Viktor Kanižai, master*
OTP banka Srbija a.d. Novi Sad, Novi Sad,
Republika Srbija

UDK 004.7 : 004.056.53
Stručni članak
Primljen: 15. III 2013.

PREVENTIVNA ZAŠTITA KORISNIČKIH NALOGA

SAŽETAK: Danas gotovo da ne postoji korisnik računara koji ne poseduje korisnički nalog. Da li je u pitanju nalog za prijavljivanje na računar, e-banking, e-mail sistem, društvene mreže, čet sesije, internet telefoniranje, itd., identifikacija korisnika, pa nakon toga i autorizacija se realizuje pomoću određenog korisničkog naloga. Taj nalog omogućava pristup željenom servisu, kao i upotrebu obezbeđenih usluga. Međutim, većina vlasnika korisničkih naloga ne vodi računa o njihovoj bezbednosti. Zloupotrebom korisničkih naloga može se izvršti krađa identiteta (npr. društvena mreža, e-uprava), može se naneti reputaciona šteta (npr. e-mail nalog), i ono najvažnije: materijalna šteta (npr. e-banking, krađa podataka). Počinioce visokotehnološkog kriminala nije jednostavno identifikovati, te stoga vlasnici korisničkih naloga moraju biti maksimalno oprezni i preduzeti sve preventivne mere kako bi zaštitili svoje naloge.

KLJUČNE REČI: korisnički nalog, IT bezbednost, zaštita podataka, hakovanje.

Uvod

Svaki korisnik datih usluga u domenu informacionih tehnologija, mora biti identifikovan, a u određenim slučajevima i autorizovan. S jedne strane, autentifikacija računara koji je sredstvo komunikacije neophodna je da bi se sama komunikacija realizovala (određivanje po MAC adresi ili IP adresi), a sa druge strane za upotrebu, najčešće onlajn servisa, neophodna je identifikacija i samog korisnika računara. Identifikacija digitalnog korisnika, tj. korisnika računarskog sistema odvija se upotrebom korisničkih naloga. U želji upotrebe personalizovanih onlajn usluga, korisnik mora da se autentifikuje i uspešno prijavi na dati sistem pomoću prethodno definisanog korisničkog naloga. Bez toga, dostupne su samo nepersonalizovane usluge, kao npr. mašinsko prevođenje teksta sa jednog jezika na drugi, pretraga interneta po zadatim ključnim rečima, vesti i vremenska prognoza, itd. Ovde je važno napomenuti da se u nekim slučajevima, bez znanja korisnika, računar identifikuje od strane nekog web sajta u smislu da je korisnik tog računara ranije već posetio taj sajt i gledao određene stranice tog sajta – ovo se vrši pomoću tzv. „Cookies“-a, međutim, fokus ovog rada predstavlja bezbednu upotrebu i zaštitu korisničkih naloga korišćenih za identifikaciju samog korisnika.

1. Korisnički nalog

Digitalni identitet korisnika informacionih tehnologija (IT) oformljuje se preko korisničkih naloga. Korisnički nalog omogućava korisniku da se autentifikuje nad sistemskim uslugama i bude autorizovan da im pristupi. Treba naglasiti da autentifikacija ne podrazumeva i autorizaciju. Da bi se korisnik prijavio na svoj nalog, obično je neophodna autentifikacija parom korisnički nalog–lozinka. Pored navedenog, upotreba naloga omogućava logovanje događaja sa

* kanizsai.viktor@gmail.com

aspekta izvršilaca na određenom resursu, povećava bezbednost usluge i obezbeđuje mogućnost pozivanja na odgovornost.

1.1. Upotreba korisničkih naloga

Postoje različite vrste korisničkih naloga: e-mail, e-banking, internet telefonija, društvene mreže, skladištenje podataka onlajn, četovanje, itd. Različite vrste, pored obezbeđivanja upotrebe različitih tipova usluga, traže različiti nivo povezivanja stvarnog identiteta korisnika za datim korisničkim nalogom. Tako, npr. korisnički nalog za usluge četovanja ne zahteva bilo kakvu povezanost sa stvarnim identitetom vlasnika, na njemu je da odluči da li će koristiti svoje ime, nadimak ili nešto treće kao naziv svog naloga. Sa druge strane, nalog za e-banking je strogo vezan za stvarni identitet korisnika, što je i potpuno očekivano s obzirom da se radi o finansijskim transakacijama.

