LOZINKA KAO KRITIČNI SIGURNOSNI ASPEKT DIGITALNE EKONOMIJE

PASSWORD AS A CRITICAL SECURITY ASPECT OF THE DIGITAL ECONOMY

Džemal Kulašin*

ABSTRAKT

Cilj ovog rada je da se, problematizirajući lozinku kao jedan od bitnih kriptografskih segmenata u sistemu zaštite informacijskih resursa, ukaže na veliki značaj sigurnosti u sferi savremene, digitalne ekonomije. U njegovom prvom dijelu rada naglašava se opći problem informacijske sigurnosti, koja se forsiranjem digitalne transformacije pozicionirala gotovo do preduvjeta funkcioniranja digitalne ekonomije. Naime, mrežna instrastruktura kao jedan od glavnih nositelja digitaliziranih procesa, organizacijama svih tipova ujedno se nametnula i kao vrlo ozbiljna sigurnosna ranjivost. Potom, u drugom dijelu rada, elaborira se lozinka kao najdostupnija i prva mjera u sistemu zaštite kojima se provodi nužna autentifikacija korisnika informacionih sistema. I dok nije nimalo iznenađujuće da su lozinke jedna od prvih meta cyber kriminalaca, ipak je iznenađujuća površnost u pristupu lozinkama, što rezultira brojnim i skupim sigurnosnim incidentima, zbog čega se lozinka može smatrati kritičnim sigurnosnim aspektom digitalne ekonomije. Stoga se u dijelu rada posebno naglašavaju i tzv. passwordless rješenja, odnosno mehanizmi autentifikacije bez korištenja lozinke, kao bliska budućnost digitalne ekonomije.

Ključne riječi: Lozinka, upravitelji lozinke, passwordless rješenja, digitalna ekonomija, informacijska sigurnost

ABSTRACT

The aim of this paper is to point out the large importance of security in the sphere of digital economy, problematizing the password as one of the important cryptographic segments in the system of information resources protection. The first part of the paper emphasizes the general problem of information security, which, by forcing the digital transformation, has positioned itself almost to the preconditions for the functioning of the digital economy. Namely, the network infrastructure, as one of the main carriers of digitized processes, has also imposed itself on organizations of all types as a very serious security vulnerability. Then, in the second part of the paper, the password is elaborated as the most accessible and the first measure in the protection system by which the necessary authentication of information system users is performed. And while it's not at all surprising that passwords are one of the first targets of cybercriminals, it's still surprisingly superficial in accessing passwords, resulting in numerous and costly security incidents; due to the collision described, it is precisely the password that can be considered a critical security aspect of the digital economy. In part of this paper, therefore, special emphasis is placed on the so-called. passwordless solutions as password-free authentication mechanisms that represent the near future of the digital economy.

Keywords: Password, password managers, passwordless solutions, digital economy, information security.

* - Fakultet za menadžment i poslovnu ekonomiju Univerziteta u Travniku

UVOD

Digitalna ekonomija (eng. digital economy) je, prema definiciji (Osmanbegović, 2017), savremeni način privređivanja u kome se izrazito koriste informaciono-komunikacijske tehnologije (ICT), posebno globalna računarska mreža Internet. Ili, jednostavnije rečeno, digitalna ekonomija je konvergencija ekonomije, informatike, komunikacija, računarstva i digitalne elektronike. Ovakva dinamična struktura digitalne ekonomije otvorila je široki prostor računarskom kriminalitetu, odnosno, pravilnije reći, cyber kriminalitetu, čime se sigurnost nametnula kao važna, možda i presudna tema digitalne ekonomije. Naime, računarske mreže, posebno Internet, općenito predstavljaju kritičnu tačku sigurnosti svake organizacije sa stanovišta sigurnosti informacija koje se u sistemu prenose. Pritom, prema Cerovini i dr. (2014), najveće sigurnosne greške odnose se na krajnjeg korisnika, na korporacijske uprave, tj. menadžment i na informatičke profesionalce, dok su najčešći vidovi napada prisluškivanje, lažno predstavljanje, DDOS, virusi, kriptoanaliza, „pogađanje“ lozinke itd.

