ELEKTROTEHNIŠKI VESTNIK 87(3): 109-116, 2020
IZVIRNI ZNANSTVENI ČLANEK

Inovativni model za obvladovanje informacijskovarnostnih groženj pri uporabi informacijskih sistemov

Damjan Fujs[1,*], Simon L. R. Vrhovec[2], Damjan Vavpotič[1]

[1] *Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana, Slovenija*
[2] *Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova ulica 8, 1000 Ljubljana, Slovenija*
[*] *E-pošta: damjan.fujs@fri.uni-lj.si*

Povzetek. Uporabniki informacijskih sistemov (IS) se lahko na dnevni ravni soočajo z grožnjami informacijski varnosti, zato je treba implementirati varnostne ukrepe za uspešno obvladovanje teh tveganj. Predlagani inovativni model temelji na ugotovitvah, da je priporočljivo varnostne ukrepe implementirati s pomočjo izobraževanja in prilagajanja, ter oceni vsakega posameznega varnostnega ukrepa tako s stroškovnega vidika kot tudi z vidika njegove učinkovitosti oz. koristi za zagotavljanje informacijske varnosti. S pomočjo pregleda literature je podan vpogled v varnostne grožnje pri uporabi informacijskih sistemov ter metod za njihovo klasifikacijo oz. modeliranje, kar predstavlja osnovo za izdelavo predlaganega inovativnega modela. Trendi nakazujejo, da bo groženj zaradi pojava novih tehnologij v prihodnosti še več, kar pomeni, da bo nastala še večja potreba po kompetentnem in izobraženem kadru, ki se bo sposoben zoperstaviti grožnjam ter upravljati informacijskovarnostna tveganja in ranljivosti.

Ključne besede: modeliranje, varnost, programska oprema, podjetje, nevarnosti, organizacija, kibernetska varnost

An innovative model to manage the information systems security threats

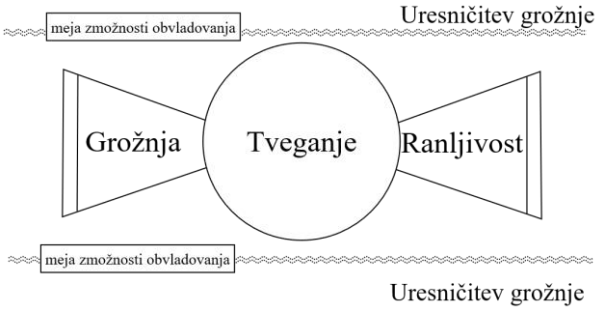
Users of information systems (IS) are daily faced with information security threats. As a response to the need to implement efficient information security measures, the paper proposes an innovative model to solve the issues through educating IS users by individually assessing each security measure in terms of its cost and efficiency or benefit for information security. Based on a literature review, an insight is given into information security threats and methods for their classification. This provided the basis for developing the proposed model to manage information security threats to IS. Judging by the current trends, threats will keep increasing in the future due to the rapidly emerging new technologies, meaning there will be an even greater need for competent and educated IS users who are able to cope with the information security threats, risks and vulnerabilities.

Keywords: modeling, security, software, enterprise, hazard, organization, cyber security, cybersecurity

1 UVOD

Grožnje informacijskim sistemom (IS) postajajo vse bolj številčne, usmerjene, prefinjene in prikrite. Po podatkih informacijskovarnostnega podjetja CyberEdge [1] približno 78 % podjetij doživi vsaj en uspešen kibernetski napad, medtem ko kar dve tretjini IT-strokovnjakov meni, da je v organizacijah nemogoče preprečiti uspešne napade in z njimi uresničitev kibernetskih groženj. Poleg tega več kot polovico vseh žrtev vdora v IS predstavlja kritična infrastruktura (organizacije javnega sektorja 16 %, zdravstvene ustanove 15 % in finančne ustanove 10 %), medtem ko preostali delež žrtev (43 %) predstavljajo manjša podjetja [2].

Slika 1 s pomočjo shematičnega prikaza izpostavlja tri ključne pojme na področju varnosti IS, ki so lahko v praksi napačno razumljeni oz. pomešani: grožnja, tveganje in ranljivost. V tem članku se bomo osredotočili na informacijskovarnostne grožnje.



Slika 1: Shematični prikaz pojmov.

Tveganje (angl. *risk*) si lahko predstavljamo kot balon, ki ga napihujejo tako grožnje (angl. *threat*) kot ranljivosti (angl. *vulnerability*). Grožnja ima potencial, da povzroči škodo, pri čemer meri na to, da čim bolj izkoristi ranljivost oz. šibkost napadenih sredstev (angl. *assets*), kar pripomore k dodatnemu tveganju [3]. Torej, večja kot je grožnja in bolj kot je ranljiv sistem, večje je tveganje,

Prejet 24. februar, 2020
Odobren 20. april, 2020

da se grožnja uresniči. Ko je groženj in ranljivosti preveč, balon preseže mejo obvladljivosti in »poči«. Cilj vsake organizacije bi moral biti, da je ta balon čim manjši, torej, da čim bolje obvladuje tveganja, grožnje in ranljivosti.