Na osnovu identifikacije, autentifikacije korisnika sistema, usluga, realizuje se i autorizacija. Različiti korisnički nalozi na istom sistemu mogu biti različito autorizovani. U pogledu prijavljivanja na računar, to znači da jedan korisnik može imati pristup određenim fajlovima i folderima, dok drugi korisnik istog računara neće imati pristup istim podacima, već nekim drugim. Administrator će uvek imati pristup svim podacima, u čemu nema ničeg spornog, jer uvek mora postojati tzv. „super korisnik“ koji će moći da u skladu sa potrebama izvršava zahtevane aktivnosti, bez ograničenja. U suprotnom, sistem ne bi bio održiv, već bi pri prvoj promeni ili incidentu „pao“, jer nema ko da upravlja tim sistemom u celini, a što je neophodno za nesmetan i ispravan rad.

Korisnički identifikator predstavlja digitalni identitet korisnika nekog sistema ili usluge, te je postao vrlo važan deo čovekovog života u eri kompjuterizacije. Upravo zbog velike značajnosti, ključno je da se ti nalozi adekvatno zaštite, a njihova upotreba da bude bezbedna.

2. Lozinka

Lozinka predstavlja tajni podatak koji je potrebno poznavati da bi se pristupilo određenim resursima, a preko njih se dolazi do određenih podataka ili usluga. Lozinka se čuva od onih koji tim resursima ne smeju da imaju pristup, a pri pokušaju pristupanja određenim resursima vrši se provera poznavanja lozinke, i na osnovu rezultata provere pristup resursima se dozvoljava ili odbija.

Lozinka se sastoji od kombinacije znakova (zavisno od datog sistema: slova, simbola, brojeva itd.) koje sistem pamti, i svaki put kada korisnik želi da se prijavi na svoj korisnički nalog, od njega se traži upisivanje te lozinke, vršeći autorizaciju na taj način.

3. Neovlašćen pristup

Autorizovan pristup preko para korisničko ime–lozinke, ne znači uvek i ovlašćen pristup. Naime, pristup nalogu se uspešno izvrši upisivanjem korisničkog imena i ispravne lozinke. Međutim, pristup se ne smatra ovlašćenim ako nije vlasnik naloga taj koji je pristup izvršio, ili lice koje je vlasnik ovlastio za pristup pod njegovim identifikatorom.

Mogućnosti neovlašćenog pristupa često su izvori vršenja krivičnih dela iz oblasti visokotehnološkog kriminala, kao i internih zloupotreba. Cilj izvršioca može biti protivpravno pribaljvanje materijalne koristi za sebe ili drugog, kao i nematerijalne koristi, a takođe i osveta, pokazivanje moći ili hakerskog znanja, ucena, itd.

Rasprostranjeni ciljevi zloupotrebe korisničkih naloga mogu podrazumevati i šale. Na primer, radi ilustracije, muž i žena su postali roditelji, dobili su sina, i neka se on zove Petar Petrović. Prijatelji muža kreirali su sutradan korisnički nalog „petar.petrovic“ na jednom web-mail servisu, i kao vlasnika imenovali Petra Petrovića. Zatim su poslali e-mail roditeljima stvarnog, novorođenog Petra Petrovića sa sledećim tekstom: „Dragi Mama i Tata! Hvala vam što ste me doveli na ovaj svet. Trudiću se da vam budem dobar i uzoran sin. Puno pozdrava, vaš sin.“ Kada su roditelji primili ovaj e-mail bili su zaista šokirani. Da bi im posle zajednički prijatelj javio da se radi o šali, i da su oni bili ti koji su kreirali taj nalog i poslali e-mail, a zatim su roditeljima predali potrebne kredencijale. Šala je možda dobro smišljena, ali treba se postaviti u poziciju roditelja koji primaju e-mail u ime novorođenčeta...

3.1. Slabe lozinke

Vlasnici korisničkih naloga često biraju „slabe“ lozinke, i na taj način u mnogome pojednostavljuju napadaču neovlašćen pristup tom nalogu. Te lozinke su u većini slučajeva identične sa korisničkim nalogom, ili predstavljaju ime vlasnika, supružnika, roditelja, kućnih ljubimaca. Često se kao lozinka koristi godina rođenja vlasnika (ili supružnika, dece), broj lične karte, JMBG, itd. Poznavajući vlasnika korisničkog naloga u ovakvim slučajevima lako se može pogoditi lozinka i obezbediti pristup datom nalogu, a samim tim i podacima, resursima ili uslugama.

