Darko Matotek, dipl. oec.[1]

UDK 316.776.32
Pregledni članak

ANALIZA UPORABE TEHNIKA TEORIJE NEUTRALIZACIJE U KRŠENJU INFORMACIJSKE SIGURNOSTI

Sažetak

Teorija neutralizacije pojavljuje se 1957. godine na području kriminologije. Teorija objašnjava ponašanje osoba koje krše pravila i propise, ali sebe ne vide kao nekoga tko je prekršitelj pravila i propisa. U pojedinim tehnikama nalaze opravdanje za sebe i svoje postupke i na neki se način odriču odgovornosti. U sklopu ovog rada s pomoću anketnog upitnika, hipotetskog scenarija i pitanja intenziteta utvrđuje se da li osobe primjenjuju teoriju neutralizacije na svoje ponašanje glede kršenja pravila informacijske sigurnosti. U drugom dijelu upitnika ispituje se svjesnost ispitanika o značenju pojma jake zaporke, kao i o sigurnim načinima postupanja sa zaporkom.

Ključne riječi: informacijska sigurnost, zaporka, teorija neutralizacije

1 Student doktorskog studija
Fakultet organizacije i informatike Varaždin
E-mail: dmatotek@foi.hr

1. Uvod

Sigurnost informacijskog sustava pojedine tvrtke ovisi o nizu čimbenika. U suvremenom načinu poslovanja sve je važnija softverska podrška poslovanju. Razmjerno tomu sve više se važnih informacija za opstojnost same tvrtke ugrađuje u informacijski sustav. Bez obzira na važnost tehničke razine implementacije informacijskog sustava, i do savršenstva razvijenih metoda enkripcije, i same tehničke razine sigurnosti, još uvijek s tim sustavima mora raditi čovjek. Čovjek, odnosno zaposlenik konkretne tvrtke, predstavlja najslabiju kariku u lancu informacijske sigurnosti. Iskorištavajući ljudske slabosti zbog kojih je žrtva u stanju umanjiti ili u potpunosti zanemariti provjeru autentičnosti napadača, on vrlo lako može komunikacijom sa zaposlenikom ili uz lošu politiku zaporki ući unutar ciljanoga informacijskog sustava. Neke od mjera za smanjenje rizika bile bi donošenje kvalitetne sigurnosne politike, efikasnom edukacijom zaposlenika i korisnika informacijskog sustava.

Ovaj se rad razvija u dva smjera. Prvo se promatraju opravdanja koja osobe navode za kršenje pravila informacijske sigurnosti korištenjem teorije neutralizacije u šest tehnika koje su dalje u radu detaljnije pojašnjene. S druge strane, ispituje se svjesnost osoba o načinima korištenja i kreiranja zaporki za pristup na računalo i na aplikacije u koje su ovlaštene pristupati

Cilj rada je istražiti primjenu jedne teorije, koja izvorno potječe iz kriminologije, na informacijsku sigurnost, i usporediti rezultate s drugim autorima koji su istraživali slično područje.

Postavljaju se sljedeća istraživačka pitanja: Zašto ljudi krše pravila informacijske sigurnosti? Je su li možda nesvjesni toga kako bi trebala izgledati jaka zaporka i kako s njom trebaju postupati? Kako racionaliziraju svoje ponašanje? Istraživanje ne daje potpuni odgovor na sva pitanja, ali predstavlja jedan mali pomak u pravom smjeru.

Rad je komponiran tako da nakon uvoda s hipotezama istraživanja slijedi teorijski okvir u kojem se ukratko objašnjavaju osnovne tehnike teorije neutralizacije i definira se što predstavlja jaku zaporku, nakon toga navode se metodologija i tehnologija istraživanja, rezultati i ograničenja istraživanja te se na kraju izvode zaključci.

Hipoteza prvog dijela istraživanja H_1 : O*sobe za kršenje pravila informacijske sigurnosti opravdanje nalaze korištenjem tehnika teorije neutralizacije.*

Drugi dio rada analizira svjesnost ispitanika o tome što predstavlja snagu zaporke, kako se formira zaporka, što se preporučuje koristiti u zaporkama, kao i načine postupanja sa zaporkama vezanim uz njihovu sigurnosti. Iz toga se izvode dvije hipoteze.

