ali količinske spremembe. S tem želimo primerjati pomembnost posameznih lastnosti IS za izbrano populacijo, ko te doživijo očitne spremembe.

Za merilni instrument smo izbrali vprašalnik v obliki spletne ankete. Opazovani informacijski sistem je bila spletna banka največje slovenske banke. Osnovni opis današnje spletne banke je obsegal 5 lastnosti za vsako izmed naslednjih komponent sistema: strojna oprema, programska oprema, podatki, ljudje in postopki. Prednost smo dali tistim opisom sistema, ki so pomembni tako za lastnika IS kot za končne uporabnike. V naslednjem koraku smo za izbrane lastnosti poiskali enakovredne lastnosti spletne banke iz oddaljene preteklosti. Podatke za opazovani sistem smo dobili za leto 2000 (RIS, 2014). Nazadnje smo za vsako od osnovnih komponent IS izbrali po 3 lastnosti. Izbrali smo le takšne lastnosti, pri katerih smo ugotovili, da so v obdobju od leta 2000 do danes doživele očitne kakovostne ali količinske spremembe. Ostale lastnosti smo izločili iz nadaljnje obravnave.

V vprašalniku smo anketirance spraševali kako pomembne so oz. so bile po njihovem mnenju posamezne lastnosti IS za naslednje skupine napadalcev oz. uporabnikov (v oklepaju je navedeno ali gre za sistem iz oddaljene preteklosti ali za današnji sistem):

- tat (2000),
- tat (2018),
- terorist (2018) in
- običajen uporabnik (2018).

Merilni instrument smo razvili v dveh korakih. Vprašalnik za pilotno študijo je vseboval 3 lastnosti za vsako komponento informacijskega sistema. Ob tem smo namenoma dodali še kontrolno lastnost, ki se v obdobju od leta 2000 do danes ni spremenila. Ustreznost vprašalnika smo najprej preizkusili v zaprtem krogu v okviru laboratorija. Pri tem je sodelovalo 11 oseb, ki kasneje niso bile vključene v anketiranje. Na podlagi njihovih odgovorov in pripomb glede nekaterih nejasnih opisov lastnosti, smo pripravili končno različico vprašalnika. V njej smo ohranili samo 2 lastnosti za opis vsake izmed osnovnih komponent IS (strojna oprema, programska oprema, podatki, ljudje in postopki), saj smo želeli ohraniti razumno dolg čas za izpolnjevanje ankete. Končno različico lastnosti, ki smo jih vključili v anketni vprašalnik, podajata naslednja seznama:

Spletna banka leta 2000

- PROC1: Možno je sprotno plačevanje položnic in nakazovanje denarja.
- PROC2: Možna je izmenjava sporočil z bančnim operaterjem.
- CTRL: Sistem omogoča uporabo 24/7.
- USER1: Uporablja ga okrog 3.500 posameznikov.
- USER2: Uporabniki so pogosti in dolgoletni uporabniki interneta.
- DATA1: Hrani osnovne podatke o komitentih.
- DATA2: Hrani podatke o transakcijskih računih.
- SW1: Aplikacija pri delu preverja certifikat.
- SW2: Aplikacija beleži vsak vstop v spletno banko.
- HW1: Fizični strežnik se nahaja v računskem centru banke.
- HW2: Dostop je možen samo preko računalnikov s fizično povezavo.

Spletna banka 2018

- PROC1: Možno je sprotno in odloženo plačevanje ter prenašanje denarja med računi.
- PROC1: Možno je naročanje številnih bančnih storitev (trajniki, krediti, limiti, …).
- CTRL: Sistem omogoča uporabo 24/7.
- USER1: Spletno banko uporablja več kot 200.000 uporabnikov.
- USER2: Med uporabniki so od računalniških začetnikov do IT ekspertov.
- DATA1: Hrani osnovne podatke o komitentih in njihovih nakupovalnih navadah.
- DATA2: Hrani podatke o bančnih računih, karticah, vrednostnih papirjih.