3.2. Inicijalne lozinke

Inicijalne (default) lozinke su one koje proizvođač datog resursa ili pružalac određenih usluga sam definiše i na taj način omogućava trenutnu upotrebu resursa ili usluge, a korisnika obavezuje da što pre promeni tu lozinku. Problem nastaje kada korisnik videći da „sve radi“ zaboravi da promeni tu inicijalnu lozinku, ili to ne učini iz neznanja. S obzirom da su u većini slučajeva sve inicijalne lozinke datih proizvoda iste, poznavajući jednom tu lozinku, napadač može da je iskoristi i za pristup za koji nije ovlašćen.

Tenutno postoji veliki broj internet stranica na kojima su ove inicijalne lozinke objavljene. Tako, na primer, na jednom od sajtova mogu se pronaći inicijalne lozinke od 473 proizvođača, i to u ukupnom broju od 1952 lozinki. I to je samo jedan od spiskova inicijalnih lozinki...

Autor ovog rada je uz odobrenje vlasnika resursa isprobao pristup jednom resursu sa inicijalnim korisničkim nalogom i lozinkom, i pristup je bio uspešno izvršen. Vlasnik resursa je potom odmah izvršio potrebne modifikacije.

3.3. Hakovanje naloga

Neovlašćen pristup korisničkom nalogu može se realizovati i tzv. „hakovanjem“. Sama reč hakovanje (eng. *Hack*) označava pojam vezan za zaobilaženje sistema zaštite računarskih ili telekomunikacionih sistema.

Hakovanje za pristup korisničkom nalogu može se izvršiti npr. zbog prisutnih ranjivosti datog sistema. Drugim rečima, napadač ustanovi da je sistem ranjiv na napade za privilegovan pristup i iskoristi, tj. eksploatiše tu ranjivost za dobijanje željenog, najčešće administratorskog pristupa. Autor ovog rada ne želi da navede primere takvih ranjivosti, kako rad ne bi bio potencijalni izvor zloupotreba, već će radi ilustracije opisati jedan takav slučaj, konkretno administatorski pristup web sajtu određene kompanije. Napadač prvo identifikuje operativni sistem web servera, zatim aplikaciju kojom je sama prezentacija na web sajtu napravljena. Ukoliko utvrdi da neki od ovih sistema ima ranjivost, preostaje mu „samo“ da tu ranjivost eksploatiše. To čak može da znači da će mu administratorski pristup biti omogućen u roku od 10 sekundi (!). Nakon izvršenog pristupa napadač može i da promeni lozinku i u potpunosti preuzme upravljanje web sajtom, sve dok vlasnik tog sajta fizički ne odvoji web server sa interneta i izvrši potrebne konfiguracije (ponekad i reinstalaciju) za ispravan rad.

Drugi vid hakerskog pristupa može se realizovati upisivanjem „ključnih reči“ na web sajtu, tamo gde sistem inicijalno ne treba da prima takve reči. Te ključne reči su komande za izvršavanje upisane, na primer, u polju za pretragu na web sajtu. Polje nije zaštićeno i sistem prihvata komandu i na taj način napadač ostvaruje pristup. I za ovakvu vrstu napada ne treba više od 10 sekundi ukoliko se naiđe na takav web sajt koji nije zaštićen od ovakvih napada.

Treći primer hakerskog pristupa je kada napadač, imajući pristup fajlovima na datom računaru, želi da ukrade lozinke drugih korisnika. Najčešće se za tu svrhu koriste tzv. keš fajlovi koji skladište lozinke u cilju autentifikacije korisnika. Napadač preuzme keš fajl i iz njega raznim alatima iščita lozinke.

Hakovanje se može izvršiti i pomoću tzv. „brute force“ alatima, koji imaju spisak mogućih lozinki, njihove kombinacije ili podešljiv skup karaktera za lozinku, a hakeri pokušavaju da izvrše pristup tako što pri svakom pokušaju koriste drugu potencijalnu lozinku sve dok se pristup uspešno ne ostvari.

3.4. Statistički primeri

U ovom radu neće se navesti sistemi koji su hakovani, niti imena hakovanih korisničkih naloga, već će se samo prikazati statistički podaci vezani za lozinke hakovanih naloga. Autor rada nije ni u jednom trenutku pokušao da izvrši neovlašćen pristup bilo kom korisničkom nalogu, a podatke o njima preuzeo je sa javno dostupnih sajtova.

