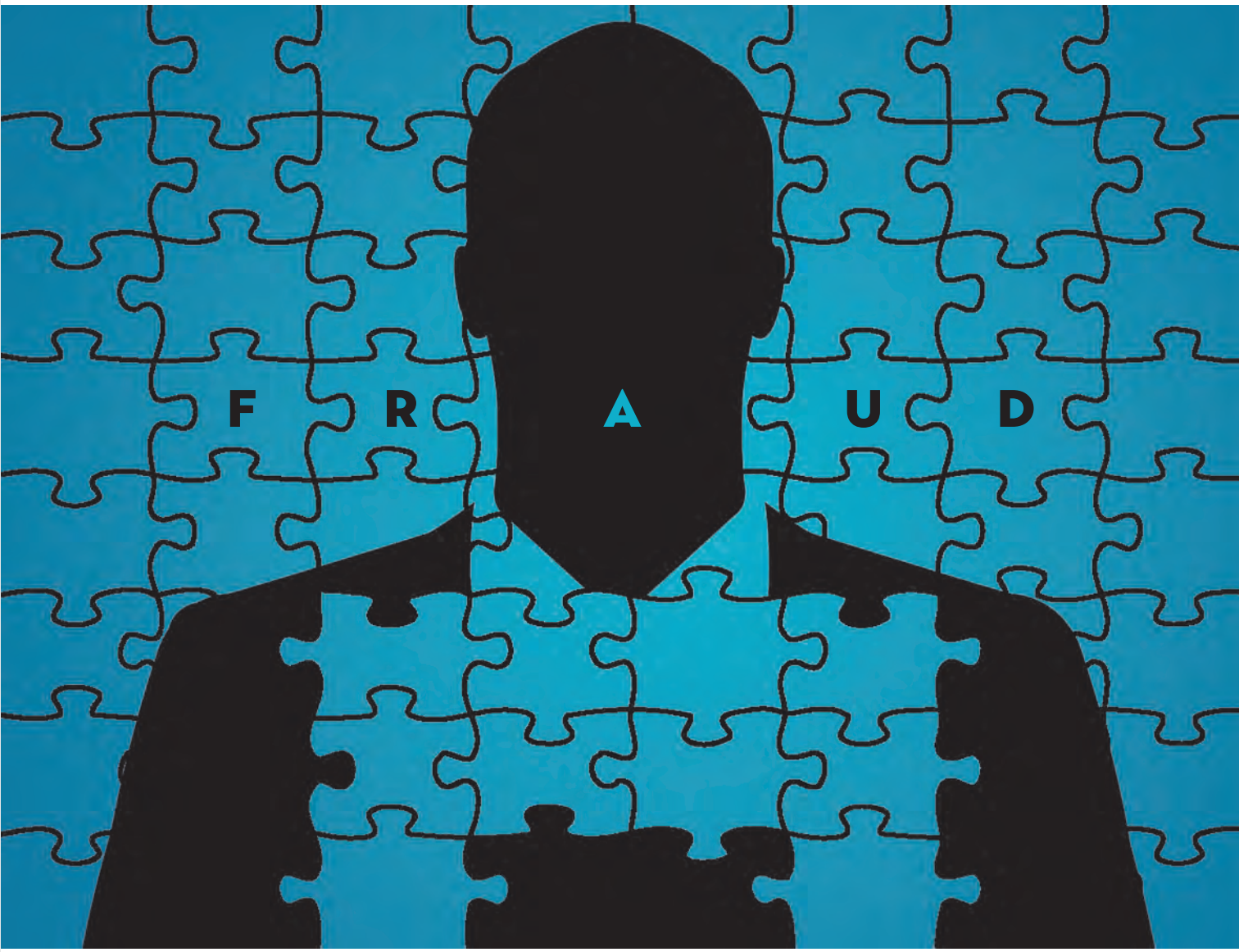
GOD. 3 . BR. 3/4 [2019] EDUKATIVNI ČASOPIS ZA BANKARSKI I FINANSIJSKI SEKTOR U BiH ISSN 2566-3100

FRAUDinfo

UDRUŽENJE PROFESIONALNIH RIZIK MENADŽERA U BOSNI I HERCEGOVINI



9 772566 310008

UPRMBiH
Udruženje profesionalnih rizik menadžera

EFSE
EUROPEAN FUND FOR SOUTHEAST EUROPE
DEVELOPMENT FACILITY

Amir Softić
Predsjednik Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini

Amar Brkan
Generalni sekretar Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini

Dragi čitaoci!

Pred vama je treće izdanje stručnog časopisa Fraud Info koje izdaje Udruženje profesionalnih rizik menadžera u BiH. Sam časopis se bavi rizicima prevara kako u realnom, tako i u finansijskom sektoru. U njegovom fokusu su najaktuelnije teme koje se tiču svih nas, neovisno u kojoj industriji bili zaposleni, uključujući i rizike sa kojima se naše društvo i naše porodice svakodnevno suočavaju. Danas smo svjedoci u kojoj su mjeri tehnološke inovacije praćene i brojnim rizicima prevarnih radnji, od onih koji su vezani za zloupotrebe ličnih podataka, do novih tehnika direktnih prevara i kriminalnih aktivnosti. U ovom, nezaustavljivom, tehnološkom razvoju niko nije pošteđen mogućeg napada i niko se ne može osjećati sigurnim. Zbog toga podizanje svijesti, nivoa razumjevanja obrazaca prevara i stručnih znanja iz oblasti zaštite protiv mogućih prevara, postaje *qonditio sine qua non* naših života.

Kao i u prethodna dva izdanja, naši urednici i saradnici su i za ovo izdanje pripremili veliki broj stručnih članaka, osvrta i analiza. Spektar tema je veoma širok, počevši od Uredbe o zaštiti podataka (GDPR) i zaštiti identiteta u savremenom vremenu, do cyber kriminala i samih tehnika prevencije i odbrane. U ovom broju, naši autori otvaraju pitanja poštivanja etičke usklađenosti i korištenja povlaštenih informacija na tržištu kapitala u BiH, temu koju smo odavno izgubili iz vida. Tu je i tema koja nas najviše muči i vezana je za odlazak stanovništva iz BiH, a što se višestruko reflektuje na ukupne rizike poslovanja u BiH. I naravno tu su i brojne druge zanimljivosti.

Fraud Forum izdajemo pred našu Drugu regionalnu konferenciju risk menadžera, koja u svom fokusu upravo ima rizike poslovanja u BiH i jačanje bankarskog sektora. Sigurni smo da će i ova konferencija otvoriti brojna pitanja koja su usko vezana za naše svakodnevne obaveze i područja odgovornosti. Zato se radujemo našem skorom susretu!

Vas dragi čitaoci, pozivamo da nam se pridružite i kroz svoje sugestije, pitanja i prijedloge pomognete da ovaj bilten bude što kvalitetniji i sadržajniji. Sve Vaše sugestije, pitanja i prijedloge možete slati na oficijelnu e-mail adresu UPRMBIH **amar.brkan@uprmbih.ba**.

Ovu priliku koristimo da se posebno zahvalimo našem partneru Odjelu tehničke podrške Evropskog fonda za Jugoistočnu Evropu (EFSE DF), koji je podržao cjelokupan projekat i omogućio nam da Fraud Info bude distribuiran do vas i u 2019 godini!

UPRMBiH
Udruženje profesionalnih rizik menadžera

FRAUDinfo

Udruženje profesionalnih rizik menadžera u BiH

Zagrebačka 50/IV,
71 000 Sarajevo - BiH

tel.:
+387 62 393 568

e-mail:
amar.brkan@uprmbih.ba

Izdavač:
UDRUŽENJE
PROFESIONALNIH
RIZIK MENADŽERA

Design, DTP & Print:
PERFECTA, Sarajevo

perfecta

Branilaca Šipa 33

tel.:
+387 61 214 222

e-mail:
info@perfecta.ba

ISSN 2566-3100

UVODNA RIJEČ

Dragi čitaoci,

treće izdanje Fraud Info časopisa predstavlja produkt kontinuirane saradnje finansijskih institucija u domeni prevara (fraud), uz podršku i pokroviteljstvo Udruženja profesionalnih rizik menadžera BiH. Savremeni način poslovanja putem raznih kanala, otvara sve više prostora za nove oblike prevara, posebno vezanih za finansijski sektor. Samim tim, nameće se potreba o podizanju svijesti o istima, kao i potreba za pojačanim monitoringom i prevencijom, praćenom primjenom adekvatnih mjera i alata.

Tim eksperata ispred Fraud foruma pored redovnih diskusija iz domene prevara, nastoji kroz časopis Fraud Info dati osvrt na posljednje fraud trendove, kao i kako ih prepoznati i prevenirati. Prevencija od prevara postaje i odgovornost pojedinca, te upravo iz tog razloga tim ukazuje kako se na jednostavan način zaštititi od pojedinih oblika. Tim ujedno prati i zakonske i ekonomske promjene na tržištu koje također mogu uticati na redovno poslovanje finansijskog sektora posebno u domeni sprečavanja prevara, te s tim u vezi obrađuje aktuelne teme ukazujući na eventualnu problematiku i potencijalna unaprjeđenja.

Cyber prevare su uvijek u fokusu tako da autori pišu o nekoliko oblika prevara u BiH i regionu koje su obilježile 2018. godinu, zloupotrebi identiteta, te nekreditnim prevarama (cyber crime),

Sadržaj

uz preporuku kako se pojedinci i poslovni subjekti mogu zaštititi od virtuelnih počinioca prevara. Što se tiče kreditnih prevara, uposlenici finansijskih institucija su definitivno najbolji izvor prevencije potencijalnih kreditnih prevara, te u tom pogledu autori ukazuju na nužnost kontinuirane i kvalitetne edukacije.

U ovom broju donosimo nekoliko zanimljivih ekspertiza, gdje autori sa aspekta postojeće zakonske regulative i praktične primjene ukazuju na prostor za unaprjeđenja poput nužnosti uspostavljanja i upravljanja rizikom etičke usklađenosti i integriteta na tržištu kapitala u BiH i optimizacije iskorištenosti polica osiguranja u domeni bankarskog poslovanja, te stručno obrađuju primjenu regulative i prakse u BiH i Europskoj Uniji u domeni zloupotrebe povlaštenih informacija na tržištu kapitala.

GDPR regulativa (General Data Protection Regulation), odnosno Opća Uredba o zaštiti osobnih podataka koja generalno regulira zaštitu osobnih podataka građana Europske unije, svojom kompleksnošću i sveobuhvatnošću predstavlja veliki zaokret na polju zaštite osobnih podataka, te čitaocima u ovom broju prezentiramo izazove koje ova regulativa donosi u kontekstu upravljanja fraud-om. Sigurni smo da će biti jako korisno upoznati se sa detaljima o stvarnim pravima koncesionara i problemima sa kojima se isti mogu susresti.

Vjerujemo da novo, treće izdanje Fraud Info časopisa donosi dosta zanimljivih tema i aktuelnosti. Cilj eksperata okupljenih u okviru Fraud foruma je da ukažu na posebne oblike prevara i predlože mjere prevencije primjenjive čak na nivou pojedinca, kao i da prate relevantne tržišne i zakonodavne promjene koje utiču na poslovanje finansijskog sektora. Djelovanje finansijskih institucija kroz ovakvu vrstu saradnje primarno doprinosi zajedničkoj borbi protiv prevara koje sve više postaju „brzorastuća industrija“. ■

UREDNIČKI TIM ČASOPISA

Kontinuirana edukacija je najsigurnija prevencija od prevara

UPOSLENICI
- NAJBOLJI „IZVOR“ PREVENCIJE POTENCIJALNIH KREDITNIH PREVARA

Klijent dolazi u kontakt sa uposlenikom koji svojim kompetencijama identificira znakove sumnjivog ponašanja klijenta te poduzima aktivnosti sprečavanja prevare

Autori:
Berina Kapa
Vedran Vinšalek

Temelj kvalitetnog i efikasnog procesa sprečavanja kreditnih prevara predstavljaju adekvatno definisane politike, procedure i radni procesi unutar organizacije. Nužno je osigurati da su svi uposlenici, koji su uključeni u proces odobrenja kredita, dobro upoznati sa istima. Dakle, znanje je preduslov da bi se podigla svijest uposlenika o značaju prevencije i sprečavanja potencijalnih kreditnih prevara.

> *Redovna i kvalitetna edukacija je nužna kako bi uposlenici bili što kompetentniji da u kreditnom procesu identificiraju znakove sumnjivog ponašanja klijenata i aktivnosti koje mogu predstavljati prevaru.*

Usvajanjem neophodnog znanja iz oblasti upravljanja kreditnim prevarama podižemo svijest kod uposlenika koji su uključeni u proces odobrenja kredita. Kada uposlenik prepozna prevarnu aktivnost, banka može biti sigurna u predanost uposlenika kodeksu i želji da spriječi prevaru. Redovna i kvalitetna edukacija je nužna kako bi uposlenici bili što kompetentniji da u kreditnom procesu identificiraju znakove sumnjivog ponašanja klijenata i aktivnosti koje mogu predstavljati prevaru. Pored navedenog je veoma bitno biti upoznat sa načinom postupanja prilikom uočavanja sumnje na prevaru.

Edukacija kao strateški cilj
Bilo koja vrsta edukacijske metode kojom banke mogu obezbjediti prenos znanja i prakse iz oblasti sprečavanja kreditnih prevara uposlenicima u prodajnoj mreži, smatra se efikasnom. Kako se radi o posebnoj vrsti rizika po banke u kreditnom poslovanju, ovakve edukacije bi trebale biti i sastavni dio godišnjeg strateškog cilja na polju ulaganja u znanje i vještine uposlenika koji vode poslovni odnos direktno sa klijentima. Ključnu ulogu u realizaciji edukacija nose specijalisti za sprečavanje kreditnih prevara.

> *Edukacije trebaju biti sastavni dio godišnjeg strateškog cilja na polju ulaganja u znanje i vještine uposlenika koji vode poslovni odnos direktno sa klijentima.*

Online edukacije su jednostavnije za pripremu i realizaciju, ali isto tako pružaju i fleksibilnost uposlenicima u pogledu vremena koje će odvojiti za edukaciju. Ova vrsta prezentacija omogućava prezentiranje ključnih preporuka, poruka i mjera u borbi

> *Svaka vrsta podrške ili savjeta je dragocijena kada je u pitanju širenje svijesti o riziku od potencijalnih kreditnih prevara.*

sa potencijalnim kreditnim prevarama uz primjere prevarnih šablona i vrsta prevare iz prakse, kao i trendova prevara u regionu i na globalnom nivou. Uz teoretski dio, prezentacija omogućava efikasan vizuelni prikaz praktičnih primjera kako prepoznati elemente potencijalno krivotvorene dokumentacije (npr. *platna lista*), odnosno elemenata na dokumentaciji poput *Zahtjeva za kredit* (npr. ID broj poslodavca, kontakt telefon, ime ovlaštene osobe, pečat poslodavca itd.).

Trening je tradicionalni tip organiziranja edukacija uposlenika, a u oblasti sprečavanja kreditnih prevara još uvijek važi za najefikasniji način razmjene znanja i iskustva između trenera (specijalist za kreditne prevare) i uposlenika prodajne mreže. Za razliku od *online* edukacija, trening ipak omogućava interakciju učesnika i prostor za praktične vježbe

i diskusiju o primjerima potencijalnih prevara iz prakse. Dakle, pored izlaganja o teoretskom dijelu iz oblasti politika i procedura sprečavanja kreditnih prevara, kroz interaktivne vježbe uposlenici su u prilici iskazati svoje vještine i usvojena znanja kako uočiti potencijalno sumnjivo ponašanje klijenta, nedosljednosti i potencijalni falsifikat dokumenta ili nekog elementa sa *Zahtjeva za kredit* i sl. Ovakva vrsta treninga doprinosi i jačanju samopouzdanja kod uposlenika jer sa treninga nose potrebnu vrstu znanja i iskustva koju će primjenjivati u svakodnevnom radu.

Savjetodavna uloga specijalista za kreditne prevare također se može smatrati metodom edukacije, budući da pruža individualnu edukativnu podršku uposlenicima u prodajnoj mreži u svom svakodnevnom radu. Bilo pismeno ili usmeno, svaka vrsta podrške ili savjeta je dragocijena kada je u pitanju širenje svijesti o riziku od potencijalnih kreditnih prevara. Veoma je bitno da uposlenici u prodajnoj mreži imaju podršku i oslonac od strane specijalista za sprečavanje kreditnih prevara, odnosno da u svakom momentu znaju na koju adresu se obratiti za bilo koju vrstu pomoći i podrške u slučaju sumnje na potencijalnu kreditnu prevaru.

Dijeljenje konkretnih primjera iz prakse (*best practice share*) je izrazito učinkovit vid educiranja poslovne mreže o karakteristikama i tehnikama pokušaja kreditnih prevara. U slučaju otkrivanja potencijalne prevare, preporuka je poslovnu mrežu pravovremeno upoznati sa osnovnim karakteristikama i elementima konkretnog slučaja kroz detaljan opis koji su podaci na *Zahtjevu za kredit* krivotvoreni, a koja dokumentacija skupa sa određenim elementima je falsificirana u odnosu na standardnu. U instrukciji se potrebno treba pozvati na važeće procedure i upute o sprečavanju kreditnih prevara te sugerisati konkretne mjere i tehnike kako prepoznati i prevenirati buduće potencijalne prevare. Na ovaj način se efikasno pojašnjava primjena relevantnih procedura i mjera na konkretnom primjeru u praksi, a što veoma efikasno utiče na podizanje svijesti uposlenika o potrebi za kontinuiranim oprezom u svakodnevnom radu. ■

OPĆA UREDBA O ZAŠTITI PODATAKA *(GDPR) I FRAUD*

Kako uspostaviti ravnotežu između *Zakona o zaštiti ličnih podataka BiH* i sankcionisanja počinioca *frauda* objavljivanjem njegovog identiteta, a u svrhu sprečavanja počinjenja novog krivičnog djela

Autor:
Mujo Vilašević

Zašto *fraud* i zaštita ličnih podataka?

Bilo koja diskusija o *fraudu* u finansijskom sektoru neminovno za sobom povlači pitanje zaštite ličnih podataka. Naime, *fraudom* oštećena strana zainteresirana je naročito za zaštitu od "povratnika u počinjenju *frauda*", a što je u vrijeme visoko razvijenih informacionih tehnologija i sofisticiranog kriminala gotovo u većini slučajeva *frauda* i očekivana pojava. Jedan od alata takve zaštite je svakako informacija, i to informacija o počiniocu *frauda*, a naročito o "povratniku u počinjenju *frauda*". U tom smislu je neminovno suočavanje sa terenom zaštite ličnih podataka. U biti se problem svodi na uspostavljanje ravnoteže legitimnih interesa. S jedne strane, legitiman interes oštećenog (subjekta finansijskog sektora) je sankcija počinitelja *frauda* i prevencija

> *Legitiman interes oštećenog je sankcija počinitelja frauda i prevencija od novog počinjenja frauda, a legitimni interesi počinioca frauda se tiču zaštite njegovih ličnih podataka, naročito podataka koji se tiču sudskih osuda, postupaka ili optužnica.*

od novog počinjenja *frauda*. Ujedno je to i legitiman interes društva da se zaštiti od počinjenja krivičnog djela, što je *fraud* u svojoj suštini. Međutim, s druge strane tu su legitimni interesi počinioca *frauda*, a oni se tiču zaštite njegovih ličnih podataka, naročito podataka koji se tiču sudskih osuda, postupaka ili optužnica. Nije ni bezazleno, podaci o krivičnim osudama ulaze u tzv. "posebnu kategoriju" ličnih podataka, koje lokalni, a naročito evropski propisi posebno štite.

U konfrotaciji, ili preciznije rečeno uspostavljanju ravnoteže ovih interesa, svoj poseban značaj daje novi okvir zaštite podataka u Evropskoj uniji, odnosno, **Opća uredba o zaštiti podataka (GDPR)**.

Šta donosi GDPR?

Godine 2017. i 2018. obilježili su brojni javni diskursi na temu GDPR-a. Revolucija ili evolucija u zaštiti ličnih podataka, sada je sasvim i svejedno, s obzirom na to da je državama EU rok za usklađivanje bio 25. maj 2018. godine, a za države u procesu pridruženja (kao što je BiH) obaveza usklađivanja sa GDRP-om je neminovna i trajna, s obzirom na odredbe *Sporazuma o stabilizaciji i pridruživanju* koje obavezuju BiH na preuzimanje cjelokupne pravne stečevine (*aquis communitare*) EU, a koja

> *GDPR donosi određene pravne obaveze, npr. pravo na zaborav, specifična prava kod automatske obrade podataka, pravo na prenos podataka kod drugog kontrolora, uspostava Data Protection officera, precizno definisanje institucionalne zaštite ličnih podataka u prekograničnoj obradi podataka, itd.*

uključuje i GDPR. Kroz svoj pravni karakter Uredbe, koja kao takva formalno-pravno neposredno obavezuje i u cjelosti se primjenjuje u svakoj državi članici, diskusije o djelomičnoj ili relativizirajućoj primjeni GDPR-a su izlišne jednako kao i nesvrsishodne. Dakle, GDPR će se akceptirati i primjenjivati u cjelosti i u BiH, a prema stanju najava lokalnih regulatora kroz sasvim novi *Zakon o zaštiti ličnih podataka u BiH*.

GDPR donosi određene, do sada nepoznate pravne obaveze svim članicama, odnosno, subjektima kontrolorima i procesorima ličnih podataka, a koje se odnose npr. na pravo na zaborav, specifična prava kod automatske obrade podataka, pravo na prenos podataka kod drugog kontrolora, uspostava *Data Protection officera*, precizno definisanje institucionalne zaštite ličnih podataka u prekograničnoj obradi podataka, itd. Ono što GDPR naročito uvažava jesu činjenice elektronske obrade ličnih podataka, pa naposljetku i elektronskog i digitalnog poslovanja EU, na osnovu čega uvodi nove kategorije poput "elektronske saglasnosti za obradu ličnih podataka".

