GOD. 4 . BR. 5 [2020] 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


UPRMBiH
Udruženje profesionalnih rizik menadžera
Dragi čitaoci, članovi i partneri,
Sretne nastupajuće praznike i
uspješnu i bolju novu 2021. godinu žele Vam
Amir Softić
Predsjednik Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini
Amar Brkan
Generalni sekretar Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini

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,

nesumnjivo ćemo svi skupa pamtiti 2020. godinu kao prekretnicu u našim životima i u životima ljudi širom svijeta upravo zbog pandemije COVID-19. Još uvijek se prilagođavamo ograničenjima u pogledu svakodnevne slobode kretanja i drugačijim radnim navikama dok se vlade i međunarodne organizacije suočavaju sa izazovima provođenja javnih zdravstvenih mjera i minimiziranja ekonomske štete. Pandemija COVID-19 ima dalekosežne posljedice na društvo i ekonomiju, ali i na povećanje kriminalnih i prevarnih radnji. Počinioci prevara ne sjede skrštenih ruku te su svoje prevarne radnje organizovali u skladu sa novonastalom situacijom.

Iz gore navedenih razloga, u petom izdanju ***FraudInfo*** časopisa naši urednici, odnosno autori, upravo obrađuju teme o globalnim trendovima prevara proizašlim iz pandemije (pojačan *cyber* kriminal, falsifikovanje, klasične prevare i sl.). Također, donose stručan osvrt o tome kako funkcije praćenja usklađenosti u bankarskim institucijama ovakve izazove mogu iskoristiti za jačanje i unaprijeđenje rada iz svoje domene.

Pored tema vezanih za uticaj pandemije, naš tim autora ispred **Fraud foruma** kroz časopis ***FraudInfo*** posvećuje pažnju i drugim prisutnim *fraud* trendovima, kao i načine kako ih prepoznati

Sadržaj

i prevenirati. U ovom broju upoznajte se detaljnije sa svim onim što stoji iza pojma haker te koji su indikatori počinjenja finansijske prevare i zašto dolazi do istih. Također, sigurni smo da će vam koristiti ponuđene preporuke vezane za sistem praćenja i prevencije prevara putem online kanala plaćanja koji bilježe porast upotrebe od strane potrošača.

S obzirom na to da naš tim ujedno prati i zakonske i ekonomske promjene na tržištu, koje mogu uticati na redovno poslovanje finansijskog sektora, obrađujemo i aktuelne teme ukazujući na eventualnu problematiku i potencijalna unaprijeđenja. U ovom broju donosimo stručni rad usmjeren na osnovne elemente ugovora o kreditu koji obavezno moraju biti navedeni prilikom zaključenja ugovora o kreditu između banke i fizičkog ili banke i pravnog lica.

Za one čitaoce koji do sada nisu bili upućeni u pojam i primjenu tzv. *Blockchain* tehnologije, ovo je upravo prilika da saznate nešto detaljnije i o ovoj vrsti moderne tehnologije.

Vjerujemo da će vam i naše peto izdanje ***FraudInfo*** časopisa donijeti dosta zanimljivih tema i aktuelnosti. Tim eksperata okupljenih u okviru Fraud foruma nastoji i kroz časopis ukazati na posebne oblike prevara te predložiti mjere prevencije, a ujedno prati relevantne tržišne i zakonodavne promjene koje utiču na poslovanje finansijskog sektora. Djelovanje finansijskih institucija kroz ovakvu vrstu saradnje ima za cilj doprinijeti zajedničkoj i efikasnijoj borbi protiv raznih oblika prevara. ■

UREDNIČKI TIM ČASOPISA

Neodvojiv način poslovanja bilo koje kompanije ili organizacije

KULTURA RIZIKA U POSLOVANJU

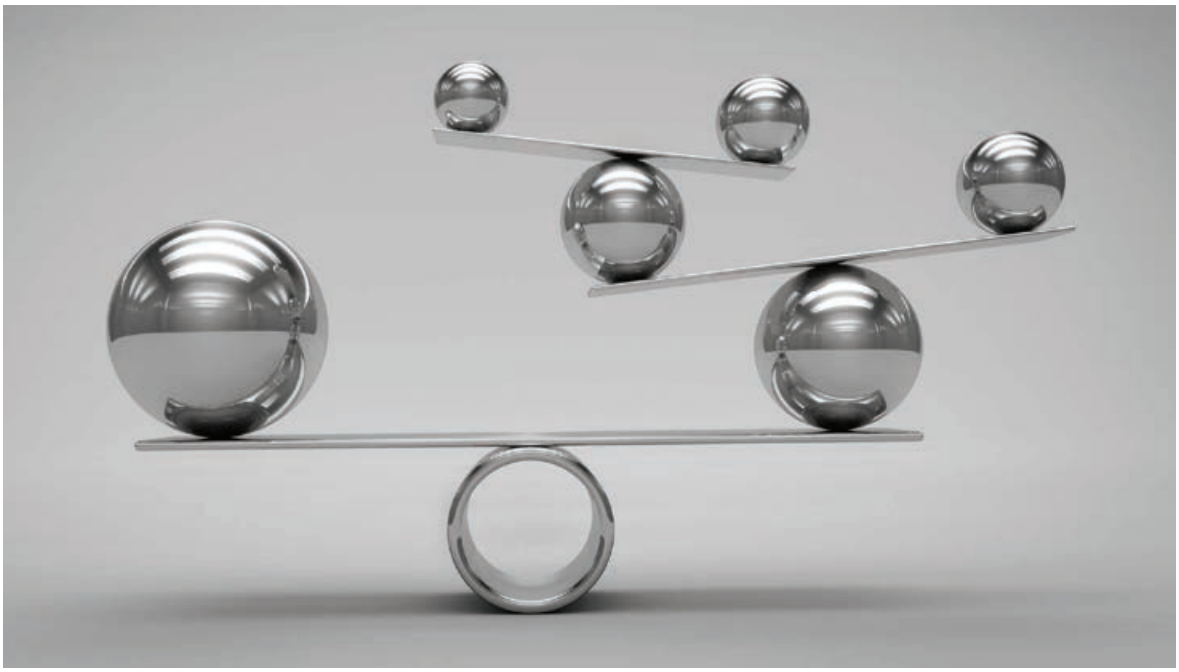
Organizacija koja posjeduje svijest o kulturi rizika otpornija je na vanjske uticaje i može se bolje adaptirati u poslovnom okruženju

Autorica:
Berina Kapa

Definicija kulture rizika

Iako se kultura rizika najčešće vezuje za poslovanje u okviru finansijskog sektora, u današnjem poslovnom okruženju ova kultura se nameće kao neodvojiv način poslovanja bilo koje kompanije ili organizacije.

Pojam *kultura rizika* je nomenklatura koja se koristi za određivanje načina na koji organizacija – bez obzira na njeno sjedište u svijetu, industriju ili strukturu



(javna, privatna, neprofitna organizacija), demonstira kroz aktivnosti i prihvaćeno ponašanje svoja zajednička uvjerenja, vrijednosti i razumijevanje o upravljanju rizicima tokom ostvarivanja svojih poslovnih ciljeva.[1] Kultura rizika nadasve dopunjuje organizacijsku kulturu.

Još jedna od općeprihvaćenih definicija kojima se opisuje kultura rizika jeste da ista predstavlja norme i ponašanja pojedinaca i grupa unutar organizacije koje određuju način na koji identificiraju, razumiju, diskutuju i djeluju na rizike s kojima se organizacija suočava.

> *Kultura rizika predstavlja norme i ponašanja pojedinaca i grupa unutar organizacije koje određuju način na koji identificiraju, razumiju, diskutuju i djeluju na rizike s kojima se organizacija suočava.*

Učinkovita kultura rizika

Stručnjaci i istraživanja pokazuju da je kultura rizika najučinkovitija kada je potpuno integrirana u poslovanje i neodvojiva od organizacijske kulture. Prvi korak ka utvrđivanju važnosti kulture rizika za organizaciju je početak razgovora na nivou menadžmenta o nekoliko ključnih tema. Prvo, organizacija bi trebala ispitati svoj *ton s vrha* i *u sredini*. Da bi se kultura rizika promijenila, vođstvo mora biti pokretač te promjene. Viši i srednji

[1] Reform in the financial services industry: Strengthening Practices for a More Stable System, Institute of international finance, 2009.

menadžment igraju ključne uloge jer pokreću *ton* i prenose ga na ponašanje svih uposlenika u organizaciji. Kako bi se promovirao snažan ton s vrha, poželjno je da menadžment na svim razinama prođe obuku o upravljanju rizicima, slijedi politiku upravljanja rizicima organizacije i analizira odluke sa aspekta zvaničnih *risk politika* organizacije.[2]

Nadalje, organizacije bi trebale osigurati i učinkovitu komunikaciju vezano za etike i rizik. Promjena kulture rizika zahtijeva stalne i dosljedne poruke uposlenicima da je upravljanje rizikom ključni dio njihovih svakodnevnih odgovornosti. Komunikacija bi trebala uključivati rad na kontinuiranom poboljšanju načina funkcioniranja poslovnih linija kako bi se osiguralo da su informacije o riziku podijeljene unutar svih sfera poslovanja.

Također, vrlo je važno da uposlenici razumiju da se pravila o riziku i usklađenosti primjenjuju na sve njih u svakodnevnom radu i pri ostvarenju poslovnih ciljeva. Takvo razumijevanje može osigurati da organizacija *učini pravu stvar* i temeljni je dio dobre prakse upravljanja rizikom. Kako bi se osiguralo ponašanje konzistentno sa rizikom unutar organizacije, i uposlenici trebaju proći obuku kako bi razumjeli kako se donose educirane odluke vezane uz rizik.

> *Vrlo je važno da uposlenici razumiju da se pravila o riziku i usklađenosti primjenjuju na sve njih u svakodnevnom radu i pri ostvarenju poslovnih ciljeva. Takvo razumijevanje može osigurati da organizacija učini pravu stvar i temeljni je dio dobre prakse upravljanja rizikom.*

Svijest o kulturi rizika

Stvaranje ili oblikovanje kulture koja je svjesnija rizika potencijalno je najveća vrijednost koja će pomoći organizaciji u izazovima neizvjesnih i promjenjivih okruženja. Ugrađivanje kulture rizika je način života. Kontinuirani proces obrazovanja i pripovijedanja o rizicima mijenja ne samo ponašanje nego i *mindset* koji pokreće razmišljanje, donošenje odluka i ponašanje zaposlenika. Bez kontinuiranog dijaloga koji omogućuje zaposlenicima da testiraju i usavrše svoje razumijevanje kako izgleda *dobra* kultura i kultura rizika kao njezina podskupina, postaje ustajala i ne uspijeva održati korak s dinamičnim okruženjem u kojem organizacije posluju.[3]

Organizacija koja posjeduje svijest o kulturi rizika otpornija je na vanjske uticaje i bolje se može adaptirati u poslovnom okruženju.

Međutim, izgradnja zdrave kulture rizika zahtjeva vrijeme jer to nije jednokratni projekat. Za ono što bi trebalo izgledati i osjetiti se kao konzistentna demonstracija snažne kulture rizika, potrebno je vrijeme da se iskomunicira i spusti sa višeg rukovodstva u sve sfere poslovanja. ■

[2] Importance of risk management mindset, Abstract of source article authored by ERM Initiative Faculty. URL: https://erm.ncsu.edu/library/article/risk-management-mindset (2019-06-25)
[3] CRO Forum, A Guide to Defining, Embedding and Managing Risk Culture. URL: https://www.thecroforum.org/2017/10/06/a-guide-to-defining-embedding-and-managing-risk-culture/(2019-06-25)

Novi izazovi

FUNKCIJA PRAĆENJA USKLAĐENOSTI (*COMPLIANCE*) I COVID-19

Istraživali smo o dobrim praksama koje mogu dati pozitivne efekte te doprinijeti tome da se funkcija praćenja usklađenosti adekvatno prilagodi novonastalim okolnostima pandemije COVID-19

Autor:
Nermin Ibradžić

Izmjene zakonodavnog okvira koje su nastupile novim zakonima o bankama oba entiteta i sa njima povezanim podzakonskim aktima, donijele su mnogo novina na području bankarskog poslovanja.

Jedna od njih je i definisanje nadležnosti, odgovornosti i prava funkcije praćenja usklađenosti kao jedne od kontrolnih funkcija. Pri tome valja naglasiti da pojam *novina* označava isključivo novinu u načinu na koji pozitivni propisi, primjenjivi u Bosni i Hercegovini, vide i definiraju funkciju praćenja usklađenosti kao kontrolnu funkciju. U pojedinim bankama na području BiH ova funkcija je zaživjela i implementirana je i prije stupanja na snagu novih zakona o bankama. Ovo je posebno slučaj u bankama koje su dijelovi međunarodnih bankarskih grupacija gdje je funkcija praćenja usklađenosti i ranije uspostavljena kao standard i obaveza na nivou bankarske grupe.

Lokalno bosanskohercegovačko zakonodavstvo je funkciju praćenja usklađenosti, popularni *Compliance*, osim zakonima o bankama obuhvatilo i drugim podzakonskim aktima koji se odnose na sistem internih kontrola, upravljanje rizicima, ICAAP/ILAAP, planove oporavka i dr.

Ravnajući se po lokalnim propisima, uloga funkcije praćenja usklađenosti se može sažeti u navedenom: praćenje regulatornih izmjena

> *Lokalno bosanskohercegovačko zakonodavstvo je funkciju praćenja usklađenosti , popularni **Compliance**, osim zakonima o bankama obuhvatilo i drugim podzakonskim aktima koji se odnose na sistem internih kontrola, upravljanje rizicima, ICAAP/ILAAP, planove oporavka i dr.*

i izmjena standarda i praksi koje mogu imati uticaja na poslovanje banke i procjena njihovih efekata, praćenje usklađenosti poslovanja sa navedenim propisima i standardima, identifikacija i procjena rizika koji mogu nastati kao posljedica neusklađenosti te savjetovanje (u pravilu) višeg rukovodstva i srednjeg nivoa upravljanja vezano za primjenu propisa i standarda.

U protekle 3 do 4 godine funkcija praćenja usklađenosti je implementirana u svim bankama, prošla je fazu početnih *dječijih bolesti* i nedostataka te je uspjela, manje ili više uspješno, da uspostavi linije razgraničenja u odnosu na druge funkcije unutar banke, prvenstveno u odnosu na funkciju interne revizije, pravnu službu i funkciju upravljanja rizicima.

Kako je i zakonodavni okvir za funkciju praćenja usklađenosti prilično široko postavljen, to je i njena organizacija u pojedinim bankama drugačije definirana. To je i očekivano jer svaka banka je ovu funkciju trebala da prilagodi svom načinu poslovanja, poziciji na tržištu, standardima grupacije kojoj pripada, apetitu za rizik i sl. Tako je funkcija praćenja usklađenosti u pojedinim institucijama uspostavljena u onom okviru koji propisuje Zakon o bankama, odnosno kao čisti regulatory compliance, negdje su funkciji praćenja usklađenosti pribrojane i druge aktivnosti vezane za etiku i etično poslovanje, integritet, interne ili eksterne prevare, fit & proper, koordinaciju internih kontrola, informacionu sigurnost te zaštitu ličnih podataka ili je funkcija praćenja usklađenosti inkorporirana u okviru drugih organizacionih jedinica. Da ne bude dilema, ništa od navedenog nije pogrešno sve dok ne predstavlja odstupanje od zakonom propisanog minimuma.

I upravo u momentu kada su se, nakon nekog vremena, stvari za funkciju praćenja usklađenosti poslovanja malo slegle, kada su uspostavljeni i kao praksa prihvaćeni programi rada i metodologije za praćenje usklađenosti i procjene rizika, kada su operativni planovi postali naša svakodnevnica, a planiranje edukacija za naše drage radne kolege aktivnost koja daje dodatnu vrijednost banci kao instituciji, desio se COVID-19.

I sve se promijenilo.

Promijenio se način na koji komuniciramo, promijenile su se mnoge paradigme, manje značajni rizici su postali vrlo značajni, promijenila se naša svakodnevnica, način na koji razmišljamo, način na koji gledamo druge i način na koji drugi vide nas. Gotovo preko noći smo postali individue bombardovane gomilom informacija koje treba da nas nauče šta je to *novo normalno*, od kojih mnoge i nisu baš od velike pomoći.

Bez obzira na navedeno, COVID-19 i *novo normalno* je imalo uticaja i na funkciju praćenja usklađenosti. Pitanje je u kojem obimu, da li treba da nešto mijenjamo i na koji način?

Nakon pet mjeseci (članak je rađen početkom avgusta 2020. godine) pretraga i čitanja stručnih članaka, raznih blogova, prezentacija i webinara, došao sam, a vjerujem da ste i vi, do zaključka da ne postoji univerzalan sistem, jasno propisan red koraka koje je potrebno napraviti da bismo se prilagodili i koji jamče uspjeh, ne postoji uputstvo ili *rule book* kojeg se treba pridržavati da bi funkcija praćenja usklađenosti bila zagarantovano uspješna u ovim izazovnim vremenima.

> *Ne postoji univerzalan sistem, jasno propisan red koraka koje je potrebno napraviti da bi se prilagodili i koji jamče uspjeh, ne postoji uputstvo ili rule book kojeg se treba pridržavati da bi funkcija praćenja usklađenosti bila zagarantovano uspješna u ovim izazovnim vremenima.*

Ipak, vrijeme provedeno na traganju za *pravim odgovorima* nije bilo potrošeno uzalud.

Rezultiralo je nekim dobrim praksama koje su provodive i koje mogu dati pozitivne efekte te doprinijeti tome da se funkcija praćenja usklađenosti adekvatno prilagodi novonastalim okolnostima.

Neke od praksi, koje se odnose na nove izazove za funkciju praćenja usklađenosti i koje bi mogle biti od pomoći, prezentirane su u nastavku teksta.

Biti svjestan uloge i ovlaštenja funkcije praćenja usklađenosti

Funkcija praćenja usklađenosti (dalje označena kao FPU) prema pozitivnim propisima, primjenjivim standardima i dobrim praksama, treba imati odgovarajuće alate za svoj rad. To podrazumijeva odgovarajuće ljudske kapacitete, tehničku podršku te pristup svim relevantnim podacima i dokumentaciji. Možda i značajniji od pobrojanih alata je položaj FPU unutar organizacije, ne u kontekstu sistematizacije radnih mjesta nego kako drugi unutar organizacije vide FPU.

Možda najznačajnija stvar u ovom segmetnu je *ton s vrha* (engl. *tone from the top*) i promoviranje uloge FPU od strane višeg rukovodstva. FPU koja ima adekvatnu podršku Uprave i Nadzornog odbora, FPU koja razumije svoju ulogu i čiju ulogu razumiju i druge organizacione jedinice, zasigurno može očekivati i bolje rezultate u svom radu.

Ukoliko to nije slučaj, upravo je kriza izazvana pandemijom COVID-19 možda i pravi momenat za jačanje i promociju uloge i značaja FPU, prije svega zbog izmjene regulative, standarda i praksi u koje FPU svakako mora biti uključen. Pri tome za promociju i jačanje uloge FPU nije potrebno puno. Edukacija u ovom dijelu treba da bude usmjerena na srednji i viši nivo menadžmenta, a praksa je pokazala da i kratke, ciljane edukacije kroz prezentaciju uloge i značaja FPU mogu dati izvrsne rezulatate, posebno ukoliko se bave aktuelnim temama. Promocija je moguća

i putem članaka na intranet stranicama, kroz e-edukacije, putem e-mail-a i sl.

Proaktivnost i informiranost

Proaktivnost je u opisu poslova FPU, tu nema dileme. Međutim, danas govorimo o novoj vrsti proaktivnosti. Ukoliko u obzir uzmemo samo regulatorne promjene, svjedoci smo da većina ima rok stupanja na snagu sljedeći dan od dana objave u službenim novinama ili čak i prije toga - od dana donošenja, bez obzira na dan objave.

Evidentno je da ovo ne ostavlja puno vremena za opširne i dugotrajne *Gap analize* jer je potrebno djelovati odmah, fokusirati se na bitno bez puno birokracije te jasno definirati prioritete.

Više nego ikad, izmjene propisa i standarda je potrebno pratiti na dnevnom nivou i iz različitih izvora. Dodatno, analize efekata je potrebno pojednostaviti i prilagoditi novonastalim okolnostima.
Jasno da takve analize efekata promjena nisu potpune bez informacija koje dobijamo od relevantih organizacionih jedinica kao učesnika procesa. Iz tog razloga je potrebno unaprijediti i komunikaciju sa drugim organizacionim jedinicama na način da je ista jednostavnija i brža. Pri tome je od ključnog značaja jasno iskomunicirati sa kolegama da su rokovi za prilagođavanje na nove zahtjeve izuzetno kratki pa se i sa njihove strane očekuju povratne informacije o izmjenama koje je potrebno učiniti u jako kratkom roku, pri čemu očekivani kvalitet informacija ne smije izostati.

Virtuelni kanali komunikacije i razne platforme za komunikaciju omogućavaju brži protok informacija. Relevantne organizacione jedinice mogu odrediti jednu osobu ili više njih, a koje bi bile nadležne za komunikaciju sa FPU, što bi u ovom slučaju bilo od velike pomoći.