$H_{2\text{-}1}$: *Ispitanici znaju kako se formira snažna zaporka.*

$H_{2\text{-}2}$: *Ispitanici postupaju sa svojim zaporka*ma za pristup na računalo na preporučeni način.

2. Teorijski okvir

Za potrebe ovog istraživanja korištena je literatura odnosno znanstveni članci s on-line baza znanstvenih članaka koji su bili dostupni autoru. Na početku ovog poglavlja definira se teorija neutralizacije.

2.1. Teorija neutralizacije

Prvi put je predstavljena u radu Davida Matze i Gresham Sykesa 1957. godine u vrijeme kad su navedeni autori proučavali maloljetničku delikvenciju. Po toj teoriji ljudi, iako su svjesni da čine nešto protuzakonito, nastoje opravdati svoje ponašanje korištenjem različitih tehnika poput

- Denial of responsibility (Poricanje odgovornosti).
  Tom tehnikom osoba racionalizira svoje ponašanje na način da kaže da je to izvan njezine kontrole. Prekršitelj vidi sebe kao biljarsku kuglu koju okolnosti guraju u različite situacije.
- Denial of injury (Poricanje štete)
  Tom tehnikom osoba prekršitelj opravdava svoje ponašanje minimizirajući štetu koju je počinila.
- Defence of necessity (Obrana neizbježnošću)
  Temelji se na opravdanju da ako se kršenje pravila vidi kao neizbježno, onda se osoba ne bi trebala osjećati krivom ako to i učini: npr. zaposlenici mogu tvditi da nisu imali dovoljno vremena za poštivanje Politika informacijske sigurnosti zbog kratkih rokova za dovršenje posla.
- Condemnation of the Condemners (Osuda onih koji me osuđuju)
  Osoba neutralizira svoje ponašanje na način da optužuje onoga koji ga napada: npr. zaposlenik može tvrditi da je opravdano prekršiti neko pravilo informacijske sigurnosti koje je neopravdano.
- Appeal to higher loyalties (Lojalnost višim

ciljevima)
Ovu tehniku koriste osobe koje osjećaju da su u nedoumici koju moraju riješiti kršenjem zakona ili propisa. Osoba tvrdi da je njezino ponašanje u cilju većeg dobra s dugoročnim posljedicama koje će opravdati njezine postupke: npr. osoba tvrdi da mora prekršiti pravila informacijske sigurnosti da bi dovršila posao.

- Metaphor of the Ledger (Saldiranje dobrih i loših djela)
Koristi ideju da dobra djela kompenziraju loša djela. Npr. zaposlenici mogu opravdati povremeno surfanje internetom svojim dobrim radnim rezultatima.

U svojem radu Sipnen i Vance [2010] istražuju mogućnosti primjene tehnika neutralizacije kao opravdanja za postupke osoba koje iako krše pravila informacijske sigurnosti sebe vide kao osobe koje poštuju ta pravila. Prema njihovim rezultatima teorija neutralizacije puno bolje objašnjava predispoziciju osobe da krši pravila informacijske sigurnosti u odnosu na suprotstavljenu teoriju zastrašivanja (sram, neformalne i formalne sankcije).

Zbog iznimne važnosti za drugi dio rada temeljem raspoložive literature definiraju se ključni pojmovi kao i načini njihovoga proučavanja u prethodnim istraživanjima.

2.2. Zaporka

Postavlja se pitanje: Što je jaka zaporka (strong password)?

Općenito se u literaturi jakom zaporkom smatra ona koja ima najmanje osam znakova i u kojoj se koristi kombinacija velikih i malih slova, brojki i posebnih znakova.

Na temelju istraživanja u koje je bilo uključeno skoro 900 zaposlenika trgovačke tvrtke Hoonekker et. al. (citirano prema McCrohan et al [2010;26]) utvrđeno je da ispitanici koriste ili jednostavnu zaporku koju je lako zapamtiti i lako probiti ili koriste složenu zaporku koju je teško zapamtiti. Dodatno je utvrđeno da ispitanici često:

- Koriste istu zaporku uvijek
- Koriste relativno jednostavne zaporke
- Ponovno koriste stare zaporke
- Zapisuju zaporke ili na papirić ili u datoteku bez dodatne zaštite
- Dijele zaporke s kolegama.