Da li GDPR pomaže prevenciju frauda?

Nesporno je da brojni procesi u vezi sa *fraudom* uključuju obradu ličnih podataka.

GDPR prepoznaje važnost prevencije *frauda* kroz dvije odredbe:

Recital 47: *Obrada ličnih podataka, isključivo neophodno za prevenciju frauda podrazumijeva legitimni interes involviranog kontrolora podataka...*

Recital 71: *Donošenje odluka zasnovano na profiliranju bi trebalo biti dozvoljeno tamo gdje postoji zakonsko ovlaštenje, uključujući fraud i nadzor nad poreskim prevarama i u svrhe prevencije.*

Također, propisan je veoma važan izuzetak u vezi sa pravom na brisanje ličnih podataka nosioca, *u vezi sa uspostavom, izvršenjem ili zaštitom pravnih interesa*.

Bez obzira čiji interesi se uzimali u obzir, obrada ličnih podataka u smislu GDPR-a, pa i u vezi sa *fraud* počiniocima i *fraud* prevencijom, mora biti u skladu sa GDPR principima koji uključuju i princip zakonite obrade, transparentnost u obradi, pravnu osnovanost obrade i zakonitost svrhe obrade. Obrada ličnih podataka u svrhu *fraud* prevencije mora biti obuhvaćena pristankom nosioca podataka. Jedini moguć izuzetak za to je ako bi obrada podataka isključivala lične podatke i obavljala se isključivo u statističke svrhe. Iako je pristanak nosioca podataka u većini slučajeva dio ugovornog sadržaja, saglasnost na zasebnom dokumentu je u svakom slučaju poželjna. Naravno,

> *Automatska rješenja za prevenciju frauda neće biti dostatna i ljudski faktor će i dalje biti neophodan i prisutan u finansijskim organizacijama kod procjene parametara i rizika frauda.*

postavlja se pitanje koliko bi takav tekst na saglasnostima bio odvraćujući klijentima, a naročito u finansijskom sektoru, jer bi mogao ukazivati na potencijalnu presumpciju prevare za svakog klijenta. Vjerovatno je da bi takva opcija u procjeni uticaja izgubila na podršci, bar u finansijskom sektoru.

Prevencija *frauda* najčešće uključuje automatsku obradu podataka, posebno prilikom akvizicije klijenata. Međutim, GDPR nalaže kontrolorima odgovarajuća obavještenja koja moraju biti upućena nosiocima podataka u vezi sa automatskom obradom podataka. Ovo pravo nosioca podataka uključuje dostupno, detaljno i logično obavještenje o obradi i svrsi obrade automatskim putem, kao i potencijalnim posljedicama takve obrade (što u slučaju *frauda* može biti i obustava transakcije). Nosiocima podataka ostavljeno je i pravo prigovora na odluke koje su izvršene u cjelosti automatikom – što znači, ako je sistem podešen tako da automatski obrađuje podatke, detektuje indiciju (npr. kartični *fraud)* i zaustavi transakciju (blokada kartice), nosilac podataka, tj. klijent, ima pravo prigovora na takvu odluku o obustavi. Način na koji se ovaj problem može prevazići jeste da se kalkulacija parametara *frauda* u tom slučaju vrati na manuelni izračun i da prednost ima ono što je zaključeno kao proces takvog izračuna. Konsekventno, automatska

rješenja za prevenciju *frauda* neće biti dostatna i ljudski faktor će i dalje biti neophodan i prisutan u finansijskim organizacijama kod procjene parametara i rizika *frauda*. Prethodno, samo kao jedan od primjera veze između GDPR-a i *frauda*, a u određenoj mjeri je i odgovor na pitanje u podnaslovu teksta.

Kako dalje?

Da li je finansijskom sektoru generalno bio potreban "novi sloj" zaštite podataka, nova regulativa koja donosi nove obaveze, operativno, troškovno, procesno? Možda bi odgovor bez detaljne analize bio i potvrdan, posebno kada se uzme u obzir šta sve u kontekstu prevencije *frauda* donosi GDPR.

> *U finansijskom sektoru edukacija o najboljim praksama implementacije GDPR-a, pa i u kontekstu prevencije frauda, je neupitno neophodna, posebno u uslovima poslovanja u Bosni i Hercegovini.*

Međutim, sigurnost ličnih podataka bi se mogla (i trebala) posmatrati i iz drugog ugla. Takva sigurnost štiti od krađe identiteta, zloupotrebe podataka, elektronskih i automatiziranih manipulacija podacima koji mogu itekako biti u srži *frauda*, naročito u finansijskom sektoru. Stoga, odgovori na pitanja postavljena u ovom tekstu nisu jednostavni, nisu jednoobrazni i sigurno da GDPR i *fraud* nisu suprostavljene teme. Ove teme, za početak, iziskuju edukaciju. U finansijskom sektoru edukacija o najboljim praksama implementacije GDPR-a, pa i u kontekstu prevencije *frauda*, je neupitno neophodna, posebno u uslovima poslovanja u Bosni i Hercegovini. Zaštita ličnih podataka jeste i bit će sve aktuelnija tema. S druge strane, *fraud* jeste i bit će sve sofisticiraniji oblik kriminala.

Iz takvih razloga, finansijski sektor može ovu temu prihvatiti jedino kao izazov. Izazov koji valja prevazići, a možda i u decenijama koje dolaze. ■

(tekst je objavljen u magazinu Banke i Biznis, broj 202, januar/februar 2019.)

Krađa identiteta je polazna tačka za izvršavanje kriminalnih djela

ZLOUPOTREBA IDENTITETA U SAVREMENOM VREMENU

Krađa i zloupotreba identiteta je jedna od najzastupljenih prevara u svijetu kako u online, tako i u offline okruženju

Autorica:
Berina Kapa

Krađa i zloupotreba identiteta *(engl. identity theft)* je prevarno korištenje osobnih podataka fizičke osobe od strane treće osobe. Cilj krađe identiteta je, na primjer, prikrivanje kriminalnih aktivnosti, postizanje prevarne finansijske koristi, prodaja podataka dotične osobe zainteresiranim stranama i sl.

Sa razvojem novih i sofisticiranih tehnologija pojavili su se i novi pristupi neetičkom ponašanju, odnosno načinima na koje se mogu zloupotrijebiti lične informacije, posebno putem interneta. Osoba koja ukrade identitet može da zloupotrijebi isti, kupuje određenu robu i mnoge druge stvari. Ova vrsta zloupotrebe je u svijetu jedna od najzastupljenijih, kako u *online*, tako i u *offline* okruženju. Ono što je zanimljivo jeste činjenica da različite vrste drugih oblika kriminalnih aktivnosti, koje se dovode u vezu sa računalnim kriminalom, u osnovi imaju krađu identiteta kao polaznu tačku za izvršavanje kriminalnih djela.

> *Cilj krađe identiteta je, na primjer, prikrivanje kriminalnih aktivnosti, postizanje prevarne finansijske koristi, prodaja podataka dotične osobe zainteresiranim stranama i sl.*

VRSTE KRAĐE IDENTITETA

Neke od vrsta krađe identiteta na globalnom nivou uključuju finansijsku, kriminalnu, sintetičku, medicinsku krađu te kloniranje identiteta.

Finansijski motivirana krađa identiteta

Krađa finansijskog identiteta se događa kada počinilac krade osobni identitet pojedinca i počini zločin koji rezultira finansijskom povredom žrtve.

Kriminalna krađa identiteta

To je vrsta zloupotrebe u kojoj osoba ima pristup tuđim identifikacijskim podacima. Počinilac se lažno predstavlja kao neko drugo lice tokom hapšenja da bi pokušao da izbjegne pozive, spriječi otkrivanje naloga izdatog u njegovo pravo ime ili izbjegava zapisnik o hapšenju ili osudi.

Sintetička krađa identiteta

Ova prevara uključuje upotrebu fiktivnog identiteta. Počinioci stvaraju nove identitete koristeći kombinaciju stvarnih i izmišljenih informacija ili ponekad potpuno fiktivne informacije.

Medicinska krađa identiteta

Zloupotreba medicinskog identiteta se događa kada neko krade osobne podatke kako bi dobio medicinsku skrb, kupio lijekove ili kada želi da podnese lažne naplate na ime žrtava.

Kloniranje identiteta

To je način prevare gdje se počinilac predstavlja kao druga osoba u svakodnevnom životu.

NAJČEŠĆI NAČINI KRAĐE I ZLOUPOTREBE IDENTITETA

Kada je riječ o krađi i zloupotrebi osobnih podataka, mogući su ipak razni scenariji u kojima dolazi do takvih situacija. Ako se osobni podaci lakovjerno dostavljaju nepoznatim osobama ili se ne štite adekvatno te se u prevelikom opsegu objavljuju na društvenim mrežama, internetu i slično, postoji opasnost od njihove zloupotrebe.

Samo neki od najčešćih načina na koji počinioci mogu izvršiti zloupotrebu identiteta su:

- neovlašteni upad u računalni sistem,
- *malware* koji se obično instalira u sistem računala bez znanja korisnika ili

posebnog odobrenja, odnosno zlonamjerni softver gdje hakeri zaključaju vaše računalo te traže otkupninu,
- *phishing* koji funkcionira tako što žrtva primi krivotvorenu e-poštu koja izgleda kao da stiže od velike tvrtke, institucije ili druge organizacije,
- spam poruka koja se šalje primatelju bez njegovog dopuštenja, a koja često sadrži i prevaru.

> *Ako se osobni podaci lakovjerno dostavljaju nepoznatim osobama ili se ne štite adekvatno, postoji opasnost od njihove zloupotrebe.*

Jedan od praktičnih primjera jeste odgovaranje na e-mail nepoznate osobe koja tvrdi da ste dobili veliko nasljedstvo u inostranstvu te traži Vaše osobne podatke i/ili uplatu na njen račun, budući da je ona advokat koji mora poduzeti odgovarajuće pravne radnje u svrhu prenosa nasljedstva. Iako se čini previše naivnim odgovaranje na e-mail u svrhu dobijanja nepostojećeg nasljedstva, ovakvih prevarnih slučajeva je zaista bilo u praksi.

PREVENCIJA KAO NAJBOLJI OBLIK ZAŠTITE

Najbolja zaštita od krađe identiteta jeste biti svjestan iste te znati kako je prepoznati. Postoje brojni načini na koje je moguće zaštititi se od potencijalne zloupotrebe:
- Vodite računa o vašim ličnim dokumentima i pazite gdje ih ostavljate.
- Račune sa imenom, adresom, brojem računa, potpisom i sl. ne ostavljajte dostupnim drugim licima.
- Ne bacajte dokumenta sa vašim informacijama u otpad koji je dostupan svima. Prijedlog je čuvati sva važna dokumenta.
- Redovno ažurirajte računare i antivirusne programe.
- Vodite računa o javnim WiFi mrežama na koje se spajate.
- Ne otvarajte raznorazne reklame na web sajtovima.
- Pazite koje e-mail poruke otvarate.
- Ne ulazite na sajtove koji su manje poznati i dobro pogledajte adresu bolje poznatih sajtova kako ne biste 'nasjeli' na prevaru.

Ne treba ostavljati lične podatke na društvenim mrežama. Kradljivci identiteta najčešće koriste informacije sa društvenih mreža za „upad" u lozinke vašeg e-maila ili drugih šifri koje koristite. ■

(tekst je objavljen u magazinu Banke i Biznis, broj 206, juni 2019.)

Zanimljivosti

DA LI STE I VI ŽRTVA *DATA BROKERA*?

Autorica:
Sanela Stupar

Da li i vi imate karticu lojalnosti trgovačkih centara?

Data Brokeri su specijalisti koji prikupljaju vaše lične podatke, fotografije, kontakte, informacije koja mjesta posjećujte, ko su vaši prijatelji i prijatelji vaših prijatelja, vašu medicinsku dokumentaciju, vaše potrošačke navike.

Sve podatke koje prikupe o vama *Data Brokeri* prodaje firmama obično u marketinške svrhe.

Data Broker angažovan je u kompanijama za posredovanje podataka koje imaju višemilionsku zaradu radi skupljanja podataka o potrošačima. Širom svijeta postoji preko 5.000 kompanija za posredovanje podataka.

Acxiom, jedan od najvećih, ima 23.000 servera koji prikupljaju i analiziraju podatke o potrošačima. Raspolažu sa podacima za 500 miliona potrošača širom svijeta i do 1.500 podataka po osobi.

Zato nemojte se iznenaditi kada dobijete telefonski poziv, SMS ili mail u kojem vam neka kompanija nudi svoje usluge ili proizvode ciljane baš za vas na osnovu vaših navika.

Na internetu možete potražiti informacije kako da izbrišete podatke o sebi, a za koje ste možda dali slučajno saglasnost. ■

Finansijsko tržište na meti *insajdera*

ZLOUPOTREBA POVLAŠTENIH INFORMACIJA:

REGULATIVA I PRAKSA U BOSNI I HERCEGOVINI I EVROPSKOJ UNIJI

Iako je zakonska regulativa iz ove oblasti u BiH uređena, do sada u našoj državi nisu vođeni značajniji sudski sporovi koji se tiču zloupotrebe povlaštenih informacija, a to možemo pripisati skromnom finansijskom tržištu i nedostatku značajnije prakse, kao i činjenici beskonačnog procesa privatizacije kapitala u BiH.
Međutim, iskustva iz Evropske unije nam govore drugačije...

Autori:
Nermin Ibradžić
Mujo Vilašević

Operacija *Tabernula*

U maju 2016. godine na kraljevskom sudu Southwark (London, UK) **Martin Dodgson i Andrew Hind** osuđeni su na kazne zatvora u trajanju od 4,5 i 3,5 godine zbog urote radi korištenja insajderskih (povlaštenih) informacija.

Rezultat je ovo osmogodišnje istrage koju je provodio **FCA** (*Financial Conduct Authority of U.K.*) kao regulator finansijskih tržišta u Ujedinjenom Kraljevstvu, kojem je dodijeljena i nadležnost provođenja istraga sumnji na zloupotrebe insajderskih informacija. Istraga je provedena pod kodnim imenom ***Operacija Tabernula***.

Za dvojac Dodgson – Hind je dokazano da su djelovali na sljedeći način.

Dodgson je kao visokopozicionirani menadžer u više kompanija (*Morgan Stanley, Lehman Brothers i Deutsche Bank*) imao pristup povlaštenim informacijama. U jednom od slučajeva Dodgson je imao pristup informacijama ili je i lično učestvovao u pregovorima proizvođača pića ***Carlsberg*** i ***Heineken*** koji su za cilj imali preuzimanje lokalnog proizvođača pića ***Scottish & Newcastle***. Ovu informaciju Dodgson je proslijedio Hindu prije nego je namjera preuzimanja od

Carlsberga i *Heinekena* bila objavljena široj javnosti.

To je omogućilo Hindu da dionice *Scottish & Newcastla* kupi po nižoj cijeni, i da ih nakon objave namjere preuzimanja od strane *Carlsberga* i *Heinekena* proda za veći iznos, jer je u tom momentu cijena dionica *Scottish & Newcastla* porasla za cca. 18 %, što je kod trgovanja dionicama respektabilan rast cijene dionica.

Na ovaj način Dodgson i Hind su iskoristili povlaštene (insajderske) informacije kako bi u odnosu na ostale učesnike na finansijskom tržištu stekli nedopuštenu prednost, a samim tim i nedopuštenu imovinsku korist. Gotovo isti način rada Dogson i Hind su koristili i u slučajevima ***Paragon Group of Companies*** u julu 2008, ***Just Retirement plc*** u oktobru 2008, ***Legal & General plc*** u februaru 2009. i ***BSkyB plc*** u martu 2010. godine.

Dodgson i Hind su učinili sve kako ne bi bili otkriveni. Tako su za ostvarenje svog plana koristili jednokratne SMS kartice i mobitele za stupanje u kontakt, *iron keys* memorijske USB stikove (flash memoriju u kojoj se podaci kriptuju i nemoguće ih je očitati bez lozinke) za razmjenu podataka i vođenje evidencije i kodna imena za komunikaciju.

Isplate koje je Hind vršio Dodgsonu nisu vršene preko računa. Često je to bila „isplata“ u uslugama kao što je renoviranje kuće, plaćeni letovi British Airwaysa ili isplata u gotovini predajom koverte sa novcem na javnim mjestima (restoranima).

Koliko je komplikovana bila operacija otkrivanja i praćenja učesnika govori i činjenica da je operacija *Tabernula* koštala 14 miliona £, uključivala je više od 40 eksperata,

istražitelja, analizirano je preko 500.000 zapisa telekom podataka, 120 računa za trgovanje dionicama i preko 600 različitih digitalnih uređaja. Dogson i Hind su naknadno obavezani i da vrate iznos od 1,7 miliona £.

Po ovom pitanju stav i poruka FCA su bili jasni: FCA je odlučna u otkrivanju zloupotrebe insajderskih informacija i progonu učesnika, bez obzira koliko istraga bila kompleksna i koliko to sve skupa koštalo.

Prilikom izricanja presude sudac **Jeffrey Pegden** je izrekao jednu tvrdnju koja najbolje opisuje suštinu zloupotrebe povlaštenih informacija – *zlupotreba insajderskih informacija nije zločin bez žrtve*. I zaista je tako. Iako, za razliku od ostalih krivičnih djela, u ovim slučajevima ne postoji žrtva koju je moguće identificirati imenom i prezimenom, žrtva je u stvari cijelo finansijsko tržiše i svi učesnici na tom tržištu koji su stavljeni u nepovoljniji položaj u odnosu na osobe koje su neovlašteno iskoristile povlaštene informacije.

Ne treba posebno naglašavati da je ovaj slučaj svojevremeno privukao veliku pažnju medija.

Regulativa u BiH

Kada je riječ o finansijskom tržištu u BiH, tako zvučnih medijskih natpisa do sad nije bilo, što se prije može pripisati skromnom obimu finansijskog tržišta i nedostatku značajnije prakse, kao i činjenici beskonačnog procesa privatizacije kapitala u BiH, nego nedostatku zakonskog okvira koji u osnovi postoji.

Finansijska tržišta, pri čemu prvenstveno mislimo na tržišta kapitala, u dijelu zloupotrebe povlaštenih informacija u BiH su uređena na entitetskom nivou. U kontekstu ustavno proklamirane

> *Finansijska tržišta, pri čemu prvenstveno mislimo na tržišta kapitala, u dijelu zloupotrebe povlaštenih informacija u BiH su uređena na entitetskom nivou.*
> *Sa aspekta ekonomske efikasnosti to svakako nije bilo jedno od boljih postratnih rješenja u BiH.*

slobode kretanja kapitala na nivou cijele BiH, upitno je i podložno kritici entitetsko uređenje tržišta kapitala. Sa aspekta ekonomske efikasnosti to svakako nije bilo jedno od boljih postratnih rješenja u BiH.

U tom smislu i entitetski propisi koji uređuju ovu materiju u Federaciji Bosne i Hercegovine su ***Zakon o tržištu vrijedonosnih papira*** (Službene novine F BiH broj 85/08, 109/12, 86/15 i 25/17), a u Republici Srpskoj ***Zakon o tržištu hartija od vrijednosti*** (Službeni glasnik Republike Srpske broj 92/06, 34/09, 30/12, 59/13, 108/13 i 04/17) i ***Pravilnik o načinu sprečavanja zloupotreba povlaštenih informacija*** (Službeni glasnik Republike Srpske, broj: 29/09 i 37/09). Iako većim dijelom usklađeni, propisi entiteta u dijelu povlaštenih informacija i zabrana njihovog korištenja imaju određene razlike.

Radnju zloupotrebe povlaštene informacije određuju tri pojma:

- pojam povlaštene/insajderske informacije,
- pojam lica koje ima pristup povlaštenim informacijama (insajder) i
- opis radnji koje se smatraju zloupotrebom povlaštenih informacija.

Pojam povlaštene informacije dat je u članu 220. *Zakona o tržištu vrijedonosnih papira FBiH* (dalje označen kao: ZOTVP) iz kojeg proizilazi da povlaštena informacija u kontekstu naprijed navedenog propisa treba da ispuni određene kriterije i to:

– da se radi o povlaštenoj, privilegovanoj ili drugoj informaciji ili događaju koja njenom imaocu daje određenu prednost u odnosu na ostale učesnike u prometu vrijedonosnih papira;
– koja može imati uticaj na emitenta vrijedonosnih papira ili na tržište na kojem se prometuje vrijedonosnim papirima, uključivo cijenu vrijedonosnih papira;
– koja još nije javno objavljena.

Bitno je naglasiti da su navedeni kriteriji definisani kumulativno.

Zakonodavac je u istoj odredbi naveo i primjere **povlaštene informacije**. Tako bi se u svakom slučaju radilo o povlaštenoj informaciji ukoliko je u pitanju precizna informacija o emitentu i njegovim vrijedonosnim papirima (pod uslovom da informacija sadrži okolnosti koje postoje ili se očekuju ili se odnosi na događaj koji se zbio ili se očekuje ili ako je informacija dovoljno specifična da se može zaključiti o mogućem efektu okolnosti ili događaja koji bi uticali na cijenu vrijednosnih papira), ukoliko se radi o informaciji koju bi investitor

> *U pitanju je događaj ili informacija koji nisu poznati javnosti, koji da su poznati javnosti mogu imati uticaj na cijenu vrijedonosnog papira i koji imaocu takve informacije daju prednost na tržištu vrijedonosnih papira u odnosu na druge učesnike koji takvu informaciju nemaju.*

na osnovu razumne procjene mogao uzeti u obzir kod donošenja odluke ili ako je u pitanju „druga informacija" u skladu sa zakonom i drugim propisima.

Bitno je naglasiti da navedeni primjeri povlaštenih informacija ne predstavljaju konačan broj *(numerus clausus)* informacija koje se svrstavaju pod pojam *povlaštene informacije*. Tako bi i bilo koja druga informacija, koja bi ispunjavala opšte kriterije za povlaštenu informaciju, mogla biti cijenjena kao takva.