> *Izvori informacija su u novim okolnostima veoma bitni. Novi rizici ili novi načini na koji se mogu realizirati ranije identificirani rizici za vrijeme pandemije COVID-19 zahtijevaju i da se preispitaju izvori informacija za potrebe procjene rizika.*

Sve navedeno zahtijeva dodatni napor od svih sudionika u procesu, ali radi se o vanrednim okolnostima u kojima svi zajedno moramo dati dodatni doprinos kako sutra ne bi svjedočili neželjenim situacijama.

Izvori informacija su u novim okolnostima veoma bitni. Novi rizici ili novi načini na koji se mogu realizirati ranije identificirani rizici za vrijeme pandemije COVID-19 zahtijevaju i da se preispitaju izvori informacija za potrebe procjene rizika. Na primjer, regulatorne izmjene vezane za posebne uslove povrata kredita zahtijevaju veći fokus na vrsti i broju prigovora klijenata, povećanje potrošnje po osnovu kartica preko platformi za elektronska plaćanja zahtijeva dodatne informacije sa područja kartičnih prevara (povećanje ili smanjenje broja prijavljenih prevara, vrsta prijavljenih prevara i sl.) i dodatne informacije sa područja sprečavanja pranja novca. Više nego ikad potrebna je bliska komunikacija

sa kolegama koje su prva linija odbrane.

Dakle, usljed novih okolnosti proces analize, procjene efekata i određivanja potrebnih mjera za prilagođavanje i postizanje potrebnog nivoa usklađenosti u okolnostima COVID-19 trebaju biti efikasniji i trajati kraće nego što smo to navikli. To nužno ne znači da treba smanjiti kriterije i standarde kojima se rukovodimo, nego je iste potrebno prilagoditi nastalim okolnostima. To posebno vrijedi za naknadnu provjeru da li su sve planirane aktivnosti i mjere provedene (tzv. *follow up*).

Budite fleksibilni, spremite se da mijenjate prioritete

Program i planovi rada su osnova funkcionisanja svake FPU. Dok program rada daje odgovor na pitanje zašto i kako nešto radimo, plan rada je usmjeren na aktivnosti koje planiramo poduzeti i vrijeme kada ih namjeravamo poduzeti.

U pravilu, svaka FPU kroz plan rada svoje aktivnosti planira dugoročno, utvrđuje i po potrebi usklađuje termine sa drugim organizacionim jedinicama uzimajući u obzir najznačajnije rizike prepoznate u tom momentu.

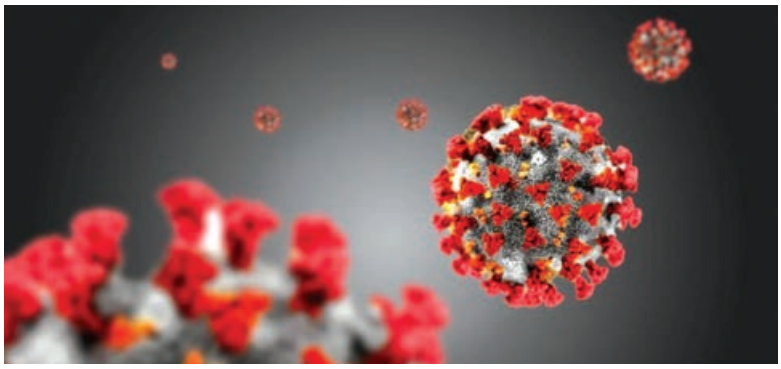
Svaka FPU je svjesna toga da izrada plana rada nije jednostavan proces jer treba zadovoljiti određene standarde i uvjeriti da će ključni ciljevi biti ostvareni. Također, podliježe usvajanju od strane višeg rukovodstva, što mu daje posebnu težinu.

Međutim, sa pandemijom COVID-19 i navedeni princip dugoročnog planiranja se promijenio. Okolnosti od FPU zahtijevaju veću fleksibilnost i mogućnost prilagođavanja. Naprimjer, da li je u ovom momentu bitnija planirana edukacija iz područja sukoba interesa ili *follow up* odluka i preporuka regulatora čija neadekvatna primjena može rezultirati finansijskim sankcijama i gubicima te značajnim reputacijskim rizikom? Imajući u vidu novonastalu situaciju i rizike, FPU bi trebala preispitati postojeći plan rada u smislu provjere da li je isti dovoljno fleksibilan i sveobuhvatan da bi bio primjenjiv i na nove okolnosti.

Unapređenje i prilagođavanje postojećih kontrola

Gotovo svaka značajnija izmjena u čijoj implementaciji učešće uzima FPU (izmjena regulative, novi proizvod ili proces i sl.) u konačnici rezultira i uspostavljanjem određenog kontrolnog okruženja, odnosno određenih unutarnjih kontrola, čiji je zadatak da u najvećoj mogućoj mjeri spriječi da se određeni identificirani rizik i ostvari.
U praksi, tipovi unutrašnjih kontrola su razni, od onih koje su implementirane u same procese, automatizova-

> *Tamo gdje je situacija sa COVID-19 dovela do izmjene određenih procesa, očekuje se i da se preispitaju postojeće kontrole ili uvedu nove. Čak i u slučajevima u kojima procesi nisu značajnije mijenjani, postojeće kontrole je korisno preispitati iz razloga što prijetnje i rizici prije COVID-19 nisu isti kao oni koji su generisani za vrijeme pandemije COVID-19.*



nih kontrola, *ručnih* kontrola, kontrola iste ili druge organizacione jedinice i sl.

Tamo gdje je situacija sa COVID-19 dovela do izmjene određenih procesa, očekuje se i da se preispitaju postojeće kontrole ili uvedu nove. Čak i u slučajevima u kojima procesi nisu značajnije mijenjani, postojeće kontrole je korisno preispitati iz razloga što prijetnje i rizici prije COVID-19 nisu isti kao oni koji su generisani za vrijeme pandemije COVID-19.

Upravo tu leže novi izazovi za FPU koja treba da insistira ne samo na adekvatnim unutrašnjim kontrolama za nove ili izmijenjene procese, nego i na preispitivanju kontrola u postojećim procesima, a na koje COVID-19 može imati uticaja (npr. kartična plaćanja putem raznih elektronskih platformi, korištenje e-bankarstva i sl.). Za navedenu aktivnost FPU ima dostatnu *polugu* jer je jedan od zadataka kontrolnih funkcija, prema pozitivnim propisima, i ocjena adekvatnosti i efikasnosti sistema unutrašnjih kontrola.

Izvještavanje

Izvještavanje višeg rukovodstva je jedan od osnovnih zadataka FPU. Novi izazovi, prilagođavanje planova rada, eventualne izmjene metodologije rada te novi rizici i prijetnje mogu od FPU zahtijevati i izmjenu načina izvještavanja, naravno poštujući strukturu izvještaja propisanu od strane regulatora. Korisno je fokusirati se na bitno, bez suvišnih detalja, rizici i efekti izmjena te poduzete aktivnosti i mjere bi trebale biti jasno prezentirane.

Nove prilike

Situacija sa COVID-19 je pogodila cijeli svijet i sve sektore poslovanja, to je činjenica koju niko neće osporiti. U domenu FPU situaciju možemo posmatrati na dva načina. Jedan je da energiju usmjerimo na to kako je relevantnih izmjena sve više, kako ih je teško pratiti, kako nam se čini da je situacija za FPU sve teža i teža.

Drugi je da situaciju prihvatimo kao novu priliku, da promoviramo FPU i njene vrijednosti, da se prilagodimo novim trendovima i okolnostima, da ostalim kolegama pokažemo kako je to moguće i da unaprijedimo postojeće ili razvijemo nove metodologije rada.

Prošlost je pokazala da se kod svake krize FPU nadograđivala, unapređivala i dobijala sve značajniju ulogu u svakom segmentu u kojem je djelovala.

Nema razloga da se u ovim vremenima razmišlja na drugačiji način, a do svakog je pojedinca da li će takvu priliku i iskoristiti. ■

Preciznim definisanjem obaveza ugovornih strana gradimo povjerenje između banaka i klijenata

ELEMENTI UGOVORA O KREDITU

Koji elementi ugovora o kreditu moraju biti navedeni prilikom zaključenja ugovora između banke i fizičkog ili banke i pravnog lica, kojim zakonskim i podzakonskim aktima su propisani obavezni elementi ugovora o kreditu te koje sankcije su predviđene od strane nadležnih organa u slučaju nedostatka elemenata ugovora

Autor:
Muris Bešić

Kredit predstavlja imovinsko-pravni odnos između povjerioca i dužnika u kome povjerilac novac ili druge potrošne stvari daje dužniku na određeno vrijeme i uz određene uslove[1]. S obzirom na to da su predmet analize kroz ovaj rad elementi ugovora o kreditu koje banke zaključuju sa svojim klijentima u okviru svoje osnovne djelatnosti, dalji tekst se ne odnosi na kredite koji se odobravaju u drugim potrošnim stvarima.

Kada se govori o elementima ugovora o kreditu, prije svega treba imati na umu da ugovor o kreditu, kao i ostali obligaciono-pravni ugovori, pored bitnih elemenata mogu sadržavati i sporedne elemente. Sporednim elementima se detaljnije uređuju prava i obaveze ugovornih strana u konkretnom pravnom poslu. Imajuću vidu kompleksnost teme koja je predmet ovog izlaganja, ali i značaj iste, u okviru ovog rada pažnja će biti usmjerena na elemente ugovora o kreditu koji obavezno moraju biti navedeni prilikom zaključenja ugovora o kreditu između banke i fizičkog ili banke i pravnog lica - obavezni elementi. Naime, usljed specifičnih zahtjeva postavljenih pozitivno-pravnim propisima, ugovori o kreditu zaključeni sa fizičkim ili pravnim licem obavezno ne sadržavaju identične elemente, iako je, u suštini, u najvećem broju slučajeva riječ o skoro identičnim pravnim poslovima.

[1] Pravna enciklopedija, knjiga 1; Izdavač „Savremena administracija Beograd“ 1983, strana 670.

Kao pravni izvori elemenata ugovora o kreditu koji se obavezno navode u okviru ugovora o kreditu, u pravnom sistemu BiH postoji više pravno-relevantnih izvora koje donose različiti organi u okviru svojih nadležnosti. Tako pored zakona imamo niz podzakonskih akata donesenih u formi odluka ili instrukcija shodno kojima su propisani obavezni elementi ugovora o kreditu. Zbog obimnosti materije, u okviru ovog rada će biti obrađeni elementi koji proizilaze iz zakona, a elementi koji proizilaze iz podzakonskih akata mogli bi biti tema posebnog rada. Ipak, zbog specifične veze jednog podzakonskog akta sa zakonom i posebnih okolnosti u kojima je isti donesen, bit će prikazani elementi koji proizilaze iz tog podzakonskog akta.

Vrlo su bitne i posljedice nedostataka pojedinih elemenata ugovora u okviru istih. Posljedice se mogu ogledati, osim posljedica predviđenih za obligaciono-pravne poslove, i u posljedicama koje se odnose na sankcije od strane nadležnih organa zbog nedostatka nekih elemenata ugovora.

Pravni izvori
Zakon o obligacionim odnosima

Primarni pravni izvor kojima su propisani obavezni elementi ugovora o kreditu je svakako *Zakon o obligacionim odnosima FBiH/RS*[2] *(u daljem tekstu: ZOO). S obzirom na to da je ZOO najznačajniji izvor prava kada je riječ o ugovorima o kreditu, naglasit ću da su odredbe o ugovoru o kreditu propisane odredbama 1065-1068 navedenog propisa. Elementi ugovora o kreditu se bliže propisuju članom 1066. stav 2. ZOO shodno kojem je propisano: Ugovorom o kreditu utvrđuju se iznos, kao i uslovi davanja, korišćenja i vraćanja kredita*. S obzirom na to da se navedenim članom propisuju elementi ugovora o kreditu, opravdano se postavlja pitanje da li su svi navedeni elementi obavezni elementi navedenog ugovora, imajući u vidu da sam zakon ne implicira imperativno dejstvo cjelokupne navedene odredbe kao i imajući u vidu

> *Prema stavu 2 člana 1066. ZOO, elemente ugovora o kreditu čine:*
> ***iznos kredita*** *(novčani iznos koji korisniku kredita banka odobrava i stavlja na raspolaganje),*
> ***uslovi davanja kredita*** *(uslovi pod kojima banka odobrava kredit fizičkom ili pravnom licu),*
> ***uslovi korištenja kredita*** *(namjenski i nenamjenski krediti) te uslovi vraćanja kredita (od precizne formulacije uslova vraćanja kredita zavisi jasnost ispunjenja obaveze dužnika).*

prirodu samog kreditnog posla u odnosu na radnje koje prethode zaključenju ugovora o kreditu.

Ukoliko sumiramo sadržaj stava 2 člana 1066. ZOO, elemente ugovora o kreditu čine: iznos kredita, uslovi davanja kredita, uslovi korištenja kredita te uslovi vraćanja kredita. Kako bi se iznio zaključak

[2] Zakon o obligacionim odnosima je objavljen u okviru SFRJ 1978. godine, Službeni list 28/78, u pravni sistem Bosne i Hercegovine je preuzet 1992. godine, Službeni list RBiH 2/92, 13/93, 13/94. U okviru RS relevantna službena glasila koja se tiču ovog zakona su Službeni list RS broj: 17/93 i 3/96.

o obaveznom navođenju određenog elementa u pisanu formu ugovora[3], potrebno je pojedinačno razmotriti svaki od navedenih elemenata.

Iznos kredita predstavlja novčani iznos koji korisniku kredita banka odobrava i stavlja na raspolaganje. Uzimajući u obzir razloge zaključenja ugovora o kreditu, iznos kredita svakako da predstavlja bitan element ugovora o kreditu[4]. Kada se govori o iznosu, potrebno je napomenuti da iznos ne mora biti striktno naveden, sam iznos je moguće utvrditi i na drugi način, ali ukoliko iznos nije tačno određen, mora biti barem odrediv. U slučajevima u kojima iznos kredita nije precizno određen, kao adekvatan način ugovaranja iznosa kredita može se primijeniti ugovaranje maksimalnog iznosa novčanih sredstava koja korisnik kredita može koristiti.

Drugi element, u skladu sa članom 1066. stav 2, predstavljaju **uslovi davanja kredita**. Uslovi davanja kredita predstavljaju uslove pod kojima banka odobrava kredit fizičkom ili pravnom licu i isti se ispituju u fazi koja prethodi zaključenju ugovora o kreditu[5]. S obzirom na to da se radnje koje se odnose na odobravanje kredita u suštini odvijaju prije zaključenja ugovora o kreditu, a nisu od praktične važnosti u izvršenju prava i obaveza ugovornih strana u pogledu ugovora o kreditu, svakako da se može zauzeti stav da uslovi odobrenja kredita nisu bitni elementi ugovora o kreditu koji bi morao obavezno biti naveden u ugovoru o kreditu[6].

Treći element čine **uslovi korištenja kredita**. Uslovi korištenja kredita predstavljaju uslove koje ugovorne strane saglasno ugovoraju. Ukoliko je kredit odobren u tačno određenu svhu, korisnik kredita može odobrena sredstva koristiti jedino u svrhu u koju je kredit odobren, a ne u druge svrhe. Krediti kod kojih je određena namjena nazivaju se *namjenskim kreditima*. S druge strane, postoje krediti kod kojih namjena korištenja odobrenog novčanog iznosa nije predmet preciziranja između ugovornih strana te korisnik kredita može odobreni novčani kredit koristiti prema vlastitoj odluci na koju banka kao druga ugovorna strana nema uticaj. Ove vrste kredita nazivaju se *nenamjeskim kreditima*. Kroz sagledavanje podjele kredita na namjenske i nemamjenske, logično se nameće zaključak da je kod namjenskih kredita uslov korištenje kredita bitni element ugovora i mora biti naveden. Kod nenamjenskih kredita vrlo je jasno da jedan takav element nema svoju svrhu i stoga ne predstavlja bitni element ugovora o kreditu.

---

[3] Članom 1066. stav 1. ZOO propisano je da je ugovor o kreditu koji banka zaključuje u okviru svog poslovanja strogo formalni pravni posao, što pretpostavlja da je preduslov za njegov nastanak i punovažnost pisana forma. Također, svaka izmjena ugovora o kreditu mora biti sačinjena u istoj formi kako bi se osigurala pravna valjnost ugovora, a u skladu sa članom 67. stav 2. ZOO. Izuzeci u pogledu izmjene ugovora predviđeni članom 67. stav 3. i 4. se, prema mišljenju autora, ne mogu primjeniti na ugovor o kreditu.

[4] Komentar Zakona o obligacionim odnosima II knjiga drugo izdanje; Redaktori: Prof.dr. Borislav T. Blagojević i prof.dr. Vrleta Krulj; Izdavač „Savremena administracija Beograd" 1983. godine; str. 2165. komentar na stav 2. člana 1066.

[5] Komentar Zakona o obligacionim odnosima II knjiga drugo izdanje; Redaktori: Prof.dr. Borislav T. Blagojević i prof.dr. Vrleta Krulj; Izdavač „Savremena administracija Beograd" 1983. godine; str. 2165. komentar na stav 2. člana 1066.

[6] Kao potvrda navedenog stava može se navesti podzakonski akt koji je objavila *Agencija za bankrastvo FBIH* pod nazivom *Odluka o uslovima za procjenu i dokumentovanje kreditne sposobnosti*; Službene novine FBiH broj: 23/14, shodno kojem su procjene kreditne sposobnosti od strane tijela koje kontroliše rad banaka propisane kao obavezne.

Možemo zaključiti da uslovi kredita mogu, a i ne moraju, biti obavezni element ugovora o kreditu, u zavisnosti da li se kredit koristi u određenu svrhu ili je korištenje kredita stvar slobodnog izbora korisnika kredita.

Kao posljednji element, koji je propisan članom 1066. stav 2. ZOO, navode se **uslovi vraćanja kredita**. Uslovi vraćanja kredita predstavljaju konstituvni element ugovora o kreditu i naravno da se smatraju bitnim elementom ugovora koji mora biti naveden u ugovoru o kreditu. Od precizne formulacije uslova vraćanja kredita zavisi jasnost ispunjenja obaveze dužnika te, ako navedeni uslovi nisu jasno definisani, u praksi može doći do raznih nejasnih situacija u kojima obje ugovorne strane tumačeći odredbe ugovora, pa i bez namjere zloupotrebe, mogu imati različita tumačenja ugovornih odredbi što u konačnici može dovesti do spornih situacija. Stoga, uslovi vraćanja kredita su, bez sumnje, veoma bitan element ugovora o kreditu.

Zakon o zaštiti korisnika finansijskih usluga FBiH i Zakon o bankama RS

U razmatranju pravnih izvora nezaobilazni propisi u pravnom sistemu BiH, koji moraju biti uzeti u obzir, svakako su *Zakon o zaštiti korisnika finansijskih usluga FBiH*[7] *(u daljem tekstu ZZKFUFBiH) kao i Zakon o Bankama RS*[8] *(u daljem tekstu ZOBRS). ZZKFUFBIH predstavlja zakon koji je usvojen kao direktna posljedica usklađivanja zakonodavstva FBiH sa propisima Evropske unije u oblasti zaštite potrošača. Skoro identična rješenja sa istim ciljem u pravni sistem RS-a uvedena su kroz ZOBRS. Imajući u vidu da sam zakonodavac kroz ove propise ima namjeru zaštititi potrošače kao slabije ugovorne strane, o bitnosti obaveze navođenja ovog elemenata u sam ugovor ukazuje član 7. stav 3. ZZKFUFBiH shodno kojem se propisuje da se korisnik usluge ne može odreći prava koja su mu garantovana zakonom. Korisnik kredita ne može u dogovoru sa bankom izabrati da neke od elemenata ugovora navede u ugovoru, a da druge izostavi. Svi elementi propisani zakonom moraju biti navedeni u ugovoru o kreditu. Pored navedene odredbe, odredbom člana 8. stav 5. ZZKFUFBiH propisuje se da ugovori ne mogu sadržavati upućujuće norme na poslovnu politiku ukoliko su u pitanju obavezni elementi ugovora propisani ovim zakonom. Analogno navedenoj odredbi, članom 141. stav 6. ZOBRS*

> *Prema članu 7. stav 3 ZZKFUFBiH, korisnik usluge ne može se odreći prava koja su mu garantovana zakonom. Korisnik kredita ne može u dogovoru sa bankom izabrati da neke od elemenata ugovora navede u ugovoru, a da druge izostavi. Svi elementi propisani zakonom moraju biti navedeni u ugovoru o kreditu.*
>
> *Kroz ove propise zakonodavac štititi potrošače kao slabije ugovorne strane.*

[7] Zakon o zaštiti korisnika finansijskih usluga Federacije Bosne i Hercegovine je objavljen i stupio na snagu 2014. godine, Službene novine FBiH broj: 31/14.
[8] Zakon o bankama Republike Srpske. Službene novine RS broj: 4/17.

propisuje identičnu obavezu. Predmetne odredbe bez sumnje ukazuju na impretivni karakter odredbi navedenih propisa čime se u cilju zaštite korisnika usluga[9] *u cijelosti derogira načelo slobode uređivanja obligacionih odnosa. Obavezne elemente ugovora o kreditu ZZKFUFBiH i ZOBRS ne propisuju na identičan način. Kod zakona koji se primjenjuje u FBIH, svi obavezni elementi ugovora o kreditu navode u u okviru iste odredbe, član 17. ZZKFUFBiH, a kod zakona u primjeni u okviru RS-a, obavezne elemente ugovora o kreditu možemo podijeliti na dvije grupe. U prvu grupu bi spadali elemeti koji se, pored ugovora o kreditu, odnose i na druge ugovore koji su predviđeni navedenim propisima, a to su: Ugovor o otvaranju i vođenju tekućeg računa, Ugovor o oročenom novčanom depozitu* i drugi ugovori, član 142. ZOBRS (opšti obavezni elementi). U drugu grupu obaveznih elemenata spadaju elementi koji se isključivo odnose na ugovor kreditu, a propisani su članom 148. ZOBRS (posebni obavezni elementi).