Autori dodatno primjećuju da je stvarnost vjerojatno još i gora jer ispitanici nisu željeli priznati da krše pravila.

S druge strane u istraživanju koje je proveo Schneider 2006. godine (citirano prema McCrohan et al [2010;26]) proučavajući 34.000 korisničkih imena i zaporki na društvenoj mreži MySpace, utvrđeno je da 65% svih zaporki sadržava osam znakova ili manje. Najčešće korištene zaporke su bile: password1, abc123, myspace1 i password.

Istraživanje interesantno za ovaj rad [McCrohan et al;2010;31] promatra povezanost svjesnosti internetskih prijetnji i ponašanja koje se tiču informacijske sigurnosti koje se utvrđuju poboljšanjem jakosti zaporke. Istraživanjem je potvrđena temeljna hipoteza da postoji značajna povezanost između svjesnosti internetske prijetnje i snage zaporke. Ispitanici su nakon dva tjedna kreirali snažnije zaporke nego što je to učinila kontrolna skupina koja nije bila svjesna prijetnji za sigurnost.

Prema istraživanju [Ostojic, Phillips; 2009; 959] više od 90% studenata koristi se svojim osobnim značajkama pri oblikovanju zaporke poput datuma rođenja i nadimka. U svojem istraživanju autori promatraju mogućnosti pamćenja različitih zaporki.

Pavić i Jelenković [2007] promatraju problem autentikacije i autorizacije korisnika kroz SSO (Single Sign-on) sustav koji omogućava korisniku predočenje svojih akreditacijskih podataka samo jednom. Proces autentikacije, odnosno provjera korisničkog identiteta, iznimno je važan element informacijske sigurnosti. Budući da predstavlja prvi korak prijave korisnika u sustav, sigurnosni zahtjevi koji se pred njega postavljaju prilično su visoki. Također, osim visoke razine sigurnosti, da bi bio upotrebljiv u praksi, proces autentikacije mora zadovoljavati i brojne druge zahtjeve (npr. praktičnost, financijska isplativost, jednostavnost održavanja i upravljanja i sl.). Kao primjer slabe isplativosti mogu se navesti biometrijski uređaji koji usprkos visokoj razini sigurnosti koju nude, još uvijek nisu šire prihvaćeni kao mehanizam autentikacije. U svakodnevnom poslu postoji potreba za čestim prijavljivanjem na više sustava, pritom se upotrebljavaju različita korisnička imena i autentikacijske informacije.

Sigurnost kao jedna od temeljnih mjera kakvoće informacijskih sustava, ovisi o velikom broju tehničkih ali i netehničkih faktora. Suprotno općemu mišljenju kako se ranjivosti informacijskih sustava nalaze isključivo u softverskom dijelu sustava, zapravo je ljudski faktor onaj koji predstavlja najveću prijetnju sigurnosti. Iskorištavajući tipične ljudske karakterne osobine i uzorke ponašanja, napadač može na vrlo jednostavan način doći do vrijednih informacija o ciljanom informacijskom sustavu. Autori [Pavković, Perkov; 2010; 159] promatraju metode napada koje dijele na netehničke metode (lažno predstavljanje, izgradnja povjerenja, kopanje po otpadu, dohvaćanje informacija iz javno dostupnih izvora, lažna anketa), tehničke metode (phishing, vishing, specijalno oblikovani CD/DVD mediji ili USB memorijski uređaji) i različite alate (Asteriks, metaspoilt framework, scocial-engineering toolkit, hardware keylogger). Kao mjere zaštite autori [Pavković, Perkov; 2010; 159] predlažu: sigurnosnu politiku, osvješćivanje i edukaciju zaposlenika, edukaciju ključnog osoblja, kontinuirano podsjećanje na prijetnju, prepoznavanje aktivnog napada, reagiranje na incidente, penetracijsko testiranje.