U pogledu definicije pojma povlaštene informacije, *Zakon o tržištu hartija od vrijednosti Republike Srpske* (dalje označen kao : ZOTHOV) u odnosu na ZOTVP sadrži nešto drugačije rješenje. Tako se povlaštenim informacijama smatraju sve činjenice koje nisu poznate javnosti, a odnose se na jednog ili više emitenata hartija od vrijednosti ili na hartije od vrijednosti koje bi, da su poznate javnosti, mogle uticati na cijenu hartija od vrijednosti. U *Pravilniku o načinu sprečavanja zloupotreba povlaštenih informacija* (delje označen kao: Pravilnik) pojam povlaštene informacije je dopunjen u dijelu preciznijeg određenja šta se sve može smatrati povlaštenom informacijom pa su to sve činjenice, događaji, radnje i pisani i/ili elektronski dokumenti.

Bez obzira na razlike entitetskih propisa u dijelu određenja pojma povlaštene informacije, oba propisa definišu osnovne elemente povlaštene informacije na identičan način: u pitanju je događaj ili informacija koji nisu poznati javnosti, koji da su poznati javnosti mogu imati uticaj na cijenu vrijedonosnog papira

> *Insajderima se smatraju članovi upravljačkih i nadzornih tijela emitenta, kao i članovi upravljačkih i nadzornih tijela društava povezanih sa emitentom, sa tom razlikom da propis u FBiH kao osnov povezanosti definira indirektno ili direktno učešće u minimalno 10% dionica emitenta, dok propis u RS-u takav uslov ne sadrži. Insajderima se smatraju i zaposlenici emitenta te druga lica profesionalno ili na drugi način angažirana kod emitenta.*

i koji imaocu takve informacije daju prednost na tržištu vrijedonosnih papira u odnosu na druge učesnike koji takvu informaciju nemaju.

Zakonom o tržištu vrijedonosnih papira propisani su i izuzeci od povlaštene informacije. Tako su to javno raspoložive informacije, zaključci, procjene ili rezultati analiza bazirani na javno raspoloživim informacijama, glasine ili nagađanja i informacije o

ponudi ili potražnji vrijednosnih papira stečene kao redovna posljedica prometa. Kod izuzetaka od povlaštene informacije zakonodavac je definisao i jedno odstupanje. Tako su glasine ili nagađanja predviđeni kao izuzetak od povlaštene informacije, ali samo u slučaju kada između glasine i nagađanja ne postoji očigledna veza sa *pouzdanim izvorom*. U pouzdane izvore je zakonodavac pri tome uvrstio lica iz člana 224. ZOTVP, takozvane *insajdere*, što uključuje i treća lica koja bi posredstvom *insajdera* došla u posjed povlaštene informacije.

Činjenica da glasine ili nagađanja iz pouzdanog izvora nisu isključeni iz pojma povlaštene informacije ipak ne daje mjesta tvrdnji da se glasine ili nagađanja iz pouzdanog izvora imaju po automatizmu smatrati povlaštenom informacijom. I za takve glasine ili nagađanja valjalo bi prethodno utvrditi da li iste ispunjavaju opće uslove povlaštene informacije iz člana 221. ZOTVP prije nego se iznese tvrdnja da je u pitanju povlaštena informacija. U budućim slučajevima zloupotrebe povlaštenih informacija uspostavljanje jasne granice između glasine ili nagađanja i povlaštene informacije za pravnu praksu bi svakako mogao biti poseban izazov.

Kroz član 224. ZOTVP i član 272. ZOTHOV definisan je pojam *insajdera* kao mogućeg izvora povlaštenih informacija. Propisi oba entiteta BiH ne prave podjelu na primarne (u pravilu lica koja su vezana za emitenta i imaju rukovodne funkcije) i sekundarne insajdere, što bi moglo imati uticaja na postojanje ili nepostojanje presumpcije posjedovanja povlaštenih informacija.

Bez obzira na navedeno, pojam mogućih insajdera zakonima oba entiteta je dovoljno široko i precizno određen.
Tako se insajderima smatraju članovi upravljačkih i nadzornih tijela emitenta (uprava, nadzorni odbor , a u FBiH i odbor za reviziju), kao i članovi upravljačkih i nadzornih tijela društava povezanih sa emitentom, sa tom razlikom da propis u FBiH kao osnov povezanosti definira indirektno ili direktno učešće u minimalno 10% dionica emitenta, dok propis u RS-u takav uslov ne sadrži.

Insajderima se smatraju i zaposlenici emitenta te druga lica profesionalno ili na drugi način angažirana kod emitenta. *Pravilnikom o načinu sprečavanja zloupotreba povlaštenih informacija* koji se primjenjuje u RS-u preciznije je definisan krug navedenih lica na: revizore, finansijske analitičare, računovođe, knjigovođe, savjetnike/konsultante, advokate, aktuare, procjenjivače, vještake, brokere, investicione savjetnike i druga lica koja vrše određene poslove ili dužnosti kod emitenta i koja imaju pristup povlaštenim informacijama. Kao posebna kategorija insajdera defiisani su i članovi upravnih i nadzornih tijela i zaposlenici ovlaštenog učesnika na tržištu vrijedonosnih papira sa tim da su u ovo kategoriju u FBiH uključeni i investicioni fondovi i društva za upravljanje investicionim fondovima.

Kao insajderi pozitivnim propisima su definisani srodnici

do prvog stepena pobrojanih lica-insajdera (ako su u pitanju fizička lica), dok su ovoj kategoriji u FBiH pridodati i supružnici ranije navedenih insajdera.

Insajderima se prema ZOTVP imaju smatrati i treća fizička ili pravna lica koja nisu naprijed označena kao insajderi, ali za koja je utvrđeno da su došla do povlaštenih informacija dok ZOTHOV za ovu kategoriju zahtjeva i da je *Komisija za hartije od vrijednosti* utvrdila da su povlaštene informacije i iskoristili.

Bez obzira kojoj od pobrojanih grupa pripadali, insajderima su zabranjenjene iste vrste aktivnosti, a to je:

- da koriste povlaštene informacije prilikom neposredne ili posredne kupovine ili prodaje vrijedonosnih papira;
- da otkriju ili učine dostupnim povlaštene informacije drugim licima i
- da koriste povlaštene informacije prilikom davanja savjeta drugim licima o kupovini ili prodaji vrijednosnih papira.

Iz naprijed navedenog proizilazi da su zabranjenjene radnje insajderima vezano za povlaštene informacije precizno definirane entitetskim propisima. Sa jedne strane to ima određenu prednost jer ne postoji nedorečenost pravne norme, dok sa druge strane može imati određene nedostatke. Tako se kod prve zabrane korištenja povlaštene informacije zakonodavac ograničio samo na dvije radnje: **kupovinu** ili **prodaju** vrijedonosnih papira (posrednu ili neposrednu), dok ostala raspolaganja vrijedonosnim papirima na osnovu povlaštenih informacija nisu definisana (npr. zalaganje vrijedonosnih papira radi osiguranja povrata novčane tražbine, znajući prethodno povlaštenu informaciju koja ukazuje da će cijena vrijedonosnog papira na tržištu padati).

Druga zabrana se odnosi na **otkrivanje** ili **činjenje dostupnim** povlaštenih informacija drugim licima. Svakako da na osnovu povlaštenih informacija ne samo primarni ili sekundarni insajderi, nego i treća lica, mogu imati materijalnu korist i doći u povoljniji položaj u odnosu na druge investitore koji takvu informaciju nemaju. Tako i pozitivni propisi **treće lice** kojem je insajder otkrio povlaštenu informaciju također svrstavaju pod pojam insajdera. Izazovi sa kojim bi se mogla sresti pravna praksa vezano za treća lica koja indirektno dođu u posjed povlaštene informacije su vezana za svijest trećeg lica koje prima povlaštenu informaciju u smislu da li u momentu prijema takve informacije zna ili treba da zna da je informacija koju prima povlaštena i da li zna ili treba da zna da takvu informaciju dobija od insajdera pa time i to treće lice postaje insajder sa povlaštenom informacijom. Navedeno bi svakako moglo biti od značaja za utvrđenje obima odgovornosti trećeg lica u slučaju zloupotrebe povlaštenih informacija.

Osim korištenja povlaštenih informacija za ličnu korist ili otkrivanja trećim licima, pozitivni propisi zabranjuju i korištenje povlaštenih informacija radi savjetovanja drugih lica o prodaji ili kupovini vrijedonosnih papira. Kao i kod prve zabrane, indirektne

ili direktne kupovine/prodaje, i zabrana savjetovanja se ograničava samo na savjetovanje kod kupovine ili prodaje vrijedonosnih papira, ali ne i na druge vrste prometovanja vrijedonosnim papirima.

Iz naprijed navedenog proizilazi da su pozitivnim propisima primjenjivim u BiH utvrđeni osnovni elementi potrebni za procjenu da li konkretan slučaj spada u domen zloupotrebe povlaštenih informacija ili ne. Tako imamo uređen pojam ***povlaštene informacije*** (predmet zloupotrebe), pojam ***insajdera*** (potencijalnog prekršioca) i pojam ***zabranjenje radnje*** (sredstvo/način zloupotrebe).

Pored navedenih osnovnih elemenata na osnovu kojih je moguće cijeniti zloupotrebu povlaštenih informacija, važeće zakonodavstvo u BiH za sam čin zloupotrebe predviđa i sankcije.

Sankcije propisane važećim zakonima

Članom 259. ZOTVP zaprijećena je novčana kazna ili kazna zatvora u trajanju od 90 dana do 5 godina za korištenje povlaštenih informacija suprotno zakonskoj zabrani sa namjerom sticanja imovinske koristi za sebe ili drugoga, odnosno sa namjerom nanošenja materijalne štete drugome. ZOTVP ne pretpostavlja lakši i kvalifikovani (teži) oblik ovog krivičnog djela za različite kategorije insajdera kao učinilaca ili za različite iznose materijalne štete, nego su jednom pravnom normom na jednak način obuhvaćeni kako „obični“ insajderi, tako i profesionalni posrednici. Iz opisa navedene norme proizilazi uslov postojanja namjere učinioca za sticanje materijalne koristi ili nanošenje materijalne štete, kao i uslov postojanja svijesti učinioca o statusu informacije u smislu njene povlaštenosti.

> *Osim korištenja povlaštenih informacija za ličnu korist ili otkrivanja trećim licima, pozitivni propisi zabranjuju i korištenje povlaštenih informacija radi savjetovanja drugih lica o prodaji ili kupovini vrijedonosnih papira.*

I ZOTHOV neovlašteno korištenje i odavanje povlaštenih informacija predviđa kao krivično djelo kroz odredbu člana 291. zakona, pri čemu se kažnjivo ponašanje veže za zabrane iz člana 273. istog zakona. Zaprijećena kazna za ovo krivično djelo prema ZOTHOV je novčana kazna ili kazna zatvora u trajanju do godinu dana sa tim da, ako pribavljena protupravna korist ili učinjena šteta prelaze iznos od 1.500,00 KM, učinilac se može kazniti kaznom zatvora u trajanju do dvije godine.
Pored krivičnog djela propisanog ZOTVP i ZOTHOV koji se odnose na sankcije za zloupotrebu povlaštenih informacija generalno, Krivični zakon FBiH u članu 255. kao i Krivični zakon RS u članu 270. kao krivično djelo propisuju ***Odavanje i korištenje burzovnih tajnih podataka***, odnosno ***Odavanje i korištenje berzanske tajne***. Opis ovog krivičnog djela je znatno uži od opisa krivičnog djela zloupotrebe povlaštenih informacija iz ZOTVP i ZOTHOV, kako u pogledu mogućeg

učinioca, tako i u pogledu objekta nad kojim se vrši krivično djelo. Tako se protuzakonito odavanje i korištenje podataka iz pomenutih odredbi krivičnih zakona odnosi isključivo na podatke sa berze koji nisu dostupni svim sudionicima berze, ali ne i na neke druge podatke koji bi mogli predstavljati povlaštenu informaciju. Imajući u vidu da se radi o berzanskim podacima kao zaštićenom objektu, jasno je da je i krug potencijalnih učinilaca u tom slučaju sužen na ona lica koja imaju pristup berzanskim podacima koji se smatraju tajnim. Zaprijećena kazna za navedeno krivično dijelo je kazna zatvora u trajanju od tri mjeseca do pet godina, odnosno kazna zatvora u trajanju od dvije do deset godina za najteži oblik djela ukoliko imovinska korist prelazi iznos od 50.000,00 KM.

"Mjere sankcionisanja lica koja učine radnje zlouporebe povlaštenih informacija u pravilu stižu prekasno kad je šteta na tržištu već učinjena i reputacija emitenta vjerovatno izgubljena na duži period."

I ZOTVP i ZOTHOV, pored krivičnog djela kao teže povrede, za pojedina protupravna postupanja koja uključuju povlaštene informacije predviđa i prekršaje kao lakšu povredu.

Tako će prema ZOTVP novčanom kaznom za učinjeni prekršaj u iznosu od 15.000,00 do 200.000,00 KM kao pravno lice biti kažnjen emitent koji ne poduzme mjere kontrole pristupa povlaštenim informacijama propisane zakonom, emitent koji Komisiji za vrijedonosne papire u propisanom roku od 30 dana ne dostavi spisak insajdera, emitent i posrednik koji ne prijave transakciju izvršenu na osnovu povlaštenih informacija, kao i profesionalni posrednik (pravno lice) koji sa povlaštenim informacijama postupa na protupravan način.

Novčanom kaznom u iznosu od 3.000,00 do 20.000 KM kazniće se fizičko lice-insajder koji koristi povlaštene informacije suprotno zabrani, kao i profesionalni posrednik-fizičko lice koje postupa suprotno zabrani korištenja povlaštenih informacija definisanom zakonom.
ZOTHOV u dijelu prekršaja

propisuje sankcije samo za fizička lica i to u slučaju nedostavljanja podataka Komisiji za hartije od vrijednosti radi utvrđivanja zloupotrebe ili ukoliko u propisanom roku ne dostavi obavještenje o transakcijama lica koja se smatraju insajderima.

Mjere sankcionisanja lica koja učine radnje zloupotrebe povlaštenih informacija u pravilu stižu prekasno kad je šteta na tržištu već učinjena i reputacija emitenta vjerovatno izgubljena na duži period. Kako ne bi dolazilo do neželjenih scenarija, emitenti su ti koji bi trebali, a i prema pozitivnim propisima su

obavezni, da poduzmu preventivne mjere usmjerene na ograničavanje dostupnosti povlaštenih informacija i pravovremeno i tačno identifikovanje insajdera. Koje preventivne mjere emitenti mogu poduzeti, sa kojim efektima i uz koje troškove, svakako je procjena svakog emitenta pojedinačno i jedna posebna tema za dalju razradu.

Očekivano, regulative i praksa u koju bi se BiH mogla (i trebala) ugledati vezuje se uz Evropsku uniju, posebno imajući u vidu tendencije stvaranja **Evropske unije tržišta kapitala** (*Capital Markets Union*).

Evropska unija – regulativa i praksa

Zaštita tržišta kapitala, primarno od zloupotrebe tržišta, i zaštita povlaštenih informacija aktuelna je u Evropskoj uniji, naročito od prethodne dvije decenije, i to u širem smislu sa ciljem uspostave jedinstvenog tržišta koje propisuje član 3(3) Ugovora o Evropskoj uniji, odnosno jedinstvenog prostora slobode kretanja ljudi, robe, usluga i kapitala, kako ga definiše član 6. Ugovora o funkcionisanju Evropske unije. U užem smislu, zaštita od zloupotrebe tržišta kapitala referiše se u EU na zaštitu potrošača i njihovih prava.

Prvi regulatorni korak EU u ovom kontekstu bila je **Direktiva iz 1989**. (Direktiva 89/592/EEZ) kojom je zapravo po prvi put definisano *evropsko protupravno djelo zloupotrebe tržišta kapitala* koje u početku nije bilo definisano kao krivično djelo, ali je nalagalo državama članicama uspostavu sankcija za zloupotrebu tržišta i špekulativne radnje na način da takve sankcije trebaju biti efikasne, proporcionalne djelu i odvraćujuće. Za tadašnju Uniju, odnosno Zajednicu država, ovo je bio impozantan korak u borbi protiv kriminalnih aktivnosti na tržištu kapitala.
Od tada do danas, Evropska unija prošla je značajan put uspostave regulatornog okvira za zaštitu tržišta kapitala u čemu je posebnu ulogu odigrala ***Evropska agencija za vrijednosne papire i tržište kapitala*** (*European Securities and Market Authority* – ESMA) u svojstvu upravnog, regulatornog i nadzornog nadnacionalnog tijela za zaštitu tržišta kapitala u EU. S tim u vezi, od posebnog značaja je ***Uredba o zloupotrebi tržišta 2014/596*** (*Market abuse Regulation* – MAR) koja je sa primjenom otpočela 2016. godine i koja je uspostavila sasvim novi, neposredno obavezujući okvir za sve države članice. U "paketu" s ovom Uredbom, usvojena je i ***Direktiva o zaštiti tržišta 2014/57*** (*Market abuse Directive* – MAD). Danas ovi propisi čine jedinstveni regulatorni okvir zaštite tržišta kapitala u Evropskoj uniji. Ovim regulatornim okvirom zloupotreba tržišta postavljena je na nivo krivičnog djela, s obzirom na to da je članom 3. MAD-a propisano da će *države članice poduzeti odgovarajuće mjere radi omogućavanja da špekulativne radnje (manipulacija tržištem), pomaganje ili učestvovanje u špekulativnim radnjama, definisano članom 2-8 ove Direktive, bude definisano kao krivično djelo, bar u ozbiljnim slučajevima koji su počinjeni iz namjere.*

Značajna sudska praksa u Evropskoj uniji povodom novog regulatornog paketa (MAD i MAR) još uvijek nije uspostavljena. Međutim, da bi se kriminalizacija zloupotrebe tržišta i povlaštenih informacija u EU jasnije sagledala, možda može poslužiti primjer nešto starije sudske prakse koja govori i o značajnom napretku koji donosi MAD i MAR, a posebno u smislu uvođenja *mensrea* principa za kriminalizaciju ovih djela.

Presuda Suda Evropske unije u predmetu *Spector Photo Group NV, Chris Van Raemdonck vs Commissievoor het Bank, Financie en Assurantiewezen (CBFA)*, broj C-45/08 iz 2008. godine ukazuje na primjenu evropske regulative kada je riječ o tržištu kapitala. ***Spector Photo*** je belgijska kompanija, dioničko društvo sa dionicama uvrštenim na berzi. Kompanija je svojim zaposlenicima nudila opcije na dionice. Kako bi zadovoljila svoje obaveze prema zaposlenicima, kompanija je sticala vlastite dionice na tržištu samostalno i putem trećeg lica *gdina Van Raemdoncka*. Nakon sticanja vlastitih dionica, kompanija je najavila planirano preuzimanje od strane druge, konkurentske kompanije te objavila svoje finansijske rezultate, što je dovelo do rasta cijene dionice. Ova saznanja kompanija je očito imala u trenutku kada je sticala vlastite dionice po nižoj cijeni. Navedeno je dovelo do procesa pred Sudom EU od strane belgijskog finansijskog regulatora, s obzirom na to da je belgijski regulator ocijenio da se očito radi o zloupotrebi povlaštenih informacija s ciljem sticanja vlastite koristi. Sud EU u ovom slučaju dao je mišljenje koje se, između ostalog, odnosi na sljedeće: kada pojedinici ili kompanije djeluju i poduzimaju poslovne aktivnosti, a pri tome posjeduju informacije koje su "insajderske", povlaštene, odnosno, mogu uticati na tržište, ponudu i potražnju, upotreba takvih informacija u vlastitu korist se pretpostavlja. Ova presumpcija je oboriva, ukoliko dođe do sudskog spora, i obaveza je tužene strane (takvog pojedinca ili kompanije) da dokaže da nije poduzimao tržišne radnje s namjerom zloupotrebe "insajderskih" informacija, odnosno zloupotrebe tržišta. Ovom presudom Sud je nagovijestio i da bi kompanije u sličnim situacijama trebale revidirati svoj proces donošenja odluka kako bi isti bio lišen potencijalne sumnje povezanosti sa zloupotrebama povlaštenih informacija koje lica uključena u proces donošenja odluka neminovno imaju.

Kakvu sudsku praksu će obezbijediti MAD i MAR uvodeći i umišljajni element u listu uvjeta za postojanje krivičnog djela zloupotrebe tržišta, ostaje da se vidi u godinama koje dolaze.

Ono što sigurno ostaje dugoročna dilema – koliko regulative je dovoljno, a koliko previše za bilo koje tržište kapitala? Koja je to granica na kojoj legislator treba stati i prepustiti tržištu da se samoreguliše? U kontekstu uspostavljanja **Unije tržišta kapitala** kao dodatnog nivoa integracije država članica (pored tržišne, monetarne i bankarske) za očekivati je da će i ova pitanja zahtijevati opsežnije analize i istraživanja. ■

Zakonska regulativa u BiH

STVARNA PRAVA KONCESIONARA

Kako važeći propisi u BiH ne pružaju cjelovit okvir za provedbu stvarno-pravnih ovlaštenja koncesionara, nudimo moguća rješenja putem kojih bi se upotpunile praznine dosadašnjih zakona te kako bi se omogućilo ostvarenje imovinskih prava nosilaca prava koncesije u punom kapacitetu

Autor:
Muris Bešić

U ovom radu bavit ću se problematikom koja se odnosi na stvarna prava koncesionara u skladu sa *Zakonom o koncesiji BiH*[1]. Riječ je stvarnim pravima nosioca prava iz koncesije koja isti ima u odnosu na nekretnine u vezi sa kojima ostvaruje prava po osnovu koncesije, kao i pravima koncesionara na nekretninama koje izgradi na zemljištu na kojem ima zasnovanu koncesiju. Kako bi se olakšalo razumijevanje materije koja će biti izložena, na početku rada će biti dat historijski osvrt na razvoj instituta koncesije, kao i osvrt na koncesiju u pravnom sistemu SFRJ. Iako je navedena tema rada vezana za ZKBiH, problematika vezana za stvarna prava koncesionara ne može biti razmatrana bez analize odredaba *Zakona o stvarnim pravima FBiH*[2], *Zakona o zemljišnim knjigama FBiH*[3], kao i *Pravilnika o postupanju u zemljišnoknjižnim stvarima FBIH*[4]. Analiza navedenih propisa je bitna jer se navedenim propisima određuje pravni položaj nekretnina izgrađenih na zemljištu na kojem je zasnovana koncesija te uređuje način evidentiranja prava na koncesiju u odgovarajućim javnim registrima i zemljišnim knjigama.