- SW1: Aplikacija preverja certifikat in pri plačevanju zahteva še dodatno geslo.
- SW2: Aplikacija lahko preko SMS obvešča uporabnika o vsaki prijavi v sistem.
- HW1: Fizični strežnik se nahaja v posebej prirejenih in varovanih prostorih.
- HW2: Dostop do banke je možen tudi z mobilnimi napravami.

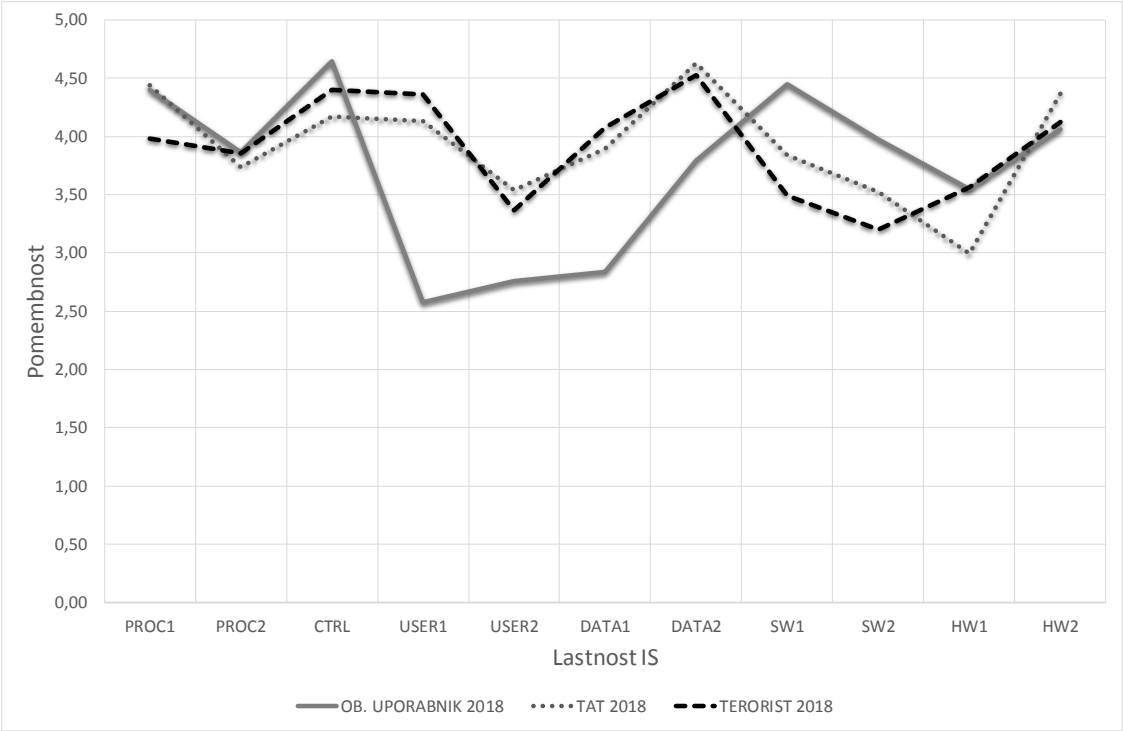
Anketiranci so imeli pri izpolnjevanju vprašalnika nalogo, da se vživijo v vlogo posameznega akterja (tat, terorist, običajni uporabnik) in ocenijo pomembnost posameznih lastnosti zanje po Likertovi lestvici (1 – nepomembno, 5 – zelo pomembno). Pri testiranju hipotez smo uporabili t-test.

Pri zbiranju empiričnih podatkov smo uporabili metodo vzorčenja »Respondent-Driven Sampling technique«, ki se uporablja za vzorčenje in ocenjevanje v skritih populacijah (Salganik & Heckathorn, 2004). Vzorec smo namreč izbrali z metodo snežene kepe. Naš namen je bil privabiti čim več ljudi, ki se dobro spoznajo na računalniško varnost ali so celo seznanjeni s postopki izvajanja napadov. Začetna semena so bili študenti na fakulteti za informatiko, ki so se prijavili na naše povabilo. Kasneje smo jih pozvali, da k izpolnjevanju povabijo svoje znance z omenjenimi znanji. Predpostavljamo, da takšen pristop ustvari dovolj reprezentativen vzorec. Težko bi za sodelovanje v takšni raziskavi pridobili prave napadalce.