S druge strane, prema istraživanju Verizon Business date Breach Investigation Report skoro 87% svih proboja sustava sigurnosti moglo se spriječiti osnovnim sigurnosnim kontrolama.

3. Metodologija i tehnologija istraživanja

U radu je korištena metoda deskriptivne statistike, s temeljnim pokazateljima poput aritmetičke sredine, medijana, moda, standardne devijacije i koeficijenta varijacije da bi se bolje opisale promatrane pojave.

U skladu s navedenim teorijskim okvirom razvijen je anketni upitnik. Dio anketnog upitnika koji se odnosi na teoriju neutralizacije prilagođen je na temelju prethodnih istraživanja [Siponen & Vance; 2010; apendix 1-3], a dio koji se odnosi na načine kreiranja i postupanja sa zaporkama u radnom okružju razvio je sam autor. Anketni se upitnik sastoji od triju dijelova : u prvom su dijelu opći demografski podaci o ispitanicima, u drugom je dijelu dan kratki scenarij kao uvod (osoba u tom scenariju grubo krši definirana pravila informacijske sigurnosti dajući svoju zaporku suradniku) u problem. U tom drugom dijelu ispitanici ocjenjuju realnost navedenog scenarija i odgovaraju na pitanje da li bi postupili isto kao osoba u scenariju. Imaju samo dva moguća odgovora: da ili ne. U trećem dijelu anketnog upitnika nalazi se 29 pitanja na koja ispitanici odgovaraju zaokruživanjem brojeva na 7-stupanjskoj skali Likertova tipa, gdje 1 označava odgovor Uopće se ne slažem, a 7 označava odgovor Potpuno se slažem. Pitanja su razvrstana u skupine od po tri pitanja za svaku tehniku teorije neutralizacije, snaga zaporke provjerava se kroz šest pitanja i postupanje sa zaporkom kroz pet pitanja.

Podaci su prikupljani pomoću anketnog upitnika od tri kategorije ispitanika s ciljem dobivanja što većeg broja odgovora i sagledavanja problema iz različitih kutova. Prva kategorija ispitanika jesu polaznici tečaja obrazovanja odraslih u Pučkome otvorenom učilištu u Osijeku, druga kategorija su polaznici poslijediplomskog (doktorskog) studija na Fakultetu organizacije i informatike u Varaždinu, i posljednja, ali ujedno najbrojnija skupina ispitanika jesu zaposlenici jedne agencije za financijsko posredovanje u Osijeku.

Ispitanici su popunjavali anketne upitnike samostalno, nakon čega su ih stavili u priloženu omotnicu, zalijepili i predali ispitivaču – u svrhu osiguranja potpune anonimnosti odgovora ispitanika. Ispitivač ni na koji način nije mogao povezati odgovor s konkretnim ispitanikom.

U obradi podataka korišten je programski paket za tablične izračune – MS Excel.

4. Rezultati istraživanja

U tablici 1 dane su značajke ispitanika, koje su utvrđene na temelju prvog dijela anketnog upitnika, u kojem su prikupljani opći podaci o ispitanicima.

Tablica 1: Opis značajki ispitanika

Karakteristike uzorka							
Kategorija ispitanika	Broj ispitanika	Prosječna starost (god.)	Prosječno radno iskustvo (god.)	Muškarci	Žene	Zaposleni	Nezaposleni
Polaznici obrazovanja odraslih	37	31,4	7,6	9	28	18	19
Doktorski studij FOI	14	32,2	8,1	8	6	12	2
Agencija za financijske usluge	85	43,6	20,9	17	67	85	0
Ukupno	136	38,9	15,8	34	101	115	21

U tablici 2. dan je prikaz prikupljenih ocjena realnosti hipotetskog scenarija koji je ujedno predstavljao i uvod u najvažniji dio istraživanja.

Tablica 2 : Ocjena realnosti hipotetskog scenarija

Da li je scenarij realan ?		
da	111	83%
ne	23	17%

U tablici 3. prikazani su rezultati namjere ispitanika da prekrše pravila informacijske sigurnosti. Većina se ispitanika pokazala sklonom prekršiti pravila i dati svoju zaporku uz pristup na svoje računalo svom kolegi/kolegici.