[1] Zakon o koncesijama Bosne i Hercegovine, Službeni glasnik BiH broj 32 od 07.11.2002. godine, u daljem tekstu ZKBIH.

[2] Zakon o stvarnim pravima Federacije Bosne i Hercegovine, Službene novine FBiH broj 66/13 od 28.08.2013. godine, u daljem tekstu ZSPFBiH.

[3] Zakon o zemljišnim knjigama Federacija Bosne i Hercegovine, Službene novine FBiH broj 19/03 od 13.05.2003. godine, izmjena i dopuna navedenog zakona je izvršena Zakonom o izmjenana i dopunama Zakon o zamljišnim knjigama Federacija Bosne i Hercegovine, Službene novine FBiH broj 54/04 od 16.10.2004. godine. U daljem tekstu ZZKFBiH.

[4] Pravilnika o postupanju u zemljišnoknjižnim stvarima FBIH, Službene novine FBiH broj 5/03 od 10.02.2003. godine, u daljem tekstu PPZKSFBiH.

Imajući u vidu da propisi navedeni u prethodnom pasusu ne pružaju cjelovit okvir za provedbu stvarno-pravnih ovlaštenja koncesionara, u ovom radu će biti navedena i moguća rješenja putem kojih bi se upotpunile praznine dosadašnjih zakonskih rješenja i omogućilo ostvarenje imovinskih prava nosilaca prava koncesije u punom kapacitetu.

HISTORIJSKI OSVRT NA RAZVOJ INSITUTA KONCESIJE

Korijeni današnjih koncesija se mogu pronaći još u privrednom i pravnom sistemu starog Rima. Sam naziv **koncesija** potiče o latinske riječi *conceder* (dopustiti). Koncesije za vrijeme starog Rima nisu egistirale u obliku u kojem ih poznajemo danasm, već su bile primjerene stepenu pravnog i privrednog razvoja tadašnjeg doba[5].

Koncesija se prvenstveno javlja u obliku pravnog instituta pod nazivom **Superficies** što u pravnom smislu označava sve što je trajno i nerazlučivo spojeno sa površinom zemljišta iz čega se izvodi pravilo ***superficies solo cedit*** po kojem sve što se nalazi na/i/u zemljištu ima pravni status kakav ima i samo zemljište, što dalje pretpostavlja da onaj ko je nosilac određenog stvarnog prava na zemljištu ima ista prava i na sve ono što je na/i/u zemljištu. U svom daljem razvoju pravilo *superficies solo cedit* je modifikovano institutom dugoročnog zakupa po kojem lice koje sazida zgradu na tuđem zemljištu, iako zgrada pripada vlasniku zemljišta, dobija pravo dugoročnog zakupa. Pravo dugoročnog zakupa je bilo nasljedivo i zaštićeno tužbama koje su bile usmjerene prema svima. Potrebno je i napomenuti da dugoročnom zakupu radi građenja prethodi i koncesija *ad aedificandum in solo publico*. Putem ove vrste koncesije su zadovoljavane potrebe građenja na zemljištu koje je imalo status javnog zemljišta. Kao pandan ovoj vrsti, u doba republike država i gradovi u davali pojedincima na korištenje neobrađena javna zemljišta, vremenski neograničeno ili na duži rok, pretežno 100 godina, sa mogućnosti opoziva u određenim slučajevima. Kod ovog oblika koncesije je vidljivo da dolazi do izražaja i javni interes da državno zemljište bude obrađeno. Javni interes naročito dolazi do izražaja kroz ustanovu ***emfiteuze***[6]. *Emfiteuza* predstavlja oblik koncesije koja je davana uz naplatu naknade i uz obavezu ispunjenja drugih obaveza prema državi, a njen nosilac je sticao prava da zasađuje određene kulture na državnom zemljištu. Ovaj oblik koncesije je na početku dodjeljivan na period od pet godina, a kasnije u zavisnosti

> *„**Regali** se mogu okarakterisati kao prava i privilegije koje su jedino imali vladari, kao nosioci vrhovne vlasti i vrhovnog suvereniteta, za korištenje prirodnih bogatstava i dobara u opštoj upotrebi te uz naknadu ustupali trećim licima.“*

[5] Hajro, Kofrc; „Zbornik radova Aktuelnosti građanskog i trgovačkog zakonodavstva i pravne prakse br. 4.“, Mostar 2006.godine, strana 234.
[6] Grčki izvorno, Emphyteuzis – zasaditi, uvesti.

od određenih uslova i na duži period uz mogućnost produženja. U daljem razvoju tokom 4. vijeka n.e. koncesije ***emfiteuza*** i ***ad aedificandum in solo publico*** pravno se na jedinstven način uređuju i spajaju u jedinstven institut pod nazivom ***emphyteuzis*** te se i u Justinijanovom kodeksu oblikuje kao stvarno pravo na tuđoj stvari koje se može naslijediti.

Superficijarno pravo je bez dvojbe predstavljalo jednu od preteča koncesije. Ovo pravo je, kroz svoje modalitete koji se se kroz vijeme mijenjanjali i usavršavali, značajno uticalo na izgradnju koncesije kao ekonomsko-pravnog instrumenta privrednih aktivnosti te je, bez sumnje, uticalo na kasnije pravne sisteme, kako samostalno, tako u i korelaciji sa kompletnom romanističkom pravnom tradicijom[7].

Iako su naprijed navedeni instituti nesumnjivo imali uticaj na razvoj koncesije, historijski posmatrano, klasične koncesije vode porijeklo od srednjovjekovnih regala. ***Regali*** se mogu okarakterisati kao prava i privilegije koje su jedino imali vladari, kao nosioci vrhovne vlasti i vrhovnog suvereniteta, za korištenje prirodnih bogatstava i dobara u opštoj upotrebi te uz naknadu ustupali trećim licima[8]. Sa razvojem države regali se pomjeraju iz privatnog domena vladara i poprimaju državni, tj. javni karakter te u kapitalizmu prelaze u državne monopole. Rezulat navedenog je da su regali u 19. vijeku sve manje u funkciji ubiranja prihoda države, a sve više dobijaju funkciju koje je u službi funkcije postizanja opšteg blagostanja.

OSVRT NA KONCESIJU U PRAVNOM SISTEMU BOSNE I HERCEGOVINE NAKON II SVJETSKOG RATA

Nakon Drugog svjetskog rata na području bivše SFRJ putem *Zakona o stranim ulaganjima SFRJ*[9] iz 1988. godine kroz koncesiju su načelno regulisani i posebni oblici stranih ulaganja. Na navedeni način se koncesija kroz saveznim zakonom definisan institut uvodi u pravni sistem SFRJ. U smisli navedenog propisa trajanja i uslovi koncesije su utvrđivani ugovorom o koncesiji koji je zaključivan između stranog ulagača kao koncesionara i Općine. Uslov za punovažnost ugovora o koncesiji je davanje saglasnosti od strane *Saveznog sekretarijata za ekonomske odnose sa inostranstvom*. U odnosu na samu temu rada bitno je napomenuti da je ZSUSFRJ davana mogućnost da se stranom licu na osnovu odobrenja nadležnog organa na određeni rok odobri izgradnja, vođenje i iskorištavanje određenog postrojenja ili pogona kao vlastitog preduzeća. Po isteku ugovorenog roka imovina koje je izgrađena bi prelazila u društvenu svojinu i dobijala status društvenog preduzeća. Navedeni način rada je bio usklađen u skladu sa principom modernih shvatanja koncesija po *BOT aranžmanu*[10]. Iz navedenog

[7] Hajro, Kofrc; „Zbornik radova Aktuelnosti građanskog i trgovačkog zakonodavstva i pravne prakse br. 4.“, Mostar 2006.godine, strana 235.

[8] Osim u navedenom obliku regali su davani i stranim trgovcima koji su na osnovu njih mogli nesmetano trgovati na određenim teritorijama, kao i poznatim moreplovcima na ime otkrivanja novih teritorija, njihovog osvajanja i priključenja državi koja se dala koncesiju tj. regale.

[9] Službeni list SFRJ, broj 77/88, u daljem tekstu ZSUSFRJ.

[10] BOT, skraćenica od riječi eng. jezika - build, operate, transfer. Prevod na bos. jezik - izgradi, koristi, prenesi

proizilazi da bi se uspješno moglo argumentirati u prilog činjenici da je nosilac prava koncesije na osnovu zakonom datih mogućnosti prema ZSUSFRJ mogao da na objektima izgrađenim u skladu sa Ugovorom o koncesiji vrši sva vlasnička ovlaštenja u skladu sa tadašnjim propisima za vrijeme trajanja koncesije.

Potrebno je pomenuti i *Zakon o koncesijama SRRBiH* koji je donesen 1991. godine[11], ali s obzirom na to da je njegova primjena odložena zbog agresije na BiH, da je stvoren pod diretnim uticajem ZSUSFRJ te da o njegovoj primjeni nema raspoloživih podataka, navedeni propis neće biti predmet naročite analize.

KONCESIJA PREMA ZAKONU O KONCESIJAMA BiH

Prema ZKBiH koncesija znači pravo koje koncedent dodjeljuje u cilju osiguranja izgradnje infrastrukture i/ili pružanja usluga, eksploatacije prirodnih resursa, u rokovima i pod uvjetima o kojima se koncedent i koncesionar dogovore[12]. Dakle, u smislu ZKBiH, koncesija predstavlja pravo koje koncedent dodjeljuje koncesionaru. Navedena definicija je prema autorima, Duško, Medić[13] i Hajro, Kofrc[14], manjkava. Naime, kao što je vidljivo iz same definicije, govori se o dodjeljivanju prava koje koncedent dodjeljuje koncesionaru. Oba autora navode, sa čime ćemo se i složiti, da navedena definicija sadrži određene nedostatke, a koji se ogledaju u tome da je u okviru definicije nepravilno upotrebljena riječ ***dodjeljuje***. Navedena riječ ne može biti upotrebljena u definisanje koncesije jer se prilikom davanje koncesije ne radi o prenosu prava. Termin sa kojim bi definicija koncesije bila potpunija i pravilnija je ***ustupanje prava***, jer *de facto* nosilac određenih prava – koncedent koncesionaru ustupa vršenje prava.

Prava u vezi sa koncesijom koncesionar stiče po osnovu *Ugovora o koncesiji* čiji su obavezni elementi propisani ZKBiH[15]. Naravno, pored ovih obaveznih elemenata ne postoji prepreka da koncesionar i koncedent ugovorom o koncesiji odrede i druge uslove koje smatraju da je potrebno regulisati kako bi njihov ugovorni odnos bio potpunije definisan. Od obaveznih elemenata ugovora o koncesiji za potrebe ovog rada bitno je spomenuti sljedeće: sadržaj i obim koncesije te olakšice za korištenje zemljišta. Navedeni obavezni elementi su bitni jer se kroz iste može ugovoriti vrsta kao i obim stvarnih prava koje koncesionar može steći i sticati kako u vezi sa vezi predmetom koncesije, tako i sa nekretinom koju koristi povodom koncesije i nekretninama koje sam izgradi na zemljištu koje je predmet koncesije. Tako

[11] Zakon o koncesijama SRBiH, Službeni list SRBiH 27/91. Sa pravno - tehničkog aspekta, zakon je bio kratak svega 20 članova, uz maksimalno korištenje metoda jasnog jezika i stila, te pridržavanje pravila da zakonodavac treba pristupiti stvaranju prava na tako da riječima bude tijesno a mislima prostrano. Navedeni zakon je formalno pravno preuzet u pravni sistem BIH te je stavljen van snage 2002. godine u skladu sa članom 32. ZKBiH.

[12] Član 3. stav. 1. tačka 2., ZKBiH.

[13] Duško, Medić;„Pravni život br. 7-8/2008“, strana 49.

[14] Hajro, Kofrc; „Zbornik radova Aktuelnosti građanskog i trgovačkog zakonodavstva i pravne prakse br. 4“, Mostar 2006. Godine, strana 235.

[15] Član 26. ZKBiH.

ne postoji prepreka da koncesor ograniči koncesionara u pogledu sticanja stvarnih prava na nekretninama koje izgradi na zemljištu koje koristi u vezi sa koncesijom, da sticanje stvarnih prava uvjetuje njegovom prethodnom saglasnošću, da uslovi pravnu sudbinu nekretnina izgrađenih na zemljištu koje je predmet koncesije niti da odredi pod kojim uslovima i na koji način će koncesionar posjedovati i koristiti zemljište te drugu imovinu koja mu je stavljena na raspolaganje ugovorom o koncesiji.

STVARNA PRAVA KONCESIONARA

Prava koncesionara povodom sredstava i imovine koje mu koncedent stavlja na raspolaganje su propisana ZKBiH, član 29[16]. Imajući u vidu da je navedenom odredbom predviđeno da koncesionar isključivo može steći prava posjedovanja i korištenja zemljišta koje mu je dato u vezi sa pravom na koncesiju, može se izvesti zaključak da koncesionar na zemljištu i drugim nekretninama, a koji su objekt koncesije, ne može imati niti sticati stvarna prava, što znači da je ograničen isključivo na prava predviđena članom 29. ZKBiH. To znači da ne bi mogao dodijeljene nekretnine, npr. opteretiti kako bi ishodio kreditna sredstva ili otuđiti. S obzirom na to da se položaj koncesionara u velikoj mjeri definiše ugovorom o koncesiji te da zakon ne pruža dovoljno podataka na osnovu kojeg bi se mogao precizno utvrditi pravni položaj koncesonara, sa ove distance bi se moglo reći da je njegov položaj najsličniji položaju zakupca kod ugovora o zakupu nekretnine.

> *„S obzirom na to da se položaj koncesionara u velikoj mjeri definiše ugovorom o koncesiji te da zakon ne pruža dovoljno podataka na osnovu kojeg bi se mogao precizno utvrditi pravni položaj koncesonara, sa ove distance bi se moglo reći da je njegov položaj najsličniji položaju zakupca kod ugovora o zakupu nekretnine."*

Bitno drugačija je situacija povodom nekretnina koje koncesionar izgradi na zemljištu koje je predmet koncesije, ali pod uslovom da se koncesija obavlja na nekretinama koje predstavljaju opća i javna dobra. Naime, nekretine koje su izgrađene na općem i javnom dobru ili ispod njih, a koje su od tih dobara pravno odvojene koncesijom, predstavljaju samostalne nekretine te čine vlasništvo koncesionara dok koncesija traje[17]. Na tako izgrađenim nekretninama koncesionar može u punom kapacitetu ostvarivati sva vlasnička prava, kao i povodom tih nekretnina zasnovati druga stvarna prava, npr. hipoteku. Međutim, vrlo je bitno imati u vidu da su stvarna prava na nekretninama izgrađenim na pravu koncesije vremenski ograničena za vrijeme trajanja koncesije te da su prava po osnovu ugovora o koncesiji, imajući u vidu način dodjele koncesije,[18] neprenosiva. Na-

[16] Koncesionar ima pravo posjedovanja i korištenja sredstava i imovine koje mu koncedent stavlja na raspolaganje.
[17] Član 6. stav 1. ZSPFBiH. U smislu navedene odredbe dodjelu koncesije kao i izbor koncesioara vrši komisija za koncesije.
[18] Član 4. ZKBiH.

vedeno je bitno imati u vidu jer je usljed navedenih ograničenja veoma izvjesno da za predmetne nekretine ne bi bilo zainteresovanih kupaca. Naime, navedene nekretine bi vrlo vjerovatno bile napravljene radi vršenje prava prenijetih koncesijom, a pošto koncesija nije prenosiva jednostranom voljom njenog nosioca, predmetna nekretnina ne bi bila od velike koristi novom vlasniku koji ujedno ne posjeduje i pravo na obavljanje koncesije. Kada se govori o ograničenjima koja se odnose na imovinu koncesionara, bitno je napomenuti da je odredbom člana 20. stav 2. ZKBiH, predviđeno pravo da ovlašteno lice *Komisije za koncesije* koja vrši nadzor nad koncesionarem može u bilo koje normalno vrijeme stupiti na imovinu ili objekte koncesionara. S obzirom na to da nije izričito propisano da se navedeno ovlaštenje odnosi na imovinu koja čini ili je vezana za koncesiju, pretpostavka je da se navedeno ovlaštenje odnosi na cjelokupnu imovinu koncesionara jer jedino na taj način *Komisija za koncesije* može efikasno vršiti nadzor nad koncesionarem.

Kao dalje bitno pitanje koje se odnosi na nekretnine izgrađene na pravu koncesije koja je zasnovana na općem i javnom dobru je pitanje pravne sudbine takvih nekretnina nakon isteka koncesije. Status nekretnina izgrađenih na pravu koncesije nakon prestanka prava na koncesiju nije izričito predviđen ZSPFBiH kao što je to npr. predviđeno kod prava građenja[19]. Međutim, imajući u vidu da ZSPFBiH promovira načelo pravnog jedinstva nekretnine, može se izvesti zaključak da bi nekretnine koje su bile u vlasništvu koncesionara nakon isteka koncesije trebale postati dio općeg ili javnog dobra jer se istekom koncesije izgubio osnov koji je mogao nekretninu odvojiti od zemljišta koje predstavlja opće ili javno dobro.

U prethodnom dijelu je opisana situacija u pogledu nekretnina koje su pravno odvojene od općeg ili javnog dobra pravom koncesije te se osnovano postavlja pitanje da li je koncesiju moguće imati na imovini koja ne predstavlja opće i javno dobro kao i kakav je status nekretnina koje koncesionar izgradi na zemljištu koje je, za razliku od općih i javnih dobara, podobno da bude predmet prava vlasništva. Na pitanje koje se odnosi na mogućnost da objekat koji ima nosioca prava vlasništva bude objekat koncesije može se dati potvrdan odgovor a imajući u vidu da takvu mogućnost predviđa, istina indirektno, član 21. stav 1. ZKBiH[20]. U odnosu na pitanje da li postoji zakonski osnov na osnovu kojeg bi se nekretnina koje je izgrađena na objektu koncesije koja predstavlja zemljište koje ima

[19] Član 312. ZSPFBiH:„(1) S prestankom prava građenja postaje pripadnost zemljišta ono što je pravom građenja bilo od zemljišta pravno odvojeno. (2) Na odnos vlasnika zemljišta i osobe kojoj je prestalo pravo građenja na odgovarajući će se način primjenjivati pravila po kojima se prosuđuju odnosi nakon prestanka prava plodouživanja, ako nije nešto posebno određeno. (3) Vlasnik je dužan osobi kojoj je prestalo pravo građenja dati onoliku naknadu za zgradu koliko je njena nekretnina u prometu vrijednija s tom zgradom nego bez nje.“
Obzirom da i pravo građenja daje ovlašenje njegovom nosiocu da izgradi zgradu na tuđem zemljištu može se reći da je položaj nosioca prava građenje vrlo sličan položaju koncesionara u pogledu nekretnina koje je izgradio na zemljištu koje je predmet koncesije.

[20] Član 21. Stav 1. ZKBiH: „Organi u cijoj su nadležnosti djelatnosti i vlasnik objekata, odnosno imovine, izrađuju studiju ekonomske opravdanosti za svaki projekat koji je predviđen za davanje na koncesiju, prijejavnog pozivanja potencijalnih ponuđaca. Studija ekonomske opravdanosti dostavlja se Komisiji na razmatranje i odobravanje.“

vlasnika mogla odvojiti od tog zemljišta u ovom trenutku nije moguće dati potvrdan odgovor. Naime, ovakav stav je zauzet iz razloga što je mogućnost pravnog odvajanje zgrade i zemljišta u smislu člana 7. ZSPFBiH, predviđeno isključivo za opća i javna dobra. Iako bi se moglo činiti da bi, kad je ovakav slučaj u pitanju, mogla u obzir doći primjena analogije i identično postupanje kao i kod općih i javnih dobara, takav stav ne bi bio ispravan iz razloga jer zakon izričito predviđa načelo pravnog jedinstva nekretnine te bi svako odstupanje od navedenog načela trebalo biti izričito predviđeno ZSPFBiH ili drugim odgovarajućim propisom, dok bi proizvoljna primjena analogije, a usljed nedostataka pozitivnih propisa, predstavljala proizvoljno postupanje koje nema utemeljenje u pozitivnim propisima. Moguće je da za primjenu analogije, kako je naprijed opisano, u praksi nema niti potrebe jer je *Ugovorom o koncesiji* koji se odnosi na objekat koji ima vlasnika moguće putem instituta prava građenja definisati status nekretnina koje su izgrađene na objektu koncesije, a u tom slučaju bi morao biti proveden poseban postupak zasnivanja prava građenja.

UPIS KONCESIJE U ZEMLJIŠNE KNJIGE

S obzirom na to da je za sticanje stvarnih prava nephodan upis u zemljišnu knjigu, postavlja se pitanje na koji način se vrši upis koncesije kao i nekretnina izgrađenih na općim i javnim dobrima, a koje su od istih odvojene pravom koncesije u zemljišnu knjigu. Naime, ukoliko se samo pravo koncesije ne upiše u zemljišnu knjigu ne bi bilo moguće niti izvršiti upis nekretnina izgrađenih na osnovu prava koncesije na općim i javnim dobrima.