4 Rezultati

Prejeli smo 111 izpolnjenih vprašalnikov. Med njimi je bilo 78 moških (70 %) in 33 žensk (30 %). Iz najmlajše starostne skupine (do 25 let) prihaja 48 anketirancev (43 %), 62 jih je iz skupine 25 – 50 let (56 %), eden pa je starejši od 50 let. Med anketiranci je bilo 51 študentov (46 %), 54 zaposlenih oseb (49 %) in 6 nezaposlenih (5 %).

Slika 1 in tabela 1 prikazujeta povprečno pomembnost posameznih lastnosti današnje spletne banke za tri različne populacije, in sicer za običajnega uporabnika, tata in terorista. Povprečno dojemanje pomembnosti lastnosti IS je v 9 od 11 primerov pri tatu in običajnem uporabniku različno (dvostranski t-test, $\alpha = 0{,}05$). V 5 primerih je lastnost pomembnejša tatu kot običajnemu uporabniku. Glede na našo opredelitev je v enem primeru lastnost značilno pomembnejša (povprečna razlika v oceni je večja od 20%) tatu kot običajnemu uporabniku (enostranski t-test, $\alpha = 0{,}05$). Ob primerjavi terorista in običajnega uporabnika se razlika v dojemanju pomembnosti pojavi pri 7 lastnostnih. V 4 primerih je lastnost pomembnejša teroristu kot običajnemu uporabniku. V enem primeru je lastnost značilno pomembnejša teroristu kot običajnemu uporabniku. Razlika v dojemanju pomembnosti lastnosti obstaja tudi med napadalcema, in sicer smo jo prepoznali pri 2 lastnostih.



Slika 1. Prikaz povprečne pomembnosti lastnosti IS za običajnega uporabnika ter posamezne tipe napadalcev.

Skladno z našo opredelitvijo v tej raziskavi je lastnost nekomu pomembna, če njena povprečna pomembnost presega 50 % maksimalne možne vrednosti. Običajen uporabnik dojema 7 od 11 lastnosti kot pomembne. Rezultati za tata razkrivajo, da dojema 9 lastnosti kot pomembne, terorist pa dojema kot pomembne prav vseh 11 lastnosti (enostranski t-test, $\alpha = 0,05$).