V poslovnem okolju varnostne grožnje (angl. *security threats*) pri uporabi IS predstavljajo neki dogodek ali okoliščino, ki ima zmožnost škodljivega vpliva na poslovanje ali sredstva organizacije [4]. Groženj danes ne moremo pripisovati zgolj enemu tipu uporabnika (npr. samo uporabniku mobilne naprave, osebnega računalnika, pametnega avtomobila), saj je stalna povezljivost s kibernetskim prostorom zabrisala tradicionalni pogled na digitalne naprave in ustvarila hibridne grožnje [5]. Mobilni telefon je na primer lahko hkrati računalnik in obratno. To pomeni, da ima lahko tisti, ki nam ukrade mobilni telefon, poleg dostopa do naprave hkrati tudi dostop do drugih IS, kot so računi na družbenih omrežjih, sistemi za službene zadeve, elektronska pošta itd. V tem primeru ne moremo govoriti, da je tat ukradel zgolj mobilni telefon. Zaradi tega bomo v tem članku izraz IS uporabljali kot univerzalno obliko poimenovanja za vse sisteme, sestavljene iz treh ključnih elementov: strojne opreme, programske opreme in ljudi (uporabnikov).

V preteklosti, ko še ni bilo mobilne tehnologije, se je govorilo zgolj o grožnjah, povezanih z računalniki, kot so računalniški virusi (angl. *computer virus*) in omrežni črvi (angl. *network worm*) [6]. Skupina CyberEdge letno izdaja poročila o boju proti kibernetskim grožnjam. V letu 2018 so izvedli raziskavo na vzorcu 1.200 strokovnjakov za informacijsko varnost iz vsega sveta, ki so zaposleni v podjetjih s 500 ali več zaposlenimi. Ugotovljeno je bilo, da so strokovnjaki najbolj zaskrbljeni zaradi naslednjih varnostnih groženj, od najpogostejših do manj pogostih [1]:

- zlonamerna programska oprema (virusi, črvi in trojanski konji),
- zvabljanje (angl. *phishing*) in usmerjeno zvabljanje (angl. *spear phishing*),
- izsiljevalska programska oprema (angl. *ransomware*),
- prestrezanje in zloraba elektronskih poverilnic,
- ohromitev storitve (angl. *denial of service* – DoS) in porazdeljena ohromitev storitve (angl. *distributed denial of service* – DDoS),
- napadi na spletne aplikacije (prekoračitev medpomnilnika, SQL-vrinjenje, XSS-napad),
- šifrirne grožnje (angl. *SSL-encrypted threats*),
- organizirane trajne grožnje in usmerjene grožnje,
- notranje grožnje zaposlenih,
- *zero-day* napadi (grožnje ranljivostim, ki javnosti niso znane),
- okužbe pri prenosu (nehoteno nalaganje zlonamerne kode hkrati s prenosom druge datoteke).

Pri tem je treba omeniti, da je bil zgodnji spisek oblikovan le na podlagi mnenja strokovnjakov o grožnjah in ne predstavlja aktualnih groženj, s katerimi se organizacije soočajo. Kljub temu pa je to nedvomno dober indikator, s kakšnimi težavami se lahko soočajo organizacije. Vsako organizacijo ogrožajo vse oblike informacijskovarnostnih groženj. Pri tem je pomembno, da se jih organizacije zavedajo in znajo oceniti verjetnost in posledice uresničitve posameznih groženj, saj lahko na podlagi tega sprejmejo ustrezne ukrepe za obvladovanje tveganj.

Čeprav se podjetja zavedajo potencialnih groženj, pa še vedno obstajajo ovire, ki onemogočajo učinkovito zaščito pred informacijskovarnostnimi grožnjami. Skupina CyberEdge [1] navaja sledeče ovire, od najpogostejše do najmanj pogoste:

- preveč podatkov za analizo,
- pomanjkanje kompetentnega kadra,
- pomanjkanje informacijskovarnostne ozaveščenosti,
- pomanjkljiva integracija varnostnih storitev,
- pomanjkljiva avtomatizacija procesov za detekcijo groženj,
- pomanjkljive informacije programskih orodij,
- pomanjkanje podpore vodstva,
- pomanjkanje finančnih sredstev,
- veliko lažno pozitivnih primerov,
- pomanjkanje učinkovitih rešitev na trgu.

Namen tega članka je nasloviti ranljivosti organizacij, ki izvirajo iz strani uporabnikov informacijskih sistemov. Na podlagi pregleda literature so najprej identificirane informacijskovarnostne grožnje, s katerimi se srečujejo uporabniki informacijskih sistemov. Nato je na podlagi ugotovitev pregleda literature razvito teoretično ogrodje za obvladovanje informacijskovarnostnih tveganj pri uporabi informacijskih sistemov.

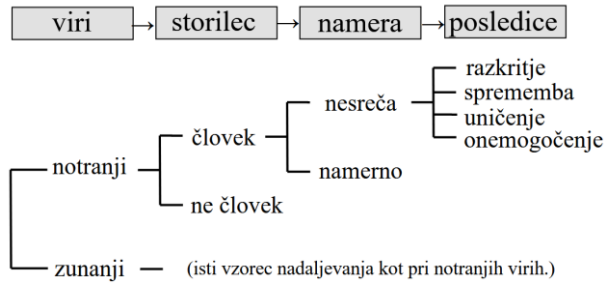
2 KLASIFIKACIJA IN MODELIRANJE INFORMACIJSKOVARNOSTNIH GROŽENJ

Ena izmed težav pri vdorih v IS je, da ne moremo natančno oceniti obsega finančnih izgub. Poleg medijsko odmevnih vdorov v IS (npr. NotPetya [5], WannaCry, Petya [7]) se vsakodnevno dogajajo »manjši vdori« in preostale oblike zlonamernih dejavnosti, ki jim organizacije pripisujejo manjši pomen (in jih morda niti ne zaznajo) in ki se zgodijo zaradi podcenjevanja groženj. Ti manjši incidenti pa lahko hitro prerastejo v večje incidente z opazno škodo za organizacijo. Zaradi tega je pomembno, da se zaposleni v organizaciji zavedajo, kaj jih ogroža pri uporabi IS in kako lahko delujejo preventivno [8].