Pitanje upisa koncesije zasnovane na općem i javnom dobru kao nekretnina nastalih na osnovu prava koncesije nije regulisano pozitivnim propisima. Sa druge strane,

> *Koncesija se upisuje u teretni list zemljišno-knjižnog uloška , ali, sa druge strane, u ovom slučaju ne možemo govoriti o sticanju stvarnih prava na nekretninama izgrađenim na pravu koncesije jer, kako je ranije konstatovano, ZSPFBiH ne daje mogućnost odvajanje izgrađenih nekretnina od zemljišta koje ima nosioca prava vlasništva.*

pitanje upisa koncesije na objektu u državnom vlasništvu je regulisano odredbom člana 10. PPZKSFBiH. Prema navedenoj odredbi koncesija se upisuje u teretni list zemljišno-knjižnog uloška[21], ali, sa druge strane, u ovom slučaju ne možemo govoriti o sticanju stvarnih prava na nekretninama izgrađenim na pravu koncesije jer, kako je ranije konstatovano, ZSPFBiH ne daje mogućnost odvajanje izgrađenih nekretnina od zemljišta koje ima nosioca prava vlasništva.

[21] Navedene mogućnsot upisa koncesije potvrđuje ranije iznijeti stav da je koncesiju moguće zasnovati na objektima tj. nekretninama koje imaju nosioca prava vlasništva.

Imajući u vidu navedene nedostatke pozitivnih propisa usljed kojih neminovno dolazi do nemogućnosti ostvarenja stvarnih prava koncesionara povodom nekretnina za koje je članom 7. ZSPFBiH predviđeno da se smatraju samostalnim nekretninama, u nastavku će biti predloženi mogući načini za koje smatram da su ispravno rješavanje problema koji se odnosi na nemogućnost upisa samostalnih nekretina izgrađenih na pravu koncesije u zemljišnju knjigu.

Kako nije donosen poseban propis kojim bi bio definisan način upisa općih i javnih dobara u zemljišne knjige, u ovom slučaju je prvenstvno potrebno omogućiti upis nekretnine koja se odnosi na objekat koncesije u zemljišnu knjigu kako bi se ugovor o koncesiji mogao upisati u teretni list zemljišno-knjižnog uloška. Nadalje, postavlja se pitanje na koji način upisati u zemljišnu knjigu kao samostalnu nekretninu onu nekretninu koja je izgrađena na općem i javnom dobru i od istog odvojena koncesijom. Kako je ranije navedeno, ZSPFBiH ne propisuje načine postupanja povodom upisa navedenih nekretnina u zemljišnu knjigu. S obzirom na nedostatke u pogledu propisa, rješenje navedenog problema bi se moglo pronaći u tome da se prvenstveno omogući upis nekretnine, koja predstavlja opće i javno dobro, u zemljišnu knjigu i da se u teretni list tog zemljišno-knjižnog uloška upiše koncesija dok bi se za nekretnine, koje su izgrađene na općem i javnom dobru i od istog odvojene koncesijom, otvorio poseban zemljišno-knjižni uložak u koji bi se upisala samostalna novoizgrađena nekretnina. Osnovni zemljišno-knjižni uložak u čiji je teretni list upisano pravo koncesije bi morao sadržavati uputu na novootvoreni zemljišno-knjižni uložak. U principu, kod koncesije bi potrebno bilo uz određene izmjene primijeniti postupak koji se primjenjuje prilikom upisa u zemljišnu knjigu prava građenja i nekretnina sagrađenih na pravu građenja. Naravno, ovaj postupak se ne bi mogao primijeniti na osnovu primjene analogije, već bi bilo neophodno izvršiti izmjene odgovarajućih propisa kako bi postupak bio u cjelosti legalan i kako se ne bi desili problemi prilikom provedbe upisa u zemljišnu knjigu.

> *Rješenje navedenog problema bi se moglo pronaći u tome da se prvenstveno omogući upis nekretnine, koja predstavlja opće i javno dobro, u zemljišnu knjigu i da se u teretni list tog zemljišno-knjižnog uloška upiše koncesija.*

ZAKLJUČAK

Na osnovu izloženog može se zaključiti da koncesionar na objektu koncesije, tačnije na zemljištu koje predstavlja objekat koncesije, ne može sticati niti imati nikakva stvarna prava jer u skladu sa ZKBiH njemu isključivo pripada pravo posjedovanja i korištenja zemljišta.

Pravni sistem daje mogućnost pod određenim uslovima sticanje stvarnih prava

na nekretninama izgrađenim na pravu koncesije, ali u zavisnosti od toga kakva je pravna priroda zemljišta u vezi sa kojim se daju prava po osnovu koncesije. Koncesionar ima zakonsku mogućnost da stekne samostalnu nekretninu ukoliko se koncesija zasniva na zemljištu koje predstavlja opće ili javno dobro, ali u tom slučaju zakon ne propisuje način upisa koncesije niti nekretnina izgrađenih na pravu koncesije u zemljišnu knjigu. Sa druge strane, ukoliko se koncesija zasniva na zemljištu koje može imati vlasnika, predviđen je način upisa koncesije u zemljišnu knjigu, ali pravni propisi ne daju mogućnost sticanje samostalne nekretnine koje je izgrađena na takvom zemljištu tako da bi nekretnina izgrađena na tom zemljištu po sili zakona postala vlasništvo onog ko je je vlasnik i samog zemljišta.

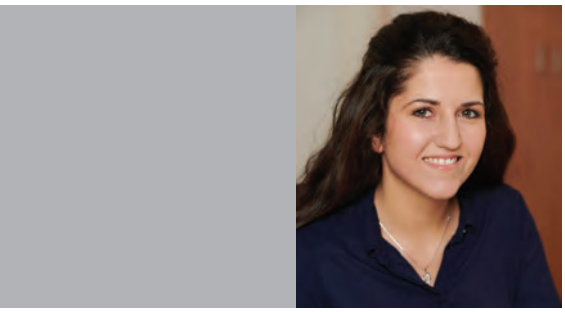
Cijeneći navedeno, a u cilju rješavanja problema sa kojim se može susresti koncesionar, potreban bi bio sistemski pristup kako bi se izvršila detaljna analiza trenutnih zakonskih rješenja te izvršile neophodne dopune odgovarajućih propisa u cilju omogućavanja ostvarenja prava koncesionara koja isti imaju u skladu sa pozitivnim propisima. ■

(tekst je objavljen u magazinu Banke i Biznis, broj 204, april 2019.)

***Malware* revolucija**

RAZVOJ CYBER KRIMINALA

Šteta prouzrokovana cyber kriminalom mjeri se milijardama dolara. Danas se zarazni virusi šire brže nego što se razvijaju alati koji se bore protiv njih. A ovako je sve počelo...



Autorica:
Ena Begić

Krajem sedamdesetih godina XX stoljeća stvoren je prvi antivirusni program ***Reaper***. Nastao je kao posljedica prvog kompjuterskog virusa ***Creeper*** koji je ciljao telefonsku kompaniju i omogućavao besplatne međunarodne pozive. *Cyber* napadi, koji su započeli iz ovog jedinstvenog virusa, danas čine ogromnu kolekciju virusa i *malwarea*. U historiji su zabilježeni mnogi slučajevi koji su promijenili svijet *cyber* kriminala.

> *„**Morisov crv** nije napisan da bi načinio štetu, već da bi izmjerio veličinu interneta, ali greška koja je nastala u mehanizmu širenja pretvorila je crva iz dobroćudnog u zarazni i načinila štetu od približno 10 miliona dolara."*

Glavni lik romana kao inspiracija *cyber* kriminalcima

Vilijem Gibson u naučno-fantastičnom romanu 1984. godine uvodi pojam ***cyber prostora***. Svojim romanom najavio je internet revoluciju i nevjerovatan razvoj tehnologije. Glavni lik romana povezuje svoju svijest sa softverom u *cyber* prostoru i pronalazi tajne informacije u obilju podataka za onoga ko može platiti njegove usluge. Već 1988. godine **Robert Tappan Morris** lansira jedan od prvih internet virusa, takozvani ***Morisov crv***. Crv nije napisan da bi načinio štetu, već da bi izmjerio veličinu interneta. Greška koja je nastala u mehanizmu širenja pretvorila je crva iz dobroćudnog u zara-

zni i načinila štetu od približno 10 miliona dolara.

Opasnosti vrebaju u e-mail sandučiću

Ključni alat i pokretač *cyber* kriminala je e-mail pošta. Današnji ***spam*** je metoda pomoću koje su zarađeni milioni dolara promovisanjem proizvoda putem neželjene e-poruke. Razvoj *antispam* sistema i *black* listi na serverima otežava spamerima slanje e-mailova, samim tim potreba za svježim računarima sa kojih se može isporučivati neželjena pošta postaje veća. Inspirisani Morisovim crvom, spameri su otkrili da bi mogli u saradnji sa kreatorima *malwarea* i putem zaraženih računara slati neželjenu poštu. Iz ove ideje rodio se poslovni model koji je nastavio slati neželjenu poštu cirkulisanjem oko *antispam* sistema, a sve pod kontrolom jednog pojedinca.

DoS

U toku *spam/malware* revolucije inovativni umovi su identifikovali nove kriminalne mogućnosti za internet robote. Godine 2000. otkriveno je da pristup većeg broja računara jednoj web stranici u istom vremenskom intervalu učini tu stranicu privremeno nedostupnom. Ovaj rani oblik **Denial of Service (DoS)** korišten je za usmjeravanje pristupa na ciljane web stranice rezultirajući štetama od oko 1,5 milijardi dolara.

Krađa ličnih podataka postala je unosan posao

Iste godine otkrivena je mogućnost prikupljanja ličnih podataka sa zaraženih računara. Stručnjaci su znali kako iznuditi finansijsku korist od ukradenih informacija, ali nisu imali vještine za pisanje i distribuciju zaraženih kodova, što dovodi do razvoja podzemnih tržišta. Na ovom tržištu pojedinci koji prikupljaju informacije prodaju svoje usluge onima koji su u stanju da iskoriste ukradene podatke, a time je omogućeno da *cyber* kriminal postane lakši, profitabilniji i efikasniji.

> *Ransomware napad se obično manifestuje putem e-maila koji sadrži prilog u obliku datoteke ili fotografije, ali može biti pokrenut na uređaju korisnika prilikom posjete web stranici koja je inficirana malwareom.*

Cyber kriminal danas

Ranije su počionici *cyber* kriminala uglavnom bili pojedinci ili manje grupe. Trenutno svjedočimo složenoj kriminalnoj mreži koja okuplja ljude iz cijelog svijeta i formira industriju zasnovanu na krivičnim djelima. Sve veći je broj onih koji rade u virtualnom podzemnom tržištu na proizvodnji usluga i proizvoda koje koriste drugi kriminalci. *Cyber* kriminal je kroz svoju historiju evaluirao do zlućudnog *ransomwarea*. ***Ransomware*** je naziv za skup malicioznih programa koji korisniku onemogućuje korištenje računala.

> *Današnji cyber kriminal je san svakog lijenog prevaranta. Sa jako malog znanja i iskustva mogu izvršiti prevaru i onda jednostavno čekati priliv novca.*

Najpoznatiji oblik *ransomwarea* je ***crypto ransomware***. To je digitalni mehanizam koji širi *malware* na cijelu mašinu i šifruje sve lične datoteke, a kreiran je za iznudu finansijskih sredstava. Nakon šifrovanja svih ličnih datoteka, korisnik je prisiljen da plati otkup bez garancije da će datoteke zaista biti vraćene. *Ransomware* napad se obično manifestuje putem e-maila koji sadrži prilog u obliku datoteke ili fotografije, ali može biti pokrenut na uređaju korisnika prilikom posjete web stranici koja je inficirana *malwareom*. Kada je uređaj korisnika zaražen, ništa vidljivo se ne dešava i *malware* radi tiho u pozadini dok se sistem ili mehanizam za zaključavanje podataka ne aktivira.

Internet nužno ne stvara nove zločine, samo nove mogućnosti za provođenje zločina. Današnji *cyber* kriminal je san svakog lijenog prevaranta. Sa jako malog znanja i iskustva mogu izvršiti prevaru i onda jednostavno čekati priliv novca. Kupovinom *ransomware softwera* na *online* podzemnim tržištima prevaranti lakše nego ikada uništavaju velike organizacije i iznuđuju ogromna finansijska sredstva.

Prevencija

Zaštita ličnih podataka i ukazivanje na opasnosti današnjeg *cyber* prostora su osnovica u borbi protiv *cyber* prevaranata. Globalna mreža je zasnovana na nesigurnim i nezaštićenim protokolima, a razvoj mehanizama za kriminalne radnje je brži od razvoja alata koji se bore protiv istih. Pored održavanja sistemskih rješenja, alata i antivirusnih programa, podizanje svijesti svakog pojedinaca ima ulogu preventivnog djelovanja. Prevencija je ključna jer u potrazi za *cyber* kriminalcima vrijedi tvrdnja – **teško ih je uhvatiti, još teže osuditi.** ■

TREND INTERNET PREVARA
U BIH I REGIONU U 2018. GODINI

Iako nam razvoj informacionih tehnologija donosi mnogo benefita, povećavaju se i opasnosti sa kojima su se u proteklom periodu suočili mnogi privredni subjekti i fizička lica u BiH i regionu

Autorica:
Selma Bušatlić

Internet nema granica, stalno stvara nove mogućnosti, ali i opasnosti. Osim što se pokazao kao globalni fenomen u komunikaciji i skladištenju informacija, pokazao se idealnim i za razne vrste prevara.

Loša finansijska situacija, nedostatak informatičke educiranosti i iskustva u korištenju *online* kanala i usluga, kao i činjenica da su informacioni sistemi i komunikacijske mreže u Bosni i Hercegovini postale dio globalne svjetske mreže koja pored mnogobrojnih benefita povećava i osjetljivost na *cyber* kriminal, razlozi su zašto se privredni subjekti i fizička lica u BiH i regionu povremeno nađu na meti nekih oblika internet prevara.

U nastavku navodimo nekoliko internet prevara koje su obilježile 2018. godinu.

Invoice fraud

To je vrsta prevare koja se odvija presretanjem e-mail komunikacije pravnih subjekata sa njihovim poslovnim partnerima u inostranstvu i izmjenom faktura u dijelu instrukcije plaćanja. Nakon što je transakcija realizovana, novac se odmah podiže u gotovini ili se vrši transfer na račune u drugim zemljama kojima je teško ući u trag.

Kako se zaštititi?

U svrhu zaštite od ovakvih vrsta prevara, pravni subjekti trebaju detaljno istražiti iznenadne promjene instrukcija plaćanja u smislu promjene banke i računa na koji je potrebno izvršiti uplatu, posebno ako se način plaćanja mijenja u posljednji čas pred samu uplatu i zahtijeva da se

plaćanje izvrši u državu različitu od uobičajene.

> *Komunikaciju sa partnerima u inostranstvu obavljajte isključivo preko već poznatih i ranije korištenih e-mail adresa ili brojeva telefona.*

U ovakvim slučajevima neophodno je sa partnerima u inostranstvu provjeriti originalnost bilo kakvih izmjena koje se odnose na plaćanje, a komunikaciju treba obavljati isključivo preko već poznatih i ranije korištenih e-mail adresa ili brojeva telefona.

Lažni krediti

Takozvani 'krediti za blokirane' sa minimalnom kamatnom stopom uz zaobilaženje neurednosti u drugim bankama i bez ijednog instrumenta obezbjeđenja, oglasi su koji su u protekloj godini kružili internetom.

Riječ je o internacionalnoj šemi prevare. Prevaranti postavljaju besplatne oglase na internet o novčanim pozajmicama. Sav kontakt odvija se putem e-maila pri čemu se koristi adresa javno dostupnih servisa (*gmail*, *hotmail* i sl). Dovoljno je samo poslati željeni iznos kredita nakon čega se dobije sačinjen ugovor na osnovu kojeg se kredit 'isplaćuje'.

Kako bi sredstva kredita bila isplaćena, potrebno je uplatiti određenu svotu novca

> *Ponuda povoljnih kredita oglašavanjem putem društvenih mreža i internet oglasa uz zaobilaženje finansijskih institucija i nerealno niske kamatne stope su znak da je riječ o prevari.*

na ime troškova realizacije kredita. Nakon uplate žrtva dobija obavijest da je novac isplaćen na račun, ali da je došlo do blokiranja sredstava kredita od strane banke te da je za deblokadu potrebno uplatiti dodatni iznos na ime 'nepredviđenih' troškova.
Uplata troškova uvijek se realizuje preko nekog od servisa za prijenos novca (najčešće Western Union), a ne preko banke, što je dodatno jedan signal za uzbunu. Prevaranti se nerijetko predstavljaju kao ovlaštene osobe ispred banke za obavljanje poslova kreditnog posredovanja. Ukoliko žrtve i plate sve troškove, prevaranti nestaju. Kredit se, naravno, nikad ne isplaćuje.

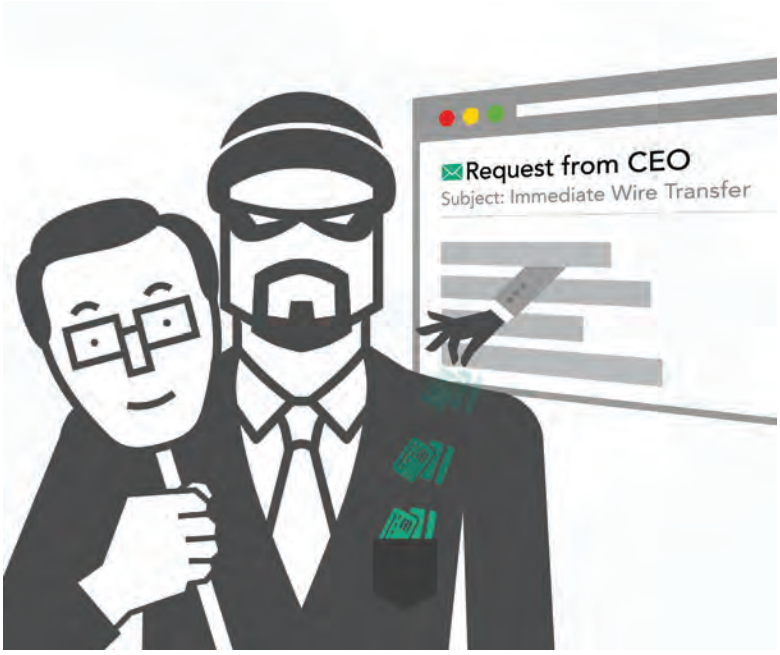
Kako se zaštititi?

Ponuda povoljnih kredita oglašavanjem putem društvenih mreža i internet oglasa uz zaobilaženje finansijskih institucija i nerealno niske kamatne stope te loše rečeničke strukture sa gramatičkim i pravopisnim greškama sami po sebi predstavljaju upozoravajući signal za prevaru pa je na takve ponude najbolje ne reagovati.

U slučaju da ipak postoji interes osobe za ovakav oblik kreditiranja, dodatna provjera vjerodostojnosti e-mail adrese i broja telefona te provjera prezentiranih informacija sa bankom, ukoliko se osoba koja stoji iza podataka predstavlja kao zastupnik banke, neke su od mjera kojima se moguće zaštititi od ovakvog oblika internet prevare.

'Direktorske' ili 'CEO' prevare

Ova vrsta prevare odvija se tako što prevarant zove ili šalje e-mail uposlenicima firme predstavljajući se kao njen direktor ili član uprave. Nalaže hitno provođenje plaćanja uz naglasak da je riječ o *osjetljivoj* situaciji (porezna kontrola, revizija i sl.) te koristi fraze



> *Konstantna edukacija i informisanost uposlenika, provođenje internih protokola vezanih za plaćanje i poštivanje sigurnosnih postupaka su samo neki od načina na koje se firma i njeni uposlenici mogu zaštititi od ovakvog oblika prevare.*

kao *strogo povjerljivo*, *firma ima povjerenje u Vas*, *trenutno sam nedostupan* i sl. Često se zahtjev odnosi na međunarodna plaćanja bankama izvan Evrope.

Kako se zaštititi?

Konstantna edukacija i informisanost uposlenika, provođenje internih protokola vezanih za plaćanje i poštivanje sigurnosnih postupaka, obavezna provjera legitimnosti instrukcija za plaćanje koje se primaju putem e-maila, ažuriranja i nadogradnja tehničke sigurnosti, izbjegavanje dijeljenja informacija o internoj organizaciji firme, njenoj sigurnosti i procedurama samo su neki od načina na koje se firma i njeni uposlenici mogu zaštititi od ovakvog oblika prevare.

Lažne nagradne igre

Prevara se odvija tako što se građani putem društvenih mreža informišu da su *sretni dobitnici* nagradne igre organizovane od strane poslovnog subjekta čiji se podaci u tu svrhu zloupotrebljavaju (trgovački lanci, banke i sl.) te kako je potrebno da dostave lične podatke i fotografiju lične karte kako bi im organizatori mogli poslati nagradu.

Kako se zaštititi?

Cilj prevaranta je prikupljanje i zloupotreba ličnih podataka te se u cilju zaštite od ovakvog i ostalih oblika internet prevare nikako ne preporučuje slanje ličnih podataka, svojih fotografija i fotografija ličnih dokumenata putem društvenih mreža ili elektronske pošte.

Prevencija kao dodatni oblik zaštite

Sa napretkom tehnologije oblici *cyber* prevara postaju raznovrsniji te su kontinuirana informiranost, edukacija i pojačana svijest o potrebi za opreznošću pri korištenju interneta preporuka svim korisnicima. Kao efikasan dio borbe protiv ovih oblika prevare pokazalo se i preduzimanje nekih osnovnih mjera opreza poput:

- ažuriranje programa na računaru,
- korištenje antivirusa,
- pojačan oprez prilikom otvaranja sumnjivih e-mailova i linkova,
- korištenje snažnih lozinki,
- podizanje svijesti o sigurnosti korištenja interneta uz redovno praćenje sigurnosnih smjernica od strane finansijskih institucija te
- oprez pri dijeljenju ličnih podataka na društvenim mrežama. ■

(tekst je objavljen u magazinu Banke i Biznis, broj 203, mart 2019.)

Zanimljivosti

NAJTRAŽENIJI HAKER NA SVIJETU

Autorica:
Sanela Stupar

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

EVGENIY MIKHAILOVICH BOGACHEV

Multimedia: Images

Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983	Hair:	Brown (usually shaves his head)
Height:	Approximately 5'9"	Eyes:	Brown
Weight:	Approximately 180 pounds	Sex:	Male
NCIC:	W890989955	Race:	White
Occupation:	Bogachev works in the Information Technology field.		