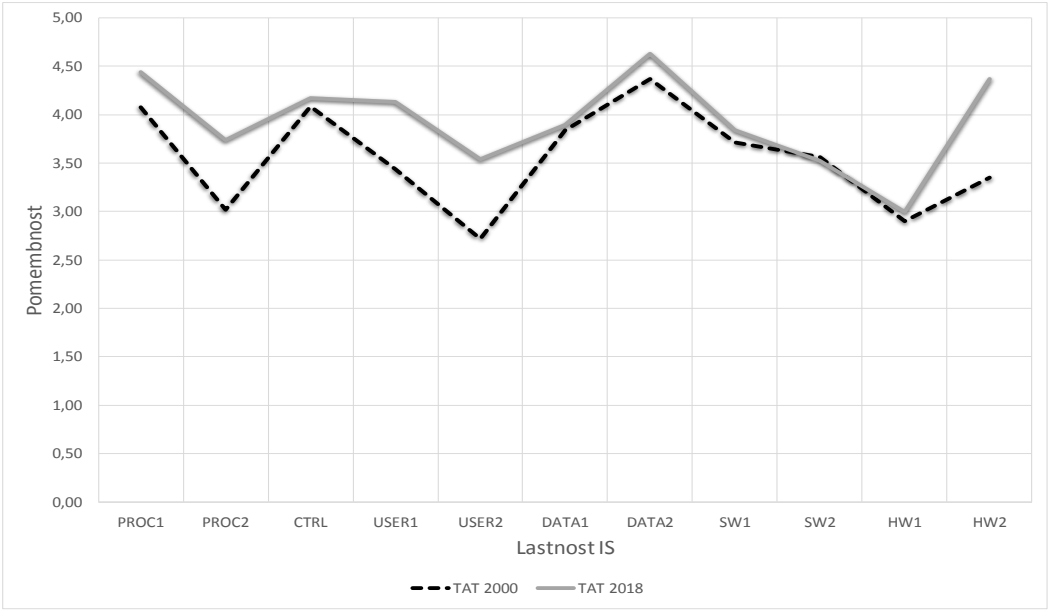
Slika 2 in tabela 2 prikazujeta pomembnost lastnosti spletne banke za tata v dveh različnih časovnih obdobjih, in sicer za sistem v letu 2000 ter današnji sistem. Lastnosti obeh sistemov se značilno razlikujejo v kakovosti ali količinsko. Lastnost z opisom *»Razpoložljivost banke je 24/7«* je nastopala kot kontrola lastnost in je bila v vključena v opisa obeh sistemov. Zato je označena z oznako CTRL. Rezultat merjenja pomembnosti kontrolne lastnosti je na obeh sistemih enak, kar dokazuje ustreznost izvedbe anketiranja. Pri ostalih lastnostih kažejo rezultati, da se je v 6 od 10 primerov povprečna pomembnost lastnosti skozi čas povečala (enostranski t-test, $\alpha = 0,05$). Rezultati so prikazani v tabeli 2.

Tabela 1. Rezultati statistične obdelave vprašalnikov pri preverjanju hipotez, ki smo jih podali v poglavju 2.

SPLETNA BANKA 2018	**PROC1**	**PROC2**	**CTRL**	**USER1**	**USER2**	**DATA1**	**DATA2**	**SW1**	**SW2**	**HW1**	**HW2**
Povp. OB.UPORABNIK 2018	4,40	3,86	4,65	2,57	2,75	2,84	3,79	4,45	3,97	3,55	4,06
Povp. TAT 2018	4,44	3,73	4,17	4,13	3,54	3,90	4,63	3,84	3,52	2,99	4,37
Povp. TERORIST 2018	3,98	3,85	4,40	4,36	3,36	4,07	4,53	3,49	3,20	3,56	4,13
H_2: OB. UPOR. <> TAT											
P vrednost, dvostranski test	0,77	0,43	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,02
Hipoteza H_2			✓	✓	✓	✓	✓	✓	✓	✓	✓
H_2: OB. UPOR. <> TERORIST											
P vrednost, dvostranski test	0,02	0,96	0,09	0,00	0,01	0,00	0,00	0,00	0,00	0,94	0,71
Hipoteza H_2	✓			✓	✓	✓	✓	✓	✓		
H_2: TAT <> TERORIST											
P vrednost, dvostranski test	0,01	0,56	0,23	0,21	0,40	0,31	0,39	0,12	0,16	0,01	0,14
Hipoteza H_2	✓									✓	
H_1: TAT > OB. UPOR.											
P vrednost, enostranski test	0,38	0,21	t < 0	0,00	0,00	0,00	0,00	t < 0	t < 0	t < 0	0,01
Hipoteza H_1				✓	✓	✓	✓				✓
H_1: TERORIST > OB. UPOR.											
P vrednost, enostranski test	t < 0	0,48	t < 0	0,00	0,00	0,00	0,00	t < 0	t < 0	0,47	0,35
Hipoteza H_1				✓	✓	✓	✓				

Tabela 2. Rezultati statističnega preverjanja razlik v povprečni pomembnosti lastnosti, merjeno v različnih časovnih obdobjih.