Celovita klasifikacija groženj lahko pomaga organizacijam pri sprejemanju varnostnih ukrepov (npr. sprejetje varnostnih politik, izvajanje izobraževanja, zagotavljanje varnostnih kopij itd.), saj omogoča predvidevanje neželenih incidentov in oblikovanje scenarijev odziva. Na ta način je mogoče zmanjšati ranljivosti IS-organizacij [9].

2.1 Klasična klasifikacija varnostnih groženj

Na sliki 2 je prikazan eden izmed prvih pristopov klasifikacije groženj na področju varnosti IS [6]. Model je sestavljen iz štirih ključnih dimenzij, to so viri, storilec, namera in posledice, pri čemer vsaka dimenzija vsebuje tudi podkategorije. Dimenzija *viri* razlikuje grožnje glede na njihov izvor. Izvor grožnje je lahko notranji (npr. zaposleni) ali zunanji (npr. hekerji). Dimenzija *storilec* razlikuje med tem, ali je izvor grožnje človeške narave ali ne (npr. naravna katastrofa). Dimenzija *namera* razlikuje med namernimi grožnjami in grožnjami, ki izvirajo iz nesrečnih slučajev. Dimenzija *posledice* pa ocenjuje posledice uresničitve groženj, tj. do kakšne mere bi bili podatki kompromitirani v primeru uresničitve grožnje.

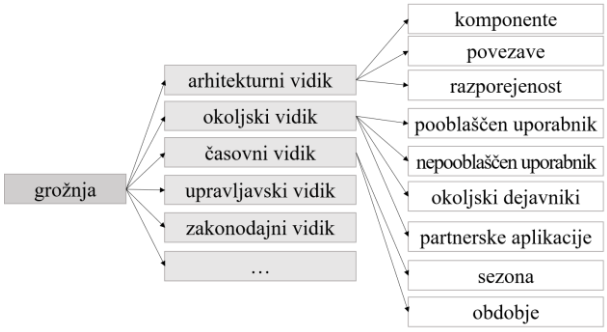


Slika 2: Klasifikacija groženj na podlagi štirih dimenzij varnosti informacijskih sistemov [6].

Ključna kritika tovrstnega pristopa je omejeno število dimenzij, kar v sodobnem svetu pri pojavu hibridnih groženj ni dovolj [8]. Predstavljeni model je sicer primeren za manjše organizacije, kjer so varnostne grožnje relativno stabilne, vendar se organizacije zaradi spreminjajočega okolja ne morejo ubraniti pred notranjimi napadi, zato je pomembno, da imajo neko vodilo pri identifikaciji groženj [8].

2.2 Večdimenzionalna klasifikacija varnostnih groženj

Da bi naslovili pomanjkljivosti omejene klasifikacije, so se začeli pojavljati večdimenzionalni [8] in stopnjevalni [9] modeli. Pri obeh vrstah klasifikacijskih modelov se lahko oddaja in prilagaja dimenzije po potrebi, s čimer se odmikajo od klasične klasifikacije varnostnih groženj.



Slika 3: Stopnjevalni model klasifikacije groženj [9].

Na sliki 3 je prikazan stopnjevalni model klasifikacije groženj, katerega glavni doprinos je uvedba klasifikacijskih kriterijev, ki omogočajo prilagodljivost modela potrebam uporabnikov [9]. Model obravnava pet glavnih vidikov: arhitekturnega, okoljskega, časovnega, upravljavskega in zakonodajnega [9]. Osnovna ideja *arhitekturnega vidika* klasificiranja groženj je poiskati grožnje, ki lahko vplivajo na arhitekturo IS. V praksi to pomeni, da iščemo grožnje, ki lahko fizično uničijo dele sistema (npr. komponente, povezave). Arhitekturni vidik je še zlasti smiselno upoštevati zaradi tega, ker so moderni IS porazdeljeni po različnih geografskih lokacijah. *Okoljski vidik* se osredotoča na izvor groženj, to je lahko pooblaščeni ali nepooblaščeni uporabnik, partnerska aplikacija ali druga okolja itd. Partnerska aplikacija je v tem primeru aplikacija, ki je sicer lahko povezana v sistem organizacije, vendar organizacija nad njo nima nadzora (npr. oskrbovalna veriga). *Časovni vidik* klasificira grožnje IS glede na čas nastanka, npr. zunaj nakupovalne sezone, ponoči ali pozimi. *Upravljavski vidik* obravnava grožnje glede na kulturo upravljavcev v podjetju (npr. da varnosti ne pripisujejo pomembnosti). Pri *zakonodajnem vidiku* je treba upoštevati specifiko zakonodaje in geografske lokacije sistema. To npr. pomeni, da je uresničitev neke grožnje v določenih državah izrecno kazniva, v drugih pa ne.