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

Obično hakere zamišljamo kako nose crnu garderobu sa crnom kapuljačom na glavi, ali to su *obični ljudi* koji možda sjede do vas u restoranu. Jedan od najtraženijih hakera je **Jevgenij Mihailovič Bogačev**.

Bogačev je poznat i kao **Slavik** koji je izumio malvere *Zeus* i *GameOver Zeus* koje je koristio za krađu podataka i šifara za bakarske račune. Na taj način je ukrao 100 miliona dolara. Za informaciju o njemu FBA daje do tri miliona dolara. Na listi su njegovi učenici, članovi grupe ***Jabber Zeus***.

Nova usluga na dark web-u: Iznajmljivanje virusa na određeni period

Popularni android trojani poput *Anubisa*, *Red Alert 2.0*, *GM bot-a i Exobota* nisu više toliko aktuelni jer se pojavio novi zlonamjerni softver sa sličnim mogućnostima.

Trojan pod nazivom ***Cerberus*** daljinskim pristupom omogućava udaljenim napadačima da preuzmu potpunu kontrolu nad zaraženim android uređajima, a u sebi sadrži bankarski trojan sa kojim upravlja SMS tekstovima, pruzima kontakate iz imenika, lične podatke, brojeve kreditnih kartica korisnika, bankarske akreditive i lozinke za intrenetske račune. Virus se pretvara da je *Flash Player* ili neko drugo ažuriranje softvera.

Zanimljivo za ***Cerberus*** je to da se ovaj zlonamjerni softver može kupiti na *Dark webu* kao usluga za 2.000 dolara mjesečno, 7.000 dolara godišnje ili 12.000 dolara godišnje.

Prema istraživačima, ***Cerberus*** već sadrži obrasce za napad prikrivanja sa ukupno 30 jedinstvenih ciljeva uključujući:

- 7 francuskih bankarskih aplikacija,
- 7 U.S. bankarskih aplikacija,
- 1 japansku aplikaciju za bankarstvo i
- 15 nebankarskih aplikacija.

Trojan ***Cerberus*** koristi zanimljive tehnike kako bi izbjegao otkrivanje antivirusnih rješenja i spriječio njegovu analizu, poput korištenja senzora ubrzanja uređaja za mjerenje pokreta žrtve (preko aplikacija kao što je *Pedometer* koja prati broj koraka, vrijeme aktivnosti, brzinu i prijeđenu udaljenost). Naime, android uređaj obično generira određenu količinu podataka senzora pokreta. Zlonamjerni softver prati korake korisnika putem senzora kretanja na uređaju kako bi provjerio radi li na stvarnom android uređaju ili je sandbox za skeniranje malware koji nema senzor pokreta te isti neće ni pokrenuti zlonamjerni kod.

Sigurnosne preporuke:

- Nikada ne pristupajte poveznicama koje su poslane SMS ili MMS porukama!
- U slučajevima kada stigne poruka koja se doima legitimnom, dvostruko provjerite pošiljatelja!
- Onemogućite instalaciju neslužbenih aplikacija iz nepoznatih izvora u postavkama uređaja!
- Ovoj se opciji pristupa putem izbornika "Postavke", zatim je potrebno odabrati "Napredne postavke" te na kraju "Sigurnost". U izborniku "Sigurnost" treba onemogućiti instalaciju neslužbenih aplikacija čime osiguravate instalaciju aplikacija preuzetih isključivo s trgovine *Google Play*.
- Redovito izvršavajte nadogradnje operativnog sistema, aplikacija te antivirusnih programa na uređaju. ■

Najsigurnija metoda za kontrolu pristupa podacima i aplikacijama

MULTIFAKTORSKA AUTENTIFIKACIJA

NAJBOLJA PRAKSA ZA PREVENCIJU NEAUTORIZOVANOG PRISTUPA

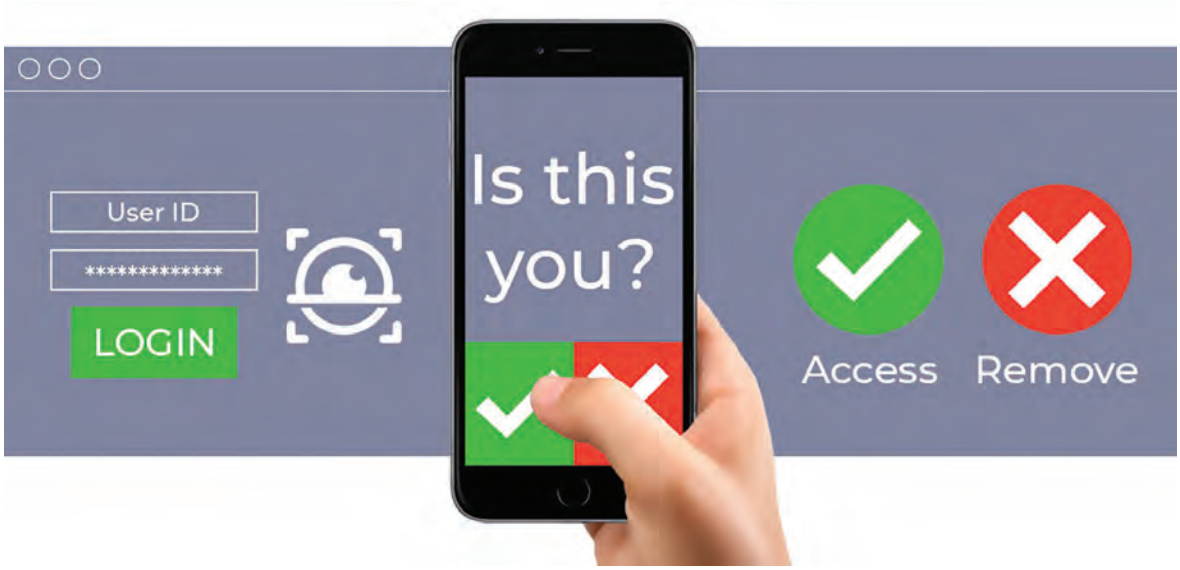
Sigurnost za IT, jednostavnost za korisnika, manje glavobolje za sve - to je multifaktorska autentifikacija

Autorica:
Sanela Vrana

Nemojte ostaviti *'ključ ispod otirača'*!

Autentifikacija predstavlja proces utvrđivanja istinitosti nečije tvrdnje o svom identitetu. *Username* (korisničko ime) i *password* (šifra) su primjer najjednostavnijeg načina autentifikacije – jednostruke autentifikacije (SFA-*single factor authentication*). *Password*, kao najčešće korišteni način kontrole pristupa, ujedno je i najranjivija tačka u arhitekturi sigurnosti informacionog sistema. On nam daje dodatnu sigurnost kod korištenja *online* usluge ili pristupa traženom uređaju, ali vrlo lako može biti „dvosjekli mač" ukoliko ga ne koristimo odgovorno i oprezno te može nanijeti više štete nego koristi. Korisnici i njihove šifre su najslabija karika u sigurnosti informacionog sistema i mogu uzrokovati da ostane nejasno ko stvarno koristi sistem i pristupa podacima i aplikacijama. Iz izvještaja o povredama podataka uzrokovanim *cyber security* napadima možemo pronaći da se 80% njih odnosi na korištenje ukradenih *passworda* i slabih *passworda*, tj. onih koji se lako

> *Cyber kriminalci koriste metode socijalnog inžinjeringa, tj. manipulišu ljudskom prirodom: povjerenjem, radoznalošću, strahom, velikodušnošću ili čak dobrotom kako bi došli do naših kredencijala te do našeg novca ili novca poslodavca.*



otkrivaju. *Cyber* kriminalci koriste metode socijalnog inžinjeringa, tj. manipulišu ljudskom prirodom: povjerenjem, radoznalošću, strahom, velikodušnošću ili čak dobrotom kako bi došli do naših kredencijala te do našeg novca ili novca poslodavca. Ranjivost *passworda* leži u činjenici da isti ne obezbjeđuje jedinstven identitet korisnika. Bilo ko da dođe u njegov posjed može pristupiti računu, uređaju ili usluzi. Često je sigurnost *passworda* ugrožena već od strane njegovog vlasnika izborom lako pamtljivih riječi umjesto jedinstvenih nizova brojeva, karaktera i simbola.

Zašto je multifaktorska autentifikacija tako važna?

Odgovor je vrlo jednostavan: jednostruka autentifikacija više nije dovoljna. Logiranje, odnosno spajanje na određenu *online* aplikaciju, servis ili nešto treće, samo sa korisničkim imenom i šifrom više nije sigurno. Sve veći poslovni zahtjevi, sve veći broj servisa koji se iz svakodnevnog života sele u digitalni svijet te svakodnevna pojava novih prijetnji, rizika i ranjivosti upućuju na stalnu potrebu osnaživanja pristupa provjere identiteta zadržavajući pri tom zahtjev za jednostavnim korištenjem i neometanim pružanjem usluga. Zato se uvodi dvofaktorska (dvostruka) ili multifaktorska (višestruka) autentifikacija kako bi se onemogućio neovlašteni pristup pod nečijim tuđim identitetom.

> *Često je sigurnost passworda ugrožena već od strane njegovog vlasnika izborom lako pamtljivih riječi umjesto jedinstvenih nizova brojeva, karaktera i simbola.*

Šta je multifaktorska autentifikacija (MFA)?

Multifaktorska autentifikacija obezbjeđuje da je korisnik stvarno onaj koji on tvrdi da jeste. Što se više faktora autentifikacije koristi, to je veća pouzdanost same autentifikacije. Multifaktorska autentifikacija priznata je kao najsigurniji metod za kontrolu pristupa podacima i aplikacijama, a predstavlja naprednu proceduru kontrole pristupa koja potvrđuje identitet korisnika kombinujući više jedinstvenih faktora.

Dvofaktorska autentifikacija (2FA) vs. multifaktorska autentifikacija (MFA)

Dvofaktorska autentifikacija (2FA) je najjednostavnija i najčešće korištena forma multifaktorske autentifikacije (MFA). Najobičniji primjer dvofaktorske autentifikacije je povlačenje novca sa ATM uređaja koje zahtjeva od korisnika da potvrdi svoj identitet fizičkim ubacivanjem kartice i unosom PIN-a. Najčešći primjer dvofaktorske autentifikacije u *online* uslugama je dvostruka digitalna autentifikacija uz pomoć *passworda* i koda koji je poslan korisniku na neki od njegovih uređaja u formi teksta. Dvofaktorska autentifikacija je na neki način podskup metoda multifaktorske autentifikacije. Multifaktorska autentifikacija je, sa druge strane, autentifikacija koja zahtijeva provjeru i potvrdu više parametara/faktora. Iako dvofaktorska autentifikacija ima značajne prednosti nad jednostrukom autentifikacijom (SFA-*single factor authentication*), ona i dalje predstavlja određeni stepen ranjivosti, pogotovu što zahtijeva prisustvo mobilnog uređaja koji može biti ukraden ili tehnički neispravan.

> *Sve veći poslovni zahtjevi, sve veći broj servisa koji se iz svakodnevnog života sele u digitalni svijet te svakodnevna pojava novih prijetnji, rizika i ranjivosti upućuju na stalnu potrebu osnaživanja pristupa provjere identiteta zadržavajući pri tom zahtjev za jednostavnim korištenjem i neometanim pružanjem usluga.*

> *I dvofaktorska autentifikacija predstavlja određeni stepen ranjivosti jer zahtijeva prisustvo mobilnog uređaja koji može biti ukraden ili tehnički neispravan.*

Kako radi multifaktorska autentifikacija?

Multifaktorska autentifikacija potvrđuje identitet korisnika prilikom logiranja na *online* servis, aplikaciju, uređaj ili nešto drugo sa više nezavisnih faktora:

- nešto što korisnik zna (*password* ili PIN),
- nešto što korisnik posjeduje (token ili smart kartica),
- nešto što korisnik jeste (biometrija - otisak prsta, prepoznavanje glasa, prepoznavanje lica, skeniranje šarenice oka...).

Upotrebljavajući više nezavisnih faktora prilikom auten-

tifikacije, praktično onemogućavamo da se neko drugi predstavi, odnosno logira umjesto nas. Broj nezavisnih faktora je jako važan jer što ih je više, to je manja vjerovatnoća da će svi biti otuđeni istovremeno, a to je ključno u konceptu multifaktorske autentifikacije. Neki od faktora su u „virtuelnom svijetu" (npr. *password* koji se može ukrasti), a neki u „realnom svijetu" (npr. mobilni uređaj, token i sl.) i do njih je već teže doći. U tom slučaju korisnik posjeduje nešto što nema niti onaj ko pruža određenu uslugu te se, samim tim, ne može ni otuđiti iz sistema i iskoristiti umjesto ili protiv korisnika. Dodatna sigurnost je kratki vremenski period za koji vrijedi generisani kod poslan na neki od mobilnih uređaja. Korištenje mobilnih telefona za potrebe autentifikacije sve je popularnije, a u prilog mu idu i pokazatelji da prosječna osoba ima jaču svijest o svom telefonu i njegovoj lokaciji nego što je to slučaj sa novčanikom ili ključevima.

Kada je riječ o biometriji, ona se kod *online* servisa rijetko koristi (jer je teško obezbijediti da svi klijenti posjeduju čitač otiska prsta ili nešto slično), ali u velikim kompanijama i sistemima biometrija ulazi na velika vrata i koristi se često za onemogućavanje pristupa dijelovima kompanije za čiji pristup korisnici nemaju ovlaštenje. Cijene biometrijskih rješenja su u padu širom svijeta, a napredak je svakodnevan u segmentu kontaktnih i beskontaktnih rješenja. Jedno od najčešće korištenih kontaktnih rješenja su otisci prstiju. Beskontaktna biome-

Korištenje mobilnih telefona za potrebe autentifikacije sve je popularnije, a u prilog mu idu i pokazatelji da prosječna osoba ima jaču svijest o svom telefonu i njegovoj lokaciji nego što je to slučaj sa novčanikom ili ključevima.

trijska rješenja su u prvom redu skeniranje šarenice oka i prepoznavanje lica, pri čemu biometrija doživljava uspon u segmentu prepoznavanja lica, a čini se da koncept skeniranja šarenice oka ne spada više u rastuću tehnologiju.

Integracija sigurnosnih rješenja kontrole pristupa

Savršen sistem autentifikacije ne postoji jer ga kreira čovjek pa ga čovjek može i probiti. Ono što možemo jeste primijeniti snažan multifaktorski sistem autentifikacije te educirati korisnike o najnovijim opasnostima, kao i o najnovijim trendovima sigurnosti. Budućnost nam donosi integraciju različitih sistema kontrole pristupa, videonadzora, kontrole perimetara, a menadžerima sigurnosti se na taj način olakšava nadzor i obezbjeđuje holistički pregled situacije.

> *Moramo voditi računa kako o potrebi za što većom sigurnošću, tako i o brzoj i praktičnoj upotrebi sistema, optimizaciji rada i sigurnosti, tj. o njihovoj ravnoteži.*

Govoreći o multifaktorskoj autentifikaciji i integraciji sigurnosnih rješenja kontrole pristupa, moramo ipak voditi računa kako o potrebi za što većom sigurnošću, tako i o brzoj i praktičnoj upotrebi sistema, optimizaciji rada i sigurnosti, tj. o njihovoj ravnoteži. ■

Pljačka banke može se obaviti bilo gdje

KAKO SE ODBRANITI
OD VIRTUELNIH PLJAČKAŠA

Opasnosti od *cyber* napada ne prestaju. U cilju edukacije i podizanja svijesti u oblasti informacione sigurnosti, banke svoje klijente savjetuju i pomažu im da zaštite svoju imovinu od virtuelnih napada.

Autorica:
Sanela Stupar

Banke su često bile mete pljačke. Prva potvrđena pljačka banke izvršena od strane Franka i Jesse James 1869. godine. Jedan od pljačkaša prišao je blagajniku i pitao ga da mu zamijeni novčanicu od 100 dolara. Dok je blagajnik pisao račun, pljačkaš je izvadio revolver i ustrijelio ga u prsa i čelo, čime ga je na mjestu usmrtio. Pljačkaši su zgrabili ono za što su mislili da je novac, ali to je bila hrpa bezvrijednog papira. Organizovana je potjera, no pljačkaši su uspjeli pobjeći.

U tom periodu maksimalni iznos plijena je bio ograničen na fizičku valutu imovine jedne poslovnice banke.

Danas, u doba interneta, pljačka banke može se obaviti bilo gdje, a ukupni plijen pljačkaša povećao se na imovinu banaka širom svijeta. Virtuelni pljačkaš banke nalazi se u nekoj drugoj zemlji, daleko od od klijentele koju želi da opljačka, a samim tim šanse da se suoči sa sudskim postupkom su veoma male.

> *Pljačka banke može se obaviti bilo gdje.*
> *Virtuelni pljačkaš banke nalazi se u nekoj drugoj zemlji,*
> *daleko od od klijentele koju želi da opljačka,*
> *a samim tim šanse da se suoči sa sudskim postupkom*
> *su veoma male.*

Opasnosti od prevare

Virtuelni pljačkaši banke danas koriste ***malware*** (zlonamjerni softwer) koji je dizajniran da uzrokuje velike štete

na podacima i sistemima ili da dobije neovlašteni pristup računaru ili mreži informacionog sistema. *Malware* se obično sastoji od koda koji su razvili *cyber* napadači i obično se isporučuje u obliku veze ili datoteke putem e-pošte, a koje izgledaju kao da su iz ciljane banke da bi prevarile korisnike i naveli ih da kliknu na vezu ili otvore datoteku kako bi instalirali zlonamjerni softver pomoću kojeg mogu kasnije ukrasti, odnosno preusmjeriti finansijske transakcije.

Kako se banke štite od *cyber* napada

Banke su izgradile visoko integriranu zaštitu od ciljanih napada i uspostavile mjere zaštite informacionog sistema od *cyber* napada u cilju zaštite svoje imovine i imovine koja im je povjerena od strane klijenta.
Kako bi osigurale što bolju zaštitu za svoje klijente, implementirale su aplikacije koje vrše nadzor transakcija, a sve to u svrhu sprečavanja, otkrivanja i blokiranja sumnjivih platnih transakcija u okviru sistema elektronskog bankarstva. Autentifikacija klijenata vrši se sa najmanje dva elementa za potvrđivanje identiteta (na primjer: SMS, pametna kartica, biometrijski otisak prsta…).

> *Banke klijentima preporučuju korištenje licenciranih antivirusa, da ne preuzimaju sumnjivu e-poštu, da uvijek provjeravaju ispravnost adrese web stranice, da ne šalju podatke za broj bankovnog računa, lične podatke i PIN.*

Detekcija novih tipova prevara, *cyber* napada, aktivnih prijetnji inteligentnih *malwera* i zlonamjernih IP adresa su redovne aktivnosti stručnjaka za sigurnost u cilju što bolje odbrane.

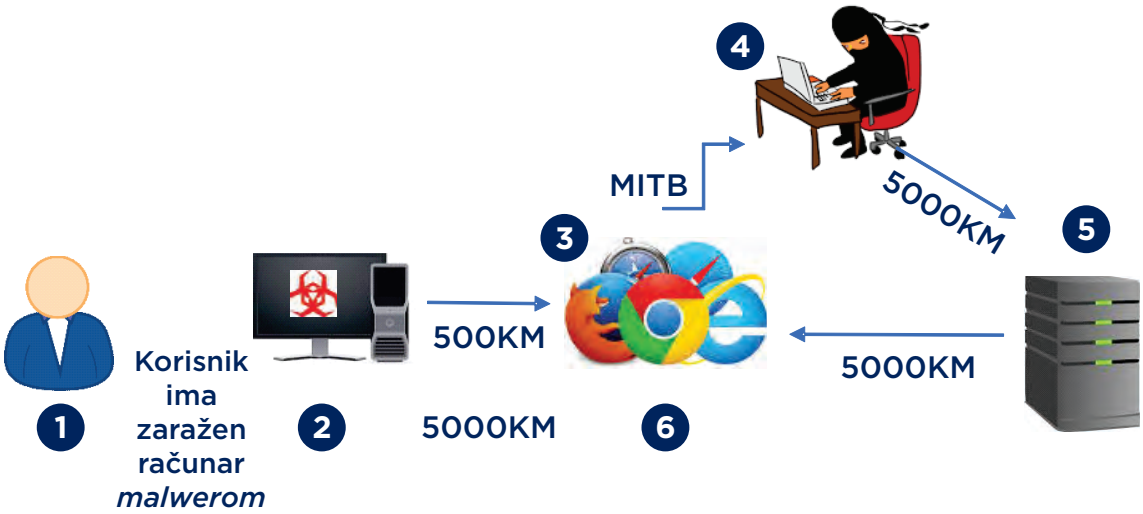
U cilju edukacije i podizanja svijesti u oblasti informacione sigurnosti, banke svojim klijentima savjetuju da koriste licencirane operativne sisteme koje redovno ažuriraju sa novim paketima zaštite, a u cilju smanjenja ranjivosti operativnog sistema njihovih računara. Klijentima preporučuju korištenje licenciranih antivirusa, da ne preuzimaju sumnjivu e-poštu, da uvijek provjeravaju ispravnost adrese web stranice, da ne šalju podatke za broj bankovnog računa, lične podatke i PIN.

Primjer jednog zlonamjernog softvera je *The man-in-the-browser* – MITB, napad koji se obično koristi za ciljanje finansijskih (bankarskih) transakcija. Zlonamjerni softver će biti u mogućnosti obavljati lažne novčane transfere ili plaćanja, a bankarska aplikacija neće moći otkriti bilo kakve lažne aktivnosti dok su ispravni podaci uneseni.

Korištenjem višestruke provjere autentičnosti, npr. OTP ili biometrije, možete se odbraniti od ovakvih napada.