H_4: TAT 2018 > TAT 2000	**PROC1**	**PROC2**	**CTRL**	**USER1**	**USER2**	**DATA1**	**DATA2**	**SW1**	**SW2**	**HW1**	**HW2**
Povp. TAT 2018	4,44	3,73	4,17	4,13	3,54	3,90	4,63	3,84	3,52	2,99	4,37
Povp. TAT 2000	4,08	3,02	4,08	3,43	2,72	3,84	4,37	3,72	3,57	2,90	3,35
P vrednost, enostranski test	0,01	0,00	0,30	0,00	0,00	0,35	0,01	0,25	0,41	0,31	0,00
Hipoteza H_4	✓	✓		✓	✓		✓				✓



Slika 2. Prikaz povprečne pomembnosti lastnosti IS za tata v različnih časovnih obdobjih.

5 Razprava

Eno od naših raziskovalnih vprašanj je bilo osredotočeno na napadalčev vidik na IS. Rezultati razkrivajo nekatere osnovne značilnosti o njihovem odnosu. Prvi zaključek je, da napadalci dojemajo IS precej drugače od običajnih uporabnikov. V primeru tata smo pri 7 lastnostih odkrili razlike v dojemanju pomembnosti, kar je več kot polovica opazovanih lastnosti. Še bolj očitne razlike so v primeru terorista. Samo pri eni lastnosti nismo zaznali razlike. Ugotovitve pritrjujejo ideji, da je pri oceni tveganj smiselno upoštevati pogled napadalca.

Primerjava med tatom in teroristom potrjuje hipotezo (hipoteza H2), da obstajajo razlike v odnosu do posameznih lastnosti IS tudi med posameznimi tipi napadalcev. V naši študiji sta bili odkriti dve takšni razhajanji, kar pritrjuje ideji, da je treba posamezne napadalce obravnavati ločeno. Sklepamo lahko, da posamezne lastnosti IS vplivajo na različne elemente človeške grožnje (sposobnost, priložnost, motivacija) in posledično se napadalci odzivajo drugače. Slednje lahko preverimo v bodočih raziskavah.

Čeprav je vprašalnik vključeval le lastnosti, ki bi morale biti v osnovi zanimive običajnim uporabnikom spletne banke in lastniku IS, se je izkazalo, da je več lastnosti zanimivih tatu in teroristu. Pri nekaterih lastnostnih se je celo izkazalo, da so napadalcem lastnosti pomembne (vrednost je višja od 2,5 oz. 50 % maksimalne vrednosti), uporabniki pa so jih prepoznali kot nepomembne (npr. lastnosti USER1, USER2 in DATA1). Razlike v pomembnosti so v več primerih očitne. Na podlagi rezultatov lahko zaključimo, da napadalci najdejo med lastnostmi IS spletne banke več uporabnih lastnosti kot uporabniki (potrditev hipotez H1 in H3). Takšne lastnosti so lahko dobri indikatorji obstoja tveganja. Enako velja tudi za lastnosti IS, ki smo jih merili v različnih časovnih obdobjih, saj smo v več primerih izmerili očitne razlike. Cilj proaktivnega zagotavljanja informacijske varnosti je torej odkriti takšne lastnosti IS.

6 Zaključek

Z raziskavo smo potrdili naslednje domneve:

- napadalci dojemajo lastnosti IS bistveno drugače kot običajni uporabniki,
- napadalci prepoznajo več lastnosti IS kot pomembne kot običajni uporabniki,
- različne skupine napadalcev različno vrednotijo posamezne lastnosti IS.

Lastnosti IS, pri katerih zaznamo značilne razlike med pogledom običajnega uporabnika in pogledom potencialnih napadalcev, so lahko dober indikator tveganja. Takšne informacije lahko izboljšajo odločanje pri oceni bodočih tveganj. Domnevamo, da omenjene lastnosti prispevajo k oblikovanju človeške grožnje, ki se pojavi v nekem izbranem časovnem obdobju.

Anketiranje smo izvedli med poznavalci informacijske varnosti in ne neposredno z napadalci, kar predstavlja večjo omejitev raziskave. Izsledke raziskave bomo kljub vsemu lahko uporabili pri nadaljnjem proučevanju pomena lastnosti IS na oblikovanje človeške grožnje. Predvsem je smiselno preveriti, v kakšnem obsegu posamezne lastnosti IS prispevajo k

posameznim komponentam grožnje (motivaciji, prepoznavi priložnosti, preverjanju sposobnosti).