3.4.1. Hakovano 442.773 korisničkih naloga

Hakeri su prisvojili 442.773 para korisnički nalog–lozinka određenog sistema u 2012. godini. Statističkom obradom lozinki zaključuje se:

- Jedinstvenih lozinki bilo je 342.478

- 10 najčešćih lozinki su („lozinka = broj takvih lozinki (procenat od ukupnog broja)“):
  - 123456 = 1666 (0.38 %)
  - password = 780 (0.18 %)
  - welcome = 436 (0.1 %)
  - ninja = 333 (0.08 %)
  - abc123 = 250 (0.06 %)
  - 123456789 = 222 (0.05 %)
  - 12345678 = 208 (0.05 %)
  - sunshine = 205 (0.05 %)
  - princess = 202 (0.05 %)
  - qwerty = 172 (0.04 %)
- Imena meseci kao lozinke:
  - january = 106 (0.02 %)
  - february = 30 (0.01 %)
  - march = 192 (0.04 %)
  - april = 284 (0.06 %)
  - may = 725 (0.16 %)
  - june = 386 (0.09 %)
  - july = 245 (0.06 %)
  - august = 238 (0.05 %)
  - september = 68 (0.02 %)
  - october = 182 (0.04 %)
  - november = 154 (0.03 %)
  - december = 130 (0.03 %)

3.4.2. Hakovano 37.058 korisničkih naloga

Hakeri su prisvojili 37.058 para korisnički nalog–lozinka određenog sistema. Statističkom obradom lozinki zaključuje se:

- Jedinstvenih lozinki bilo je 21.215
- 10 najčešćih lozinki su („lozinka = broj takvih lozinki (procenat od ukupnog broja)“):
  - 123456 = 688 (1.86 %)
  - 123456789 = 258 (0.7 %)
  - 102030 = 92 (0.25 %)
  - 123 = 86 (0.23 %)
  - 12345 = 74 (0.2 %)
  - 1234 = 67 (0.18 %)
  - 242424 = 41 (0.11 %)
  - 101010 = 40 (0.11 %)
  - 12345678 = 38 (0.1 %)
  - 010203 = 35 (0.09 %)
- Imena meseci kao lozinke:
  - march = 2 (0.01 %)

- april = 2 (0.01 %)
- may = 34 (0.09 %)
- august = 22 (0.06 %)

4. Zaštita korisničkih naloga

Kako bi se obezbedilo da neovlašćena lica nemaju pristup korisničkom nalogu, moraju se preduzeti sve preventivne mere zaštite i njihove bezbedne upotrebe.

Prvi i najvažniji vid zaštite jeste fizička zaštita datog resursa nad kojim se vrši pristup. Ako napadač dođe u posed resursa, bez obzira kakva je logička zaštita podataka, pre ili kasnije uspeće da dođe u posed podataka pohranjenih na tom resursu.

4.1. Zakonska regulativa

Krivični zakonik Republike Srbije (nadalje: KZRS) u članu 302. i 304. reguliše slučajeve neovlašćenih pristupa. Po članu 302. KZRS, ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko upotrebi podatak dobijen na način predviđen u stavu 1. ovog člana, kazniće se novčanom kaznom ili zatvorom do dve godine. Ako je usled dela iz stava 1. ovog člana došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posledice, učinilac će se kazniti zatvorom do tri godine. Po članu 304. KZRS, ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri meseca. Gonjenje za delo iz stava 1. ovog člana preduzima se po privatnoj tužbi.

4.2. Bezbednosna svest

Bezbednosna svest korisnika je od ključnog značaja za sprečavanje vršenja zloupotrebe korisničkih naloga. Ako sam korisnik nije svestan izvora pretnji i rizika koji postoje u ovom domenu, tada je sve jedno kakve će mere zaštite biti implementirane, jer je korisnik taj koji drži ključ u rukama. Ako nije pažljiv i ako on sam nije bezbednosno svestan, uvek će postojati način da se izvrši željena zloupotreba, a upravo se na ovu činjenicu i oslanjaju napadači.