Slijedom naprijed iznesenog, u ***obavezne elemente ugovora o kreditu u skladu sa ZZKFUFBiH spadaju***: vrsta kredita, period na koji se kredit odobrava; poslovno ime, ime i adresa ugovornih strana; iznos kredita i uslove povlačenja sredstava; kod kredita indeksiranih u stranoj valuti - valutu u kojoj banka indeksira kredit, tip kursa valute koji se primjenjuje pri odobravanju i otplati kredita (kupovni ili prodajni kurs Centralne banke Bosne i Hercegovine ili službeni srednji kurs, ili kupovni ili prodajni kurs banke) kao i datum obračuna, visina nominalne kamatne stope uz određenje da li je fiksna ili promjenljiva, a ako je promjenljiva, elementi na osnovu kojih se određuje (referentna kamatna stopa, indeks potrošačkih cijena i dr.), njihova visina u vrijeme zaključenja ugovora, periodi u kojima će se mijenjati, kao i fiksni element ako je ugovoren; efektivna kamatna stopa i ukupan iznos koji korisnik treba platiti, a izračunat je na dan zaključenja ugovora; plan otplate kredita i pravo korisnika da tokom trajanja ugovora, u slučaju promjene plana otplate, odnosno jedanput godišnje, ako nije došlo do ove promjene, dobije besplatno plan otplate, a ako se kamata i troškovi otplaćuju bez istovremene otplate glavnice, plan otplate kredita treba sadržiti samo rokove i uvjete otplate kamate i troškova; metod koji se primjenjuje kod obračuna kamate; stopa zatezne kamate u trenutku zaključenja ugovora koja se primjenjuje u slučaju kašnjenja u izmirenju obaveza i pravila za njeno prilagođavanje te sve druge naknade koje se plaćaju u slučaju neispunjenja obaveza; upozorenje o posljedicama u slučaju neizmirivanja obaveza, uslovi, postupak i posljedice otkaza, odnosno raskida ugovora o kreditu u skladu sa zakonom kojim se uređuju obligacioni odnosi, kao i obavještenje o uvjetima i načinu ustupanja potraživanja u slučaju neizmirenja obaveza; vrsta i visina svih naknada koje padaju na teret korisnika kredita, uz određenje da li su fiksne ili promjenljive, a ako su promjenljive, rokovi u kojima će ih banka mijenjati, kao i vrsta

[9] Korisnikom finansijskih/bankarskih usluga se smatraju lica definisana članom 2. stav 1. tačka 10. ZZKFUFBiH, odnosno lica definisana članom 116. stav. 2. ZOBRS.

i visina drugih troškova; vrste sredstava osiguranja, mogućnost za njihovu zamjenu tokom perioda otplate kredita, kao i uvjeti aktiviranja tih sredstava u slučaju neizmirivanja obaveza; uvjete i način prijevremene otplate kredita i visina naknade u vezi s tim; pravo korisnika na odustanak od ugovora, uvjeti i način odustanka; pravo na prigovor i mogućnost pokretanja postupka posredovanja radi vansudskog rješavanja spornog odnosa; prema potrebi, odredba o obavezi korištenja i plaćanja troškova notarskih usluga; ukupni troškovi kredita za korisnika kredita; ukupan iznos koji korisnik kredita treba platiti i plan otplate koji se smatra sastavnim dijelom ugovora.

Iako se i u okviru ZOBRS kao bitni elementi ugovora o kreditu u najvećem dijelu navode isti elementi kao i u ZZKFUFBiH, radi sistematičnijeg pregleda u nastavku ću dati prikaz svih obaveznih elemenata u skladu sa ZOBRS. U skladu sa podjelom obaveznih elemanata ugovora u okviru ZOBRS, ***u opšte obavezne elemente ugovora o kreditu u skladu sa ZOBRS spadaju***: vrsta usluge; naziv, ime i adresa ugovornih strana; iznos, oznaka valute i uslovi korišćenja usluge, period na koji se usluga ugovara; visina nominalne kamatne stope uz određenje da li je fiksna ili promjenljiva, a ako je promjenljiva – elemente na osnovu kojih se određuje (referentna kamatna stopa, indeks potrošačkih cijena i drugo), njihovu visinu u vrijeme zaključenja ugovora, periode u kojima će se mijenjati, kao i fiksni element ako je ugovoren; efektivna kamatna stopa i ukupan iznos koji korisnik treba da plati, odnosno koji treba da mu se isplati, izračunat na dan zaključenja ugovora; metod koji se primjenjuje prilikom obračuna kamatne stope; troškovi održavanja jednog ili više računa na kojima se evidentiraju transakcije uplata i povlačenja sredstava, izuzev ako to otvaranje računa nije samo ponuđena opcija, zajedno sa troškovima korišćenja određenog sredstva otplate, kako za transakcije plaćanja, tako i za povlačenja sredstava, te sve druge naknade i troškovi koji proizlaze iz ugovora uz određenje da li su fiksni ili promjenljivi i uslovi pod kojima se mogu mijenjati; stopa zatezne kamate koja se primjenjuje u slučaju kašnjenja u izmirenju obaveza i pravila za njeno prilagođavanje, te sve druge naknade koje se plaćaju u slučaju neispunjenja obaveza; upozorenje u vezi sa posljedicama propuštanja izmirenja obaveza; postupak zaštite prava korisnika, korišćenje vansudskog prigovora i adresa institucije kojoj se podnosi. U posebne obavezne elemente ugovora o kreditu spadaju: kod kredita indeksiranih u stranoj valuti – valuta u kojoj banka indeksira kredit, tip kursa valute koji se primjenjuje pri odobravanju i otplati kredita (kupovni ili prodajni kurs Centralne banke Bosne i Hercegovine, ili zvanični srednji kurs, ili kupovni ili prodajni kurs banke), kao i datum obračuna; pravo korisnika da od banke na ugovoreni način, a najmanje jednom godišnje, bez naknade dobije u pisanoj formi izvod o stanju njegovog kreditnog zaduženja, uključujući podatke o iznosu otplaćene glavnice i kamate, kao i iznosu preostalog duga; ukupne troškove kredita; ukupan iznos koji korisnik treba

da plati; ako se primjenjuje, odredbu o obavezi korišćenja i plaćanja troškova notarskih usluga; instrumente obezbjeđenja ispunjenja obaveza sa informacijom o redoslijedu i načinu izmirenja obaveza iz instrumenata obezbjeđenja; pravo korisnika na odustajanje od ugovora, uslove i način ostvarenja tog prava; uslove i način prijevremene otplate kredita i visinu naknade banke po ovom osnovu; ukupni troškovi kredita za korisnika kredita; ukupan iznos koji korisnik treba da plati i plan otplate kredita.

Na kraju izlaganja o obaveznim elementima ugovora koji su naprijed izloženi u skladu sa ZZKFUFBiH i ZOBRS, treba podsjetiti da se isti odnose samo na određene ugovore o kreditu koji su zaključeni sa određenom kategorijom lica[10]. Dalji kriterij koji se primjenju u cilju utvrđivanja primjene obaveznih elemenata ugovora o kreditu je da se ne odnose na ugovore o kreditu propisane članom 3. ZZKFUFBIH[11] kao i na ugovore o kreditu koji su navedeni u članu 156. ZOBRS[12].

Iako je u bankarskoj praksi prisutan stav da se naprijed navedeni propisi primjenjuju na sva fizička lica, a ne primjenjuju na pravna lica, takav stav je djelimično tačan. Takav stav tačan je u odnosu na pravna lica, dok je, kada govorimo o ugovorima koji se zaključuju sa fizičkim licima, potrebno voditi računa o naprijed opisanim kriterijima primjene, odnosno neprimjene ZZKFUFBiH i ZOBRS.

Zakon o zaštiti jemaca/žiranata FBiH

Iako je donošenje navedenog propisa kao i početak njegove primjene bilo propraćeno mnogim nejasnoćama usljed kojih su u praksi u određenom vremenskom periodu bile nejasne obaveze banaka, nesumnjivo i *Zakon o zaštiti jemaca FBiH*[13] *(u daljem tekstu: ZZJFBiH) po određenim uslovima predstavlja nezaobilazan pravni izvor kada su u pitanju obavezni elementi ugovora. Obaveza primjene ovog propisa se odnosi na ugovore o kreditu zaključene i sa fizičkim i pravnim licima ukoliko je njihova obaveze osigurana jemstvom fizičkog ili pravnog lica. Obavezni elementi ugovora o kreditu su navedeni u članu 7. ZZJFBiH, ali imajući u vidu da se uglavnom*

[10] Ibidem, bilješka broj: 9.

[11] Ugovori o kreditu na koje se ZZKFUFBiH ne odnosi su: ugovori o kreditu u iznosu manjem od 400,00 KM i većem od 150.000,00 KM; ugovori o kreditu kod kojih ne postoji obaveza plaćanja bilo kakvih troškova i ugovori kod kojih se kredit mora otplatiti u roku tri mjeseca; ugovori o kreditu koji su osigurani založnim pravom na pokretnosti, ako je odgovornost korisnika strogo ograničena na vrijednost založne stvari; finansijskim pogodbama s trajnim izvršenjem kojima se trgovac obavezuje da korisniku isporučuje određenu vrstu robe, odnosno pruža određenu uslugu u dužem periodu, a korisnik se obavezuje da za to plaća cijenu u ratama za vrijeme trajanja isporuke robe, odnosno pružanja usluge; ugovori o kreditu kod kojih je potraživanje osigurano hipotekom na nekretnini ili drugim uporedivim sredstvom osiguranja na nekretnini, odnosno drugim pravom na nekretnini, osim na ugovore o kreditu čija je svrha renoviranje postojećih zgrada ili povećanje njihove vrijednosti; ugovor o kreditu kada je kredit namijenjen za sticanje ili zadržavanje prava vlasništva na postojećoj ili planiranoj nekretnini/zgradi; ugovori o kreditu koji se odnose na kredite koji se odobravaju užoj javnosti prema zakonskim odredbama radi općeg interesa i po nižim kamatnim stopama od onih koje prevladavaju na tržištu ili oslobođene plaćanja kamata ili prema nekim drugim uvjetima koji su povoljniji za korisnika od onih koji prevladavaju na tržištu, te po kamatnim stopama koje nisu više od onih koje prevladavaju na tržištu.

[12] Ugovori o kreditu na koje se ZOBRS ne odnosi su: ugovori o kreditu u iznosu manjem od 400 KM i većem od 150.000 KM; ugovori o kreditu kod kojih ne postoji obaveza plaćanja bilo kakvih troškova i ugovori kod kojih se kredit obavezno otplaćuje u roku od tri mjeseca, uz plaćanje samo zanemarljivih ukupnih troškova kredita; ugovori o kreditu koji su obezbijeđeni založnim pravom na pokretnim stvarima, ako je odgovornost korisnika strogo ograničena na vrijednost založene stvari.

[13] Zakon o zaštiti jemaca je objavljen u Službenim novinama FBiH broj: 100/13.

ponavljaju elementi propisani ZZKFUFBiH i ZOBRS kao i da je usljed ograničenja propisanih ZZJFBiH[14] *jamstvo u praksi izgubilo značaj i primjenu kakvu je imalo ranije. Stoga ću u ovom dijelu napomenuti samo elemente koji su propisani predmetnim zakonom. Slijedeći navedeno, obavezni elementi ugovora o kreditu koji se isključivo crpe iz ZZJFBiH su: odredba prema kojoj je povjerilac, putem instrumenta osiguranja kredita predviđenog zakonom, osigurao naplatu svojih potraživanja od glavnog dužnika; odredba prema kojoj je povjerilac nadležan i dužan da naplatu kreditnih sredstava, u slučaju kašnjenja, izvrši koristeći sve instrumente osiguranja kredita glavnog dužnika; odredba prema kojoj povjerilac u vezi s odredbom iz prethodnog stava, prije utuženja žiranta, treba iscrpiti sva pravna sredstva u namirenju svojih potraživanja prema glavnom dužniku; odredba prema kojoj žirant neće vraćati kredit prije nego što povjerilac poduzme sve radnje iz prethodnog stava ovog člana, a ukoliko ipak dođe do otplate kredita žiranta, visina rate ne smije prelaziti trećinu redovnih primanja svakog žiranta pojedinačno i svih žiranta solidarno.*[15]

S obzirom na nejasnoće u primjeni ovog propisa, Agencija za bankarstvo FBiH (u daljem tekstu: FBA) je u okviru svojih ovlaštenja, a radi adekvatne primjene ZZJFBiH, dana 02.07.2015. godine, donijela *Instrukcije za postupanja u primjeni ZZKFUFBiH i ZZJFBiH, broj: 04-2-2710/15* u skladu sa kojom su propisani dodatni elementi koji se moraju definisati u ugovorima o kreditu. U skladu sa navedenom instrukcijom propisano je da u okviru ugovora o kreditu obavezno se: definiše status izdavaoca mjenica (žirant/sudužnik) u osnovnom ugovoru, te osigurava njihov potpis na ugovoru u cilju upoznavanja izdavaoca mjenica sa pravima i obavezama iz ugovora, kao i osnova izdate mjenice; upoznaje sudužnik sa njegovim pravima i obavezama u slučaju pristanka na sudužništvo (solidarna odgovornost, mogućnost prava na regres), s obzirom na to da je sudužnik lice koje je odgovorno za izmirenje svih povjeriočevih potraživanja jednako kao i glavni dužnik. Predmetnom instrukijom se u suštini kao obavezni element predviđa upoznavanje jemaca/sudužnika sa njihovim pravima koja imaju u skladu sa zakonom.

Pravne posljedice nedostatka obaveznih elemenata u ugovorima o kreditu

Kada govorimo o pravnim posljedicama, ukoliko ugovori o kreditu ne sadržavaju određene elemente predviđene naprijed navedenim propisima, isti zavise od propisa iz kojeg obavezni elementi potiču. Prije svega, ukoliko se radi o nekom nedostaku koji je predviđen odredbama ZOO, pravna posljedica nedostatka bi bila nepostojanje ugovora o kreditu jer nisu ispunjeni uslovi za njegovu valjanost. Nadalje, u zavisnosti koji od bitnih elemenata nedostaje, mogli bismo govoriti o prividnom ugovoru,[16] same

[14] Član 15. i 17. ZZJFBiH.
[15] Predmetni elementi ugovora o kreditu predviđeni su članom 7. stav 3. tačke 12.13.14.15. ZZJFBiH.
[16] Član 66. ZOO.

posljedice zaključenja takvog ugovora mogu biti ništavost ugovora ili postojanje drugog ugovora čije postojanje ugovorne strane nisu željele ili, u konačnici, postojanje takvog ugovora može da ne odgovara nekoj od ugovornih strana. Usljed nedostatka nekog elementa, pa i u slučajevima da ugovorne strane ne ističu prigovore koji se odnose na valjanost ugovora, nedostaci pojedinih elemenata bi svakako u praksi mogli izazvati mnoge nesporazume u pogledu izvršenja obaveza između ugovornih strana.

U odnosu na nedostake elemenata koji su predviđeni ZZKFUFBiH, ZOBRS i ZZJFBiH, potrebno je naglasiti da se i na njihove nedostatke mogu odnositi posljedice koje su predviđene za nedostatke iz ZOO. Pored navedenih posljedica, nedostatak bitnih elementa iz ovih propisa može predstavljati i prekršaj banke. Za prekršaje ove vrste predviđene su sankcije u vidu novčanih kazni. Prema ZZKFUFBiH novčane kazne mogu biti izrečene u iznosu od 5.000,00KM do 15.000,00KM. Za počinjeni prekršaj ZOBRS

"Nedostatak bitnih elementa iz propisa navedenih u ovom tekstu može predstavljati i prekršaj banke. Za prekršaje ove vrste predviđene su sankcije u vidu novčanih kazni.

ZZKFUFBiH za počinjeni prekršaj predviđa novčane kazne u iznosu od 5.000,00KM do 15.000,00KM.

ZOBRS predviđa i najveće novčane kazne koje se kreću u rasponu od 10.000,00KM do 50.000,00KM.

ZZJFBiH predviđa novčane kazne zbog nedostataka bitnih elemenata u rasponu od 10.000,00KM do 15.000,00KM."

predviđa i najveće novčane kazne koje se kreću u rasponu od 10.000,00KM do 50.000,00KM. U skladu sa ZZJFBiH novčane kazne zbog nedostataka bitnih elemenata se kreću u rasponu od 10.000,00KM do 15.000,00KM.

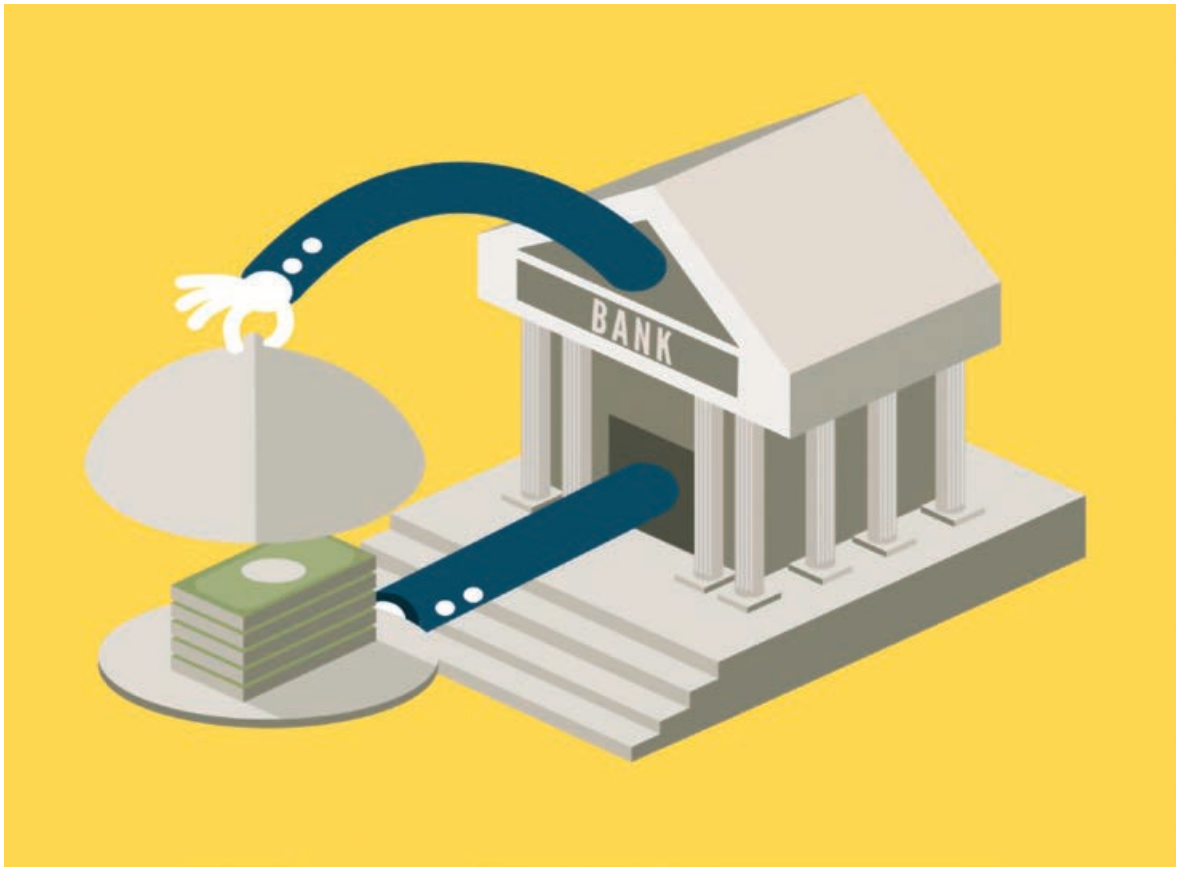
S obzirom na iznesene posljedice nedostataka bitnih elemenata ugovora o kreditu, vrlo je bitno da se prilikom definisanja odredbi ugovora o kreditu naročita pažnja pokloni prije svega tome da ugovori sadrže sve bitne elemente, ali, također, pažnja se mora posvetiti i adekvatnom definisanju ugovornih bitnih i drugih elemenata ugovora. Od pravilnog i jasnog definisanja ugovornih odredbi zavisi izvršenje glavnih i sporednih obaveza iz ugovora o kreditu. U konačnici, puno manje sporova i nesuglasica između banaka i klijenata ćemo imati ukoliko su prava i obaveze ugovornih strana precizno definisane.