Doduše, već u samim postavkama digitalne ekonomije pojavljuju se potencijalni rizici, poput ugrožavanja sigurnosti i privatnosti kao i (cyber) kriminal[1]. Konkretne činjenice u ovom pogledu su, na žalost, neumoljive. Naime, zadnjih nekoliko godina, upravo sa ekspanzijom (digitalne) ekonomije, kada se kompanije transformiraju sa klasičnog na elektronsko poslovanje, bilježi se i zabrinjavajući trend rasta cyber kriminala. Zanimljivo, ovaj trend rasta cyber kriminala dodatno se još i ubrzao u vrijeme pandemije (kada je i inače došlo do novih, možda i iznuđenih oblika digitalizacije u raznim poslovnim funkcijama) tako da je u pojedinim svojim pojavnim oblicima, npr. ransomware, zabilježio porast od nevjerovatnih 250%.

Stoga, posve je jasno da se problemu (informacijske) sigurnosti u digitalnoj ekonomiji doista mora poklanjati ogromna pažnja, što bi u praksi trebalo značiti i dosljednu uspostavu i primjenu dostupnih mjera zaštite informacionih sistema. No, praksa ne slijedi teoriju, te u velikom broju poslovnih sistema izostaje sistemski pristup informacijskoj sigurnosti i napori na edukaciji zaposlenika u smislu svjesnosti opasnosti cyber kriminala, čime je i tehnologija autentifikacije informacionih resursa mehanizmom lozinke postala ozbiljna sigurnosna ranjivost.

UPRAVLJANJE LOZINKAMA

Određeni oblici identifikacije korisnika datiraju još od samih početaka računarstva, ali se intenziviraju razvojem poslovne informatike, gdje se izdvaja CTSS sistem (eng. Compatible Time-Sharing System) razvijen 1961. godine na MIT-u (eng. Massachusetts Institute of Technology) u Sjedinjenim američkim državama, koji je od korisnika zahtijevao upis pristupne lozinke (Centar informacijske sigurnosti Hrvatske, 2012). Od tada, pa do danas, lozinka (eng. password) je, u osnovi, oblik povjerljivog (tajnog) podatka kojeg je potrebno znati kako bi se moglo pristupiti određenim informacijskim resursima. Time se lozinka (Stallings, 2014) svrstava u prvu kategoriju tzv. sigurnosnih usluga koje kroz protokolni komunikacijski sloj sistema omogućavaju sigurnost sistema i transfer podataka.

Zbog svojih određenih prednosti (brzina realizacije, jednostavnost, izostanak dodatnog hardvera), mehanizam lozinke (još uvijek) se intenzivno koristi za autentifikaciju i dokazivanje identiteta korisnika koji pristupaju informacijskim resursima informacionog sistema. No, u ovakvim turbulentnim i globaliziranim tehnološkim okolnostima, u organizacijama svih tipova nedvosmislena je nužnost definiranja formalnih procedura generiranja jakih, sigurnih lozinki i potom njihovog manipuliranja, u prvom redu, dodjeljivanja krajnjim korisnicima.

1 Ibid.

Prema Krivokapiću i dr. (2019), u upravljanju lozinkama potrebno bi bilo koristiti načela, inače karakteristična za IKT sisteme od posebnog značaja, poznata kao privacy by design i security by design, koji u ovom kontekstu podrazumijevaju:

- svaki korisnik sistema ima svoj nalog za pristup,
- svaki korisnik sistema ima ovlaštenja za obradu samo onih podataka neophodnih za njegov rad,
- šifre, tj. lozinke za pristup ne objavljuju se putem javne mreže,
- u organizaciji postoji odgovarajući standard o složenosti lozinke,
- ograničen je broj unosa pogrešne šifre, odnosno lozinke.