Sa novim prijetnjama dolaze i nova tehnička rješenja. Softverske kuće razvile su svoje *antifraud* aplikacije za e-bankarstvo na način da provjeravaju računare korisnika

Grafički prikaz napada The man-in-the-browser – MITB



e-bankarstva. Provjeru vrše tako što provjere da li je ažuriran operativni sistem sa novim sigurnosnim zakrpama, da li je ažuran antivirus i da li ima na računaru *malwere*.

Ako je pronašao bilo koju ranjivost, korisnik dobije upozorenje na moguće opasnosti, a neke aplikacije čak blokiraju izvršenje transakcije i usmjeravaju korisnika da transakciju izvrši na sigurnoj platformi.

Cilj aplikacije *antifraud* za e-bankarstvo je da se ne oslanja na znanje korisnika o sigurnosti e-bankarstva ili da se korisnici upozore na to šta trebaju poduzeti kako ne bi bili žrtve *cyber* napada.

Do implementacije ovakvih aplikacija najbolja odbrana je poštivanje autentifikacije sa dva faktora, provjera autentičnosti svojih transakcija te treba slijediti sigurnosne upute koje se od banaka dobiju.

Zaključak

Opasnosti od prevara ne prestaju. Banke će nastaviti da pružaju proizvode svojim klijentima u skladu sa novim tehnologijama, štitit će komunikacione kanale kako bi zaštitili svoju imovinu i imovinu koja im je povjerena od strane klijenata i kontinuirano će uvoditi dodatne sigurnosne mjere za zaštitu kranjih korisnika.

Nažalost, i prevaranti će nastaviti da razvijaju svoje napade.

Radeći zajedno na odbrani od *cyber* napada smanjuje se rizik prijetnji od prevara. ■

(tekst je objavljen u magazinu Banke i Biznis, broj 205, maj 2019.)

UPRAVLJANJE RIZIKOM
ETIČKE USKLAĐENOSTI I INTEGRITETA NA TRŽIŠTU KAPITALA

Tržište kapitala u BiH nije na zavidnom nivou. U posljednjih nekoliko godina sve veća pažnja posvećuje se upravljanju rizikom usklađenosti, a pri tome se prvenstveno misli na usklađenost sa pozitivnim propisima i primjenjivim standardima u EU. Otkrivamo da li banke i drugi učesnici na tržištu kapitala u BiH upravljaju rizikom etičke usklađenosti i zašto je za ovo pitanje potrebno hitno usvajanje zakonskih propisa

Autor:
Mujo Vilašević

Tržište kapitala u Bosni i Hercegovini

Tržište kapitala, u pojednostavljenoj definiciji je tržište finansijskih instrumenata i finansijskih derivata na uređenom tržištu ili izvan njega.

Ne bi bilo objektivno pretpostaviti da je tržište kapitala u Bosni i Hercegovini na zavidnom nivou. Počev od formalno-pravnih pretpostavki, ovaj segment finansijskog tržišta entitetski je uređen i ima entitetski nadzor (uostalom, gotovo kao i cjelokupan finansijski sistem BiH, isključivši osiguranje depozita i monetarnu politiku). Iako ova polazna tačka može otvoriti pitanja ustavnosti takve raspodjele nadležnosti u državi, fokus analize tržišta kapitala ipak bi trebale biti najbolje prakse koje mogu ponuditi neke države u regionu, a naročito Evropska unija.

> *Fokus analize tržišta kapitala trebaju biti najbolje prakse koje mogu ponuditi neke države u regionu, a naročito Evropska unija.*

Tržište kapitala u Evropskoj uniji

Evropska unija od 2014. godine intezivno radi na "mobilizaciji kapitala u Evropi",

sa ciljem poboljšanja investiranja na tržištu kapitala, kreiranja otpornijeg finansijskog sistema i kreiranja novih radnih mjesta. Prema posljednjim objavljenim rezultatima, *Plan investiranja u Evropskoj uniji* do 2019. godine dosegao je promet od cca 410 milijardi EUR na tržištu kapitala. Ovi podaci govore o tome šta praktično znači **Jedinstveno tržište kapitala Evropske unije**, kao još jedan vid integracije država članica.

Teret upravljanja rizicima usklađenosti

Međutim, tržište kapitala sa sobom nosi i značajan "teret" upravljanja rizicima. Otporniji finansijski sistem, kakvom teži Evropska unija, moguć je i uz primjenu odgovarajućih *risk* standarda, politika i mehanizama koji mogu osigurati otpornost na snažne finansijske i tržišne promjene, očekivane i one manje očekivane tržišne turbulencije uzrokovane političkim dešavanjima (čitaj: npr. Brexit). U posljednjih nekoliko godina sve veća pažnja posvećuje se upravljanju rizikom usklađenosti. Pri tome se prvenstveno misli na usklađenost sa pozitivnim propisima i primjenjivim standardima, zaštita reputacije, interesa vlasnika i povjerioca, a u cilju izbjegavanja regulatornih sankcija. Zapravo, kada govorimo o upravljanju rizikom usklađenosti u finansijskom sektoru općenito, govorimo o različitim izvedenicama Baselskih načela *Compliance and compliance function in banks* iz 2005. godine. U posljednje vrijeme se ipak sve više čuju termini poput *ethics compliance*, ili *integrity compliance*, a naročito kada se govori o tržištu kapitala. O čemu se radi?

> *Kada govorimo o upravljanju rizikom usklađenosti u finansijskom sektoru općenito, govorimo o različitim izvedenicama Baselskih načela* ***Compliance and compliance function in banks*** *iz 2005. godine.*

Upravljanje rizikom etičke usklađenosti u bankama

Ako bismo tragali za upravljanjem rizikom etičke usklađenosti u bankama, ne bi bilo teško pronaći adekvatne izvore. Novi regulatorni okvir za banke uspostavio je "Funkciju praćenja usklađenosti" koja, u skladu s primjenjivim odlukama entitetskih agencija za bankarstvo, ima obavezu da *poznaje, prati izmjenu zakonske regulative i uticaj tih izmjena na poslovanje banke, da poznaje pravila struke, dobre poslovne običaje i poslovnu etiku*. Citirana odredba, identična u oba entiteta, iako vrlo lako može pobjeći pažnji čitaoca, ipak otvara vrata jednom novom aspektu upravljanja rizikom usklađenosti i na formalnoj razini (nije rijetkost da su pojedine banke etičku usklađenost imale uspostavljene daleko prije nego su pozitivni propisi u BiH krenuli ukorak s EU propisima i to zahvaljujući matičnim grupacijama sa unijskim sjedištem i standardima koji su se tim putem preslikavali u lokalne banke-kćeri). Pretpostavka je, dakle, da banke

na formalnoj i suštinskoj razini imaju uspostavljene mehanizme upravljanja rizikom etičke usklađenosti.

Etička usklađenost kod drugih učesnika tržišta kapitala

No, može li se ova (vjerovatno oboriva) pretpostavka makar teoretski primijeniti na ostale učesnike tržišta kapitala? Zašto je drugim učesnicima tržišta kapitala neophodno upravljanje rizikom etičke usklađenosti, upravljanje integritetom poslovanja? Primjenjivi propisi kažu da su ovlašteni učesnici na tržištu kapitala pored banaka i profesionalni posrednici, Registar vrijednosnih papira, Komisija za vrijednosne papire, berza i drugo uređeno javno tržište, brokeri, dileri, investicijski savjetnici i menadžeri. Dakle, očigledno su u pitanju subjekti različitih pravnih subjektiviteta, i javnog i privatno-pravnog sektora.

> *Ovlašteni učesnici na tržištu kapitala pored banaka su i profesionalni posrednici, Registar vrijednosnih papira, Komisija za vrijednosne papire, berza i drugo uređeno javno tržište, brokeri, dileri, investicijski savjetnici i menadžeri.*

Svim navedenim subjektima, nesporno, potrebno i nužno je formalno uspostavljanje upravljanja rizikom etičke usklađenosti i integriteta, usvajanjem novih ili prilagodbom postojećih važećih propisa u oba entiteta.

Osjetljivost tržišta kapitala na zloupotrebe

Odgovor za prethodno postavljena pitanja leži u činjenici "osjetljivosti" tržišta kapitala, visokog stepena ka otvorenosti zloupotrebama, pogotovo imajući u vidu da je Bosna i Hercegovina zemlja nedovršene privatizacije i tranzicije prethodnih skoro 30 godina. Iako neki od pobrojanih subjekata imaju, što uslovljeno pripadnosti matičnim finansijskim institucijama, što samostalno kreirano, uspostavljene mehanizme praćenja usklađenosti, formalizacija ovog pitanja kroz pozitivno-pravne propise je nužna. Preslika uspostavljanja "Funkcije praćenja usklađenosti" iz bankarskog sektora nije idealno, ali jeste zadovoljavajuće početno rješenje. Cilj je, dakle, uspostavljanje mehanizma koji će da identifikuje, prati i poduzima mjere na reduciranju rizika etičke usklađenosti i integriteta. Rizični događaji koji mogu nastupiti i biti "okidač" ovoj vrsti rizika možda nose i veću težinu od finansijskih sankcija (iako se može raspravljati da se u konačnici svaka sankcija svodi na finansijsku), s obzirom na to da nosi sa sobom reputacijske posljedice koje su iznimno teško popravljive.

Uspostavljanjem sistema etičke usklađenosti čuva se ugled kompanije

Uspostaviti "savjest organizacije" nije jednostavan ni jednokratan proces. Radi se o pitanju koje zahtijeva vrijeme, znanje i predanost ka cilju. Pri tome, važno je ne izgubiti iz vida suštinu – etička

> *Etička usklađenost i poslovanje s integritetom nalažu svakom pojedincu u organizaciji da drži do uspostavljenih pravila i principa, čak i kada to nije najprofitabilnije rješenje ("ponašati se etično, čak i kada niko ne gleda").*

usklađenost i poslovanje s integritetom nalažu svakom pojedincu u organizaciji da drži do uspostavljenih pravila i principa, čak i kada to nije najprofitabilnije rješenje ("ponašati se etično, čak i kada niko ne gleda"). Bilo mjesta za prihvatanje toga ili ne, vrijeme nas postepeno uči da je zapravo "identitet kompanije" ono što će sve više da postaje tržišna prednost, potiskujući cijenu i diverzitet proizvoda, pa i na tržištu kapitala (ili kako to neki autori pominju *competition in personality*).

Polaznih tačaka ima dovoljno.

Jedinstveno tržište kapitala EU nije savršena postavka. Na tom istom tržištu trenutno je u toku sudski spor vrijednosti cca 9 milijardi EUR protiv kompanije Volkswagen zbog zloupotrebe tržišta i povjerljivih informacija. Sigurno da je jedan od razloga takvog spora neadekvatno upravljanje etičkom usklađenosti i integritetom; možda čak i jednostavnije, izostanak integriteta u kompaniji i nerazvijena svijest zaposlenika o ovom riziku.

Pravna regulativa

Navedeni i i slični slučajevi doveli su i do unijskog ažuriranja propisa o tržištu kapitala, pri čemu se misli na ***Uredbe (EU) br. 596/2014 o zloupotrebi tržišta (MAR)***, odnosno ***Direktivu (EU) br.57/2014 o zloupotrebi tržišta (MAD II)***. Ovi dokumenti u svakom su slučaju obaveza za BiH, država ih je dužna implementirati prije ili kasnije. Uz ove, unijske dokumente, postoji još i niz izvora koji zakonodavcu mogu biti adekvatan alat za uspostavljanje upravljanja rizikom etičke usklađenosti i integriteta i na formalnoj razini, za sve učesnike tržišta kapitala. Naročito značajan izvor u tom smislu mogu biti ***Etički standardi CFA Instituta*** (*Institut za ovlaštene finansijske analitičare*), a i pojedini već usvojeni propisi, kao što su propisi o dobrovoljnim penzijskim fondovima, koji su u praksi zaživjeli u RS-u, a u FBiH još uvijek čekaju potpunu realizaciju sa novim propisima o porezu na dohodak. Funkcija praćenja usklađenosti bit će obavezna za društva koja budu upravljala ovim fondovima, a koja su istovremeno profesionalni posrednici i učesnici tržišta kapitala.

Težina ovog zadatka, za sada, primarno je kod zakonodavca pa bi pitanje etike i usklađenosti trebalo da bude "na stolu" kod razmatranja ažuriranja propisa o tržištu kapitala. ■

Ovaj rad ne izražava stavove i mišljenja institucije u kojoj je autor zaposlen.

(tekst je objavljen u magazinu Banke i Biznis, broj 207, juli/august 2019.)

Police osiguranja su najefikasnije sredstvo osiguranja kredita

PRIMJENA OSIGURANJA U BANKARSTVU

Iako u našem društvu nije dovoljno razvijena svijest o koristi od osiguranja, police osiguranja kao sredstvo pokrića određene vrste rizika predstavljaju benefite za osiguravajuće kuće, klijente i banke ukoliko bi se uspostavili propisi i rješenja koja osiguravaju ravnopravan tretman svih učesnika u postupku

Autor:
Muris Bešić

Police osiguranja kao sredstvo osiguranja kredita ili police osiguranja kao sredstvo pokrića određene vrste rizika, koji se može desiti korištenjem kreditnih ili drugih proizvoda banke, predstavljaju vrlo značajan instument iz kojeg se mogu pokriti eventualni gubici koje korisnici usluga ili banka mogu imati u slučaju povodom korištenja određene bankarske usluge.
Ukoliko se prodaja navedenih polica posmatra i sa aspekta osiguranja, sigurno je da to i za osiguravajuće kuće predstavlja odličnu priliku za prodaju velikog broja polica, pogotovo imajući u vidu broj korisnika bankarskih usluga uz koje bi se vršila prodaja polica osiguranja.

Iz trenutne perspektive svakako da se teško oteti dojmu da nije dovoljno iskorištena mogućnost upotrebe polica osiguranja ove vrste. Kao jedan od bitnijih razloga zašto je to tako, prvenstveno bih istakao nedovoljnu ponudu adekvatnih proizvoda osiguranja koji bi zadovoljili potrebe korisnika bankarskih usluga i banke, a naravno i istovremeno bili dovoljno atraktivni za same osiguravajuće kuće. Zajedno sa navedenim razlogom svakako da se može navesti i nedovoljna svijest građana i drugih subjekata o koristi od osiguranja.

POLICA OSIGURANJA KAO SREDSTVO OSIGURANJA KREDITA

Kao najprostiji primjer korištenja police osiguranja može se uzeti zalaganje police životnog osiguranja sa otkupom vrijednosti kao sredstvo osiguranja kredita. Polica životnog osiguranja sa štednom komponentom osim što

nudi mogućnost isplate osigurane sume u slučaju smrti, pruža i dodatnu pogodnost koja se ogleda u generisanju otkupne vrijednosti police. Ukoliko bi se se navedena polica založila kao sredstvo osiguranja, svakako da imamo jedno vrlo kvalitetno i brzo naplativo sredstvo osiguranja kredita ili drugog proizvoda banke. Međutim, iako se na prvi pogled stvari čine vrlo jasne, vjerovatno bi, nakon što detaljno proučimo uslove osiguranja, naišli na niz ograničenja (izuzev onih propisanih zakonom) u pogledu naplate osigurane sume, ali to svakako treba procijeniti na pravi način prilikom procjene rizičnosti svakog pojedinog klijenta. Iako u vrijeme pisanja ovog članka nisu dostpuni podaci o broju založenih polica kao sredstava osiguranja, sa velikom vjerovatnoćom se može tvrditi da ova mogućnost nije iskorištena ni u približno dovoljnoj mjeri. Svakako da bi se promocijom ove mogućnosti olakšao pristup prozvodima banaka koji zahtijevaju osiguranje i tako bi se osigurao adekvatan kolateral.

> *Primarana svrha većine polica osiguranja je osiguranje određenog rizika, a ne osiguranje potraživanja. Kao osiguranje potraživanja se posmatra eventualna novčana korist koja bi bila isplaćena ukoliko se desi osigurani slučaj.*

Međutim, iz vida se ne smije gubiti niti činjenica da police osiguranja, bar velika većina, ne osigurava bezuslovnu mogućnost naplate potraživanja na što upućuje i sama svrha osiguranja koja pruža pokriće za budući neizvjesni događaj koji u trenutku zaključenja ugovora nije nastao niti je u nastanku. Ukoliko je osigurani slučaj u momentu

zaključenja ugovora o osiguranju nastao, sam ugovor o osiguranju može biti nevažeći i u tom slučaju se gubi mogućnost naplate osigurane sume. Primarana svrha većine polica osiguranja je osiguranje određenog rizika, a ne osiguranje potraživanja. Kao osiguranje potraživanja se posmatra eventualna novčana korist koja bi bila isplaćena ukoliko se desi osigurani slučaj.

Svakako da se može istaći da osiguravajuće kuće putem klauzula u okviru Uslova osiguranja predviđaju za sebe određena prava koja mogu uticati na eventulanu isplatu osigurane sume. Predmetna prava su u određenim slučajevima vrlo široko postavljena te daju mogućnost osiguranjima da postupaju na osnovu diskrecione ocjene. Kao najočitiji primjer navedenog postupanja je mogućnost zahtijevanja dodatne dokumentacije prilikom rješavanja odštetnog zahtjeva čime se otvara mogućnost zloupotreba u cilju odugovlačenja ili stvaranja prilike za neisplatu osigrurane sume. Predmetna mogućnost ne bi postojala ukoliko bi sva potrebna dokumentacija koja je potrebna za isplatu odštetnog zahtjeva bila precizno navedena u okviru uslova osiguranja. Ovakva mogućnost, odnosno slične odredbe uslova osiguranja, zbog neizvjesnosti u postupanju predstavljaju vrlo visok rizik za banke koje bi police osiguranja koristile kao sredstvo obezbjeđenja svojih potraživanja.

Posmatrajući policu osiguranja sa aspekta instumenta osiguranja proizvoda banaka, što svakako nije njena primarna svrha, banke imaju interes za što sigurnijom isplatom iz sredstava obezbjeđenja kredita. Potrebno je imati u vidu da bezuslovnu isplatu sredstava iz police osiguranja nije moguće predvidjeti jer bi u tom slučaju osiguravajuće kuće došle u situaciju da imaju isplate osiguranih suma koje nisu osnovane, a što predstavlja nepovoljnost za osiguravajuće kuće. Kao primjer predmetnog postupanje može se navesti situacija u kojoj osiguranje odbije isplatu štete jer je klijent prilikom zaključenja ugovora o osiguranju dao netačne podatke koji su takve prirode da osiguravajuća kuća, da je znala za iste, ne bi pristupila zaključenju ugovora. Navedena situacija svakako je vrlo rizična za banke čiji se kolateral osigurava jer neće moći ostvariti naplatu iz osigurane sume, dok u većini ovih situacija osiguranje nema rizika u navedenom postupanja s obzirom na to da u određenim slučajevima imaju osnov da zadrže do tada uplaćenu premiju osiguranja. Dakle, ukoliko bi se osiguravajuće kuće obavezale na bezuslovne isplate osiguranih suma, izložene su riziku nezakonitog postupanja usljed čega bi, osim finansijskih gubitaka, mogle biti izložene neusklađenosti sa propisima, a što za posljedicu može imati i novčane kazne tijela zaduženih za kontrolu rada osiguranja.

Pošto se evidentno radi o suprotstavljenim interesima koji mogu uzrokovati probleme u radu zbog neprimjerenog korištenja ovlaštenja prilikom rješavanja odšetnog zahtjeva, kao i zbog mogućih očekivanja na isplate koje nemaju osnove u budućem periodu, treba poraditi na uza-

> *Slučajeve u kojima je moguće odbiti odštetni zahtjev jako je bitno prepoznati upravo kako bi se u što manjoj mjeri izbjegle sporne situacije između svih uključenih strana u ovom procesu, tj. banke, korisnika uluga i osiguravajuće kuće.*

jamnom dijalogu kako bi se zajednički i vrlo transparentno definisali načini rada koji neće ostavljati prostora za bilo kakve nedomice u pogledu postupanja i očekivanja. Tako da nastavno na navedeno, vrlo bitno je sa aspekta banke i korisnika njene usluge precizno odrediti u kojim slučajevima može doći do toga da osiguravajuća kuća može opravdano odbiti odštetni zahtjev. Slučajeve u kojima je moguće odbiti odštetni zahtjev jako je bitno prepoznati upravo kako bi se u što manjoj mjeri izbjegle sporne situacije između svih uključenih strana u ovom procesu, tj. banke, korisnika uluga i osiguravajuće kuće. Sami modaliteti saradnje mogu biti različiti, ali u svakom od njih bitno je utvrditi pravni status svakog učesnika kao i uslove pod kojima se vrši osiguranje. Jedino takav pristup će u najvećoj mjeri osigurati izbjegavanje spornih situacija, nezadovoljstvo učesnika te učiniti police osiguranja atraktivnim i korisnim za sve učesnike u postupku.

Da bi se postigao nivo kvaliteta proizvoda koji bi bio zadovoljavajući za sve korisnika i istovremno se osigurala ravnopravnost svih učesnika, svakako da bi bilo korisno izvršiti konsultacije predstavnika stručnih službi banke i osiguravajuće kuće. Kroz zajednički pristup sigurno bi se iznašla povoljna rješenja.

Klijenti banke koji zaključuju police osiguranja u određenom broju slučajeva nisu svjesni da davanje netačne izjave prilikom zaključenja ugovora o osiguranju može imati za posljedicu ništavnost ugovora o osiguranju, a što u konačnici dovodi do nesuglasica između osiguranja i lica koja polažu prava iz police. Edukacija korisnika o navedenim posljedicama je jedan od ključnih elemenata na kojem je potrebno raditi kako bi se izbjegle neželjene posljedice nemogućnosti isplate osigurane sume koje pogađaju korisnike prava iz police. Na navedenoj edukaciji bi osim osiguravajućih kuća morale raditi i same banke jer su upravo one vrlo zainteresovane da ne nastupe štetne posljedice davanja netačnih izjava. U navedenom pogledu postoje i određeni modeli rada koje banke i osiguravajuće kuće mogu usaglasiti, ali to bi predstavljalo predmet razmatranja u svakom pojedinom slučaju tako da u ovom tekstu nije moguće dati preciznije upute.