Zaključak

Iako je u ovom radu prikazana većina bitnih elemenata koje trebaju sadržavati ugovori o kreditu, naravno u zavisnosti od vrste korisnika kredita i drugih specifičnosti pojedinih slučajeva, ipak je potrebno istaći da postoji još niz podzakonskih akata izdatih prvenstveno od entitetskih agencija za bankarstvo koje sadržavaju odredbe koje se obavezno

navode u okviru ugovora o kreditu. Kao primjer može se navesti obavezno navođenje efektivne kamatne stope[17]. Ali, imajući u vidu obimnost svih elemenata, obavezni elementi predviđeni podzakonskim aktima bi mogli biti tema zasebnog rada, kako je već navedeno u uvodu. Svakako da je predmetne podzakonske akte ovdje bitno napomenuti kako se ne bi stekao dojam da su elementi navedeni u ovom radu jedini bitni elementi ugovora o kreditu.

Trenutna situacija u pravnom sistemu BiH je takva da su bitni elementi ugovora propisani nizom pozitivno-pravnih propisa kao i da se navedeni elementi razlikuju na entitetskom nivou. Cijeneći navedeno, na nivou bankarskog sektora bi bilo vrlo korisno utvrditi registar bitnih elemenata ugovora koji bi zaposlenicima bankarskog sektora služio kao orijentir prilikom rada na kreiranju ugovora i kako bi se na jedinstven način osiguralo poštivanje pozitivnih propisa i, u konačnici, osigurao zakonit rad banaka kao vrlo važnih učesnika na tržištu. ■



[17] Odluka o jedinstvenom načinu obračuna i iskazivanja efektivne kamatne stope na kredite i depozite izdata od strane FBA, Službeni list FBiH 81/17; član 7.; Odluka o jedinstvenom načinu obračuna i iskazivanja efektivne kamatne stope na kredite i depozite izdata od strane Agencije za bankastvo RS; Službeni list RS broj: 75/17; član 7.

Moćna i sigurna tehnologija

BLOCKCHAIN TEHNOLOGIJA

Da li je blockchain budućnost bankarstva i hoće li zamijeniti tradicionalne banke?

Autorica:
Sanela Stupar

Blockchain je jedna od najsigurnijih tehnologija ikad izumljenih. Kao što je internet promijenio pravila modernog života, ova će tehnologija, koju još ne poznajemo dovoljno, promijeniti način na koji živimo i radimo.

Kada je **Satoshi Nakamoto**, oko čijeg identiteta još uvijek postoji misterija, objavio dokument *Bitcoin: A Peer to Peer Electronic Cash System*[1] 2008. godine te osmislio i predložio *istinsku verziju elektronskog novca kroz mrežu ravnopravnih korisnika* zvanu ***Bitcoin***, prvi put se blockchain tehnologija pojavljuje u javnosti. Nedugo nakon obajvljivanja dokumenta, tačnije 2009. godine, *Bitcoin* biva ponuđen *open source* javnosti.

Blockchain bilježi važne informacije u javnom prostoru ne dozvoljavajući da se informacije mijenjaju ili brišu. Blockchain je transparentan, vremenski obilježen i decentraliziran. *Blockhain je Bitcoin-u ono što je internet e-mail-u. Veliki sistem koji se može nadograditi aplikacijama. Valuta je samo jedna*, rekla je **Sally Davies**, reporterka za *FT Technology*.

Mnogi ljudi misle da je *Bitcoin* isto što i Blockchain tehnologija, iako su to dva različita pojma, ali od 2014. godine uočene su razlike i ustanovljeno je da se blockchain može koristiti i za druge podatke osim za kriptovalute.

U svojoj osnovi, blockchain je digitalna, otvorena i decentralizirana *knjiga* koja trajno

[1] Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, [bitcion.org], dostupno na https://bitcoin.org/bitcoin.pdf, pristupljeno 13.1.2019.

> *U svojoj osnovi, blockchain je digitalna, otvorena i decentralizirana knjiga koja trajno bilježi sve transakcije između dvije strane od početka korištenja aplikacije, bez potrebe za posredovanjem, odnosno autentifikacijom od strane trećeg lica. Ovaj proces je veoma efikasan i predviđa se da će troškovi transakcija u budućnosti biti drastično smanjeni.*

bilježi sve transakcije između dvije strane od početka korištenja aplikacije, bez potrebe za posredovanjem, odnosno autentifikacijom od strane trećeg lica. Ovaj proces je veoma efikasan i predviđa se da će troškovi transakcija u budućnosti biti drastično smanjeni.

Satoshi Nakamoto je došao na genijalnu zamisao da napravi sistem koji je digitalna apstrakcija knjige salda i da taj sistem učini javnim za sve praktične operacije vezane za račune i transakcije, koje se, kada se pojednostave, svode samo na proste operacije sabiranja i oduzimanja. Iskoristio je osobinu digitalnog medija da pravi savršene sopstvene kopije pa je distribuirao ovu kopiju knjige salda na svaki računar u mreži (decentralizovani sistem) i dobio jedinstvenu (strukturalno nepromjenljivu) i globalnu (javnu) knjigu salda.

Pomoću Blockchain tehnologije se, osim evidencije transakcija *Bitcoin*-a, vrše i evidencije transakcija svih drugih kriptovaluta, kao i evidencije transakcija bilo kakvog vlasništva (imovine), stana, kuće, zemlje, auta, informacije o porijeklu nekretnina, automobila, medicinski podaci, grunt, katastar, evidencije diploma. Sve transakcije u bilo kojem području primjene sa bitnim elementima transakcije (kao što je u primjeru kriptovalute broj računa sa kojeg se plaća ili jedinstveni identifikacioni broj onoga koji plaća, iznos koji se plaća, broj računa na koji se plaća ili jedinstveni identifikacioni broj onoga kome se plaća, itd.) bilježe se digitalno i pohranjuju u jednu jedinu datoteku čija kopija se distribuira na veliki broj računara (servera ili čvorova povezanih u mrežu) i javno je dostupna svim članovima mreže. Jedna transakcija se bilježi u jednom slogu ili zapisu i pakuje u **blok transakcija**. Svaka naredna transakcija se dodaje i pakuje u isti blok.[2]

Ključna ideja blockchain tehnologije je da ovaj jedinstveni centralni registar zamijeni kopijama blockchain fajlova na velikom broju moćnih računara (servera) koji će se nalaziti na različitim lokacijama, a koji se **nazivaju nodovi.** Svaki put kada se desi nova transakcija, ona se momentalno ažurira na svim nodovima.

Da bi verifikovao blok transakcija, učesnik (***rudar*** ili ***miner***) koji održava mrežu, odnosno ***čvor*** (eng. *node*), mora riješiti vrlo kompleksan matematički zadatak koji se sastoji u pronalaženju (tačnije slučajnom pogađanju) broja zadatog od strane blockcain protokola, koji je potreban za verifikaciju aktuelnog bloka transakcija. Svrha rješavanja tog zadatka krije se u tome

[2] Izjava od Savo Stupar, „NEW TECHNO-LOGIES NT-2019“ Development and Application

da se dokaže da je server rudara morao imati veliki broj pokušaja i trošiti veliku količinu električne energije da bi postigao cilj. Kao protuuslugu za verifikaciju bloka transakcija, rudar biva nagrađen određenim iznosom kriptovalute uvećanim za cijenu transakcija iz aktuelnog bloka, koji plaćaju učesnici u transakcijama. Jedini način na koji bi *rudari* (čvorovi) koji održavaju mrežu mogli manipulirati sistemom je taj da posjeduju 51% ukupne računarske snage cijele mreže. Čak i tada je nemoguće mijenjati već unesene transakcije, ali je moguće zaustaviti naredne transakcije. Što više računarske snage rudar ima[3], veća je vjerovatnoća da će prvi *pogoditi* traženi broj i kao protuuslugu dobiti nagradu, a upravo to je razlog zašto se rudari udružuju u grupe (engl. ***mining pool***), odnosno kompanije koje koriste resurse (računare) i rad malih pojedinačnih (kućnih) rudara. *Mining pool* se prema mreži ponaša kao jedan korisnik, ali interno posao raspodjeljuje na sve svoje članove koji onda, proporcionalno snazi svojih računara, dijele zarađene *bitcoine*.

Dva veoma bitna pitanja na koja treba odgovoriti su:

1. Kako obezbijediti da sve kopije blockchain fajla, koje se nalaze disperzirane na nodovima, budu identične u svakom trenutku?
2. Kako se ove transakcije uopšte izvršavaju?

Svaki od tih servera čuva na svom hard disku najažurniju kopiju blockchain fajla sa svim transakcijama od početka korištenja aplikacije. Svaki put kada se dogodi nova transakcija, ona se trenutno ažurira na svakom od ovih servera (*nodova*). Zbog činjenice da bi eventualnu zlonamjernu radnju izmjene ili brisanja neke transakcije trebalo uraditi ne samo na jednom (centralnom) računaru nego na svim kopijama blockchain fajla, postupkom decentralizacije evidencije o transakcijama, odnosno kopiranjem evidencijskog fajla na veliki broj računara, praktično je onemogućeno izvršenje takvih zlonamjernih aktivnosti.

Prvi korak u izvršenju neke transakcije je iniciranje transakcije kojim se kontroliše da li inicijator transakcije ima dovoljno sredstava na računu da bi mogao izvršiti tu transakciju, tako što program *prečešlja* kompletan blockchain fajl, odnosno *pročita* sve transakcije (transakciju po transakciju) koje je on ikada imao da bi izračunao stanje na računu te provjerio da li je iznos inicirane transakcije

> *Pošto u registru transakcija ne postoji zapis transakcije sa zabilježenim stanjem računa nekog korisnika, nego se to stanje svaki put ponovo izračunava na osnovu svih transakcija koje je on ikad imao, to predstavlja još jedan (viši) nivo bezbjednosti i kontrole transakcija. Kada bi neko zlonamjerno pokušao da promijeni raspoloživo stanje na računu korisnika, morao bi da promijeni sve transakcije po tom računu ikad izvršene, što je praktično nemoguće.*

[3] G. Konstantopoulos, Understanding Block-chain Fundamentals, Part 2: Proof of Work & Proof of Stake, A Medium Corporation, 2017, dostupno na: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb, pristupljeno 27.1.2019. godine

(koji se prenosi na neki drugi račun) veći od izračunatog stanja računa. Pošto u registru transakcija ne postoji zapis transakcije sa zabilježenim stanjem računa nekog korisnika (koje bi se jednostavno moglo hakirati), nego se to stanje svaki put ponovo izračunava na osnovu svih transakcija koje je on ikad imao, to predstavlja još jedan (viši) nivo bezbjednosti i kontrole transakcija. Kada bi neko zlonamjerno pokušao da promijeni raspoloživo stanje na računu korisnika, morao bi da promijeni sve transakcije po tom računu ikad izvršene, što je praktično nemoguće.

Drugi korak u tom procesu je nadmetanje koji će *majner* prvi uspjeti da ugradi blok transakcija, kojem ta transakcija pripada u *blockchain fajlu* (registar transakcija) i da ga trajno doda (zabilježi) kao sljedeći blok u lancu transakcija. Da bi se nova transakcija definitivno zabilježila (upisala) u registar svih transakcija i dodala nova karika (blok transakcija) u lancu, potrebno je da majneri (slučajnim generisanjem) počnu tražiti odgovarajući broj**.** Taj se broj ne može izračunati nekom formulom (algoritmom). To je broj koji se jedini uklapa u kariku lanca kojom se povezuje posljednja verifikovana transakcija sa novom transakcijom. On se može dobiti samo slučajnim pogađanjem. To se praktično može raditi samo uz pomoć računarskog programa, generisanjem slučajnih brojeva *random* funkcijom i provjerom da li taj broj odgovara (*pasuje*).

Sve još nepotvrđene transakcije obavljene u određenom vremenskom periodu, koji obično traje 10 minuta, sakupljaju se i stavljaju (pakuju) u jedan blok. Informacije pohranjene u tom bloku

> *Zbog toga što je hash svakog bloka generisan pomoću hasha bloka prije njega, taj blok postaje digitalni oblik pečata ili potpisa. On potvrđuje da je taj blok, i svaki blok poslije njega, validan jer, ukoliko bi neko pokušao da ga izmijeni, svi u mreži bi to znali i ne bi to dozvolili. Time je eliminisan cyber rizik.*

koriste *rudari* tako što na njih primjenjuju matematičku formulu, pretvarajući te informacije u nešto puno kraće, naizgled slučajno generisani niz brojeva i slova koji zovemo ***hash***. Taj *hash* je pohranjen zajedno sa blokom na kraju lanca blokova. *Hashevi* imaju neke karakteristične osobine. Vrlo je lako proizvesti *hash* iz podataka kao što je blok transakcija, ali je gotovo nemoguće obrnuto - generisati blok transakcija samo na osnovu *hash*-a. Veoma je lako proizvesti *hash* iz velike količine podataka, ali svaki *hash* je unikatan. Ako se u ulaznom nizu (poruci) promijeni samo jedno slovo ili brojka, *hash* se kompletno mijenja. Međutim, rudari ne koriste samo transakcijski blok da bi generisali *hash*, već koriste i neke druge podatke. Jedan od tih podataka jeste *hash* zadnjeg bloka pohranjenog u lancu blokova. Zbog toga što je *hash* svakog bloka generisan pomoću *hasha* bloka prije njega, taj blok postaje digitalni oblik pečata ili potpisa. On potvrđuje da je taj blok, i svaki blok poslije njega, validan jer, ukoliko bi neko pokušao da ga izmijeni, svi u mreži bi to znali i ne bi

to dozvolili. Time je eliminisan *cyber* rizik.

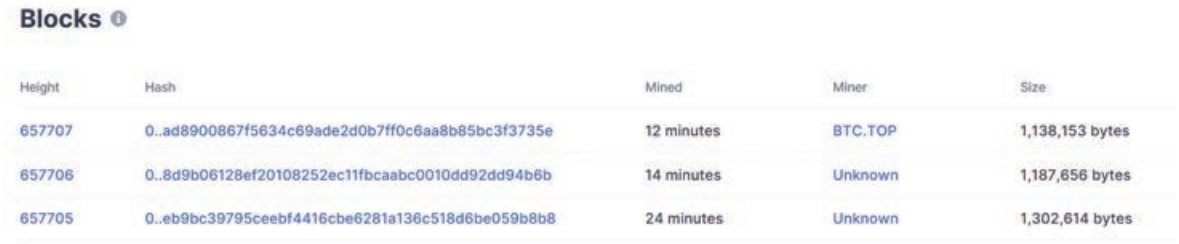
Rudari se takmiče ko će prije digitalno potpisati novi blok i dodati ga u lanac zato što to nosi vrijedne nagrade: 1. ***fiksnu vrijednost novih bitcoina*** koja je propisana *bitcoin* protokolom i 2. ***varijabilnu vrijednost bitcoina*** koju su korisnici mreže odlučili zakačiti na svoje transakcije da bi motivisali rudare da im transakciju verifikuju. Za verifikaciju bloka koristi se ponovo SHA256 algoritam, a izvodi se nad sljedećim podacima – indeks bloka + *hash* prethodnog bloka + podaci (dakle, BTC transakcije) + *timestamp* (novog bloka kandidata) + *nonce*, vrlo bitnog broja koji pokazuje koliko intenzivno rudar mora računati (*rudariti*) da dođe do validnog, odnosno odgovarajućeg *hasha* za aktuelni blok.

Problem i jeste u tome što je uz pomoć računara vrlo lako kreirati *hash* od ulaznih podataka. Zbog toga je *Bitcoin mreža* morala učiniti stvari težima, inače bi svi stvarali hiljade *hasheva* svake sekunde, a svi *bitcoini* bi bili *izrudareni* za kratko vrijeme. Blockchain protokol neće prihvatiti bilo kakav *hash*.

"*Hash* novog bloka mora biti izveden prema aktualnoj specifikaciji *bitcoin* algoritma, a taj parametar naziva se *difficulty* (u slobodnom prijevodu – težina izračuna). Ako *difficulty* diktira da *hash* novog bloka mora na početku imati četiri nule, hardver računa novi *hash* dok prvi put ne dođe do kompatibilne vrijednosti. Od svih vrijednosti koje se *hashiraju* samo je jednu dozvoljeno mijenjati, a to je ***nonce***. Vrijednost kreće od nule, u svakom se ciklusu ponovnog izračuna *hasha* povećava za jedan, čime se dobiva drugačija vrijednost konačnog *hasha*. Ako rudar uspije pronaći ispravan *hash* za novi blok prije nego što mu neki kolega s mreže ne pošalje vlastiti ispravan blok, dodaje ga u svoj lokalni *blockchain* i šalje natrag prema mreži. Ako novi blok ipak stigne s mreže ranije, izračuni se prekidaju, čisti se lista pristiglih transakcija od onih koje su uključene u novopristigli blok, stvara se nova lista transakcija za verificiranje i počinje izračun za sljedeći blok."[4] Jasno je zašto se rudari takmiče ko će prvi izračunati blok koji nastavlja *blockchain*, upravo to takmičenje garantuje sigurnost i nezavisnost sistema do prihvatljivog nivoa. *Difficulty* algoritam je inače varijabilan, a izračunava se na bazi brzine verifikacije prethodnih 2.016 blokova. Algoritam koji podešava *difficulty* za cilj da se novi blok verifikuje okvirno svakih 10 minuta, čime se održava računska zahtjevnost i intenzivnost kompletnog procesa. Održavanje zahtjevnosti i intenzivnosti procesa verifikacije svakog novog bloka transakcija izuzetno je bitno jer značajno otežava mogućnost prevare unutar mreže.

> *"Kada su rudari definitivno verifikovali blok, on se zatim dodaje (uvezuje) u lanac blokova (engl. block chain), koji sadrže prethodne transakcije. Dakle, posao rudara je potvrđivanje (verifikacija) i zapisivanje transakcija u glavnu knjigu (eng. General ledger). Tako nastaje lanac (engl. chain) svih transakcija."*

[4] https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011



Blocks

Height	Hash	Mined	Miner	Size
657707	0..ad8900867f5634c69ade2d0b7ff0c6aa8b85bc3f3735e	12 minutes	BTC.TOP	1,138,153 bytes
657706	0..8d9b06128ef20108252ec11fbcaabc0010dd92dd94b6b	14 minutes	Unknown	1,187,656 bytes
657705	0..eb9bc39795ceebf4416cbe6281a136c518d6be059b8b8	24 minutes	Unknown	1,302,614 bytes

Kada su rudari definitivno verifikovali blok, on se zatim dodaje (uvezuje) u lanac blokova (engl. *block chain*), koji sadrže prethodne transakcije. Dakle, posao rudara je potvrđivanje (verifikacija) i zapisivanje transakcija u glavnu knjigu (eng. *General ledger*). Tako nastaje lanac (engl. *chain*) svih transakcija.

Pošto su se prednosti *blockcahin tehnologije* pokazale u poslovanju sa kriptovalutama, počinje njena masovna primjena u mnogim drugim oblastima. Blockchain je javno dostupan na raznim sajtovima. Svaka osoba na svijetu može da vidi sadržaj cijelog blockchaina u svakom trenutku, sve transakcije koje su se ikada desile.[5]

Prema zadanim postavkama, blockchain tehnologija ne podržava bilo kakvu izmjenu podataka. Svi podaci koji su ušli u blok nikada se neće moći izbrisati ili izmijeniti i ostat će zauvijek.

PRIMJENA BLOCKCHAIN TEHNOLOGIJE

Primjena tehnologije, koja je nastala prvenstveno da bi podržala evidenciju transakcija *bitcoin* kriptovalute, nema granica, ali je najefikasnija u onim oblastima ljudskog djelovanja u kojima se radi o različitim vrstama evidencije transakcija (evidencija zemljišta, kuća, stanova, automobila, osiguranja, ugovora, diploma, drugih kriptovaluta itd.) gdje se traži transparentnost, eliminiše mogućnost prevare, malverzacije, mita i korupcije i izbacuje ili zaobilazi posrednik koji je vlasnik pomenutih evidencija (banka, država, advokati, sudovi, obrazovne institucije, osiguravajuće kuće, prodavci itd.)

Navest ćemo još neke vrste primjene:

1. ***Pametni ugovori*** (*smart contracts*) su jedna od mogućih varijanti usavršavanja koncepta blockchaina u kojoj se umjesto transakcije u blockchain upisuje programski kod. Razlog zašto se programski kod upisuje u blockchain jeste ona osobina blockchaina koja onemogućava da se podaci zapisani u njemu (u ovom slučaju programski kod) mijenjaju i ne zavise od povjerenja među strankama koje sklapaju ugovor;
2. ***Primjena u bankarstvu*** u servisima za međubankarske transakcije;
3. ***Primjena u evidenciji zemljišnih knjiga*** (gruntu i katastru) gdje bi jednom upisane transakcije postale javno dostupne i provjerljive za sve građane i zainteresovane strane;

[5] https://www.blockchain.com/btc/blocks

4. ***Primjena u evidenciji elektronskog glasanja na izborima*** gdje bi svaki glasač imao mogućnost da provjeri da li je njegov glas stvarno pribrojan broju glasova koje je osvojio kandidat ili stranka za koju je glasao;
5. ***Primjena u zdravstvu*** za evidenciju kartona pacijenata gdje je moguće i potrebno koristiti lance za zaštićenim pristupom podacima;
6. ***Primjena u obrazovanju*** za evidencije diploma i certifikata čime bi se značajno smanjila mogućnost zloupotrebe i falsifikovanja diploma;
7. ***Primjena kod evidencije lanaca snabdijevanja***;
8. ***Upravljanje evidencijom namirnica organskog porijekla***;
9. ***Kontrola ličnih podataka*** koji se koriste u marketinške svrhe, itd.