U konkretnoj poslovnoj praksi, međutim, često se odstupa od načela u upravljanju lozinkama, ili se implementiraju samo djelimično. Na primjer, kod informacionih sistema predviđenih za veći broj korisnika, administratori u pravilu automatski generiraju inicijalne snažne lozinke, ali ih i nerijetko distribuiraju klasičnim e-mail porukama, naprosto "zaboravljajući" da standardni protokoli za elektronske pošte (POP i IMAP), u svojoj osnovnoj formi podatke šalju kao običan tekst te ih je moguće relativno lako kompromitirati[2]. Pored toga, administratori korisnicima ostavljaju mogućnost da periodično sami generiraju (tj. biraju) nove lozinke, gdje se često dešava da korisnici kroče linijom manjeg otpora i odabiru slabe lozinke, motivirani isključivo jednostavnošću njihovog memoriranja. Kakav je uistinu odnos krajnjih korisnika prema lozinci kao jednoj od prvih sigurnosnih barijera, najbolje potvrđuju podaci o najkorištenijim lozinkama u prošloj, 2020 godini. Lista najkorištenijih "lozinki" je sljedeća (Top 200 most common passwords, 2021): 123456, 123456789, picture1, password, 12345678, 111111, 123123, 12345 itd.

Nivo sigurnosti koju pružaju ovakve lozinke korisnicima je potpuno nemjerljiv, jer je vrijeme potrebno za njihovo "razbijanje" manje od jedne sekunde, izuzev lozinke picture1, za koju treba (čak) tri sata, jer sadrži kombinaciju brojeva i (samo jednog) slova. Iako za ovakve primjere slabih lozinki i ne treba nikakav softver, treba istaknuti da čak i besplatne verzije modernog softvera za razbijanje provjeravaju milione lozinki u jednoj sekundi (npr. John the Ripper), a da ne govorimo o mogućnostima komercijalnih verzija ili udruživanju više računarskih sistema čime se gotovo relativizira čak i jak i sigurna lozinka.

Upravo zbog svega ovoga očekivanim se čine podaci iz istraživanja poslovne prakse u svijetu (FIDO authentication, 2021),, koji govore da je gotovo 80% uspješnosti curenja podataka (eng. data breaches) i neovlaštenog pristupa informacijskim resursima povezano upravo sa slabim i/ili ponavljajućim lozinkama. Ili konkretnije, u 2020. godini cyber kriminal je svjetsku ekonomiju koštao nevjerovatnih 2,9 miliona dolara u svakoj minuti, pri čemu je pomenutih 80% napada odnosno šteta direktno povezano sa lozinkama. Takođe, prema Vukić (2021), procjenjuje se i da 50% troškova korisničke podrške u globalnim kompanijama otpada na zahtjeve za resetiranje zaboravljenih ili izgubljenih lozinki, pa velike kompanije samo na takvu podršku svake godine potroše i više od milion dolara.

Kriteriji jake i sigurne lozinke

Zbog ozbiljnih reperkusija slabe lozinke, važnije je elaborirati postavke jake ali i sigurne lozinke. Općenito, jačina lozinke je mjera efikasnosti u njenom očuvanju izložene napadima pogađanjem (eng. guess attack) i ponavljanjem, tj. grubom silom (eng. brute force attack). Lozinke koje je jednostavno saznati (otkriti) nazivaju se slabe ili ranjive, dok se one druge, koje se saznaju vrlo teško ili ih nije moguće pogoditi, nazivaju jakim lozinkama; ipak, temeljem raznih istraživanja, većina ljudi, zbog jednostavne manipulacije i odsustva svijesti o opasnostima koje zbog toga prijete,

2 Ibid.

koristi upravo slabe lozinke. Jaka lozinka (Centar informacijske sigurnosti, 2012), treba zadovoljiti minimalno sljedeća dva kriterija:

– dužina lozinke i
– složenost (kompleksnost) lozinke.

Oba ova kriterija najviše utiču na mogućnost razbijanja (ili tzv. hakiranja) lozinke, jer resursi koji su potrebni za izvođenje napada tzv. grubom silom (eng. brute force) rastu eksponencijalno s povećanjem dužine lozinke. Tako, uvećanjem lozinke za dva puta potrebno je ostvariti četiri puta više operacija prilikom napada grubom silom[3]. U prilogu pojašnjenja dvaju glavnih kriterija jake i sigurne lozinke, ilustrativno je poslužiti se matematikom. Tako, lozinka od "samo" 12 znakova (isljučivo brojeva) ima 10^12 kombinacija, odnosno 1.000.000.000.000 kombinacija; no, ovakva lozinka može se tzv. grubom silom razbiti za manje od sat vremena.