Izpostavimo lahko, da je ta klasifikacijski model prilagodljiv, kar pomeni, da je mogoče uvajati dodatne vidike in elemente glede na smotrnost. Dodatna novost modela v primerjavi s prejšnjimi je nadgradnja z novimi vidiki (npr. časovni vidik) in elementi posameznega vidika (npr. partnerske aplikacije), ki so nastali kot odgovor na nove pojavljajoče se grožnje [9].

2.3 Specifične klasifikacije varnostnih groženj

Nekateri obstoječi modeli klasifikacije varnostnih groženj se nanašajo na specifične oz. točno določene informacijske sisteme. Eden izmed takih je model kategorizacije groženj na področju uporabe mobilnega računalništva »na robu« (angl. *mobile edge computing* – MEC) [10]. MEC je poleg računalništva v oblaku, računalništva v megli in mobilnega računalništva v oblaku pogosto v lasti ponudnikov telekomunikacijskih storitev, medtem ko so lastniki drugih komponent »na robu« tipično zasebne entitete [10].

Klasifikacijski model, prikazan na sliki 4, je prilagojen za področje MEC in upošteva vse njegove ključne vidike od arhitekture do končnega uporabnika. Prilagajanje klasifikacije groženj je pomembno zaradi same narave tehnologije. Arhitektura MEC je v primerjavi s klasičnim računalništvom v oblaku decentralizirana, kar pomeni, da se mora soočati z dodatnimi varnostnimi izzivi [10]. Iz slike 4 lahko razberemo, da so sredstva, ki jih varujemo pri MEC, omrežna, virtualna in skupna infrastruktura, podatkovni centri na robu ter naprave uporabnikov. Pri vsaki od teh pa so naslovljene grožnje.

Ker še ni uveljavljene ustrezne terminologije, predlagamo nekaj novih terminov v slovenščini: tatinski

dvojnik (angl. *rogue gateway*), tatinski podatkovni center (angl. *rogue datacenter*) in tatinska infrastruktura (angl. *rogue infrastructure*). Tatinski dvojnik, center in infrastruktura delujejo podobno kot napad s posrednikom (angl. *man in the middle* – MITM), vendar v večjem obsegu, saj zahtevajo vzpostavitev infrastrukture, ki deluje na podoben način kot legitimna, čeprav to ni [10].

Slika 4: Klasifikacija groženj pri mobilnem računalništvu na robu [10].

3 INFORMACIJSKOVARNOSTNE GROŽNJE

Poleg klasifikacije groženj je treba poznati tudi, kateri tipi groženj lahko povzročijo največje tveganje in dodatno izkoristijo ranljivosti IS. Avtorji v znanstveni in strokovni literaturi navajajo številne grožnje, ki lahko pretijo uporabnikom IS. V tem poglavju bomo predstavili nekaj tipov najpogostejših groženj poslovnim IS, ki smo jih identificirali na podlagi pregleda literature.

3.1 Identificirane grožnje v znanstveni literaturi

V tabeli 1 so prikazani rezultati pregleda, pri čemer so izpostavljeni avtorji raziskav in obravnavani IS, identificirane grožnje ter informacijskovarnostni ukrepi za ublažitev groženj, ki so jih avtorji izpostavili.

Iz tabele 1 lahko razberemo, da imamo pri vseh vrstah IS podobne grožnje. Do novih oz. bolj sofisticiranih groženj prihaja pri sodobnih tehnologijah, kot so pametna mesta in vesoljske misije, saj imamo opravka s povezanostjo številnih naprav. Pravimo, da prihaja do t. i. hibridnih groženj, ki jih lahko izvajajo tako navadni posamezniki kot državni uslužbenci [5]. Za varnost je treba poskrbeti na vseh treh ključnih ravneh: državni, organizacijski in osebni [20]. V literaturi je mogoče opaziti, da je možno en tip grožnje razvrstiti na več različnih dimenzij oz. vidikov.

3.2 Identificirane grožnje v strokovni literaturi

Ob znanstveni literaturi je smiselno podatke iskati v strokovnih in drugih interesnih združenjih, saj razpolagajo z dragocenimi podatki iz prakse. Ena izmed takih relevantnih organizacij je Agencija Evropske unije za kibernetsko varnost (angl. *European Union Agency for Cybersecurity* – ENISA). Po podatkih ENISA [7] so v

Tabela 1: Informacijskovarnostne grožnje.