Reference

1. Alberts, C. J., & Dorofee, A. J. (2002). *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley.
2. Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers \& Security*, *26*(3), 219–228. https://doi.org/10.1016/j.cose.2006.10.002
3. Anderson, R. J. (2010). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
4. Blyth, A., & Kovacich, G. L. (2006). *Information Assurance: Security in the Information Environment*. Springer.
5. Braber, F. Den, Hogganvik, I., & Lund, M. (2007). Model-based security analysis in seven steps—a guided tour to the CORAS method. *BT Technology Journal*, *25*(1), 101–117.
6. Bruce, A. (2011). *Risk Management and Methodologies*. RiVidium Corporation.
7. BSI. (2008). *BSI-Standard 100-3, Risk analysis based on IT-Grundschutz*. Bundesamt fur Sicherheit in der Informationstechnik.
8. BSI. (2011). *Supplement to BSI-Standard 100-3, Version 2.5, Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses.* Bundesamt fur Sicherheit in der Informationstechnik.
9. Buc, D., Corbier, J., & Deronzier Eric, Jouas Jean-Philippe, Molines Gerard, R. J.-L. (2009). *RISK MANAGEMENT - Concepts and Methods*. CLUSIF.
10. Casey, T. (2007). Threat Agent Library Helps Identify Information Security Risks. *Intel White Paper*. USA: Intel Corporation.
11. Casey, T., Koeberl, P., & Vishik, C. (2011). Defining Threat Agents: Towards a More Complete Threat Analysis. V *ISSE 2010 Securing Electronic Business Processes* (str. 214–225). Wiesbaden, Germany: Vieweg+Teubner. https://doi.org/10.1007/978-3-8348-9788-6_21
12. Dimensional Research. (2011). *THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY : A SURVEY OF IT PROFESSIONALS*. Dimensional Research.
13. Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A Systematic Approach to Define the Domain of Information System Security Risk Management. V *Intentional Perspectives on Information Systems Engineering* (str. 289–306). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-12544-7_16
14. Ekelhart, A., Fenz, S., & Neubauer, T. (2009). AURUM: A framework for information security risk management. V *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on SystemSciences* (str. 1–10).
15. Evans, S., & Heinbuch, D. (2004). Risk-based systems security engineering: Stopping attacks with intention. *Security \& Privacy, IEEE*, *2*(6), 59–62.
16. Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In which security solutions is it worth investing? *Communications of the Association for Information Systems*, *28*(1), 329–356.