No, za razliku od toga, kraća, ali kompleksna lozinka (sadrži cifre, velika i mala slova i specijalne karaktere) od 10 znakova zahtjeva čak 91800 godina[4]. Ili, jaka kompleksna lozinka od 12 znakova koja ima 475.920.310.000.000.000.000.000 kombinacija (imajući u vidu da je ukupan broj svih alfanumeričkih i specijalnih karaktera 94, dakle 2^94), iziskuje toliki broj za razbijanje čime ovaj proces tehnologijom u slobodnoj prodaji, prema Petrovskom (2015), uopće i nije moguć u realnom vremenu.

3 Ibid., str. 13

4 Ibid, str. 14.

Slika 1. Vrijeme potrebno za razbijanje lozinke

Duljina	Složenost abecede	Vrijeme pogađanja
4	a-z	1 sekunda
4	a-z, A-Z, 0-9, posebni znakovi	4.8 sekundi
5	a-z, A-Z	25 sekundi
6	a-z, A-Z, 0-9	1 sat
6	a-z, A-Z, 0-9, posebni znakovi	11 sati
7	a-z, A-Z, 0-9, posebni znakovi	6 tjedana
8	a-z, A-Z, 0-9	5 mjeseci
8	a-z, A-Z, 0-9, posebni znakovi	10 godina
9	a-z, A-Z, 0-9, posebni znakovi	1000 godina
10	a-z, A-Z, 0-9	1700 godina
10	a-z, A-Z, 0-9, posebni znakovi	91800 godina

Izvor: Centar informacijske sigurnosti, 2012
Vrijednosti u tablici kalkulirane su za sistem koji može provjeriti 15 miliona lozinki u sekundi

Treba naglasiti da se u ovom razmatranju podrazumijeva napad tzv. grubom silom na način da se softverski grade kombinacije lozinki i traži podudaranje sa dobijenom i njenom izvornom tzv. hash vrijednošću. Naime, u organizacijama je nužno praviti hash izračun lozinki i kao takve ih pohranjivati u odgovarajućoj bazi podataka (čuvati lozinke u formi čistog teksta je nedopustivo, iako se takvih slučajeva uvijek može naći!), jer je hash deterministička ali ireverzibilna funkcija (Stallings, 2014), čime je postala kriptografski standard u ovom segmentu. Inače, za generiranje hash vrijednosti koriste se softverski algoritmi, koji u imenu nose oznaku SHA (eng. Secure Hash Algorithm[5]), a najpoznatiji su SHA-1 i SHA-2. Razlika između njih je u broju bitova koje koriste u raspršivanju, a time i (ne) mogućnosti kolizije i kompromitacije; tako, SHA-1 koristi 160 bitova dok unaprijeđeni

5 Nazivaju se i algoritmima sigurnog raspršivanja

SHA-2 koristi 256 bitova ili čak i 512 bitova[6]. Pored kriterija jake lozinke, potrebno je govoriti i o kriterijima sigurne lozinke. Sigurna lozinka minimalno treba zadovoljiti sljedeća dva kriterija:

– kriteriji periodičnosti i
– kriterij raznolikosti, odnosno jedinstvenosti.

Kriteriji periodičnosti podrazumijeva redovne promjene lozinki u unaprijed određenim vremenskim razmacima, dok još važniji kriterij raznolikosti podrazumijeva korištenje različitih i jedinstvenih (eng. unique password) lozinki za korisničke naloge. Naime, procjenjuje se je u upotrebi gotovo više od 51% tzv. ponavljajućih lozinki (eng. reused password) (FIDO authentication, 2021), što najbolje ilustrira koliko se korisnici ponašaju komforno i izvan zacrtanih sigurnosnih politika u poslovnoj (i individualnoj) praksi, naprosto zanemarajući težinu koju nosi lozinka kao prva sigurnosna kapija informacijskih resursa. Problem nepoštivanja kriterija raznolikosti posebno se manifestira kroz činjenice da korisnici nerijetko svoje poslovne lozinke povezuju sa privatnim nalozima, čime problem lozinke naprosto eskalira jer se eventualna kompromitacija privatnog naloga potencijalno lako prenosi na vezani poslovni nalog.