Vir / Grožnje
Narayana idr. (2010) [11]: bolnišnični IS
× Izpad elektrike, izpad omrežja, zastarelost tehnologije, napake v programski in strojni opremi, slaba kakovost storitev, pomanjkanje izobraževanja, zlonamerna programska oprema, prestrezanje komunikacije, maskiranje, nepooblaščen dostop do podatkov, zanikanje napak zaposlenih, socialni inženiring, pomanjkanje kadra, terorizem, naravne nesreče.
Vrhovec (2016) [12]: mobilne naprave
× Zlonamerne aplikacije, škodljiva programska oprema, socialni inženiring, fizično upravljanje mobilne naprave, družbena omrežja, predhodno nameščena programska oprema, vsiljena elektronska pošta, izguba ali tatvina mobilne naprave, poškodovanje ali uničenje mobilne naprave, povezave kratkega dosega, brezžično omrežje, kompromitiran operacijski sistem.
Parkinson idr. (2017) [13]: pametni avtomobili
× Lažno predstavljanje, napad na gesla, ohromitev storitve, napadi na omrežne protokole, zvabljanje, zlonamerna posodobitev programske opreme, oddaljen dostop, senzorji, napad na GPS.
Buslowska idr. (2017) [14]: poslovni IS
✓ Nedovoljen dostop do podatkov pooblaščenih in nepooblaščenih oseb, pomanjkanje nadzorov dostopa, naravne katastrofe, napake strojne opreme.
Zatti (2017) [15]: varnost vesoljskih misij (satelitov)
✓ Vesoljsko vreme, blizu zemeljski predmeti, satelitsko sledenje, izguba ali motnja navigacije, računalniški virusi, ohromitev storitve, lažno predstavljanje, motenje telekomunikacije, nepooblaščen dostop.
Pan idr. (2018) [16]: industrija IT
× Razkritje informacij.
Fujs in Markelj (2018) [17]: pametna mesta
× Modifikacija podatkov, kraja identitete, napad s posrednikom, lažno predstavljanje, vstavljanje lažnih podatkov, prisluškovanje, ohromitev storitve, zlonamerna programska oprema.
Liang idr. (2019) [18]: pregled literature
× Tatvina mobilne naprave, neželena e-pošta, vdori v IS, vohunska programska oprema, kraja identitete, zvabljanje.
Crossler idr. (2019) [19]: računalniški sistemi
✓ Kraja identitete, izguba podatkov, znižanje zmogljivosti računalnika.

Legenda: U – varnostni ukrepi; × ni izpostavljenih varnostnih ukrepov, ✓ izpostavljeni varnostni ukrepi

letu 2018 na področju Evropske unije prevladovale grožnje, ki jih povzema tabela 2, v kateri je prikazan tudi trend oz. primerjava varnostnih groženj med letoma 2017 in 2018. Čeprav se v poročilu ne omenja izrecno grožnje poslovnim IS, gre za grožnje, ki so relevantne tudi za področje poslovnih IS.

Tabela 2: Pregled najpogostejših varnostnih groženj [7].

Mesto	Grožnja	Trend
1	Zlonamerna programska oprema	➲
2	Spletni napadi	➲
3	Napadi na spletne aplikacije	➲
4	Zvabljanje	➲
5	Ohromitev storitve	⬆
6	Neželena e-pošta	⬇
7	Omrežje robotskih računalnikov	⬆
8	Razkritje podatkov	⬆
9	Notranje grožnje	➲
10	Fizična raven groženj (poškodovanje, kraja, izguba)	➲
11	Uhajanje informacij	⬆
12	Kraja identitete	➲
13	Ugrabitev kripto rudarjenja	NOVO
14	Izsiljevalska programska oprema	⬇
15	Spletno vohunjenje	➲

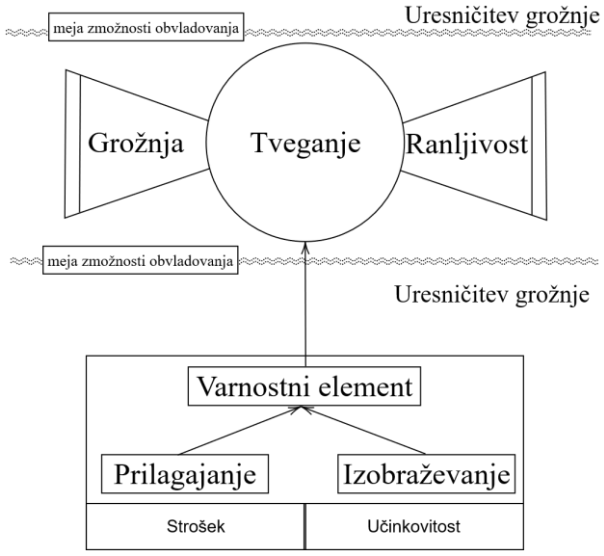
Legenda: ⬆ narašča, ⬇ pada, ➲ nespremenjeno

Iz tabele lahko razberemo, da je prišlo do bistvenih sprememb v pogostosti groženj. Pojavila se je nova varnostna grožnja, imenovana ugrabitev kriptorudarjenja (angl. *cryptojacking*), pri kateri gre za ugrabitev procesorske moči žrtvinega računalnika z namenom rudarjenja kriptovalut, brez privolitve in vedenja žrtve. Razberemo lahko tudi, da je prišlo do porasta ohromitev storitve, omrežja robotskih računalnikov (angl. *botnet*) in uhajanja informacij. Morda je spodbudna novica to, da sta upadli izsiljevalska programska oprema in neželena e-pošta. Pri interpretaciji tovrstnih podatkov moramo biti previdni, saj je lahko upad groženj posledica pojavitve novih, tudi hibridnih groženj ali še bolj sofisticiranih groženj, ki jih je težje zaznati. Lahko pa gre tudi za pokazatelja, da so drugi tipi groženj bolj aktualni. Npr. ugrabitev rudarjenja kriptovalut je do določene mere nadomestila napade z izsiljevalsko programsko opremo zaradi manjšega tveganja, napadi z izsiljevalsko programsko opremo pa so se bolj osredotočili na tarče z večjo potencialno dodano vrednostjo.