Tablica 3: Procjena ispitanika

Da li biste postupili kao osoba u scenariju ?		
da	69	53%
ne	61	47%

Promatrajući i analizirajući odgovore na sva pitanja, generalno je zaključeno da aritmetička sredina nije dobar pokazatelj glavne tendencije. Kod svih je pitanja standardna devijacija izrazito visoka, a koeficijent varijacije iznosi od 46,67% u odgovoru na pitanje 14 do 76,79% u odgovoru na pitanje 30. Iz tog je razloga odlučeno kao mjeru središnje vrijednosti koristiti medijan kao vrijednost koja se nalazi položajno u sredini. Mod je odbačen zato što mjeri samo vrijednosti koje se najčešće pojavljuje u uzorku, pa ta vrijednost može i zavarati.

Rezultati su grupirani po pojedinim tehnikama teorije neutralizacije.

Tablica 4 : Poricanje odgovornosti

Poricanje odgovornosti			
	1	2	3
Aritmetička sredina	2,99	3,63	2,74
Medijan	**2**	**3**	**2**
Mod	1	5	1
Standardna devijacija	1,88	1,87	1,82
Minimum	1	1	1
Maximum	7	7	7
Broj odgovora	135	136	136
Koeficijent varijacije	62,78%	51,57%	66,63%

Što se tiče poricanja odgovornosti (tablica 4) u odgovorima na pitanja 1 i 3 medijan iznosi 2 odnosno riječima Ne slažem se, dok odgovor na pitanje 2, ima vrijednost 3, ili rečeno riječima, Uglavnom se ne slažem. S obzirom na vrijednosti medijana nije moguće potvrditi da je tehnika „Poricanje odgovornosti" opravdanje osobama za kršenje pravila informacijske sigurnosti.

Tablica 5: Poricanje učinjene štete

Poricanje učinjene štete			
	4	5	6
Aritmetička sredina	2,75	3,10	2,90
Medijan	**2**	**3**	**2**
Mod	1	2	2
Standardna devijacija	1,76	1,83	1,75
Minimum	1	1	1
Maximum	7	7	7
Broj odgovora	136	136	135
Koeficijent varijacije	63,95%	59,09%	60,22%

Poricanje učinjene štete odgovori su od Nne slažem se do Uglavnom se ne slažem. Dakle nije moguće potvrditi da je tehnika „Poricanje učinjene štete" opravdanje osobama za kršenje pravila informacijske sigurnosti.

Tablica 6: Osuda onih koji me osuđuju

Osuda onih koji me osuđuju			
	7	8	9
Aritmetička sredina	3,48	2,67	2,97
Medijan	**3**	**2**	**3**
Mod	1	2	2
Standardna devijacija	1,93	1,62	1,62
Minimum	1	1	1
Maximum	7	7	7
Broj odgovora	135	135	135
Koeficijent varijacije	55,36%	60,78%	54,56%

Ni ovaj instrument ne daje potvrdu početne hipoteze, jer je medijan, odnosno središnja vrijednost, od Ne slažem se do Uglavnom se ne slažem.

Tablica 7: Lojalnost višim ciljevima

Lojalnost višim ciljevima			
	11	12	13
Aritmetička sredina	3,27	2,87	3,06
Medijan	**3**	**2**	**3**
Mod	2	1	1
Standardna devijacija	1,81	1,63	1,82
Minimum	1	1	1
Maximum	7	7	7
Broj odgovora	135	135	135
Koeficijent varijacije	55,27%	56,83%	59,60%

Lojalnost višim ciljevima u ovom uzorku također nije opravdanje za kršenje informacijske sigurnosti, jer je vrijednost medijana na dva pitanja Uglavnom se ne slažem i jedno pitanje Ne slažem se.