Kad se sumira navedeno, jaka i sigurna lozinka je ona lozinka koja je (dovoljno) duga i (dovoljno) kompleksna (kombinacija slova, brojeva i specijalnih znakova), jedinstvena za različite naloge te lozinka koja se periodično mijenja. Primjeri jakih lozinki mogli bi biti sljedeći:

– uTD3Kyax7s8B+u6N
– @^635JusAWtpGxH
– #q@Bd3z4+Lq3W _ gh
– -xA-GCecLe3Nq2bA
– yrPb9R2Hw9^S8Qnv

No, zapamtiti samo jednu od navedenih jakih lozinki je doista veoma teško, a da ne govorimo o tome da ih korisnik treba zapamtiti i mnogo više, nastoji li se zadovoljiti i kriterij jedinstvenosti. Ipak, odgovori u ovom smislu na tržištu već postoje, u vidu specijalnih aplikacija koje nude kvalitetna rješenja manipuliranja jakim i sigurnim lozinkama. Radi se o aplikacijama poznatim pod zajedničkim imenom upravitelji lozinke (eng. password managers), koje preuzimaju "pamćenje" jakih i sigurnih lozinki uz logiranje na odgovarajuće naloge. Među istaknutijim aplikacijama upraviteljima lozinke u poslovnom svijetu (Best business password managers, 2021) ističu se Dashlane, LastPass, NordPass, Keeper Business Password Manager, RoboForm itd.

Aplikacije upravitelji lozinki omogućavaju ne samo pamćenje jakih lozinki, već i njihovo generiranje i automatizirano periodično obnavljanje; drugim riječima, aplikacijama se zadovoljavaju kriteriji jake i sigurne lozinke. Što je posebno važno, osigurana je i visoka sigurnost lokalno spremljenih lozinki kriptografskim algoritmom AES-256. Inače, 256-bitna AES enkripcija, koju mahom koriste upravitelji lozinki je vrsta šifriranja koja do sada nije razbijena, a kao standard u zaštiti tzv. top secret podataka (Commercial National Security Algorithm, 2015) odobrena je i od strane američke sigurnosne agencije NSA (eng. National Security Agency).

AUTENTIFIKACIJA BEZ LOZINKE

Ipak, postalo je jasno da mehanizam klasične lozinke, i pored svojih određenih nepobitnih prednosti više nije idealan način autentifikacije, jer su se informacijsko-komunikacijske okolnosti radikalno promijenile i preselile u online okruženje. Zbog toga je problematika lozinke bila i istaknuta tema posljednjeg Svjetskog ekonomskog foruma održanog 2020. godine, gdje je u nacrtu prema sigurnijoj autentifikaciji zaključeno da nove tehnologije mogu i moraju u blisko vrijeme zamijeniti "zastarjelu" tehnologiju lozinki, kako bi se prekinule štete koje trpi brzorastuća digitalna ekonomija.