4 MODEL ZA OBVLADOVANJE INFORMACIJSKOVARNOSTNIH GROŽENJ PRI UPORABI INFORMACIJSKIH SISTEMOV

Tveganje, da se grožnja uresniči, narašča s številom in resnostjo groženj ter ranljivostjo IS. Za obvladovanje tveganj je pomembno upoštevati ključne procese, ki so povzeti v nadaljevanju. Prvič, pomembno je, da uporabniki IS poznajo grožnje, saj razumevanje groženj pomaga učinkovito obvladovati tveganja. Drugič, k uspešnemu obvladovanju pripomorejo izbrani varnostni ukrepi oz. *varnostni elementi*, ki so odziv na grožnjo. V številnih raziskavah je bilo dokazano, da poznavanje groženj vpliva na namero o samozaščiti oz., bolje povedano, tisti, ki se zavedajo groženj, so bolj pripravljeni uporabiti zaščitne ukrepe v primerjavi s tistimi, ki grožnje manj poznajo [21]–[23]. Smiselna je tudi uporaba najbolj ustreznih varnostnih elementov, saj ni nujno, da je vsak element enako učinkovit. V tem delu torej obstaja možnost, da se izbere en varnostni element, hkrati pa se določi še dva alternativna. To je smiselno, saj so nekateri varnostni elementi tehnološki (npr. požarni zid), drugi pa socio-tehnološki, torej povezani z obnašanjem ljudi (npr. da se gesel ne zapisuje na papir na vidnih mestih).

V tem prispevku predlagamo nov inovativni model za obvladovanje groženj pri uporabi IS, prikazan na sliki 5. Da bi izbrali primerne varnostne elemente, je potrebno poznavanje klasifikacije groženj, kar olajša obvladovanje tveganj, hkrati pa je treba poznati tudi tipe groženj, saj se navezujejo na tveganja. Na podlagi identifikacije in klasifikacije groženj lahko sklepamo, da je nekatere varnostne elemente možno prilagajati v večji ali manjši meri oz. težje ali lažje kot druge varnostne elemente. Če ponazorimo s primerom: moč gesel kot varnostnega elementa je težko prilagajati, lahko pa poskrbimo za izobraževanje o tem, kakšna so močna in varna gesla ter kaj so dobre prakse na področju zaščite (npr. uporaba dvofaktorske avtentikacije). Tako je izobraževanje neka univerzalna oblika naslavljanja varnostnih tveganj, ki omogoča izobraževanja tako o uporabi kot tudi prilagajanju izbranega varnostnega elementa.



Slika 5: Model za obvladovanje informacijskovarnostnih groženj pri uporabi informacijskih sistemov.

Predlagani model je osnovan na »personalizirani varnosti«, njegova temeljna ideja je približati kibernetsko varnost individualni ravni [24]. To pomeni, da se vseh ljudi ne izobražuje oz. usposablja na enak način, ampak se metode in materiale prilagaja potrebam vsakega posameznika ali skupine posameznikov [24]. Čeprav je bilo že v eni od prvih študij o klasifikaciji groženj pri uporabi IS [6] omenjeno, da je izobraževanje uporabnikov eden od najpomembnejših preventivnih varnostnih elementov [4], je treba upoštevati tudi stroške in učinkovitost posameznih vpeljanih varnostnih elementov. Predlagani model bi lahko dal boljše rezultate pri upravljanju tveganj, saj ni smiselno vztrajati pri potratnih in neučinkovitih oziroma nekoristnih metodah varovanja IS. Tudi posamezniki so bolj pripravljeni sodelovati v procesu izobraževanja, ki ga dojemajo kot učinkovitega, in ne stroškovno potratnega [19]. Še več, poleg usposabljanja o varni uporabi IS je treba posameznike izobraziti o smiselnosti, učinkovitosti in stroškovni nepotratnosti varnostnih ukrepov [19].

V tem primeru predpostavljamo, da je treba za uspešno obvladovanje tveganj sprejeti oz. uvesti varnostne elemente, prilagojene tveganjem in drugim potrebam za zaščito informacijskih sredstev[1]. Še več, prilagajanje je smiselno tudi zaradi različnih izkušenj in predznanj uporabnikov in/ali operaterjev varnostnega elementa. Hkrati predpostavljamo, da je treba uporabnike in/ali operaterje varnostnega elementa ustrezno izobraziti oz. usposobiti za njihovo uporabo. Vzemimo za primer uporabo močnih gesel kot enega izmed številnih možnih varnostnih elementov in hkrati najpogostejši minimalni standard zaščite pri uporabi IS. Uporabnike IS je smiselno izobraževati in jih usposabljati o tem, kako sestaviti močno geslo, kako ga ne shranjevati, zakaj ne uporabljati preprostih gesel, zakaj ne uporabljati enakega gesla za več IS hkrati itd. Pri tem pa je izobraževanje smiselno prilagajati znanju in izkušnjam uporabnikov. Izobraževanje o varnih geslih je lahko namreč bolj učinkovito, če je prilagojeno predznanju in prepričanjem izobraževanih uporabnikov. Tako je nekaterim uporabnikom treba dokazati, da slabo geslo lahko škoduje, kar lahko storimo na primer s praktičnim prikazom razbijanja preprostih gesel.