Upotrebe blockchain tehnologije u bankarstvu

Blockchain je moćna i sigurna tehnologija koja se počela primjenjivati i u bankarstvu jer je sigurnost od najveće važnosti za finansijski sektor.

> *Blockchain je moćna i sigurna tehnologija koja se počela primjenjivati i u bankarstvu jer je sigurnost od najveće važnosti za finansijski sektor.*

Finansijske transakcije nemoguće su bez provjere identiteta. Ova provjera zahtijeva puno koraka kao što su: p**rovjera licem u lice (može biti i putem video poziva, npr. putem *Skype*-a), autentifikacija (klijent banke mora dokazati svoj identitet svaki put kad se prijavi na uslugu), ovlaštenje: potreban je dokaz o namjerama klijenta.**

Sve ove korake treba poduzeti za svakog novog pružatelja usluga. Međutim, blockchain omogućuje sigurnu ponovnu upotrebu provjere identiteta za druge usluge.

Prednosti su da je blockchain u *fintehu*, korisnici mogu odabrati kako će se identificirati i s kim žele da dijele svoj identitet. I dalje trebaju registrirati svoj identitet na blockchainu, ali ne trebaju ponoviti registraciju za svakog davatelja usluga ako ti pružatelji također koriste blockchain.

Nedostaci: Standardi za provjeru identiteta na blockchainu još se razvijaju. Nakon što se podaci zabilježe na blockchainu, sve strane u mreži mogu im pristupiti pa bi korisnici trebali ograničiti sve privatne podatke koje ne žele otkriti.

ID2020 je projekt usmjeren na stvaranje digitalnih identiteta za ljude koji nemaju papirnate iskaznice. Od 2016. godine, ID2020 zalaže se za etičke pristupe digitalnog ID koji štite lične podatke i privatnost. Projekt podržavaju *Accenture*, *Microsoft* i *Rockefeller Foundation*.

Primjeri primjene blockchain tehnologije u bankarstvu su:

- ***Sindicirani krediti*** - obrada sindiciranih kredita od strane banaka može potrajati i do 19 dana. Banke, koje obrađuju sindicirane kredite, trebaju da upoznaju svog kupca (KYC) - provjere identitet klijenta, usklade poslavanje sa Zakonom i primijene obavezu čuvanja bankarske tajne (BSA), rade na

sprečavanju pranja novca i finansiranja terorističkih aktivnosti (AML) - pravne radnje usmjerene na sprečavanje, otkrivanje i prijavljivanje aktivnosti pranja novca. U primjeru se navodi da, ako je jedna banka uskladila poslovanje sa regulatornim zahtjevima, sve ostale banke to ne moraju ponoviti. Time se znatno skraćuje vrijeme obrade sindiciranih kredita i smanjuju se troškovi. Nedostaci su što blockchain ne može riješiti sve procese za sindicirane kredite jer bi sve banke trebale primijeniti blockchain tehnologiju. Primjer koji se navodi za sedam međunarodnih banaka (posebno *BNP Paribas*, *BNY Mellon*, *HSBC*, *ING*, *Natixis* i *State Street*) koje su se udružile da bi podržale *Fusion LenderComm by Finastra*, blockchain platformu za sindicirane kredite.

- ***Računovodstvo, knjigovodstvo i revizija*** - u računovodstvu je uključeno toliko papira, a digitalizira se relativno sporo. Razlog tome mogu biti strogi regulatorni zahtjevi u pogledu valjanosti i cjelovitosti podataka. Stoga je računovodstvo još jedna domena koja se može transformirati snagom finansiranja blockchain tehnologije, od pojednostavljenja usklađenosti do pojednostavljenja tradicionalnog dvostrukog knjigovodstva. Neki stručnjaci pretpostavljaju da blockchain možda nije prikladan za svaki pojedini slučaj u knjigovodstvu i može se koristiti samo za određena područja, poput međubankarskih transfera.
- ***Kreditni izvještaji za pravna i fizička lica*** - Blockchain finansije mogu pomoći pojedincima i malim preduzećima da brzo dobiju kredite na temelju njihove kreditne historije. Blockchain može pružiti alate koji će zajmoprimcima omogućiti da svoj kreditni izvještaj učine preciznijim, transparentnijim i sigurnijim za dijeljenje. Evo kako to funkcionira s blockchainom:
  - Vlasnik podataka smješta svoju povijest transakcija u blockchain i osigurava je privatnim ključem;
  - Šifrirana transakcija pohranjena je izvan blockchaina;
  - Raširena šifrirana transakcija pohranjuje se unutar blockchaina s vremenskim oznakama i metapodacima;
  - Kupac podataka podnosi kriterije za kreditnu povijest;
  - Pametni ugovori identificiraju i provjeravaju potencijalne podatke na temelju kontrolnih kriterija vlasnika podataka;
  - Blockchain engine filtrira podatke i vraća rezultate.

Prednosti su: kreditni izvještaji temeljeni na blockchainu smanjuju troškove i složenosti u vezi s provjerom podataka. Osim toga, vlasništvo nad podacima vraća se nosiocu podataka jer se više ne čuva u središnjem spremištu.

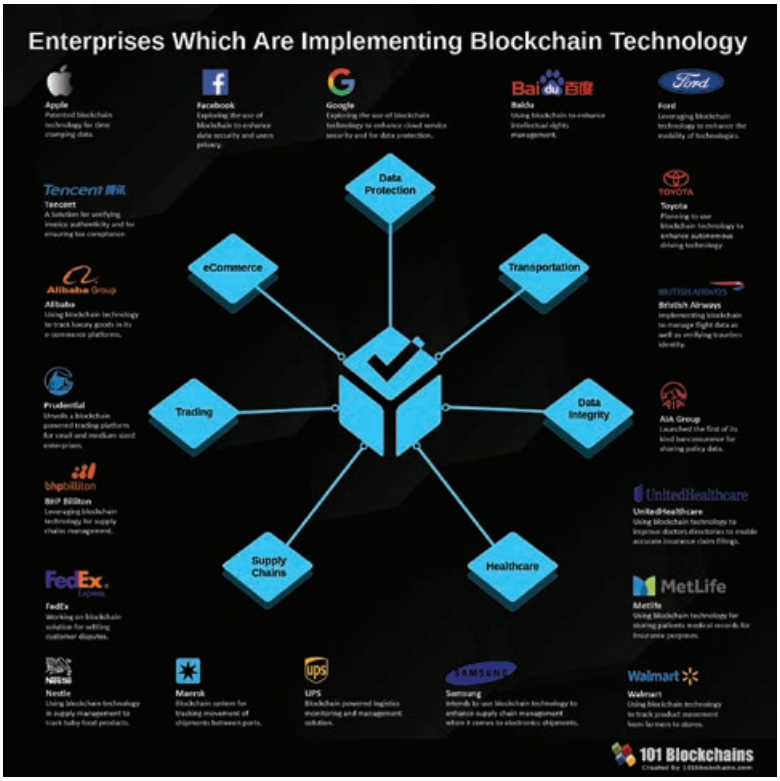
Nedostaci su: nepromjenjivost blockchaina, tj. nemogućnost poništavanja promjena, nije u skladu sa regulativom o zaštiti ličnih podataka i krši ljudska prava koja se odnose na zaštitu ličnih podataka.

Da li je blockchain budućnost bankarstva i hoće li zamijeniti tradicionalne banke?

To se još ne zna, sve se može dogoditi u najbližoj budućnosti. Blockchain tehnologija u bankarstvu i finansijama suočava se sa sljedećim izazovima:

- ***Nadogradnja propisa i zakonodavstva***. Trenutni propisi i zakonske odredbe ne dopuštaju upotrebu finansiranja tehnologije blockchain, a odnosi se na zabranu nepromjenjivosti ličnih finansijskih podataka koju smo naveli u primjeru.
- ***Poboljšana sigurnost***. Novčanici s kriptovalutama, koji se koriste za blockchain transakcije, trebali bi imati 100% zaštitu od hakera.
- ***Potrebno je razviti standarde za provjeru identiteta na blockchainu***.
- ***Treba istražiti konkretnije slučajeve upotrebe banaka i blockchaina.***

Mnoge nove informacione tehnologije, odnosno novi koncepti informacione podrške i pružanja računarskih usluga, koje su se pojavile u zadnjih dvadesetak godina, kao što su tehnologije *Data Mininga* (neuronske mreže, mašinsko učenje, skladišta podataka, vještačka inteligencija), kao otkrivanje znanja iz podataka, *Cloud Computinga* (*On Demand computing* ili pružanje kompjuterskih usluga na zahtjev, virtualizacija računarstva), *Big Data Analytics*, kao obrada ogromne količine podataka u realnom vremenu, kao i mnoge druge tehnologije nastale na bazi razvoja interneta, najavljivane su kao tehnologije s revolucionarnim potencijalom koje će promijeniti sudbinu čovječanstva. Međutim, tehnologija za koju nam se čini da ima najveći potencijal da napravi revoluciju u svim oblastima ljudskog djelovanja jeste upravo blockchain tehnologija. Primjenom blockc-



Top 20 poduzeća koja implementiraju blockchain tehnologiju[6]

[6] https://101blockchains.com/enterprises-implementing-blockchain/

hain tehnologije u bilo kojoj oblasti ljudskog djelovanja, onemogućeno je za sva vremena brisanje ili izmjena bilo koje transakcije koja je upisana u blockchain fajl konkretne aplikacije. Kao što smo naveli u primjerima, to ima i svojih nedostataka.

ŠTA JE BITCOIN?

Za *Bitcoin* se koriste razni opisni termini poput: virtuelnog i digitalnog novca te virtuelne, digitalne, elektronske, sintetičke i kriptovalute.
Američki[7] *FinCEN* i *Evropska centralna banka*[8] su klasificirale *Bitcoin* kao virtuelnu valutu. *Narodna banka Kine* je klasificirala *Bitcoin* kao nešto što *izvorno nije valuta, ali je predmet za ulaganje*.[9] Njemački sud je okarakterisao *Bitcoin* kao jedinicu mjere.[10] Finska vlada[11], kao i *Wall-Street* dnevne novine su klasificirale *Bitcoin* kao robu. *Bitcoin.org*, wiki portal za *Bitcoin* je dao sljedeću definiciju: *Bitcoin je način plaćanja baziran na konceptu digitalne kriptovalute, koji funkcioniše bez ikakve centralne vlasti ili treće stranke kao povjerioca.*
Bitcoinova najznačajnija karakteristika jeste to što je decentraliziran. Ova kriptovaluta nije bazirana na zlatnoj podlozi, nema zemlju porijekla i iza nje ne stoji nijedna država niti centralna banka neke države niti centralna banka neke unije država. Trenutni pobornici *bitcoina* to smatraju enormnim plusom, budući da do oscilacija vrijednosti dolazi jedino zbog ljudi.

Bitcoin – nova tehnologija ili tačnije protokol

Nove jedinice kriptovalute proizvode se (*štampaju se*) *rudarenjem* (engl. *mining*) kao nagrada za rješenje matematičkog zadatka postavljenog od strane *Bitcoin protokola*, kojim se verifikuje novokreirani blok i upisuje u *Bitcoin blockchain fajl*, o čemu će detaljnije biti riječi u nastavku teksta. Korisnici mogu doći u posjed kriptovalute kupovinom određenog iznosa kriptovalute te prodajom dobara ili usluga.

U prosjeku, svakih 10 minuta se generiše novi blok na *Bitcoin blockchain fajlu* pa je to ujedno i prosječno vrijeme za potvrdu transakcije. Nakon generisanja novog bloka, rudar dobiva nagradu (*incentiva*) koja trenutno iznosi 6,25 BTC i koja se svake 4 godine u pola smanjuje (BTC je skraćenica za jedinicu kriptovalute *Bitcoin*), kao i naknade za transakcije koje su zapisane u novi blok uplaćene od strane korisnika.

Rudarenje je jedini način na koji se izdaju novi BTC-ovi. Kako je opskrba *Bitcoina* ograničena na 21 milijun coina, događaji prepolovljavanja bitcoina trebali bi se nastaviti sve do 2140. godine ili do 21-milijuntog BTC-a. Do tada bi nagrada za rudarenje trebala dostići 1 *satoshi* (najmanju jedinicu bitcoina) koji iznosi 0,00000001 BTC. To je jedan od razloga zašto možemo

[7] Izjava od Jennifer Shasky Calvery, Direktora Financial Crimes Enforcement Network United States Department of the Treasury pred senatom SAD-a 19.01.2013.
[8] Evropska Centralna Banka (2012). Virtual Currency Schemes. Frankfurt. p. 5. ISBN 978-92-899-0862-7.
[9] Izjava novinarima od Sheng Songchenga, savjetnika Narodne Banke Republike Kine od 15.01.2014.
[10] CNBC (19.08.2013.) Bitcoin recognized by Germany as 'private money', Preuzeto 13.1.2019. iz www.cnbc.com
[11] Kati Pohjanpalo (2014), "Bitcoin Judged Commodity in Finland After Failing Money Test", Bloomberg novine

reći da je *Bitcoin,* ustvari, deflativna valuta.

U tome se vidi i još jedna razlika u odnosu na klasične valute koje centralne banke mogu izdavati po potrebi i procjeni i na taj način izazivati inflaciju. Do danas je *odštampano* ili *izrudareno* oko 80% od ove projektovane sume BTC-ova ili tačnije oko 18 miliona, a trenutna vrijednost 1 BTC-a je 17.925,83 USD.[12] Što je više BTC-ova, nagrada je sve manja i manja pa se tako dodatno sprečava inflacija. Kada rudari budu stvorili 21 milion *Bitcoina*, ova nagrada će biti nula i majneri će zarađivati samo od transakcija.

Najvažnije je da novi korisnik može početi koristiti *Bitcoin* bez potpunog razumijevanja tehničkih pojedinosti, na isti način kao što neko može koristiti program, a da nije niti autor programa niti poznaje programiranje. Dovoljno je da korisnik instalira aplikaciju *Bitcoin Elektronski Novčanik* (E_Wallet) na računar, smartphone ili tablet, koja će zatim generisati njegovu

Najvažnije je da novi korisnik može početi koristiti Bitcoin bez potpunog razumijevanja tehničkih pojedinosti, na isti način kao što neko može koristiti program, a da nije niti autor programa niti poznaje programiranje.

prvu *Bitcoin adresu*. Transfer *Bitcoina* sa jedne adrese na drugu, ili bankarski rečeno *sa jednog računa na drugi*, u praksi je slično slanju i primanju e-maila. Kao što kod slanja e-maila korisnik koji ga šalje treba da zna adresu korisnika kojem šalje poruku, tako i korisnik koji šalje BTC-ove, mora znati znati adresu korisnika kojem ih šalje.

Bitcoin transakcije možemo definisati kao prenos vrijednosti iz jednog digitalnog novčanika u drugi, koji se nakon toga registruje kao jedan digitalni zapis koji zajedno sa ostalim zapisima, prethodno upisanim u jedan blok transakcija, čini blok još uvijek nepotvrđenihn transakcija.

Kada se skupe sve transakcije nastale u roku od 10 minuta od trenutka upisivanja posljednjeg verifikovanog bloka u *Bitcoin Blockchain fajl*, daje se zadatak svim rudarima da pronađu odgovarajući broj, odnosno riješe matematički zadatak. Prvi koji to uradi (*dobije na lutriji*) upisuje novi blok nepotvrđenih transakcija u *Bitcoin Blockchain fajl* po sistemu ulančanih blokova tako da od tog trenutka sve transakcije u tom bloku postaju validne i javne.

Bitcoin novčanik sadrži dio podataka koji je tajan i on se naziva privatni ključ ili lozinka (šifra pristupa sefu u kojem se nalazi novac ili šifra pristupa novčaniku) i njime se potpisuju transakcije potvrđujući matematički dokaz koji povezuje ključ i vlasnika novčanika. Jednom kada je transakcija izdata, više se ne može promijeniti. Upravo zbog toga važnu ulogu igra potpis. Transakcije na *Blockchain mreži* su javne, a vidjeti se može čitava historija (arhiva) svih ikad procesiranih transakcija.

[12] https://markets.bitcoin.com/crypto/BTC

U praksi, ako entitet A želi poslati BTC-ove entitetu B, mora imati digitalni novčanik koji u sebi sadrži privatni ključ koji dozvoljava kreiranje kriptografskog (digitalnog) potpisa. Entitet A unosi iznos BTC-ova koji želi poslati entitetu B. Entitet B daje javni ključ (adresu digitalnog novčanika) entitetu A da bi mu ovaj prebacio određeni iznos.

Za mogućnost izvršenja transakcija određenog iznosa BTC-ova iz jednog digitalnog novčanika (engl. *wallet*) na drugi, potrebne su tri stvari:

1. adresa novčanika ili javni ključ (engl. *Public Key*),
2. privatni ključ ili šifra pristupa novčaniku (engl. *Private Key*) i
3. kriptografski (digitalni) potpis.

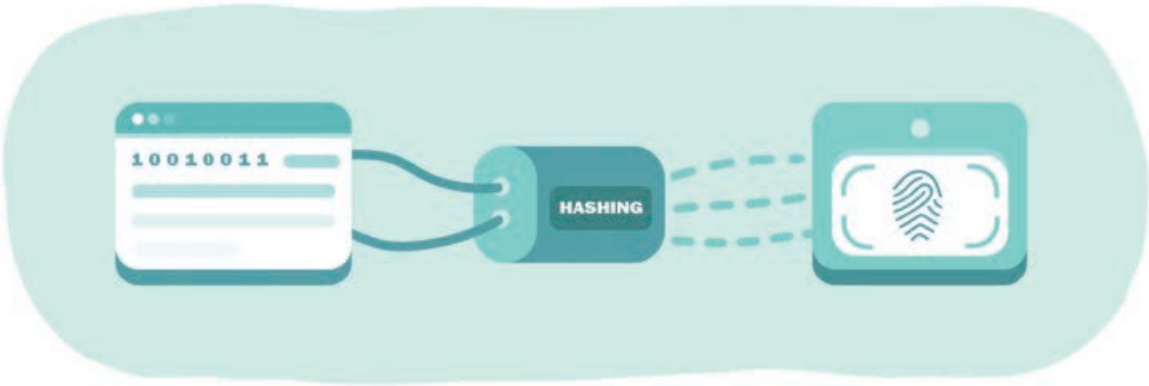
Kad opisujemo *Bitcoin protokol*, često mu pripisujemo dvije osobine: 1. ***da je potpuno transparentan*** (sa javnom knjigom salda) i 2. ***anoniman***. Ako se fokusiramo na jednu stavku knjige salda i na minimum potrebnih atributa da bi ona bila zabilježena, uočit ćemo da podaci kao što su ime i prezime te ostali lični podaci nisu potrebni za funkcionisanje knjige salda u smislu funkcionalnosti, naravno ne uzimajući u obzir KYC (engl. *Know your client*) protokole, tj. *upoznaj svog klijenta*, koje banka mora implementirati. Broj računa nas jedinstveno identificira, kao što je slučaj i sa JMBG na našim ličnim kartama. Zato, kad kreiramo *račun Bitcoin protokolom*, za razliku od kreiranja računa u banci *Bitcoin* protokol vam nikad neće tražiti lične podatke. Dakle, pošto se radi o *Bitcoin* protokolu, a ne o banci, ispravnije bi bilo koristiti izraz adresa, a ne račun kao oznaku lokacije gdje se BTC nalazi.

> *Pošto adrese učesnika u transakciji nisu vezane sa njihovim ličnim podacima, veoma je teško (praktično nemoguće, a teorijski ipak moguće) odgonetnuti kome pripada koja adresa. To dalje znači da Bitcoin nije anoniman, nego pseudo-anoniman sistem. Međutim, ne treba zaboraviti da svako u Bitcoinu može imati skoro neograničen broj adresa.*

Svaka transakcija u *Bitcoin* protokolu je javna te svako ima pristup javnoj knjizi salda koju može vidjeti na internetu u bilo kojem trenutku, kao i historiju (arhivu ili promet) svih transakcija ikad obavljenih sa svakog aktivnog računa.

Pošto adrese učesnika u transakciji nisu vezane sa njihovim ličnim podacima, veoma je teško (praktično nemoguće, a teorijski ipak moguće) odgonetnuti kome pripada koja adresa. To dalje znači da *Bitcoin* nije anoniman, nego pseudo-anoniman sistem. Međutim, ne treba zaboraviti da svako u *Bitcoinu* može imati skoro neograničen broj adresa.

Adresa je definisana kao bankovni račun. *Bitcoin* adresa je identifikator dužine 26-34 alfanumeričkih znakova, počevši od broja 1 ili 3, što predstavlja moguću destinaciju za plaćanje BTC-ova koristeći račun na mjenjačnici za kriptovalute ili putem digitalnog novčanika. Bitno je istaći da jedan korisnik, kao i u slučaju bankovnog računa, može imati i koristiti više adresa (primjer *Bitcoin* adrese:



1BQ9qza7fn9snSCyJQB3Z-cN46biBtkt4ee). Ove adrese se kreiraju koristeći kriptograske algoritme, preciznije SHA-256 za generisaanje **privatnih** ključeva i RIPE–MD160 za generisanje adresa na osnovu rada SHA-256.