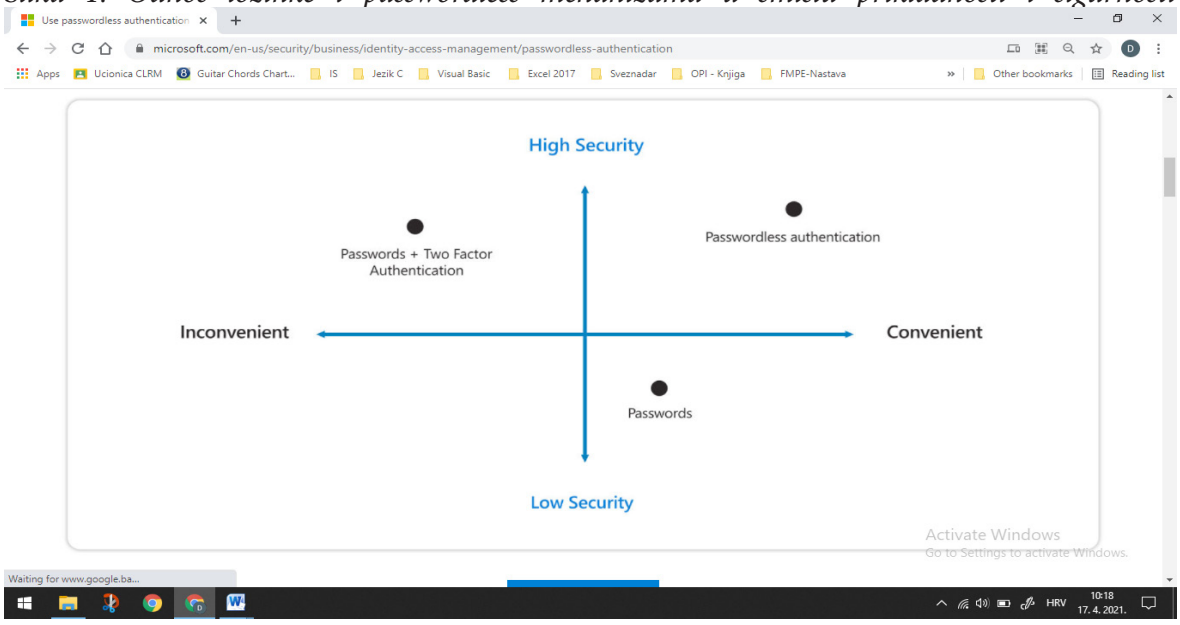
6 Broj mogućih kombinacija znakova (2^256) nadilazi čak i pretpostavljeni broj zrna pijeska na zemlji!

Na tom tragu su projekti tzv. FIDO alijanse[7] (eng. FIDO - Fast Identity Online), koja već nekoliko godina radi na implementaciji novih rješenja autentifikacije online resursa bez korištenja lozinke (eng. passwordless). Mehanizmi FIDO alijanse realizirani u vidu sigurnosnih ključeva (eng. security key) i biometrije kroz prepoznavanje lica (eng. facial recognition), prepoznavanje glasa (eng. voice recognition) i otiska prsta (eng. fingerprint) promoviraju veću prikladnost korištenja, uz viši stepen sigurnosti, između ostalog i redukciju tzv. phishing-a, kao najprominentnijeg oblika krađe digitalnog identiteta. Praktično, ovim se prave odmaci od mehanizma lozinke koja se temeljila na principu "nešto što korisnik zna", preko principa "nešto što korisnika ima" (npr. token) do finalnog principa "nešto što korisnik jest" (npr. otisak prsta, tj. biometrija) (Centar informacijske sigurnosti, 2012), i što doista ima kapacitete višeg nivoa sigurnosti u kritičnom procesu autentifikacije. U stvari, ovdje se govori o tzv. multifaktorskoj autentifikaciji (Secure access, 2021), koja se uglavnom sreće pod akronimom MFA (eng. Multi Factor Authentication).

Budućnost bez lozinki već uveliko oficijelno najavljuje i kompanija Microsoft (Hanson, 2020), u kojoj se već poduzimaju konkretni koraci na primjeni passwordless

7 Ciljana alijansa koju čine veliki svjetski IT giganti, poput Google-a, Ebay-a, Facebook-a i dr.

Slika 1. Odnos lozinke i passwordless mehanizama u smislu prikladnosti i sigurnosti



Izvor: Forget passwords, 2021

rješenja online autentifikacije (Microsoft Authenticator, Windows Hello i FIDO2 security keys). Kao razloge digitalne transformacije u Microsoft-u (Forget passwords, 2021), pored ostalog, navode i sljedeće: brže i prikladnije logiranje passwordless mehanizmima, ostvarivanje višeg stepena sigurnosti te smanjivanje IT troškova zbog resetiranja lozinki.