5 INFORMACIJSKOVARNOSTNI TRENDI IN IZZIVI

Trendi nakazujejo, da bo treba v prihodnje upoštevati tudi grožnje, ki jih je z navadnimi identifikacijskimi mehanizmi (npr. klasifikacija že znanih groženj) težko odkriti. Tak primer je na primer distribucija zlonamerne programske opreme s pomočjo steganografije [25], grožnje raznovrstnim pametnim sistemom, kot so pametni avtomobili [13] in pametna mesta [17], grožnje zoper infrastrukturo na robu (angl. *edge computing* – EDGE) [10] itd. Sodobna tehnologija pa ni omejena zgolj na zemeljsko informacijsko infrastrukturo, zato je v prihodnosti mogoče pričakovati porast vesoljske tehnologije in misij, posledično pa tudi groženj [15]. V povezavi s tem se že omenja pojem »astro hekerji« (angl. *astro-hackers*), kar pomeni, da lahko pričakujemo povečanje zlonamernih aktivnosti, usmerjenih tudi proti vesoljski tehnologiji [15].

Ključni izzivi na področju klasifikacije groženj bi lahko bili usmerjeni v iskanje učinkovitih metodologij oz. storitev na področju zaznave groženj (angl. *threat intelligence services*). Tovrstni pristopi omogočajo učinkovitejšo zaznavo groženj, oceno varnostnih opozoril in odločanje o načinu odziva na opozorila [1]. Čeprav je programska oprema za avtomatizirano zaznavo groženj v porastu [1], pa še zdaleč ni mogoče pozabiti na človeka, kar nakazuje na to, da bo še vedno veliko povpraševanja po usposobljenih kadrih za zagotavljanje informacijske varnosti. Industrija informacijske in kibernetske varnosti namreč še vedno ne more zagotoviti dovolj izobraženega kadra za zadovoljitev potreb trga po zagotavljanju informacijske varnosti oz. boju proti informacijskovarnostnim grožnjam [1]. To tudi nakazuje, da bo treba zagotoviti sredstva in človeški kapital za izobraževanje, hkrati pa motivirati mlade za izbiro tovrstne usmeritve in sprejeti strateške ukrepe za obvladovanje bega možganov.

Temam, ki jih lahko zasledimo na spletni strani ENISA [26], bo treba v prihodnosti nameniti več pozornosti, tako v akademski sferi kot v industriji. Gre za tematike s področij sodobnih tehnologij, kot je varnost industrije 4.0, varnost interneta stvari (angl. *internet of things* – IoT), mobilna omrežja 5G, kibernetska varnost pristanišč, psevdonimizacija, standardizacija itd. Kot

[1] Sredstva so vsi sistemi, ki jih je smiselno zaščititi, saj lahko v nasprotnem primeru pride do izgube, poškodbe ali uničenja informacij in posledično tudi do znižanja sredstev neke organizacije.

lahko razberemo iz vsakdanjega življenja, število naprav, povezanih v splet, stalno narašča, s tem pa premočrtno naraščajo tudi z njimi povezani informacijskovarnostni izzivi.

6 SKLEP

Ta prispevek se osredotoča na informacijskovarnostne grožnje pri uporabi poslovnih IS. V ta namen je bil izveden pregled tako znanstvene kot tudi strokovne literature. Za celovito razumevanje tematike je v tem prispevku najprej izpostavljena ključna terminologija, ki je tudi shematično prikazana. V znanstveni in strokovni literaturi prihaja do različnih interpretacij besed, kot so ranljivost, grožnja in tveganje. Pri nekaterih pojmih prihaja do dihotomije, saj na primer »notranja grožnja« [7] lahko pomeni hkrati grožnjo in tudi ranljivost. Prav tako tudi v primeru »družbenih omrežij« [12], saj lahko zaradi nezadostnih varnostnih mehanizmov pride do ranljivosti, hkrati pa do groženj, če jih spletni napadalci uporabljajo kot orodje pri napadu z uporabo socialnega inženiringa. Nato so v prispevku predstavljeni klasifikacija groženj, torej metodologija, kako klasificirati grožnje, in tipi informacijskovarnostnih groženj. V nadaljevanju se prispevek osredotoči na priložnosti za izboljšanje procesov obvladovanja informacijskovarnostnih groženj. Ključen rezultat naše raziskave je inovativni model za obvladovanje informacijskovarnostnih groženj pri uporabi IS, ki temelji na prilagajanju izobraževanja oz. usposabljanja. Predlagani inovativni model obvladovanja groženj bo v prihodnjih raziskavah tudi empirično preverjen.

LITERATURA

[1] CyberEdge, "2019 Cyberthreat Defense Report," *CyberEdge Group*, 2019. [Online]. Available: https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf.

[2] Verizon, "2019 Data Breach Investigations Report," New York, 2019.

[3] L. A. (Tony) Cox, Jr, "Some Limitations of 'Risk = Threat × Vulnerability × Consequence' for Risk Analysis of Terrorist Attacks," *Risk Anal.*, vol. 28, no. 6, pp. 1749–1761, Dec. 2008.

[4] M. E. Whitman and H. J. Mattord, "Threats to Information Protection - Industry and Academic Perspectives: An Annotated Bibliography," *J. Cybersecurity Educ. Res. Pract.*, no. 2, pp. 1–33, 2016.

[5] I. Linkov *et al.*, "Applying Resilience to Hybrid Threats," *IEEE Secur. Priv.*, vol. 17, no. 5, pp. 78–83, Sep. 2019.

[6] K. D. Loch, H. H. Carr, and M. E. Warkentin, "Threats to Information Systems: Today 's Reality, Yesterday 's Understanding," *MIS Quartely*, vol. 16, no. 2, pp. 173–186, 1992.

[7] ENISA, "ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends," Heraklion, Greece, 2019.