17. Frei, S., Schatzmann, D., Plattner, B., & Trammell, B. (2010). Modelling the Security Ecosystem - The Dynamics of (In) Security. V *Economics of Information Security and Privacy* (str. 79–106). Springer US. https://doi.org/10.1007/978-1-4419-6967-5_6
18. Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16–30. https://doi.org/10.1016/j.cose.2004.11.002
19. Hall, J. H., Sarkani, S., & Mazzuchi, T. a. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, *19*(3), 155–176. https://doi.org/10.1108/09685221111153546
20. ISO. (2011). *ISO 27005:2011 - Information Technology: Security Techniques - Information Security Risk Management*. ISO/IEC/JTC 1/SC 27.
21. IST-049. (2008). *Improving Common Security Risk Analysis* (Let. 323). The Research and Technology Organisation (RTO) of NATO.
22. Mann, I. (2008). *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. Gower.
23. Mauw, S., & Oostdijk, M. (2006). Foundations of Attack Trees. *Information Security and Cryptology - ICISC 2005*, *3935*(C), 186–198.
24. Miller, C. (2007). The Legitimate Vulnerability Market Inside the Secretive World of 0-day Exploit Sales. V *In Sixth Workshop on the Economics of Information Security* (str. 1–10).
25. Peltier, T. R. (2010). *Information Security Risk Analysis, Third Edition*. Taylor & Francis.
26. Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing (4th Edition)*. Upper Saddle River, NJ, USA: Prentice Hall PTR.
27. Rees, J., & Allen, J. (2008). The State of Risk Assessment Practices in Information Security: An Exploratory Investigation. *Journal of Organizational Computing and Electronic Commerce*, *18*(4), 255–277. https://doi.org/10.1080/10919390802421242
28. RIS. (2014). e-bančništvo. Pridobljeno 22. marec 2014., od http://www.ris.org/c/1357/ebancnistvo/?preid=0
29. Salganik, M., & Heckathorn, D. (2004). Sampling and estimation in hidden populations using respondent- driven sampling. *Sociological methodology*, *34*(2004), 193–239.
30. Schneier, B. (2012). The Vulnerabilities Market and the Future of Security. *Forbes*.
31. Smith, R. (2012). A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles. *Security & Privacy, IEEE*, (December).
32. Smith, S. W. (2003). Humans in the Loop. *IEEE Security & Privacy*, *1*(3), 75–79.
33. Stair, R., & Reynolds, G. (2013). *Principles of Information Systems*. Cengage Learning.
34. Steven, J. (2010). Threat Modeling - Perhaps It's Time. *IEEE Security \& Privacy*, *8*(3), 83–86. https://doi.org/10.1109/MSP.2010.110
35. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. *NIST …*. NIST.
36. Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. V *2009 International Conference on Availability, Reliability and Security* (str. 726–731). Ieee. https://doi.org/10.1109/ARES.2009.75
37. Vidalis, S., & Jones, A. (2005). Analyzing Threat Agents \& Their Attributes. V *Proceedings of the 5th European Conference on Information warfare and Security* (str. 1–15).
38. Whittaker, J. A., & Ford, R. (2006). How to think about security. *Security \& Privacy, IEEE*, *4*(2), 68–71.

39. Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security*, *16*(5), 463–483. https://doi.org/10.1108/09685220810920549

***

Andrej Dobrovoljc je doktoriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani s področja obvladovanja tveganj v informacijskih sistemih. Je samostojni podjetnik in večinoma deluje kot svetovalec ter projektni vodja na področju poslovne informatike. V več kot 20-letnem obdobju si je pridobil izkušnje s projekti v več kot 50 organizacijah različnih velikosti in z različnih poslovnih področij. Aktiven je tudi kot predavatelj in raziskovalec na Fakulteti za organizacijske študije v Novem mestu ter v gospodarstvu.

***

Abstract:
Detection of Potential Threats to the Information System

Research Question (RQ): Can the information system characteristics help us identify potential future threats?
Purpose: We want to examine the relationship of ordinary users and different groups of attackers to the properties of the information system. At the same time, we focus on measuring the importance of the information system properties for each population.
Method: We conducted a quantitative survey using a questionnaire. Descriptions of the information systems used in the questionnaire were defined on the basis of the available data on the web.
Results: We have confirmed the assumption that attackers mostly evaluate the same properties of the information system differently from the usual users. As a rule, attackers recognize in most properties more value than normal users, and in some cases these differences are obvious. Differences are also among the attackers. The results are a good basis for further research, namely checking which elements of the human threat are contributed by individual characteristics.
Organization: The properties of the observed information system where ordinary users and attackers experience obvious differences in valuation can be a good indicator of risk. By identifying such features, we can improve decision-making in risk assessment.
Society: The research aims to strengthen the belief that it is important to take into account the aspect of the attacker druring risk assessment, and to create a model of future human threats before they start designing the information system.
Originality: The survey confirms the idea that the aspect of the attacker should be taken into account in the risk assessment. The experiment showed that attackers give higher value to most of the information system properties than ordinary users.
Limitations/Future Research: We could include information security experts in the survey, rather than real attackers who are in fact a hidden population. In further research, we want to check how the characteristics of the information system contribute to individual elements of the human threat (motivation, recognition of opportunities, ability testing).

Keywords: threat, information system, attacker, risk assessment, information security.