Tablica 8: Obrana neizbježnošću

Obrana neizbježnošću			
	14	15	16
Aritmetička sredina	3,92	3,26	2,57
Medijan	**4**	**3**	**2**
Mod	**5**	**1**	**2**
Standardna devijacija	1,83	1,77	1,53
Minimum	1	1	1
Maximum	7	7	7
Broj odgovora	135	135	135
Koeficijent varijacije	46,67%	54,18%	59,47%

Kod ovog instrumenta odgovor na pitanje 14: *„U redu je prekršiti pravila informacijske sigurnosti u poduzeću, u okolnostima u kojima se čini da nemamo drugog izbora“* ima vrijednost Niti se slažem, niti se ne slažem, a ostala dva pitanja su Ne slažem se i Uglavnom se ne slažem. Zbog toga nije moguće potvrditi da je tehnika „Obrana neizbježnošću“ opravdanje osobama za kršenje pravila informacijske sigurnosti.

Tablica 9: Saldiranje dobrih i loših djela

Saldiranje dobrih i loših djela			
	17	18	19
Aritmetička sredina	2,98	3,01	3,01
Medijan	**3**	**2,5**	**3**
Mod	**1**	**2**	**1**
Standardna devijacija	1,73	1,76	1,67
Minimum	1	1	1
Maximum	7	7	7
Broj odgovora	133	134	134
Koeficijent varijacije	58,09%	58,23%	55,68%

Ni ovaj instrument ne predstavlja opravdanje za kršenje pravila informacijske sigurnosti.

Svih šest tehnika koje su temelj teorije neutralizacije nisu opravdanje osobama za kršenje pravila informacijske sigurnosti. Temeljem rezultata ovog istraživanja ne može se reći da korištenje tehnika u sklopu teorije neutralizacije utječe na osobe da krše pravila informacijske sigurnosti.

Tablica 10: Snaga zaporke

Snaga zaporke						
	20	21	22	23	24	26
Aritmetička sredina	3,31	3,47	3,83	2,07	2,76	2,33
Medijan	**2**	**3**	**4**	**1**	**2**	**2**
Mod	1	2	1	1	1	1
Standardna devijacija	2,21	2,11	2,21	1,54	1,94	1,45
Minimum	1	1	1	1	1	1
Maximum	7	7	7	7	7	7
Broj odgovora	134	134	134	134	134	134
Koeficijent varijacije	66,89%	60,87%	57,61%	74,45%	70,25%	62,27%

Iz podataka u tablici 10 može se zaključiti da su polaznici svjesni što predstavlja snaga zaporke jer su odgovori na pitanja koja to istražuju u rasponu od 1 do 3, osim odgovora na pitanje 22: *„Lozinka ne treba imati puno znakova (najviše pet)“* gdje je medijan 4, što predstavlja odgovor Niti se slažem niti se ne slažem. Može se potvrditi hipoteza $H_{2\text{-}1}$.

Tablica 11: Postupanje sa zaporkom

Postupanje sa zaporkom					
	25	27	28	29	30
Aritmetička sredina	1,90	2,37	2,83	1,87	2,60
Medijan	**1,5**	**2**	**2**	**1**	**2**
Mod	1	1	1	1	1
Standardna devijacija	1,29	1,57	1,90	1,39	2,00
Minimum	1	1	1	1	1
Maximum	7	7	7	7	7
Broj odgovora	134	134	134	134	134
Koeficijent varijacije	67,93%	66,49%	67,24%	74,59%	76,79%

Ispitanici se pridržavaju načina postupanja sa zaporkama kako su ti načini opisani u literaturi i svjesni su važnosti koju zaporka ima za pristup korisnika na računalo. Drugim riječima, hipoteza $H_{2\text{-}2}$ može se potvrditi.

5. Ograničenja istraživanja

Ograničenje ovog istraživanja svodi se prvenstveno na mali i neadekvatan uzorak. Riječ je o prigodnom uzorku, jer je korišten uzorak ispitanika koji je bio dostupan autoru. U uzorku su većinom bile zastupljene žene (75%), a muškarci su činili samo (25%) uzorka.

S druge strane, ispitanici koji su davali odgovore na pitanja postavljena u upitniku nisu zaista i prekršili pravila informacijske sigurnosti, pa samim time nisu ni trebali imati opravdanja za svoje postupke. 53% ispitanika reklo je da bi postupili isto kao subjekt u scenariju (dali bi svoju zaporku suradniku) da bi uštedjeli vrijeme i novac kompaniji u kojoj rade. Ali ipak oni nisu zaista to i učinili. Za točnije rezultate istraživanja trebalo bi anketirati ispitanike koji su zaista prekršili neko od pravila koja se tiču zaporki, pa čuti njihova opravdanja o razlozima koji su ih naveli na to.