PRAVNA REGULATIVA

Na našem tržištu je nedovoljno razvijena ponuda osiguranja od odgovornosti. Navedena vrsta osiguranja u zemljama Evropske unije, a posredno i kod nas, za pravna lica je postala aktuelna nakon donošenja propisa čije kršenjene za posljedicu ima sankciju koje se ogleda u

> *Police osiguranja nisu dovoljno iskorištene u domenu bankarskog poslovanja, kako zbog nedovoljne svijesti o njihovoj koristi, tako i zbog nedovoljne prilagođenosti potrebama korisnika bankarskih usluga i banke.*

plaćanju vrlo visokih novčanih kazni. Putem predmetnih polica osiguranja mogu se osigurati slučajevi u kojima osiguranjeljno pokriće obuhvata i gubitke koji su posljedica novčanih kazni. Kako bi se izbjegli pogrešni zaključci, ovdje je riječ o osiguranjima kod kojih se prilikom zaključenja ugovora o osiguranju podrazumijevaju vrlo detaljne i stručne provjere sposobnosti za prihvat u osiguranje. Navedene obaveze svakako pogoduju poslovnim subjektima koji žele u svom poslovanju biti usklađeni sa pozitivnim propisima. Posljedično ovakvom opredjeljenju, upravo usklađenost poslovanja sa pozitivnim propisima treba da bude osnova za donošenje zakona i propisa na državnom nivou kako bi se pravnim licima koja zaključuju ove vrste polica omogućile subvencije ili olakšani poreski tretman. Razlog zbog kojeg je opravdano argumentirati u korist subvencija ili olakšanja poreskog tretmana je taj što bi ova vrsta osiguranja zbog vrlo visokih osiguranih suma vjerovatno imala i visoke premije osiguranja, a kroz omogućavanje navedenih olakšica bi pravnim licima bilo olakšano zaključenje ugovora o osiguranju.

Na osnovu izloženog može se istaći da police osiguranja nisu dovoljno iskorištene u domenu bankarskog poslovanja, kako zbog nedovoljne svijesti o njihovoj koristi, tako i zbog nedovoljne prilagođenosti potrebama korisnika bankarskih usluga i banke. Na osnovu zajedničkog angažmana sigurno bi se, ukoliko za to postoji interes svih strana, mogla iznaći vrlo praktična rješenja koja osiguravaju ravnopravan tretman svih učesnika u postupku.

Police osiguranja od odgovornosti koje uključuju i pokriće od novčanih kazni zbog neusklađenosti uz njihovu pravilnu upotrebu i adekvatno postavljene uslove bi zasigurno dale doprinos u cilju usklađivanja poslovanja tržišnih subjekata sa pozitivnim propisima. A, ukoliko bi se omogućile olakšice za plaćanje premija, postale bi vrlo interesantne što bi doprinijelo razvoju tržišta navedenih polica osiguranja. ■

(tekst je objavljen u magazinu Banke i Biznis, broj 202, januar/februar 2019.)

Standardi informacione sigurnosti i njihova implementacija

MONITORING USKLAĐENOSTI POSLOVANJA

Organizacije koje prikupljaju ili obrađuju lične, finansijske ili medicinske podatke suočavaju se sa izazovima zaštite od *cyber* kriminala

Autorica:
Sanela Stupar

Kako zaštititi svoje poslovanje, informacije, proizvode, lične podatke zaposlenika i klijenata od *cyber* kriminala i hakera?

Cyber kriminalci konstantno i veoma brzo razvijaju nove vrste napada na organizacije i ključnu infrastrukturu pa zbog toga organizacije moraju stalno ulagati u *cyber* sigurnost i pratiti tehnološki razvoj.

- Prva faza *cyber* napada je ***izviđanje*** gdje je najlakše izvršiti napad ili gdje se na lak način može ostvariti finansijska dobit. Finansijska dobit se ne mora ostvariti samo preuzimanjem novca sa računa. Nju je moguće ostvariti i preuzimanjem nečijih ličnih podataka i njihovom prodajom. Ti podaci se mogu koristiti za bazu podataka kupaca i klijenata, za terorističke aktivnosti (falsifikovanje dokumenata ili kreditnih kartica na ime osobe od koje su preuzeli podatke) ili prodajom informacija o proizvodima, poslovanjima i patentima koji su u vlasništvu te osobe.

> *„Za neke cyber napade prođu i godine dok se ne otkriju, a pretpostavlja se da neki od takvih napada nisu nikad ni otkriveni."*

- Druga faza je ***skeniranje*** ključnih informacionih sistema kako bi utvrdili njihovu ranjivost i iskoristili je za dalji napad.

- Treća faza je ***dobijanje pristupa*** korištenjem raznih tehnika socijalnog inžinjeringa: *malwarea*, *phishinga*, infiltracije virusa itd.

- U četvrtoj fazi *criminal hacker* se već ***nalazi*** u Vašem

sistemu, prikriven, preuzima Vaše transakcije, preusmjerava ih na račune *mula* ili preuzima Vaše lične podatke koje može prodati na crnom tržištu.

- U petoj fazi, kada je već ostvario svoj cilj, ***napušta*** Vaš sistem i briše tragove kako ne bi mogao biti otkriven pomoću digitalne forenzike.

Vremenski faza izviđanja najduže traje dok faza održavanja pristupa i prikrivanje tragova može trajati samo par sati tako da krajnji korisnik ne može pravovremeno otkriti *cyber* napad. Za neke *cyber* napade prođu i godine dok se ne otkriju, a pretpostavlja se da neki od takvih napada nisu nikad ni otkriveni.

Organizacije koje prikupljaju ili obrađuju lične podatke te finansijske ili medicinske podatke, imaju moralnu i regulatornu obavezu da obrađuju i čuvaju podatke na način da su oni zaštićeni od *cyber* kriminala. Uskladiti poslovanje sa regulatornim zahtjevima i pri tome voditi računa o informacionoj sigurnosti predstavlja izazov za sve organizacije.

Identifikovati/prepoznati prijetnje i ranjivosti informacionog sistema, procijeniti rizike, uspostaviti kontrole, poduzeti mjere za smanjenje rizika, a zatim sve pratiti i revidirati rizike i kontrole, uz to držati korak sa razvojem informacione tehnologije i *cyber* prostora, predstavlja veoma zahtjevan i složen posao za organizacije.

Najčešće korišteni okviri upravljanja *cyber* rizicima i revizijom informacionih sistema su ISO/ IEC 27001:2013 i CobiT5.

ISO/ IEC 27001:2013 standard predstavlja uvažavanje minimalnih zahtjeva i mjera koje organizacija treba poduzeti da bi se uspostavio sistem za upravljanja sigurnošću informacija (*engl. information security management system - ISMS*). Standard ISO/ IEC 27001:2013 je usko povezan sa sigurnošću informacija i primjenjuje se u području revizije informacionih sistema te sadrži 14 kontrolnih područja, 33 kontrolna cilja i 133 kontrolne tačke.

COBIT 5 opisuje način provedbe upravljanja informaciono-komunikacionim tehno-

logijama (*eng. Information and Communication Technology - ICT*) i sadrži 5 područja, 37 ključnih informacijskih procesa i više od 300 detaljnih informacijskih provjera.

Monitoring usklađenosti poslovanja sa regulatornim zahtjevima, sigurnosnim standardima i najboljim praksama

Da bi organizacije mogle lakše pratiti implementaciju zahtjeva standarda informacione sigurnosti, kao i regulatorne zahtjeve, moraju uspostaviti bazu za monitoring usklađenosti koja sadrži:

Sigurnosne norme informacionog sistema

Uspostaviti bazu regulatornih zahtjeva, standarda i najboljih praksi te ih redovno ažurirati sa izmjenama i dopunama.

Mapiranje sa normama informacionog sistema

Mapirati regulatorne zahtjeve, standarde i najbolje prakse sa poslovnim procesima, internim aktima i procedurama, nosiocima aktivnosti i odgovornim licima.

Procjena rizika

Provesti analizu informacionih rizika za ključne informacione sisteme, pripremiti tretman rizika te praćenje realizacije i poduzetih mjera u cilju smanjenje rizika.

Kontrole

Evidentirati kontrole, revizorske preporuke i pratiti statuse realizacije koji se odnose na primjenu sigurnosnih normi i zahtjeva.

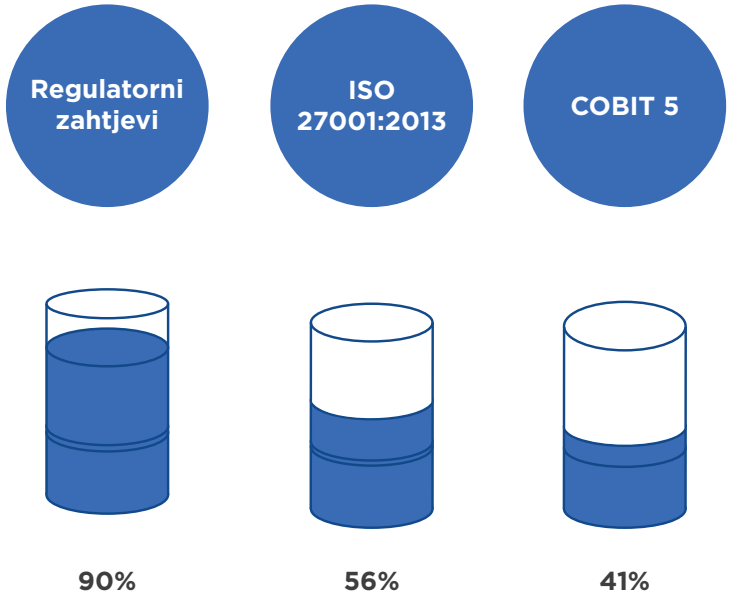
Status implementacije

U realnom vremenu raspolagati informacijama o monitoringu usklađenosti poslovanja sa sigurnosnim zahtjevima informacionog sistema.

Izvještaje

Izvještaji treba da sadrže informacije o broju sigurnosnih zahtjeva, statusu implementacije, te informacije o primjeni najbolje prakse, statusu implementacije, ocjeni rizika, poduzetim mjerama, rokovima implementacije i nosiocima aktivnosti.

Dobro uspostavljena baza monitoringa usklađenosti omogućava organizacijama da u realnom vremenu dobiju informacije na osnovu kojih će pripremati planove za kontrole, informacije na osnovu kojih će revidirati rizike usklađenosti i poduzeti odgovarajuće mjere. ■



(tekst je objavljen u magazinu Banke i Biznis, broj 207, juli/august 2019.)

EMIGRACIJA STANOVNIŠTVA IZ BIH U INOSTRANSTVO – TREND KOJI NE JENJAVA

Zemlju u najvećem broju napušta radno sposobna populacija tražeći prilike za boljim obrazovanjem, zaposlenjem i boljim radnim uslovima u odnosu na postojeće

Autori:
Berina Kapa
Ivan Pavlović

Bosna i Hercegovina se proteklih godina suočava sa sve većim trendom emigracije stanovnika u inostranstvo, o čemu se vrlo često piše i objavljuje u medijima. Proteklih godina se iz zemlje odselilo na desetine hiljada građana. Građani jednostavno ne vide perspektivu za život u svojoj domovini uslijed slabe ekonomske situacije i političke klime, te u potrazi za boljim i kvalitetnijim životom odlaze u inostranstvo, mahom u EU zemlje koje im nude prihvatljive životne i radne uslove. Zemlju ne napuštaju samo studenti i nezaposleni gradjani, već i zaposlene osobe nezadovoljne postojećim primanjima.

Šta kaže statistika?

Kada je riječ o emigraciji građana iz Bosne i Hercegovine u inostranstvo, prije svega je potrebno ukazati na nedostatak podataka koji se vode u BiH. Jedini podaci koji se mogu koristiti za statistiku su podaci koje vodi Agencija za identifikacijska dokumenta, evidenciju i razmjenu podataka BiH o broju osoba koje su se odjavile iz evidencije o prebivalištu i boravištu državljana BiH radi iseljenja u druge države. Međutim, ne postoji zakonska obaveza odjave prebivališta, tako da značajan broj onih koji napuštaju BiH zbog zaposlenja, studiranja ili nekih drugih razloga ne odjavljuju svoje prebivalište, te je broj iseljenika u inostranstvo sigurno daleko veći u odnosu na dostupne statističke podatke.

U svakom slučaju, dostupni podaci mogu ukazati na neke osnovne karakteristike trenda emigracije u inostranstvo.

Na redovnoj godišnjoj sjednici Skupštine Unije za održivi povratak i integracije u BiH, održane 26.2.2019. godine, objavljen je zvaničan podatak da je Bosnu i Hercegovinu za pet godina napustilo više od 173.011 ljudi ili 48.932 porodice. U 2018. godini BiH je napustilo 20.943, 2017. godine 35.634, a 2016. godine 34.544 lica[1]. Također, iz Unije navode da je samo od početka 2019. godine BiH napustilo 30.000 lica[2].

Prema evidenciji iz Statističkog biltena o migraciji stanovništva u 2017. godini u FBiH, najveći broj odlazaka je zabilježen iz pograničnih kantona (Tuzlanski, Unsko-sanski, Hercegovačko-neretvanski kanton), ali isto tako ne izostaju odlasci iz Sarajevskog, Zeničko-dobojskog i Srednjobosanskog kantona. Kada se usporede dostupni podaci o iseljavanju iz ranijih godina u odnosu na 2017. godinu, primjetan je trend povećanog odlaska u Njemačku i Austriju. Statistički podaci o starosti i spolu građana koji su otišli u inostranstvo iz FBiH u 2017. godini pokazuju da je riječ o populaciji starosne dobi: 20-44 godine, a odlaze gotovo podjednako i muške i ženske osobe. U istom biltenu je evidentan podatak da odlaze i građani Republike Srpske, međutim detaljniji podaci o starosnoj dobi i zemljama odredišta nisu dostupni kao za FBiH.

[1] BHRT. Dostupno na: http://www.bhrt.ba/bih-za-pet-godina-napustilo-173-011-ljudi/ [pristupljeno 26. juni 2019]

[2] N1 BiH. Dostupno na: http://ba.n1info.com/Vijesti/a348502/Sokantni-podaci-U-ovoj-godini-BiH-napustilo-30.000-gradjana.html [pristupljeno 26. juni 2019]

Dakle, osim mlade studentske populacije, zemlju u najvećem broju napušta radno sposobna populacija tražeći prilike za boljim obrazovanjem, zaposlenjem i boljim radnim uslovima u odnosu na postojeće.

Trend posredovanja u zapošljavanju BiH građana u inostranstvu

U BiH je trend zapošljavanja u inostranstvu definitivno sve popularniji. Posredstvom Agencije za rad i zapošljavanje (ARZ) BiH radni odnos u Sloveniji i Njemačkoj od 2013. godine zasnovalo je više od 31.000 radnika iz Bosne i Hercegovine. "Od aprila 2013. kada je potpisan Dogovor do 14. avgusta 2018. godine u Njemačkoj je zaposleno 4.159 radnika iz BiH", naveo je za Fenu direktor Agencije za rad i zapošljavanje BiH Muamer Bandić. Dogovor o posredovanju pri zapošljavanju radnika iz Bosne i Hercegovine u SR Njemačku, kako je poznato, provodi Agencija za rad i zapošljavanje BiH sa Saveznom agencijom za rad SR Njemačke i putem njega se medicinski radnici iz BiH koji su završili srednju medicinsku školu, opšti ili pedijatrijski smjer, mogu zaposliti na poslovima njegovatelja u Njemačkoj ako ispunjavaju uslove. Što se tiče Slovenije sa kojom BiH ima zaključen sporazum iz oblasti zapošljavanja, od marta 2013. do 30. juna 2018. godine u toj zemlji je zaposleno 26.919 radnika iz BiH.[3]

U Sloveniji se zapošljavaju uglavnom varioci, vozači, zidari, bravari, armirači, električari, tesari, elektroinstalateri. Plate svih radnika se kreću u bruto iznosu od 800 do 2.400 eura, radi se u najvećem broju o muškoj radnoj snazi, a uglavnom se zapošljava radna snaga između 25 i 40 godina starosti".[4]

Pored Agencije za rad i zapošljavanje koja pri posredovanju u zapošljavanju ipak daje prednost nezaposlenim osobama, na zvaničnim portalima privatnih agencija za zapošljavanje u BiH pored oglasa za zapošljavanje na lokalnom tržištu, svakodnevno se mogu pronaći i oglasi za rad u Njemačkoj, Hrvatskoj, Sloveniji, Slovačkoj i sl. U inostranstvu su najtraženije profesije stručnog medicinskog osoblja i KV zanimanja (monteri, instalateri, moleri, bravari, električari).[5] Dakle, za posao mogu aplicirati i zaposleni koji traže bolje radne uslove.

Analizirajući podatke dostupne ispred Federalnog zavoda za statistiku BiH, te Agencije za rad i zapošljavanje BiH, indikatori trenda iseljavanja građana idu prvenstveno u korist Njemačke i Slovenije.

Njemačka kao 'obećana' zemlja u Evropi

Evidentni su pokazatelji da Republika Njemačka privlači najveći broj naših građana

[3] Nezavisne novine. Dostupno na: https://www.nezavisne.com/ekonomija/analize/U-Sloveniji-i-Njemackoj-zaposleno-vise-od-31000-radnika-iz-BiH/494597 [pristupljeno 12. februar 2019]

[4] Poslovne novine. 2018. Zapošljavanje u Sloveniji i Njemačkoj: Izdato 23.387 radnih dozvola građanima BiH. Dostupno na http://poslovnenovine.ba/2018/03/14/zaposljavanje-u-sloveniji-njemackoj-izdato-23-387-radnih-dozvola-gradjanima-bih/ [pristupljeno 03. april 2018]

[5] Posao.ba. Dostupno na: https://m.posao.ba/#!searchjobs;lk=Njemacka [pristupljeno 03. april 2018]

koji zaposlenje traže vani. U tom kontekstu korisno je imati u vidu buduću strategiju Njemačke u zapošljavanju inostrane radne snage.

Najbolji pokazatelj odliva stanovništva u Njemačku oslikava podatak MUP-a Njemačke da smo za samo dvije godine ostali bez više od 50.000 građana što je veličina jednog grada u BiH. Njemački Savezni ured za migracije BamF objavio je novi izvještaj o useljavanju i iseljavanju iz te zemlje tokom 2016. i 2017. godine.

Prema tim podacima tokom 2016. i 2017. godine u Njemačku je doselilo 50.122 državljana BiH. Tokom 2016. godine iz BiH je doselilo 24.010 osoba, dok je iste godine iz Njemačke iselilo 16.355 državljana BiH. Tokom 2017. godine u Njemačku je doselilo 26.112 osoba iz BiH, dok ih je iz Njemačke iselilo 12.088. Dakle, tokom te dvije godine iz Njemačke je iselilo 28.433 osoba iz BiH.[6]

Na portalu *Make it in Germany*, koji je informativni portal za one koji žele živjeti i raditi u Njemačkoj, prezentirani su trendovi na njemačkom tržištu gdje se navodi da u nekim sektorima i regijama već nedostaje kvalificiranih stručnjaka. Ukoliko se ništa ne poduzme po ovom pitanju, demografske promjene

[6] Fokus.ba https://www.fokus.ba/vijesti/bih/njemacki-mup-objavio-koliko-je-gradjana-bih-u-dvije-godine-odselilo-u-njemacku/1354852/ [pristupljeno 12. februar 2019]

će kreirati manjak od nekih 6 miliona radnika u godinama koje dolaze, te da je osiguranje priliva kvalificiranih stručnjaka jedan od ključnih izazova s kojima se susreće njemački poslovni sektor.[7]

Njemačka ima veliki deficit radnika u strukama/ djelatnostima kao što su zdravstvene usluge i njega, proizvodnja i snabdjevanje energijom, građevinarstvo, IT usluge, metalska, mehanička i automobilska industrija, tehničko istraživanje i razvoj, transport željeznicama i sl.

Emigracija: trend ili prijetnja?

Prema svim dostupnim informacijama, trend emigracije može samo još više rasti, a stručnjaci procjenjuju da će se negativno odraziti na ekonomsku i demografsku sliku države. Ostajemo bez kvalificirane i stručne radne snage, a pojedina područja, posebno pogranična, ostaju bez stanovnika. Za očekivati je da će se na državnom nivou iznaći odgovarajuće strategije na polju zapošljavanja i reformnih poticaja za unaprjeđenje obrazovanja i radnih uslova, kako bi građani imali razloga ostati u državi i živjeti kvalitetniji i perspektivniji život u odnosu na postojeće stanje.

Obzirom da predmetni trend generalno utiče na ekonomiju, finansijske institucije kao neodvojiv dio iste, također monitoriraju uticaj trenda emigracije sa aspekta svoje domene poslovanja. Članice udruženja Fraud foruma aktivno sarađuju po ovom pitanju, te će i zajedničkim aktivnostima raditi na prilagođavanju poslovnih aktivnosti ovom trendu, te unaprjeđenju kvalitete poslovnog odnosa sa klijentima koji odlaze u inostranstvo. ■

[7] Make it in Germany. Background. Dostupno na: http://www.make-it-in-germany.com/en/for-qualified-professionals/about-the-portal/make-it-in-germany [pristupljeno 03. april 2018]

UREDNIČKI TIM

EUROPEAN FUND FOR SOUTHEAST EUROPE
DEVELOPMENT FACILITY

THE EFSE DEVELOPMENT FACILITY

A RELIABLE PARTNER IN CHALLENGING TIMES

The Development Facility of the European Fund for Southeast Europe (EFSE DF) was created in 2006 to support the fund's development finance mandate.

The EFSE DF deploys effective, targeted and innovative technical assistance to maximise the impact and extent of the fund's activities in target countries. The facility's services strengthen the internal capacities and operations of the fund's partner lending institutions through:

- ✓ **Capacity building**
- ✓ **Training**
- ✓ **Mentorship**
- ✓ **Applied research**
- ✓ **Financial sector support**

For more information, please contact **ta@finance-in-motion.com** or visit **www.efse.lu**