Privatni ključ je jedinstvena i tajna šifra pristupa koja obezbjeđuje pravo prebacivanja BTC-ova iz novčanika pomoću kriptografskog potpisa. Kada se stvori nova *Bitcoin* adresa, ona dolazi uz privatni ključ koji je matematički povezan s tim brojem računa. Privatni ključevi *Bitcoina* obično sadrže 51 znak i počinju s brojem 5. Ti privatni ključevi se memorišu (pohranjuju) na personalnom računaru. U slučaju korištenja softverskog ili web novčanika, pohranjuju se na serveru.

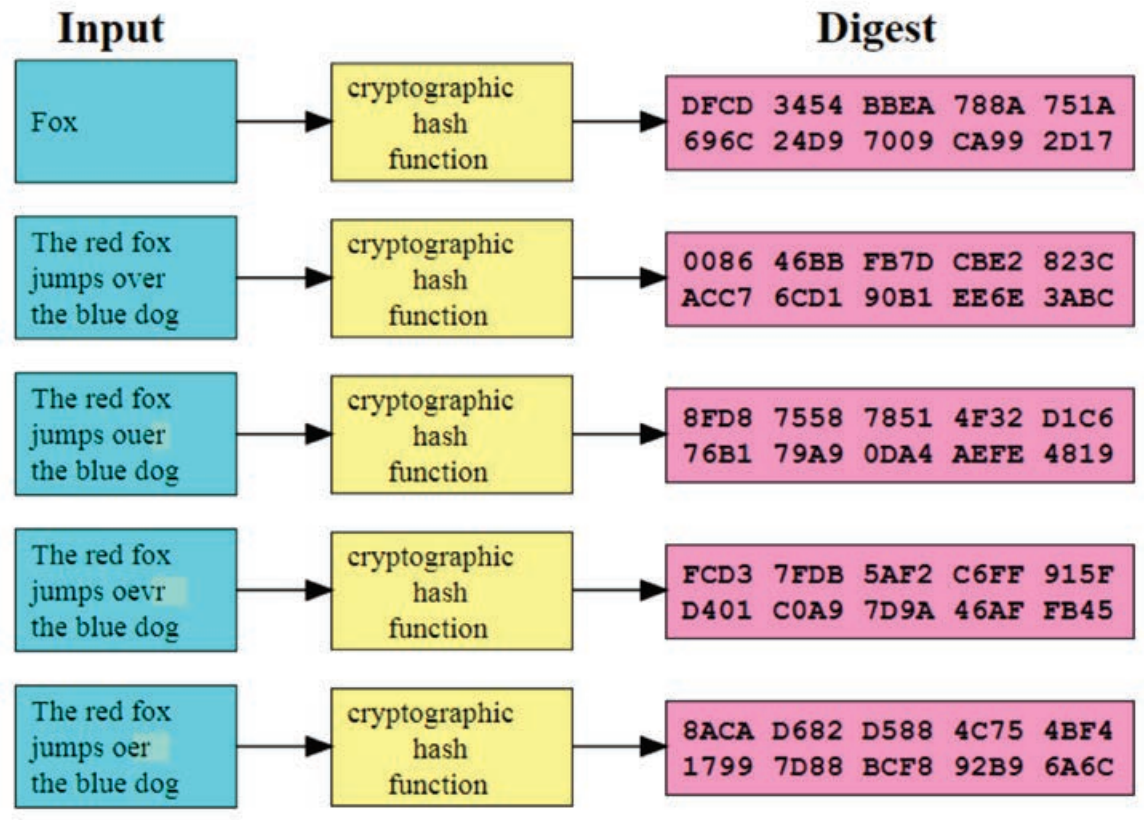
Kriptografski (digitalni) potpis je matematička metoda (algoritam) koji se koristi za provjeru porijekla i utvrđivanje integriteta informacije te na taj način omogućava vlasniku da dokaže svoje vlasništvo određene adrese, odnosno novčanika. Digitalni potpisi imaju dvije bitne karatkeristike:

- ***Osiguravaju integritet transakcije*** (dokumenta), odnosno potvrđuju da transakcija (dokument) nije izmijenjena u međufazi između čitanja (pregledanja) i potpisivanja, te da, u slučaju ugovora, nisu izmijenjeni članovi i uslovi bez saglasnosti obje strane.
- ***Nemogućnost krivotvorenja potpisa***, što znači da potpis jedinstveno identificira potpisnika te implicira da nije moguće izbjeći odgovornost za potpisanu transakciju (dokument), tvrdeći suprotno.

U trenutku kada *Bitcoin* protokol (softver) potpiše transakciju pripadajućim privatnim ključem, svima u *Bitcoin* mreži je omogućen prikaz (digitalnog) potpisa koji odgovara izvršenoj transakciji i koji je generisan kriptografskim algoritmom, ali do privatnog ključa koji štiti račun je nemoguće doći.

Kriptografska *hash* funkcija preuzima ulazne podatke, odnosno poruku ili niz znakova proizvoljne dužine i

pretvara ih u niz fiksne dužine, odnosno *šifriranu* poruku poznatiju kao *hash-code*, *hash-rezultat*, *hash-vrijednost* ili jednostavno *hash*[13]. *Taj postupak zove se hashiranje* i vrši se najčešće koristeći algoritam Sha256[14]. Iz takve šifrirane poruke je gotovo nemoguće otkriti izvorne podatke. Najmanjim promjenama na ulaznim podacima u *hash* funkciju, vrijednost *hasha* se potpuno mijenja (slika 1). Na Slici 1 prikazana je *hash* funkcija koja uzima ulazni skup znakova (naziva se *ključ*) i transformiše ga na vrijednost određene, najčešće manje, ali fiksne dužine (*digest*). ■



Slika 1. *Hash funkcija*[15]

[13] *Hash* funkcija je bilo koja funkcija koja se može koristiti za mapiranje (pretvaranje) ulaznih digitalnih podataka proizvoljne veličine u niz digitalnih podataka fiksne veličine (*hash* vrijednost). Kvalitetna *hash* funkcija je ona u kojoj male razlike u ulaznim podacima rezultiraju u vrlo velikim razlikama u izlaznim podacima. *Hashiranje* je proces dobivanja *hash* vrijednosti.

[14] *Hashiranje* je proces transformacije ulaza proizvoljne dužine i dobivanja *hash* vrijednosti fiksne dužine koja u slučaju primjene algoritma SHA-2 (Security Hashing Algorithm verzija 2) iznosi 256 bita ili 32 bajta ili 64 heksadecimalna znaka.

[15] https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg, pristupljeno 27.1.2019. godine

Indikatori upozorenja na prevaru

FINANSIJSKE PREVARE KAO NAŠA REALNOST:

KAKO IH PREPOZNATI?

Neophodno je razumjeti zašto dolazi do počinjenja prevare, naučiti prepoznati rane signale prevare te imati jasan plan reakcije i odgovora na prevaru

Autorica:
Selma Bušatlić

Udruženje certificiranih istraživača prevare ACFE (*Association of Certified Fraud Examiners*) prevaru definiše kao bilo koji nelegalan akt koji karakterišu varanje, zloupotreba ili povreda povjerenja s ciljem da se dobiju novčana sredstva ili ostvari lična i poslovna korist.

Historija pamti mnoge razrađene i profesionalne prevare koje su, nažalost, imale značajan uticaj na veliki broj ljudi. Izdvojit ćemo neke:

– ***Ponzijeva šema*** (SAD, početak 20. st.) – **Charles Ponzi** bio je jedan od najvećih prevaranata u historiji SAD-a i kreator tzv. *Ponzijeve šeme*: *poduzetnik* objavljuje da radi na veoma profitabilnom projektu koji garantuje visoke prihode i visoku dobit. Novac prikupljen od kasnijih investitora koristi za isplatu ranijim investitorima čime podiže ugled i ostavlja dojam ozbiljne i profesionalne osobe, a zapravo ne ostvaruje nikakav profit. Prevara izlazi na vidjelo kada prevarant nema dovoljno gotovine da investitorima isplati njihove uloge sa obećanim kamatama. Najpoznatija i dosad najveća prevara koja se temeljila na *Ponzijevoj šemi*, izvršena je od strane američkog biznismena **Bernija Madoffa**. Prevara je otkrivena tokom krize 2008. godine kada je postalo jasno da njegova

kompanija uopšte ne zarađuje novac za svoje klijente, već novac novih klijenata koristi za servisiranje starih, a pritom lažira svu dokumentaciju o profitabilnim investicijama.

– ***Enron*** – najveća korporacija 90-ih godina i svojevremeno energetski div SAD-a: ostvarene gubitke kompanija je prikrivala tako što ih nije upisivala u svoje bilanse, nego ih je prebacivala u komplikovani lanac partnerskih filijala, čime ih je sakrivala od ulagača. Prevara je izvršena uz pomoć firme *Arthur Andersen* koja je bila zadužena za knjigovodstvo *Enrona*.
– ***WorldCom*** – američka telekomunikaciona kompanija koja je od 1999. godine umjesto pada dobiti lažno prikazivala njen rast što je uticalo i na povećanje potražnje za dionicama firme te time i na cijenu dionica. Na ovaj način omogućeno je lažno povećanje neto dobiti za oko 3,8 milijarde dolara. Firma je bankrotirala 2002. godine.

Nažalost, ovo su samo neki primjeri finansijskih prevara koje su se događale i gotovo sigurno će se nastaviti događati i u budućnosti.

Indikatori upozorenja na prevaru

U okviru strategije borbe protiv prevara, treba uzeti u obzir činjenicu da se svaka institucija neovisno od svoje veličine, djelatnosti ili države u kojoj se nalazi, suočava sa rizikom prevare.

> *Nije dovoljno biti svjestan da se prevara može desiti, nego je potrebno biti u stanju prepoznati rane indikatore koji mogu signalizirati prevaru, tzv. red flags.*

Stoga nije dovoljno biti svjestan da se prevara može desiti, nego je potrebno biti u stanju prepoznati rane indikatore koji mogu signalizirati prevaru, tzv. *red flags*.

Indikatori upozorenja na prevaru su skup okolnosti koje su po prirodi neuobičajene ili odstupaju od normalnih, odnosno signali koji upućuju na mogućnost postojanja aktivnosti prevare.

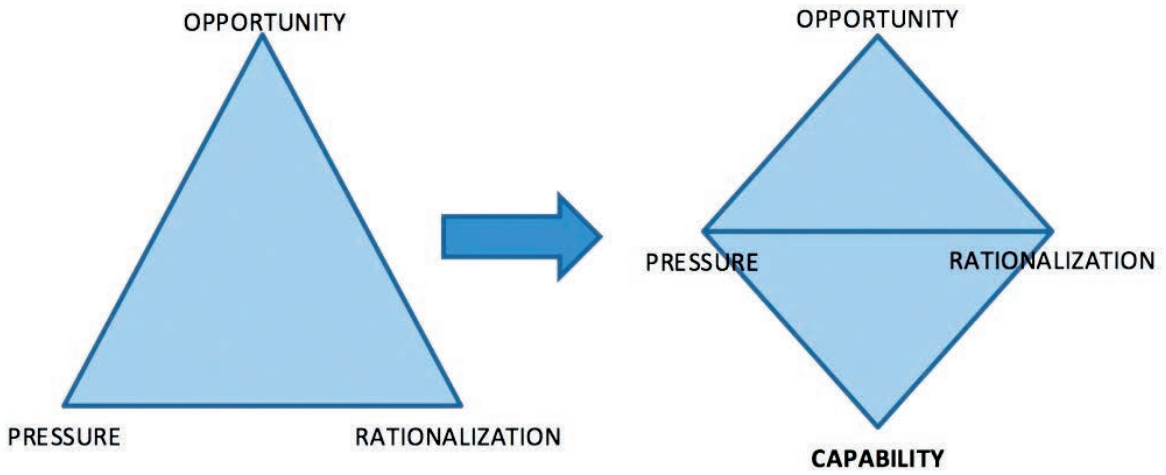
Indikatore ne bi trebalo ignorisati. Istraživanja raznih slučajeva prevara ukazuju na to da su znakovi upozorenja na prevaru bili prisutni, ali nisu bili na vrijeme identifikovani.

Zbog toga je neophodna konstantna edukacija zaposlenih i podizanje svijesti o ranim signalima, kao i jasan plan reakcije i odgovora na prevaru.

Trokut prevare

U cilju pravovremene detekcije prevarne radnje, neophodno je razumjeti zašto dolazi do počinjenja prevare. Kriminolog **Donald R. Cressey** razvio je teoriju prema kojoj svaka prevara ima tri zajednička faktora: pritisak, priliku i opravdanje/racionalizaciju. Zajedno čine tzv. *Trokut prevare*.

– ***Pritisak:***
Prvi faktor trokuta prevare je *motiv* počinitelja. Uobičajena motivacija potiče od finansijskog pritiska: ostvarenje poslovnih planova, statusnih simbola, bolest u porodici, razni oblici ovisnosti i sl. Zbog navedenih potreba i nemogućnosti da se istim udovolji na zakonit način, uz



**ACFE (Association of Certified Fraud Examiners)*

postojanje ostalih elemenata trokuta prevare, osoba se odlučuje na počinjenje prevarne radnje.

– ***Prilika***

Prema teoriji Donalda Crasseya, počinitelji uvijek imaju znanje i mogućnost za realizaciju prevare. Prevara će nastati kada osoba ima motivaciju počiniti prevaru te uz to pronalazi i način na koji to može izvesti, a da ne bude otkrivena.

– ***Opravdanje/ racionalizacija***

Postoje dva aspekta racionalizacije: *prvi* – počinitelj je siguran da je mogućnost da prođe nekažnjeno veća od šanse da bude otkriven, a *drugi* – počinitelj sam sebi opravdava svoje postupke uvjeravajući se da, pod okolnostima u kojim se nalazi, nema drugog izlaza. Ubjeđuje sebe da novac ili imovinu koju otuđuje zapravo samo posuđuje i da će je vratiti u kratkom roku ili se vodi idejom da nikoga ne povređuje svojim postupcima. Zanimljiva je činjenica da racionalizacija omogućava da čak poštene i moralne osobe počine prevaru. Statistike su pokazale da čak 93% počinitelja prevare nije imalo kriminalni dosije.

Pojedini autori smatraju da trokut prevare treba nadopuniti sa sposobnošću, kao četvrtim elementom potrebnim za počinjenje prevare. *Trokut prevare* tako postaje *Dijamant prevare**.

Sposobnost u navedenom smislu podrazumijeva inteligenciju potrebnu za osmišljavanje prevare, sposobnost potrebnu za daljnje prikrivanje prevare, vještinu prisile koju prevarant koristi da sučesnike potakne na prikrivanje prevare te učinkovito laganje i otpornost na stres.

Pravilo 10-80-10

Jedna od novijih teorija u oblasti prevencije i borbe protiv prevara donosi nam pravilo 10-80-10. Ovaj princip, koji svoje temelje pronalazi u dugogodišnjim istraživanjima u oblasti kriminologije, na osnovu klasifikacije stanovništva i vjerovatnoće izvršenja prevarne radnje, populaciju dijeli u tri grupe:

- 10% stanovništva nikada neće počiniti prevaru. To su osobe koje će uvijek pronaći način da otplate dugove i da na zakonit način zadovolje svoje potrebe za finansijskim sredstvima;
- 80% stanovništva se može kretati u bilo kojem smjeru. To su osobe koje bi mogle počiniti prevaru, zavisno od pritiska kojem su izloženi i načina na koji racionaliziraju određenu priliku;
- 10% stanovništva će sigurno počiniti prevaru ukoliko im se za to ukaže prilika.

U cilju pravovremenog sprečavanja i otkrivanja prevare, od ključne važnosti za firmu, njene vlasnike i dioničare je redovno praćenje ranih signala i upozorenja na prevaru, razvijanje adekvatnih sistema internih kontrola, konstantno educiranje uposlenika te, u slučaju detekcije prevare vodeći se principom *nulte tolerancije na prevaru*, inicirati koordinirane i pravovremene istrage nadležnih tijela što će za rezultat imati provođenje odgovarajućih kaznenih mjera kao i sankcija za počinioce prevare. ■

Internet of Things – Internet of Everything – Internet of Threats

KAKO STOJE STVARI SA *INTERNETOM STVARI*

Budućnost nam donosi povezanost digitalnog i fizičkog svijeta kakvu nam je do sada bilo nemoguće i zamisliti. Internet stvari zahtijeva od nas da mijenjamo naša shvatanja kako se živi život i kako se vodi posao, mijenja naš svijet, olakšava nam život, povećava komfor i kvalitet života, omogućava dijeljenje informacija, povjerenje i interakcije sa svijetom...

Kako će Internet stvari uticati na bankarsko poslovanje? Na koji način će banke pratiti tempo i složenost nove tehnologije i ovih nezaustavljivih promjena?

Autorica:
Sanela Vrana

Bilo koji fizički uređaj povezan na internet postaje *pametni uređaj*. Ideja *online* povezivanja, komunikacije i interakcije fizičkih uređaja vodi nas do pojma ***Internet of Things*** (IoT) ili *Internet stvari*. Ako krenemo od pametne četkice za zube, preko pametnih satova i ostale nosive ili čak implantirane tehnologije, pametnih kućanskih aparata, kao npr. kuhala za vodu, televizora, frižidera koji upravljaju nabavkom namirnica, pa do automobila, termostata, sigurnosnih sistema, cijelih pametnih kuća ili čak pametnih gradova, vidimo da se radi o prekretnici u digitalnom svijetu koja će uticati na sve i svakoga. Navedimo primjere tri vida interakcija koje se već sada odvijaju na internetu:

- **uređaj – uređaj** (komunikacija senzora i servera u svrhu praćenja sistema u realnom vremenu),
- **čovjek – uređaj** (prikupljanje informacija o zdravlju ili aktivnosti korisnika putem nosivih uređaja – *wearables*) i
- **čovjek – čovjek** (društvene mreže koje, mada funkcionišu uz pomoć mrežne infrastrukture i učinkovitih algoritama, služe za komunikaciju među ljudima).

Uočavate li da se upravo dešava nova revolucija, kako u industriji tako i u svakodnevnom životu - *Internet of Everything (IoE) ili Internet*

svega? A budućnost? Budućnost nam donosi povezanost digitalnog i fizičkog svijeta kakvu nam je do sada bilo nemoguće i zamisliti.

Trebamo li se plašiti *Interneta stvari*

Internet stvari predstavlja mrežu povezanih uređaja ili objekata koji razmjenjuju podatke sa proizvođačem, korisnikom ili drugim povezanim uređajima (snabdjevenim elektronikom, softverom i senzorima), a donosi proizvođačima tehnologije izuzetne poslovne prilike, bolje usluge, učinkovitije procese te veću uštedu energije. *Internet stvari* bit će integrisan u svako tržište koje možemo zamisliti: od zdravstva, energetike, poljoprivrede pa do transporta i skladištenja. Komunikacija uređaja nije promjena sama za sebe - pravu promjenu donosi komunikacija ljudi putem mašina, pa u tom smislu *Internet stvari* postaje medij interakcije među ljudima. Naši digitalni životi predstavljaju prirodni nastavak našeg fizičkog svijeta. A tu se krije i skriveni, ukorijenjeni sigurnosni problem lažnog predstavljanja, krađe identiteta i općenito *cyber* prijetnji.

Upravo glavne karakteristike ove nove digitalne transformacije – obim, raznolikost, brojnost povezanih objekata i mreža, kao i konstantna razmjena osjetljivih informacija – predstavljaju kritičnu slabu kariku i jedinstven izazov u zaštiti privatnosti, zaštiti podataka, sigurnosti i povjerenja. Kako *Internet stvari* postaje sve više dio našeg stvarnog života i dnevnih aktivnosti, tako postaje i primarni cilj za *cyber* kriminal, kome se svakodnevno proširuje polje mogućnosti i djelovanja te čiji se napadi iz dana u dan mijenjaju, prilagođavaju i postaju sveobuhvatniji i sofisticiraniji. *Internet stvari* u fizički svijet donosi rizike i prijetnje koje smo već susretali u industrijskim i poslovnim digitalnim sistemima. Svjesni smo da se više ne radi o uređajima sa ugrađenom elektronikom, nego o *računarima* kojima je pridružen uređaj. Možemo razlikovati potrošačke, komercijalne, industrijske i infrastrukturne pametne uređaje ili objekte. Poseban problem predstavlja pametna komercijalna, industrijska i infrastrukturna tehnologija koju, kao pojedinci, nismo kupili niti odabrali da koristimo, a izloženi smo rizicima koje ona donosi. Uz sve ove rizike i realne opasnosti nije čudno da *Internet stvari – Internet of Things* poistovjećujemo sa *Internetom prijetnji – Internet of Threats*.

> *Upravo glavne karakteristike ove nove digitalne transformacije – obim, raznolikost, brojnost povezanih objekata i mreža, kao i konstantna razmjena osjetljivih informacija – predstavljaju kritičnu slabu kariku i jedinstven izazov u zaštiti privatnosti, zaštiti podataka, sigurnosti i povjerenja.*

Trend – Anything, Anytime, Anywhere

Živjeti bez korištenja povezanih uređaja postaje sve teže, čak i nemoguće. *Internet of Things* zahtijeva od nas da mijenjamo naša shvatanja kako se živi život i kako se vodi posao.