4.3. Upotreba snažnih lozinki

Pod „snažnom“ lozinkom podrazumevaju se one koje se teško pogađaju, bilo manuelno ili automatizovano korišćenjem nekih od alata. U tom smislu snažnom lozinkom se smatraju one koje sadrže minimum 8 cifara, u kombinaciji velikih i malih slova, specijalnih karaktera (npr. tačka) i brojeva (0-9).

Da bi se pokazala opravdanost upotrebe lozinke od minimum 8 karaktera, sledi primer potrebnog vremena „probijanja“ lozinke u zavisnosti od njene dužine i složenosti – potrebno vreme, naravno, u mnogome zavisi i od procesorske i memorijske moći računara kojim se vrši

napad (http://www.toplinestrategies.com/cloudhead/security/how-much-time-is-needed-to-crack-a-password-by-brute-force/):

- Dužina: 4, kompleksnost: a-z ==> manje od 1 sekunde
- Dužina: 4, kompleksnost: a-zA-Z0-9 + simboli ==> 4.8 sekunde
- Dužina: 5, kompleksnost: a-zA-Z ==> 25 sekundi
- Dužina: 6, kompleksnost: a-zA-Z0-9 ==> 1 sat
- Dužina: 6, kompleksnost: a-zA-Z0-9 + simboli ==> 11 sati
- Dužina: 7, kompleksnost: a-zA-Z0-9 + simboli ==> 6 nedelja
- Dužina: 8, kompleksnost: a-zA-Z0-9 ==> 5 meseci
- Dužina: 8, kompleksnost: a-zA-Z0-9 + simboli ==> 10 godina
- Dužina: 9, kompleksnost: a-zA-Z0-9 + simboli ==> 1000 godina
- Dužina: 10, kompleksnost: a-zA-Z0-9 ==> 1700 godina
- Dužina: 10, kompleksnost: a-zA-Z0-9 + simboli ==> 91800 godina

Iz navedenog primera se jasno zaključuje da se lozinke manje od 5 karaktera mogu pogoditi u roku od 5 sekundi, a one manje od 7 karaktera u roku od jednog dana. Ako je dužina 8 karaktera i ako je lozinka sastavljena iz kombinacije velikih i malih slova, specijalnih karaktera i brojeva, tada je minimalno potrebno vreme za probijanje lozinke 10 godina.

Takođe, jedna vrlo ključna stavka u zaštiti lozinki je i periodična promena lozinke. Naime, ukoliko napadač na bilo koji način sazna lozinku, neće je moći dugo koristiti ako vlasnik korisničkog naloga redovno menja svoju lozinku. Najbolje je da se na svakih 45-60 dana menja lozinka.

Lozinku ni u kom slučaju ne treba zapisati na papir tako da taj papir bude nezaštićen, pogotovo u blizini datog računara. Najbolja praksa pokazuje da se dobre lozinke, pored pridržavanja napred navedenih uslova, kreiraju tako što se zamisli naziv omiljenog filma ili pesme, i početna slova tog naziva da se iskoriste za kreiranje lozinke. Na taj način vlasnik naloga sigurno neće zaboraviti lozinku, a napadač je neće lako pogoditi, jer će lozinka sasvim sigurno biti skup karaktera bez značenja. Na primer, dobra lozinka bi bila JJpomg.315 (naziv pesme: Još jedna pesma o maloj garavoj). S tim, što je ona upravo postala slaba činjenicom da je objavljena u ovom radu.

4.4. Testiranje na ranjivosti

U cilju sprečavanja neovlašćenog pristupa, neophodno je da se dati resurs ili usluga redovno testira na ranjivosti, a uočeni nedostaci u što kraćem roku da se otklone. Nepreduzimanjem ovih mera, napadaču je olakšan „posao“, i biće mu jednostavnije da izvrši neovlašćen pristup datom resursu ili usluzi. Praksa pokazuje da se resursi dostupni na internetu moraju testirati na ranjivosti minimum jednom kvartalno, poželjno je jednom mesečno, a najbolje bi bilo jednom nedeljno.

4.5. Kriptovana komunikacija

Tamo gde je moguće, potrebno je koristiti kriptovanu komunikaciju pri autentifikaciji. Na pojedinim webmail nalozima, na primer, može se podesiti da se uvek koristi kriptovana komu-

nikacija (https) između korisnika i pružaoca usluge. Na taj način ako neko presretne komunikaciju, lozinku neće pribaviti u čitljivom obliku.