ZAKLJUČAK

Može se zaključiti da digitalna ekonomija doista ima ozbiljan problem uzrokovanom mehanizmom (klasične) lozinke. Doduše, bilo bi pravilnije reći, postoji problem nedosljednog upravljanja i manipuliranja jakim i sigurnim lozinkama, što se mahom pripisuje ljudskom faktoru na administratorskoj strani i na strani krajnjih korisnika, a koji u najvećoj mjeri i generiraju problem. U svakom slučaju, (klasični)

mehanizam lozinke može se smatrati kritičnim sigurnosnim aspektom digitalne ekonomije, jer je značajan procenat šteta cyber kriminalom uzrokovan upravo njime. Stoga su potpuno očekivani veliki napori svjetskih IT giganata na iznalaženju novih tzv. passwordless mehanizama autentifikacije, kako bi okončali frustrirajuće i repetitivne probleme u primjeni (klasičnog) mehanizma lozinke. Njihov krajnji cilj je oslobođanje digitalne ekonomije od mehanizma pomalo već i anahrone lozinke, kao jedne od njenih ozbiljnih razvojnih prepreka.

No, može se također zaključiti i da će mehanizam lozinke, zbog svoje dostupnosti, jednostavnosti a posebno odsustva dodatnog hardvera (tj. cijene funkcioniranja), u većem ili manjem obimu ipak ostati prisutan u cyber prostoru. Stoga, u ovako dinamičnim tehnološkim okolnostima, nužno je dosljednije upravljati aktuelnim mehanizmima autentifikacije uz snaženje ljudskog faktora, dok digitalna ekonomija u potpunosti ne implementira (pretpostavljene) passwordless mehanizme.

LITERATURA

[1] Cerovina, D, Marković, K, Škipina, M., (2014): Sigurnost informacionih sistema, Infoteh Jahorina, Vol 13, pp. 1169-1174.

[2] Krivokapić, D., i dr., (2019): Vodič za IKT sisteme od posebnog značaja, Share fondacija, Beograd, dostupno na: https://resursi.sharefoundation.info/wp-content/uploads/2020/02/Vodic-za-IKT-sisteme-od-posebnog-znacaja-2019.pdf

[3] Osmanbegović, E., (2017): Informaciona tehnologija u digitalnoj ekonomiji, Ekonomski fakultet, Tuzla, dostupno na: http://ef.untz.ba/wp-content/uploads/2017/10/7.-Informaciona-tehnologija-u-digitalnoj-ekonomiji.pdf

[4] Petrovski, A., (2015): Bezbednost u digitalnom okruženju, Share foundation, Novi Sad, dostupno na: https://resursi.sharefoundation.info

[5] Stallings, W., (2014): Cryptography and Network Security Principles and Practice, Sixth Edition, Pearson, New Jersey, dostupno na: http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf

[6] Vukić, T., (2021): Ekonomija bi trebala zaboraviti lozinke, časopis Lider, juli 2021, dostupno na: https://lider.media/poslovna-scena/tehnopolis/ekonomija-bi-trebala-zaboraviti-lozinke-132208

[7] Rukovanje lozinkama, Centar informacijske sigurnosti Hrvatske, (2012), dostupno na: https://www.cis.hr/files/dokumenti/CIS-DOC-2012-04-046.pdf

[8] Best business password managers in 2021, (2021), https://www.techradar.com/best/business-password-management-software

[9] Commercial National Security Algorithm Suite, (2015), https://apps.nsa.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

[10] FIDO authentication in the answer, (2021), FIDO Alliance, https://fidoalliance.org

[11] Forget passwords, go passwordless, (2021), https://www.microsoft.com/en-us/security/business/identity-access-management/passwordless-authentication

[12] Hanson, M, Microsoft aims to kill off password in 2021, (2020), https://www.techradar.com/news/microsoft-aims-to-kill-off-passwords-in-2021

[13] Secure access to resources with multifactor authentication, (2021), https://www.microsoft.com/en-us/security/business/identity-access-management/mfa-multi-factor-authenticationm

[14] Top 200 most common passwords of the year 2020, (2021), https://nordpass.com/most-common-passwords-list