Broj povezanih uređaja već odavno je premašio ukupnu globalnu populaciju ljudi. Kada se gleda po regionima, Kina, sjeverna Amerika i zapadna Evropa će biti vodeće u pogledu upotrebe povezanih uređaja. Prema predviđanjima za 2020. godinu, približavamo se cifri od 50 milijardi povezanih uređaja na internetu, što uz ukupnu populaciju ljudi, koja se primiče broju od 8 milijardi, daje rezultat od približno 6 povezanih uređaja po jednoj osobi. Dok je za mnoge povećavanje broja povezanih uređaja razlog za slavlje, drugi izražavaju svoju zabrinutost jer više povezanih uređaja sa slabim sigurnosnim rješenjima predstavlja veću izloženost rizicima, više slabih tačaka čija se ranjivost može iskoristiti i na taj način čine *Internet stvari* idealnom metom za *cyber* kriminal. Uporedo sa porastom prihoda i ušteda koje nam donosi *Internet stvari*, rastu i troškovi investiranja u sigurnosna rješenja, kao i troškovi štete od *cyber* kriminala. Svi se slažu u jednom: *cyber* sigurnost je goruća tema današnjice.

Dok je za mnoge povećavanje broja povezanih uređaja razlog za slavlje, drugi izražavaju svoju zabrinutost jer više povezanih uređaja sa slabim sigurnosnim rješenjima predstavlja veću izloženost rizicima, više slabih tačaka čija se ranjivost može iskoristiti i na taj način čine Internet stvari idealnom metom za cyber kriminal.

Želimo li napraviti *pametniji* planet

Analizirajući more podataka koje obezbjeđuje ovako veliki broj povezanih uređaja opremljenih različitim senzorima, može se obezbijediti nadzor, upravljanje i ušteda energije, a što rezultira optimiziranjem usluga, smanjenjem troškova, potiče produktivnost i poboljšava kvalitet življenja. Nosiva tehnologija kreira informacije uz čiju pomoć kompanije bolje upoznaju svoje korisnike te im mogu ponuditi personalizirane i kompletnije usluge. Ovi se podaci već danas priznaju u sudnicama širom svijeta, a za

Internet stvari mijenja naš svijet, olakšava naš život, povećava komfor i kvalitet života, omogućava dijeljenje informacija, povjerenje i interakcije sa svijetom.

nosivu tehnologiju kažu da bi mogla postati *crna kutija* ljudskog tijela. *Internet stvari* mijenja naš svijet, olakšava naš život, povećava komfor i kvalitet života, omogućava dijeljenje informacija, povjerenje i interakcije sa svijetom. Samo u transportu, pametni uređaji i infrastruktura štede naše vrijeme i gorivo te smanjuju emisiju štetnih gasova. Tako, uz sve senzore kojima je opremljen naš automobil, putujemo sigurnije i brže se prilagođavamo uslovima u saobraćaju. Koristeći svu ovu tehnologiju, mi na internetu ostavljamo naš digitalni biološki otisak – svoj identitet i svoje digitalne tragove. Tu smo već u dilemi: da li želimo da sve oko nas bude *pametno*? Npr. pametni sat prikuplja podatke o našoj fizičkoj aktivnosti, otkucajima srca, stanju stresa, kondiciji tijela, pravi analizu i izvještava nas.

Šta mislite: od čega će ubuduće zavisiti da li ćemo dobiti više ili niže troškove životnog osiguranja? S druge strane, senzor unutar tijela, koji nadzire organe i tkiva, identifikuje kada je i kolika doza lijeka potrebna, te je *otpušta* na optimalan način – ova pametna tehnologija može spasiti život. Kao što vidimo, dilema ne postoji. Napravimo *pametniji* planet.

Rizik - sve što ima *firmware* može imati i *malware*

Pametni uređaji, povezani na našu kućnu mrežu ili mrežu kompanije, lako mogu biti otvorena vrata za pristup sistemu ili osjetljivim informacijama. Pametni infrastrukturni objekti koji su do jučer bili *offline* sada se suočavaju sa *cyber* napadima koji ih mogu onemogućiti u davanju usluga i uzrokovati kolaps u realnom svijetu. Medicinski implantirani uređaji sa malom tolerancijom na grešku, ukoliko su kompromitovani, mogu ugroziti naš život. S takvim bismo se rizicima mogli susresti ili se neminovno susrećemo. Rizici digitalnog

svijeta u odnosu na fizički svijet postaju obimom sve veći, mobilniji i, u konačnici, globalni. Na primjer, ukoliko ostavite vaša ulazna vrata otključana, male su šanse da

> *Rizici digitalnog svijeta u odnosu na fizički svijet postaju obimom sve veći, mobilniji i, u konačnici, globalni.*

ćete biti pokradeni, to jeste da će lopovi ići od vrata do vrata i provjeravati koja su vrata otključana, ali u *cyber* svijetu bezbroj je vrata i kvalitet njihovih brava provjerava se svakodnevno. Ukoliko imate i dodatnu funkcionalnost da vam se deaktivira alarm pametne kuće onog momenta kada, recimo, otvorite garažna vrata, to je zgodna olakšica za vas kao vlasnika koji je u žurbi, ali *cyber* kriminalci koji mogu *otključati* garažna vrata dobijaju ulaz u cijelu kuću – jer je cijeli alarmni sistem deaktiviran. Čak i u ovom slučaju gdje je riziku izložena cijela kuća, nije problem krađa u realnom svijetu nego mogućnost korištenja

> *Ono što predstavlja novu dimenziju rizika kod povezanih uređaja nije pojedinačni rizik kompromitovanja jednog povezanog uređaja, nego veliki broj povezanih uređaja i nizak nivo sigurnosti kojom su zaštićeni.*

kompromitovanog sistema kao mehanizma za novi *cyber* kriminal. Želimo reći da ono što predstavlja novu dimenziju rizika kod povezanih uređaja nije pojedinačni rizik kompromitovanja jednog povezanog uređaja, nego veliki broj povezanih uređaja i nizak nivo sigurnosti kojom su zaštićeni.

Uočavamo da je pojedinačni rizik malih razmjera lokalizovan na krađu pojedinačnog korisnika (krađa stvari, identiteta, privatnih podataka, novca sa bankovnog računa), dok je rizik korištenja kompromitovanog pametnog uređaja kao dijela *botnet* mreže (mreže inficiranih uređaja koji propagacijom učestvuju u inficiranju novih njima sličnih uređaja) mnogo veći, pa čak i globalnog karaktera, jer omogućava *cyber* kriminal sa velikim posljedicama. U rukama *cyber* kriminalaca *botnet* je veoma moćno oružje – cijela armija. Vlasnik *pametnog uređaja* ne mora uopće biti svjestan da je nosilac ili prenosnik malicioznog koda. Ono što zabrinjava je da su uređaji veoma ranjivi, često bez ugrađenih osnovnih sigurnosnih postavki i bez mogućnosti ažuriranja softvera, kao i činjenica da ih njihovi vlasnici ne vide kao *pametne* uređaje i nisu svjesni rizika koji oni donose.

Internet stvari kao odskočna daska za *cyber* kriminal

U 2016. godini masovni *cyber* napad uzrokovao je nedostupnost velikih internet platformi i servisa. Samo neki od hiljada njih su: *Amazon*, *Airbnb*, *BBC*, *CNN*, *HBO*, *Netflix*, *PayPal*, *Pinterest*, *Reddit*, *Shopify*, *Spotify*, *the New York*

Times, *Tumbir*, *Twitter*.... Ono što je bilo interesantno kod ovog – jednog od najvećih *Distributed Denial of Services* (DDoS) napada, je da su se ovaj put, umjesto računara koji bi generisali masovni promet, koristili milioni povezanih uređaja na internetu kao što su web kamere, video rekorderi, kućni ruteri, printeri, termostati, pa čak i baby monitori. Potvrđeno je da je veliki dio prometa došao sa uređaja koji su bili zaraženi posebnim tipom *malware*-a pod imenom **Mirai**. Uređaji su korišteni da pošalju strahovito veliku količinu prometa na servere kompanije *Dyn* koja pruža infrastrukturne usluge za internetske servise. Napadom na kompanije poput *Dyn*-a pričinjava se više štete nego napadom na bilo koju pojedinačnu internetsku stranicu jer, onesposobivši DNS (*Domain Name System*) servere kompanije *Dyn*, onesposobljavamo takozvanu *telefonsku centralu interneta*, a time i brojne kompanije koje posluju preko interneta. Gubici *Mirai botnet napada* procijenjeni su na 20.000$ do 100.000$ po kompaniji po satu. Kao vojska kojom se upravlja izdaleka, kućni uređaji izveli su seriju *cyber* napada tokom 2016. godine. Jedan od njih oborio je i *Deutsche Telekom* rutere, ostavljajući više od milion klijenata u Njemačkoj bez telefonske ili internet veze. Prvi poznati napad na kritičnu infrastrukturu Njemačke izveli su kućni aparati. Vaš pametni uređaj je mogao biti dijelom ovakvog *cyber* kriminala. Da li trebate biti zabrinuti? Sigurno da trebate. Jer kao što posljedica napada može biti nemogućnost ljudi da pokrenu filmove na *Netflix*-u što uzrokuje neugodnosti, zamislite da vaš uređaj bude dijelom napada na bolnicu i da pri tome životi ljudi budu ugroženi.

> *Kao što posljedica napada može biti nemogućnost ljudi da pokrenu filmove na Netflix-u, pa to uzrokuje neugodnosti, zamislite da vaš uređaj bude dijelom napada na bolnicu i da pri tome životi ljudi budu ugroženi.*

Potreba za efikasnom i učinkovitom *cyber* sigurnošću

Pametni kućni uređaji sada pružaju *cyber* kriminalcima ključeve naših domova. Ukoliko *cyber* kriminalci uspiju prići na daljinu našim pametnim automobilima i njihovim kritičnim sigurnosnim sistemima, mogu ugroziti i naš život, a koliko se proizvođači automobila utrkuju da njihova vozila budu *pametnija*, toliko ona postaju ranjivija. Normalno je da kontrole pametnog uređaja postavlja vlasnik uređaja, ali ukoliko kontrola pređe u ruke *cyber* kriminalaca, a to je često veoma jednostavno kada postoje sigurnosne rupe u sistemu zaštite, onda se otvaraju vrata nizu kriminalnih radnji koje kreću od preuzimanja kontrole nad uređajem, krađe kredencijala, instaliranja *malware*-a, širenja *malware*-a po mreži, pronalaženja i inficiranja novih uređaja – granice ne postoje, tj. granice ovise o namjeri *cyber* kriminalaca i onome što oni žele postići. A *cyber* kriminalci će, u svoju korist, pronaći nove načine kompromitovanja povezanih uređaja za postizanje

> *Ukoliko kontrola pređe u ruke cyber kriminalaca, a to je često veoma jednostavno kada postoje sigurnosne rupe u sistemu zaštite, onda se otvaraju vrata nizu kriminalnih radnji koje kreću od preuzimanja kontrole nad uređajem, krađe kredencijala, instaliranja malware-a, širenja malware-a po mreži, pronalaženja i inficiranja novih uređaja – granice ne postoje, tj. granice ovise o namjeri cyber kriminalaca i onome što oni žele postići.*

svojih ciljeva (od *proxy*-ja za sakrivanje lokacije i *web* prometa, preko iznuđivanja, do trgovine dječijom pornografijom). Između *cyber* kriminalaca postoji i saradnja – mogu imati političke ili finansijske motive, a mogu biti i teroristi, ali u osnovi svi koriste iste alate za postizanje svojih ciljeva. Jedini način za rješavanje tog problema je zatvaranje sigurnosnih rupa u povezanim uređajima.

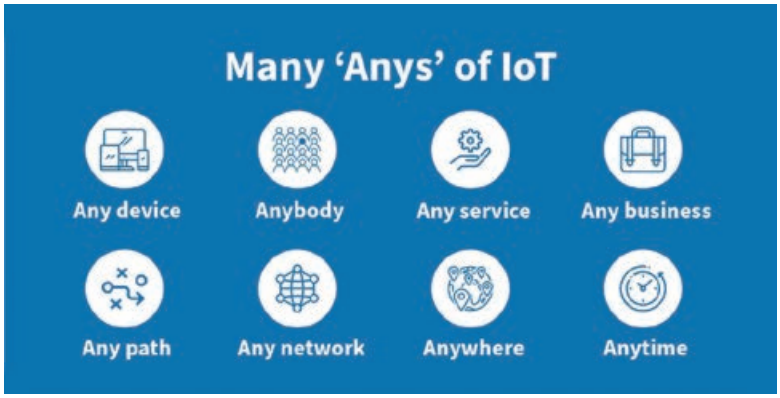
Sigurnosna rješenja, koja će negirati ovakve ciljane napade, potrebnija su nego ikad. Sigurnost industrijskog dijela *Interneta stvari* je čak važnija nego sigurnost korisničkog dijela. Količina podataka sa kojom kalkulišemo je mnogo veća, sistemi zahtijevaju zaštitu u realnom vremenu, a taj zadatak je sve teži jer sistemi rastu veličinom i kompleksnošću. Kako bi funkcionisale što je moguće efikasnije, globalna ekonomija i tržište, a naročito zdravstvo i energetika, počinju se oslanjati na ove tehnologije, pri čemu bi posljedice kompromitovanja ovakvih sistema mogle biti katastrofalne - što dovodi do potrebe za efikasnom i učinkovitom *cyber* sigurnošću.

Sigurnost u fazi dizajna i standardizacija

Pravna regulativa, sigurnosni standardi i najbolje prakse vezane za povezane uređaje treba da budu osnovni okviri za sigurnu proizvodnju i upotrebu povezanih uređaja i pametne infrastrukture. Standardi i najbolje prakse će obezbijediti ne samo sigurnost nego i interoperabilnost povezanih uređaja, a kao najvažnije i povjerenje u IoT industriju.

Cilj proizvođača pametne tehnologije, u domenu sigurnosti, trebao bi biti: kako obezbijediti sigurne uređaje ili senzore, sigurne podatke i njihov siguran prenos preko mreže. Pri tome proizvođači često nemaju nikakvo iskustvo u *cyber* sigurnosti, a trebali bi krenuti od sigurnosti u fazi dizajna, ograničenja kontrole pristupa, minimiziranja podataka koji se prikupljaju i određivanja vremena njihovog čuvanja.

Neki podaci koje generišu IoT sistemi trebaju biti dostupni svima (npr. stanje u saobraćaju ili zagađenje vazduha), a neki podaci (medicinski, npr.) moraju biti zaštićeni od neautorizovanog pristupa i dostupni samo ovlaštenim korisnicima. Kako postajemo sve više ovisni o povezanim uređajima, tako će i pitanje njihove dostupnosti biti sve značajnije (npr. mreža koja bude opsluživala sisteme kao što su medicinski neće smjeti biti nedostupna ni na sekund, a ukoliko dođe do prekida, bit će potrebno što brže ponovno uspostavljanje).



Još jedan zahtjev za proizvođače je da obezbijede razumljiv pregled stanja sigurnosti povezanih uređaja tako da upravljanje sigurnošću bude jednostavno za upotrebu i pristupačno korisnicima. Iz svega navedenog proizilazi da su posljedice s kojima se suočavaju proizvođači veliki troškovi i vrijeme koje je potrebno uložiti u izmjene, a koje su, same po sebi, teško izvodive kada uređaj jednom izađe iz proizvodnje. Zbog toga je potrebno insistirati na sigurnosti još u fazi dizajna samog uređaja.

Paralelno sa ulaganjem u stvaranje novih proizvoda, njihovu digitalizaciju i umrežavanje, treba posvetiti mnogo pažnje i uložiti mnogo sredstava u sigurnost pametnih uređaja jer čak i igračka može biti pretvorena u oružje.

Paralelno sa ulaganjem u stvaranje novih proizvoda, njihovu digitalizaciju i umrežavanje, treba posvetiti mnogo pažnje i uložiti mnogo sredstava u sigurnost pametnih uređaja jer čak i igračka može biti pretvorena u oružje.

Takvi napori u budućnosti će obezbijediti da proizvođači ponude sigurnije uređaje, a što će rezultirati i sigurnijom mrežom povezanih uređaja.

Kako ostati siguran u novom *pametnom* svijetu

Uređaji sa fabrički postavljenim kredencijalima, koji nemaju mogućnost logiranja aktivnosti, omogućavaju *cyber* kriminalcima da provedu što žele i ostanu neotkriveni. Iskorištavanje njihovih ranjivosti može ugroziti korisničke informacije, imovinu korisnika, pa čak i njegovu ličnu sigurnost.

Podizanje svijesti o sigurnosnim prijetnjama i potrebama za poboljšanjem sigurnosti uređaja može donijeti veliku promjenu, kako u edukaciji korisnika o različitim mjerama zaštite koje sami mogu preduzeti, tako i u njihovom pažljivijem odabiru i rukovanju pametnim uređajima.

Minimiziranje rizika vezanog za pametne uređaje počinje sa pametnom kupovinom uz mjere predostrožnosti (provjerite da li uređaj ima osnov-

Od baby monitora do pametnog sata - pametni uređaji su rudnik zlata za proizvođače i vjerujte da im vaša sigurnost nije bila na prvom mjestu pri njihovoj proizvodnji.
Zato birajte proizvođače na koje možete računati i koji se proaktivno odnose prema sigurnosti.

ne sigurnosne postavke kao što je *password*). Od baby monitora do pametnog sata – pametni uređaji su rudnik zlata za proizvođače i vjerujte da im vaša sigurnost nije bila na prvom mjestu pri njihovoj proizvodnji. Zato birajte proizvođače na koje možete računati i koji se proaktivno odnose prema sigurnosti. Promijenite fabrički postavljeni *password*, koristite *jake passworde*, napravite šestocifrene PIN-ove, uradite *ažuriranje softvera* ukoliko je moguće, isključite uređaj sa interneta ukoliko ga ne koristite te ga redovno isključujte sa napajanja (da bi se obrisao *malware* koji je eventualno u memoriji uređaja), a na prvom mjestu zaštitite svoju kućnu mrežu da *malware* ne može ni ući u nju. Ukoliko uređaj ima više korisnika, ograničite njihov broj i obezbijedite da svaki krajnji korisnik ima svoj *password*.

Najviše što možete učiniti za sigurnost svog uređaja i svoje mreže je *enkriptovani tunel* prema internetu koji će vam obezbijediti privatnu, sigurnu i anonimnu konekciju.

Kada ste učinili sve što je u vašoj moći da zaštitite svoju mrežu, uređaje, pa i svoju ličnu sigurnost, možete početi uživati u dobrobitima novog *pametnog* svijeta.

Internet stvari – izazov za banke

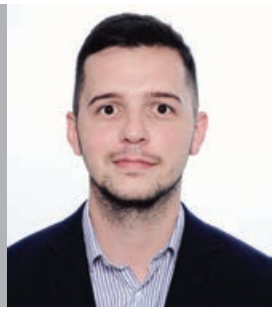
Kako će *Internet stvari* uticati na bankarsko poslovanje? Na koji način će banke pratiti tempo i složenost nove tehnologije i ovih nezaustavljivih promjena? Ne znamo šta će budućnost donijeti, ali znamo da već u ovom trenutku *Internet stvari* za banke znači bolju povezanost

> *Banke su na izvoru informacija i u stanju su da bolje razumiju ili čak predvide potrebe i želje klijenata te tako poboljšaju njihovo sveukupno iskustvo, a uz sve to zadržavajući privatnost klijenta.*

s klijentima. Uporedo s većom upotrebom vještačke inteligencije, pametnih uređaja ili objekata koji iniciraju *machine-to-machine* (M2M) transakcije, te mnoštva drugih pametnih uređaja koji obavljaju najrazličitije transakcije za svoje korisnike, do izražaja dolazi i centralna, aktivna uloga banaka. Naime, bilo kakva interakcija između kupaca/korisnika i prodavača/dobavljača zahtijeva finansijsku transakciju. Ova činjenica stavlja banke u centar svakog IoT sistema te banke počinju uviđati da IoT tehnologija donosi višestruke koristi. Banke su na izvoru informacija i u stanju su da bolje razumiju ili čak predvide potrebe i želje klijenata te tako poboljšaju njihovo sveukupno iskustvo, a uz sve to zadržavajući privatnost klijenta. S druge strane, klijenti koriste sve dobrobiti pametne tehnologije, a u interakciji sa bankama i olakšice biometrije kao jednostavnog načina autorizacije. Njihovo tijelo postaje njihova kreditna kartica. Identifikacija otiskom prsta, tj. korištenje unikatnog podatka za autorizaciju transakcije, smanjuje i mogućnost prevara. Ono što je neophodno da banke zadovolje u ovoj eri velikih tehnoloških promjena je visoki nivo sigurnosne tehnologije koja mora biti osnova svake inovacije i svake donesene odluke. ■

PREVARE PUTEM ONLINE KANALA PLAĆANJA

S obzirom na konstantno povećanje trenda online kupovine, prevaranti ne mogu odoljeti zloupotrebi podataka klijenata i njihovih platnih kartica pa su tako prevare putem online kanala plaćanja u velikom porastu



Autor:
Ivan Pranjić

Većina potencijalnih klijenata koristi *online* kanale plaćanja, bez obzira gdje se geografski nalaze. Sve više ljudi prilikom kupovine namještaja, odjevnih predmeta ili hrane preferira online kanale plaćanja umjesto tradicionalnog odlaska u trgovinu. Cijeli svijet se sve više oslanja na online kupovinu upravo zbog njene jednostavnosti. Prema istraživanju portala *Statista*, predviđa se da će globalno tržište online kupovine narasti na 4,9 triliona američkih dolara do 2021. godine, a do 2022. godine se očekuje da će online prodaja činiti čak 17% globalne potrošačke prodaje. S obzirom na rastući broj korisnika online kanala plaćanja te online spašavanja podataka o platnim karticama, prevaranti ne mogu odoljeti zloupotrebi podataka klijenata i njihovih platnih kartica pa su tako prevare putem online kanala plaćanja u velikom porastu.