[8] M. Jouini, L. B. A. Rabai and A. Ben Aissa, "Classification of Security Threats in Information Systems," *Procedia Comput. Sci.*, vol. 32, pp. 489–496, 2014.

[9] M. Jouini and L. Ben Arfa Rabai, "A Scalable Threats Classification Model in Information Systems," in *Proceedings of the 9th International Conference on Security of Information and Networks - SIN '16*, 2016, vol. 20-22-July, pp. 141–144.

[10] R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[11] G. Narayana Samy, R. Ahmad and Z. Ismail, "Security Threats Categories in Healthcare Information Systems," *Health Informatics J.*, vol. 16, no. 3, pp. 201–209, Sep. 2010.

[12] S. Vrhovec, "Safe Mobile Device Use in the Cyberspace / Varna uporaba mobilnih naprav v kibernetskem prostoru," *Elektroteh. Vestn. / Electrotech. Rev.*, vol. 83, no. 3, pp. 144–147, 2016.

[13] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[14] E. Buslowska and I. Nowak, "The Analysis of Potential Threats to Information Systems and Countermeasures," *Logist. Transp.*, vol. 36, no. 4, p. 15, 2017.

[15] S. Zatti, "The Protection of Space Missions : Threats and Cyber Threats," in *Information Systems Security, ICISS 2017*, 2017.

[16] Y. Pan, P. Huang and A. Gopal, "New Entry Threats and Information Disclosure: Evidence from the U.S. IT Industry," *Int. Conf. Inf. Syst. 2018, ICIS 2018*, pp. 1–16, 2018.

[17] D. Fujs and B. Markelj, "Privacy in Smart Cities or Privacy for Smart People?," *J. Crim. Justice Secur.*, vol. 20, no. 1, pp. 5–24, 2018.

[18] H. Liang, Y. Xue, A. Pinsonneault and Y. Wu, "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective," *MIS Quartely*, vol. 43, no. 2, pp. 373–394, 2019.

[19] R. E. Crossler, F. Bélanger and D. Ormond, "The Quest For Complete Security: An Empirical Analysis of Users' Multi-layered Protection From Security Threats," *Inf. Syst. Front.*, vol. 21, no. 2, pp. 343–357, Apr. 2019.

[20] D. Fujs, A. Mihelič and S. L. R. Vrhovec, "The power of interpretation: Qualitative methods in cybersecurity research," in *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019)*, 2019, p. 10.

[21] A. Mihelič and S. Vrhovec, "A model of self-protection in the cyberspace / Model samozaščite v kibernetskem prostoru," *Elektroteh. Vestn. / Electrotech. Rev.*, vol. 85, no. 1–2, pp. 13–22, 2018.

[22] D. Fujs, A. Mihelič and S. Vrhovec, "Social network self-protection model: What motivates users to self-protect?," *J. Cyber Secur. Mobil.*, vol. 8, no. 4, pp. 467–492, 2019.

[23] D. Fujs, S. Vrhovec and A. Mihelič, "What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats," in *Proceedings of the Central European Cybersecurity Conference 2018 on - CECC 2018*, 2018, pp. 1–6.

[24] S. Furnell and I. Vasileiou, "Security Education and Awareness: Just Let Them Burn ?," *Netw. Secur.*, vol. 2017, no. 12, pp. 5–9, 2017.

[25] K. Cabaj, L. Caviglione, W. Mazurczyk, S. Wendzel, A. Woodward and S. Zander, "The New Threats of Information Hiding: The Road Ahead," *IT Prof.*, vol. 20, no. 3, pp. 31–39, May 2018.

[26] ENISA, "Publications," *European Union Agency for Cybersecurity*, 2020. [Online]. Available: https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0. [Accessed: 11-Feb-2020].

[27] Slovensko društvo informatika, “Islovar,” *Slovenski terminološki slovar informatike, informacijske tehnologije in telekomunikacij*, 2020. [Online]. Available: http://www.islovar.org/islovar. [Accessed: 11-Feb-2020].

Damjan Fujs je doktorski študent in asistent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova raziskovalna področja zajemajo varnost informacijskih sistemov (IS), metodologije razvoja IS, prilagojeno usposabljanje in izobraževanje za varno rabo IS ter kibernetsko in informacijsko varnost.

Simon Vrhovec je docent na Fakulteti za varnostne vede Univerze v Mariboru. Leta 2015 je doktoriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. V letih 2018 in 2019 je sopredsedoval mednarodni konferenci *Central European Cybersecurity Conference* (CECC). Od leta 2019 je član usmerjevalnega odbora *European Interdisciplinary Cybersecurity Conference* (EICC) ter član uredniškega odbora revije *Journal of Cyber Security and Mobility*. Njegova glavna raziskovalna področja so človeški dejavniki v kibernetski varnosti, razvoj varne programske opreme, agilne metode, odpor do sprememb in zdravstvena informatika.

Damjan Vavpotič je izredni profesor na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegovo raziskovalno delo vključuje področja metodologije razvoja programske opreme in njihovega sprejemanja vključno z razvojem varnih informacijskih sistemov, sprejemanje metod e-učenja ter napredne metode analize podatkov v zdravstvu in turizmu. Je član programskih odborov mednarodnih konferenc s področja računalništva in informatike. Objavil je več kot 50 člankov v revijah in na konferencah. Za leto 2019 je prejel nagrado Thea Sinclair Award for Journal Article Excellence pri podjetju Sage Publishing.