4.6. Dvofaktorska autentifikacija

Dvofaktorska autentifikacija predstavlja upotrebu dva identifikaciona faktora pri autentifikaciji – lozinka (tj. „nešto što znam“) + pin kod očitan sa posebnog uređaja (tj. „nešto što imam“) ili biometrija (npr. otisak prsta, tj. „nešto što jesam“). Na taj način, ako napadač pogodi lozinku, ona mu neće biti dovoljna da ostvari pristup, jer je pored lozinke neophodan i pin kod ili otisak prsta.

Pin kodovi za dvofaktorsku identifikaciju generišu se na posebnim uređajima. Ti kodovi se menjaju najčešće na svaki minut, i mogu se koristiti samo jednom. Kodovi su pseudonasumični. Uređaji ove namene mogu biti različiti, od USB tokena, preko običnog tokena u obliku priveska za ključeve, pa do jednostavne aplikacije na mobilnom telefonu. Takođe, kod nekih rešenja, pin kod se može dobiti i sms-om od pružaoca date usluge.

Slika 1. Token za dvofaktorsku identifikaciju

U praksi to znači da se prijava na dati korisnički nalog vrši tako što se upiše korisničko ime, a u polje za lozinku upisuje se lozinka zajedno sa pin kodom. Tako, ako neko i presretne komunikaciju koja u datom slučaju nije kriptovana, pribavljeni kredencijali se neće moći upotrebiti, jer se pin kod koji je sastavni deo lozinke menja na svaki minut, a jednom korišćen kod ne može se ponovo upotrebiti.

Pored generisanih kodova, postoje i rešenja sa proizvoljnim pin kodovima, kao što je, na primer, upotreba „smart kartica“ za prijavu na sistem: kartica je „nešto što imam“, a proizvoljno zadati pin kod je „nešto što znam“.

Zaključak

Identifikacija korisnika računarskog sistema ili usluga vrši se pomoću korisničkog naloga. Naglom ekspanzijom informacionih tehnologija i onlajn usluga, spektar upotrebe korisničkih naloga eksponencijalno raste. Međutim, razvojem ovih mogućnosti rastu i mehanizmi njihove zloupotrebe. Upravo zbog toga neophodno je voditi računa o bezbednoj upotrebi korisničkih naloga i njihovoj adekvatnoj zaštiti, kako bi se broj vršenja krivičnih dela i zloupotreba iz oblasti visokotehnološkog kriminala što više približio nuli.

Postoji više metoda preventivnih mera zaštite korisničkih naloga, a najbolji rezultat postiže se kombinacijom svih metoda.

LITERATURA

[1] Krivični zakonik Republike Srbije, *Sl. glasnik RS*, br. 85/2005, 88/2005 − ispr., 107/2005 − ispr., 72/2009 i 111/2009.
[2] http://www.toplinestrategies.com/cloudhead/security/how-much-time-is-needed-to-crack-a-password-by-brute-force/, poslednji put pristupano 20. 02. 2013.
[3] Internet pretrage, http://www.google.com, poslednji put pristupano 20. 02. 2013.
[4] Najčešće korišćene lozinke na hakovanim sajtovima, http://www.24sata.rs/specijal/it/vest/pogledajte-najcesce-koriscene-lozinke-na-hakovanim-sajtovima/47564.phtml, poslednji put pristupano 23. 02. 2013.
[5] PASTEBIN #1 paste tool since 2002, http://pastebin.com, poslednji put pristupano 05. 02. 2013.
[6] Wikipedia, Slobodna enciklopedija, http://www.wikipedia.org, poslednji put pristupano 19. 02. 2013.

Viktor Kanižai, M. A.

PREVENTIVE AND PROTECTIVE MEASURES FOR USER ACCOUNTS

Summary

Today, there is almost no computer user who does not have a user account whether it is an account used to log on to the computer, e-banking, e-mail systems, social networks, chat sessions, Internet telephony, user identification, etc. Afterwards, even the authorization is realised with a given user account. The account allows access to desired service, and the use of the services provided. However, the majority of the user account owners do not take into account the safety of their accounts. Abuse of user accounts can be carried out to execute identity theft (e.g. social network, e-government), to produce reputational damage (e.g. e-mail account), and what is most important material damage (e.g. e-banking, data theft). It is not trivial to identify perpetrators of cybercrime, that is why the owners of user accounts must be very careful and take all measures possible to protect their account.

Key words: user account, IT security, data protection, hacking.