6. Zaključak

Pojedinačno je provjereno svih šest tehnika teorije neutralizacije kroz odgovarajuće instrumente. Temeljem ovog istraživanja ne može se zaključiti da tehnike teorije neutralizacije utječu na namjeru zaposlenika da krše pravila informacijske sigurnosti. Zaposlenici su svjesni onoga što predstavlja snažnu zaporku i znaju da se ona treba sastojati od naizmjeničnih velikih i malih slova, brojki i specijalnih znakova. Isto tako ispitanici razumiju važnost zaporke za pristup na računalo, kao i potrebu čuvanja privatnosti svoje zaporke.

Preporuka temeljena na rezultatima ovog istraživanja za poslovnu praksu bila bi da se javno objave pravila informacijske sigurnosti, tako da budu potpuno jasna svim zaposlenicima. Osim toga preporučuje se zaposlenike informirati koliko bi znakova trebala imati snažna zaporka. Obje preporučene aktivnosti trebale bi biti kontinuirani i dobro razrađen postupak koji će postupno dovesti do povećanja informacijske sigurnosti u pojedinoj organizaciji.

Literatura

1. *Charoen, D., Raman, M., Olfman, L. : Improving end user behavior in password utilization: An action research initiative, Systemic practise & action research, vol. 21, str. 55-72, 2008*
2. *McCrohan, K.F., Engel, K., Harvey, J. W. : Influence of awareness and training on cyber security, Journal of internet Commerce, vol. 9, str. 23-41, 2010*
3. *Ostojic, P., Phillips, J.G. : Memorabilty of alternative password systems, International Journal of pattern recognition and artificial Intelligence, vol. 23 No. 5, str. 987-1004, 2009*
4. *Pavić, T., Jelenković, L. : Autentifikacija i autorizacija korisnika na jednom mjestu, Mipro Conference Proceedings, str. 150-155, 2007*
5. *Pavlović, N., Perkov, L. : Metode i alati u socijalnom inženjerimgu, Mipro Conference Proceedings, str. 159-164, 2010*
6. *Peltier, T. R. : Implementing an information security awareness program, Security management practices, str. 37-48,may-june 2008*
7. *Shay, R., Bertino, E. : A comprehensive simulation tool for the analysis of password, International journal of information security, vol 8, str. 275-289, 2009*
8. *Siponen, M., Vance, A. : Neuralization : New insights into the problem of employee information systems security policy violations, MIS Quarterly, vol. 34 No 3 str. 487-502, 2010*
9. *Spears, J. L. , Barki, H. : User participation in information systems security risk management, MIS Quarterly, vol. 34 No 3 str. 503-522, September 2010*
10. *The Honeynet project : Know your enemy : Learning about security threats, Boston, Addison Wasley, 2004*
11. *Tsohou, A. et al. : Investigating information security awareness : Research and practice gaps, Information security journal: A global perspectice, vol.17, str. 207-227, 2008*
12. *Zviran, M., Haga, W.J., : Password security : An empirical study, Journal of management information systems, vol 15 no 4, str. 161-185, 1999*
13. *http://www.infosecurityanalysis.com/2008.html pristupljeno 14.03.2011.*

Darko Matotek

Analysis of the Use of Neutralisation Techniques in Violations of Information Security

Abstract

Neutralisation theory was postulated in 1957 in the field of criminology. The theory explains the behaviour of individuals who violate rules and regulations but do not see themselves as violators. They find justification for their acts in certain techniques and by doing so renounce their responsibility in a way. Using a questionnaire, a hypothetic scenario and intensity questions, this paper examines whether individuals apply neutralisation techniques to their behaviour with respect to violations of information security regulations. The second part of the questionnaire examines respondents' understanding of the term strong password, as well as of safe ways of password handling.

Keywords: Information security, password, theory of neutralisation