Šta su prevare prilikom online plaćanja i zbog čega su tako česte?

Prije nego što objasnimo kako se događa prevara prilikom online plaćanja, važno je saznati na kojim plaćanjima se prevare dešavaju. Razlikujemo dvije vrste plaćanja:

> *Plaćanje bez fizičke upotrebe kartice uglavnom se događa na internetu. Ovaj tip online plaćanja je glavni fokus prevaranta jer oni čak fizički i ne trebaju imati ispravnu karticu, već su za plaćanje potrebni samo detalji kartice koji mogu biti pohranjeni digitalno.*

– *ukoliko je kartica prisutna*, odnosno kada je kartica fizički korištena za kupovinu nečega u trgovini, restoranu ili tržnici i
– *ukoliko kartica nije prisutna*, odnosno kada se koriste isključivo detalji kartice, ali sama kartica fizički nije korištena od strane kupca.

Plaćanje bez fizičke upotrebe kartice uglavnom se događa na internetu. Ovaj tip online plaćanja je glavni fokus prevaranta jer oni čak fizički i ne trebaju imati ispravnu karticu, već su za plaćanje potrebni samo detalji kartice koji mogu biti pohranjeni digitalno. Također, prevarantima je mnogo lakše izvršiti zloupotrebu jer je jako teško da prodavac zna ko je stvarni kupac.

Kako nastaju prevare na online kanalima plaćanja i koje su tehnike prevencije?

Postoje različite vrste prevara prilikom online plaćanja, a jedan od najjednostavnijih primjera je tzv. *prijateljska prevara* koja se događa kada stvarni kupac primi robu koju je naručio, ali tvrdi da istu nije primio te podnosi zahtjev za povrat novca od banke. Većina online prevara prilikom plaćanja podrazumijeva krađu identiteta na način da:

1. kriminalci ukradu informacije o imaocu kartice kroz *skimming* web stranica za online plaćanja ili kupovinom na crnom tržištu interneta;
2. prevarant koristi podatke o ukradenoj kartici kako bi oponašao stvarnog korisnika kartice te kupovao stvari online;
3. online prodavac smatra da je kupovina legitimna, obrađuje plaćanje i dostavlja robu prevarantima;
4. stvarni vlasnik kartice vidi realizovanu transakciju sa računa i kontaktira banku radi naknade štete pa tako online prodavac bude pogođen sa povratom naknade plus drugim troškovima.

Kao kod bilo koje vrste kriminala, aktivnosti prevencije i detekcije online prevara su unaprijeđene vremenom. Tako u kontekstu online platnih prevara možemo reći da razlikujemo tri stuba za otkrivanje prevara. To su:

- Definisana pravila,
- *Machine learning* i
- Analiza trenda

Definisana pravila

Moderni, agilni modeli za otkrivanje prevara su učinili da se konvencionalni modeli zaštite čine zastarjelim i teškim za održavanje. Ali to ne znači da je primjena pravila definitivno zastarjela tehnika otkrivanja i prevencije od prevara. U mnogim situacijama neophodno je direktno utjecati na prevenciju, a pravila podrazumijevaju sredstvo za intervenciju. Pravila su još uvijek relevantan dio alata za prevenciju prevara koji nadopunjuju napredne tehnologije, pa tako ćemo prezentirati i situacije u kojima upotreba pravila još uvijek može biti učinkovita:

– ***Brzo djelovanje u cilju zaustavljanja napada*** – koristeći pravila, lica mogu brzo zaustaviti napad dok se isti još uvijek

nije izvršio. Naprimjer, ako se napad može povezati sa određenom lokacijom, lice može lokaciju staviti na crnu listu kako bi spriječilo sva plaćanja sa određenog geografskog područja.

– ***Proaktivno blokirati nove oblike prevara*** – ovlašteno lice može postati svjesno novog trenda u ponašanju pevaranata, ali sistem *machine learninga* se još uvijek nije prilagodio takvom ponašanju pa u toj situaciji lice može proaktivno koristiti pravila kako bi spriječilo nastanak prevare.
– ***Korištenjem pravila omogućujete poslovanje dobrim klijentima*** – važno je istaknuti da se pravila mogu koristiti kako bi se omogućila plaćanja, a ne samo spriječile neželjene i prevarne aktivnosti.
– ***Testiranje pravila*** – testiranje pravila omogućuje vam da napravite novo pravilo i da procijenite njegov utjecaj bez da ga zapravo uključite u sistem. To znači da možete testirati različite kombinacije pravila i vidjeti koja je kombinacija najučinkovitija za ono što pokušavate postići.

Machine learning

Umjesto da se sistem za praćenje i detekciju prevara osla-

> *Modeli machine learninga, analize trenda i jasno definisanih pravila se međusobno osnažuju. Naprimjer, možete naučiti svoj napredni sistem praćenja prevara tako što ćete označiti određeni segment do kojeg se došlo analizom trenda te blokirati plaćanja navedenog segmenta kako bi se spriječio nastanak prevara.*

nja samo na pravila koja daju jednostavne da ili ne odgovore, *machine learning* se oslanja na tradicionalne modele za ocjenu svake transakcije kojoj dodjeljuje niski, srednji ili visoki rizik. Bez obzira što se pravila moraju ručno unijeti, sistemi naprednih tehnologija su proaktivni i prate transakcije i plaćanja u stvarnom vremenu, kombinujući historijske podatke i nove informacije istovremeno. *Machine learning* je automatizovan i vrlo fleksibilan za rukovanje hiljadama transakcija svake sekunde pa se otkivanje prevara radi u milisekundama sa minimalnim utroškom ljudskog faktora.

Analiza trenda

Analiza trenda podrazumijeva *detektivski zid* sa povezanim osumnjičenima, datumima, lokacijama i drugim karakteristikama. Ovakva analiza vam omogućuje da pogledate sve dokaze te istim pridružite sve relevantne činjenice kako biste izgradili potpunu sliku kako izgleda prevarant te tako spriječili buduće prevare putem online plaćanja. Modeli *machine learninga*, analize trenda i jasno definisanih pravila se međusobno osnažuju. Naprimjer, možete naučiti svoj napredni sistem praćenja prevara tako što ćete označiti određeni segment do kojeg se došlo analizom trenda te blokirati plaćanja navedenog segmenta kako bi se spriječio nastanak prevara.

Zaključak

Neophodno je pronaći sistemsko rješenje za otkrivanje prevara koje će pravilno funkcionisati i odgovarati vašim poslovnim potrebama po pitanju brzine i praktičnosti. Moguće je da nakon većeg broja pokušaja i testiranja dostupnih sistema na tržištu, otkrijete da se nijedno rješenje ne uklapa u vaše moderno poslovno okruženje i realno vrijeme online plaćanja te da će biti potrebno da sami razvijete svoj sistem praćenja i prevencije prevara. Ako razmišljate o razvoju vlastitog sistema, prvenstveno provjerite da li znate odgovore na pitanja koja treba postaviti da biste razumjeli šta je ispravno za vaš posao. ■

Od kreativnih zanesenjaka, idealista, istraživača, pasioniranih programera do cyber kriminalaca, zločinaca i vandala

UPOZNAJTE HAKERE

Da li su hakeri mladi koje neko nije dobro odgojio, stručnjaci koji znaju slabosti računarskih sistema i čije znanje treba iskoristiti ili tek obični razbojnici s kojima treba tako i postupati?

Autorica:
Sanela Vrana

Pojam haker

U engleskom jeziku *hack* ima na desetine značenja. U informatičkom žargonu *hack* znači trik, dosjetka, smicalica. Autori trika (*hackeri*) bi trebali, barem nakratko, ostati nepoznati, *hack* bi trebao impresionirati druge, a da im pri tom ne nanese ni najmanju štetu. Ko su hakeri i kako oni sebe doživljavaju? Čak i sami hakeri dali bi različite odgovore na ovo pitanje. Asocijacije koje nam se javljaju pri spomenu riječi haker su *cyber kriminal*, krađa identiteta, prevare, maliciozni programi i sl. Pojam haker ne obilježava nužno informatičara nego osobu koja se pasionirano bavi onim što radi. Ipak, kad kažemo haker, najčešće mislimo na informatičare. Uz pojam haker nepotrebno ide neka mistična aura, doza nepristupačnosti i tajanstvenosti. U principu, svi stručnjaci za računarske sisteme i sigurnost su hakeri - razlika je u namjeri. Pravilno upotrijebljen pojam haker odnosi se na inteligentnog i entuzijastičnog programera koji nastoji stvoriti vrhunski softver i naučiti što više o računarima. Hakeri *stare škole* znaju reći da su *hakirali kada hakiranje nije bilo cool*. Među programerima se riječ haker upotrebljava kao znak poštovanja prema drugom programeru, a ne kao uvreda.

> *Pravilno upotrijebljeni pojam **haker** odnosi se na inteligentnog i entuzijastičnog programera koji nastoji stvoriti vrhunski softver i naučiti što više o računarima.*

Biti haker u današnjem društvu ima negativnu konotaciju. Mediji provode poprilično agresivnu politiku protiv hakera. Ipak, iako ih se nastoji

> *Prikladniji izraz za zlonamjernog hakera je **kreker** (eng. cracker), što znači razbijač ili provalnik, tj. onaj koji neovlašteno pristupa računarskim sistemima sa namjerom krađe podataka, prenosa malicioznog koda, mijenjanja ili brisanja podataka te onemogućavanja sistema.*

opisati kao kriminalce, hakeri nisu kriminalci. Veći dio njih ne nanosi štetu. U rječnicima nailazimo na dvojake definicije: haker kao osoba koja uživa u intelektualnim izazovima i programira sa posebnim entuzijazmom i/ili osoba koja koristi svoje vještine za neovlašten pristup računarskim mrežama i podacima. Prikladniji izraz za zlonamjernog hakera je *kreker* (eng. *cracker*), što znači razbijač ili provalnik, tj. onaj koji neovlašteno pristupa računarskim sistemima sa namjerom krađe podataka, prenosa malicioznog koda, mijenjanja ili brisanja podataka te onemogućavanja sistema.

Profil, osobnosti i navike hakera

Da li su hakeri mladi koje neko nije dobro odgojio, stručnjaci koji znaju slabosti računarskih sistema i čije

znanje treba iskoristiti ili tek obični razbojnici s kojima treba tako i postupati? Teško je razlučiti, a još teže razbiti stereotipe koji vladaju o hakerskoj zajednici. Počinitelji klasičnih zločina često imaju zajedničke osobine i po njima se odvajaju od ostatka stanovništva, dok se hakeri mnogo bolje uklapaju u društvo. Pronaći sličnosti i specifičnosti u njihovim osobnostima i definisati prosječnog pripadnika hakerske zajednice nezahvalan je posao. Oni dolaze iz različitih zemalja, kultura i socijalnih miljea, imaju raznovrsna zanimanja i sklonosti. Zavirimo u rječnik hakerskog žargona ***Jargon file*** kojeg su pisali/stvarali sami hakeri. Hakeri u njemu formiraju poseban vokabular koji koriste za komunikaciju, ali koji također služi za uključenje ili isključenje iz hakerske zajednice (nepoznavanje žargona ili njegova pogrešna upotreba definira hakera kao stranca ili u žargonu kao ***suit*** – haker koji nosi neudobnu odjeću ili odijelo, tj. haker koji to nije). *Jargon file* je naslijeđe hakerske kulture, a u svom dodatku ima profil prosječnog hakera kojeg ćemo pokušati vizualizirati.

Hakeri su većinom bijelci ispod 30 godina i muškog spola. Žene hakeri su također cijenjene, čak i više nego u ostalim tehničkim disciplinama. Hakeri su obično mršave konstitucije, ali u tom pogledu mogu se sresti obje krajnosti. Svijetle su puti i ne bave se sportovima, pogotovo ne timskim sportovima. Jednostavno su obučeni u

> *Psihološki profil podrazumijeva izuzetno inteligentne individue, motivisane novim saznanjima, radoznale, kreativne, sa analitičkom inteligencijom i značajnom sposobnošću uočavanja detalja. Njihovo polje znanja i interesovanja je široko; ne poštuju nikakve ograde niti autoritete; odbacuju društvene norme i ne vole monotone i obavezujuće poslove koji su sastavni dio svakodnevnog života.*

majice kratkih rukava, nerijetko crne boje, sa humorističnim aplikacijama ili aplikacijama iz računarskog svijeta. Žene hakeri su bez vidljive šminke ili ne koriste nikakav make-up. Psihološki profil podrazumijeva izuzetno inteligentne individue, motivisane novim saznanjima, radoznale, kreativne, sa analitičkom inteligencijom i značajnom sposobnošću uočavanja detalja. Njihovo polje znanja i interesovanja je široko; ne poštuju nikakve ograde niti autoritete; odbacuju društvene norme i ne vole monotone i obavezujuće poslove koji su sastavni dio svakodnevnog života. Motivacija im u većini slučajeva nije novac. Hakere njihov posao oduševljava te ih ujedno puni pozitivnom energijom. Bude se u rano poslijepodne jer svakodnevno programiraju do duboko u noć. Privlači ih izazov, individualni su i teško se identifikuju sa drugim ljudima. Iz tog razloga znaju biti arogantni i nestrpljivi. Religijski su ateisti, agnostici, politički liberalno orijentirani, ne žele izabrati ni lijevu ni desnu stranu te su tolerantni po pitanju seksualnog opredjeljenja. Ljubitelji su naučne fantastike, vole muziku, video igrice i sve vrste intelektualnih igara, a čitajući rječnik hakerskog žargona, zaključuje se da hakeri vole igre riječima i veoma kreativno upotrebljavaju jezik. Kod profiliranja hakera bilo bi potrebno uzeti u obzir i njihovu podjelu prema računarskim i hakerskim vještinama, sposobnostima, znanju i iskustvu. Tek tada bismo određene osobine mogli pobliže vezati za određene vrste hakera.

Hakerska etika

Hakerska etika je naziv za jedan načelno strastven odnos prema radu koji se razvija u našem informacijskom dobu, a u skladu s tim haker je stručnjak ili entuzijast bilo koje vrste. Prema knjizi o hakerskoj kulturi američkog novinara **Stevena Levyja** – *Hakeri: Heroji računarske revolucije*, osnovni princip hakerske etike je slobodan, tj. neograničen i potpun pristup računarima i svemu što vas može naučiti o načinu na koji svijet funkcioniše. Također, **Eric S. Raymond**, softveraš i jedan od autora štiva *Jargon File*, definiše etičku dužnost hakera kao razmjenjivanje stručnog znanja s drugima i pisanje slobodnog softvera kako bi, kad god je

> *Etička dužnost hakera je razmjenjivanje stručnog znanja s drugima i pisanje slobodnog softvera kako bi, kad god je to moguće, olakšali pristup informacijama i računarima.*
>
> *(Eric S. Raymond, Jargon File)*

to moguće, olakšali pristup informacijama i računarima. Neslaganja među samim hakerima nastaju kod vjerovanja da je rušenje sistema u svrhu zabave i istraživanja etički prihvatljivo sve dok haker ne počini nikakvu krađu, vandalizam ili kršenje povjerljivosti. **Himanen Pekka**, najmlađi doktor nauka u Finskoj, autor štiva *Hakerska etika i duh informacijskog doba*, koje je doživjelo šesnaest svjetskih izdanja u samo godinu dana, prikazuje hakere kao ljude koji se pasionirano bave onim što vole: "Oni su idealistički pioniri, istraživači, radosni pustolovi digitalnog doba, istinski arhitekti nove ekonomije. Oni stvaraju ne samo vrhunsku tehnologiju nego i novu radnu i životnu etiku otvorenosti, uključivanja i saradnje." To znači da su hakeri osobe koje vole, kroz pozitivnu znatiželju, istraživati granice onoga što je moguće, a što često uključuje prepravljanje postojećih hardverskih i softverskih rješenja kako bi se dobila nova funkcija ili otključala neka skrivena.

> *"Hakeri su idealistički pioniri, istraživači, radosni pustolovi digitalnog doba, istinski arhitekti nove ekonomije. Oni stvaraju ne samo vrhunsku tehnologiju nego i novu radnu i životnu etiku otvorenosti, uključivanja i saradnje."*
>
> *(Himanen Pekka, Hakerska etika i duh informacijskog doba)*

Etički hakeri se bore protiv virtualnih kriminalaca tako što otkrivaju pogreške u računarskom sistemu (u ime vlasnika i uz njegovu dozvolu) kako bi mogli otkloniti sigurnosne nedostatke. U žargonu se etički hakeri nazivaju *bijelim šeširima* (analogija sa starim vestern filmovima u kojima su *dobri* kauboji uvijek imali bijele šešire). Za razliku od etičkih hakera, krekeri kao zlonamjerni hakeri se nazivaju *crnim šeširima*.

> *"Etički hakeri se bore protiv virtualnih kriminalaca tako što otkrivaju pogreške u računarskom sistemu (u ime vlasnika i uz njegovu dozvolu) kako bi mogli ukloniti sigurnosne nedostatke."*

Sivi šeširi su između dobrih i loših momaka, što često zavisi od same prilike. Oni vjeruju da to što rade, rade u interesu drugih. Često provaljuju u računarske sisteme iz zabave i bez dopuštenja, pronalaze propuste u sistemu i prijavljuju ih vlasnicima te najčešće traže naknadu za svoj trud. Od *bijelih šešira* ih odvaja to što u sisteme provaljuju bez dopuštenja vlasnika, što se smatra kaznenim djelom. Danas na internetu možemo pronaći i definicije *crvenih šešira* (savjetnici koji nude probijanje u sisteme kao dio svojih usluga), *plavih šešira* (osobe izvan domena računarske sigurnosti unajmljene za testiranje sistema prije njegovog objavljivanja) i *zelenih šešira* (oni koji tek počinju učiti o hakiranju). Na kraju, potrebno je reći da postoji tanka linija između raznih vrsta hakera. Mnogi hakeri kroz život promijene boje svojih *šešira*. Prilike u hakerskom svijetu promijenile su se u zadnjih desetak godina pa se hakerima puno više isplati nositi *bijeli šešir* umjesto *crnog*.

Motivacija

Pričali smo o znatiželji kao motivaciji *hakera stare škole* te spomenuli da novac nije njihov najčešći motiv. Kada govorimo o *cyber* kriminalcima, zabava kao motiv ne izostaje (jer većina *cyber* kriminalaca smatra da ih nikada neće uhvatiti), ali najčešći motiv za *cyber* kriminal je novac. Emocije, kao čest motiv kod *cyber* kriminala, nalazimo kao i u svakoj vrsti klasičnog kriminala počinjenog u izuzetno emotivnom stanju iz bijesa ili ljubomore, s tim da kod *cyber* kriminala postoji i doza anonimnosti koja dozvoljava da se emocionalna osveta rasplamsa zbog osjećaja da se za ponašanje

> *„Kada govorimo o cyber kriminalcima, zabava kao motiv ne izostaje (jer većina cyber kriminalaca smatra da ih nikada neće uhvatiti), ali najčešći motiv za cyber kriminal je novac."*

neće odgovarati. Političke rasprave i religijska neslaganja znaju dovesti do obračuna putem *cyber* kriminala, dok seksualni motivi često prelaze iz *cyber* kriminala u maltretiranja, ucjene, dječiju pornografiju, pa i u silovanje ili pedofiliju kao teške zločine.

Zlatna povijest hakera

Aktivnosti hakera, pa tako i razumijevanje pojma haker, mijenjale su se kroz historiju te kroz različite interpretacije. Pedesetih godina prošlog stoljeća pojam haker značio je da se odlično razumijete u računare. Hakeri su se računarima bavili strastveno, entuzijastično ili čak opsesivno, bili su ponosni zaljubljenici i poštovani izumitelji nove tehnologije. Baveći se hakiranjem i unapređivanjem programa, uspjeli su stvoriti i nove programe. Operativni sistem UNIX nastao je na taj način. Njegovi tvorci, **Dennis Ritchie** i **Ken Thompson**, ostat će upamćeni kao povijesna imena računarske tehnologije. Dennis Ritchie je ujedno i autor popularnog programskog jezika C. Hakeri stvaraju mogućnost da nove stvari dođu na svijet. Ne mora značiti da su te nove stvari uvijek dobre, ali otvaraju nova vrata i pružaju nove vidike, bilo da se radi o umjetnosti, nauci, filozofiji ili kulturi. U zlatnoj povijesti hakera ostat će zabilježeni i genijalci kao što je **Richard Stallman**, pokretač *Fondacije za slobodni softver* i *Linus Torvalds*, koji je 1991. godine napravio svjetski popularani operativni sistem LINUX.

> *Pedesetih godina prošlog stoljeća pojam haker značio je da se odlično razumijete u računare. Hakeri su se računarima bavili strastveno, entuzijastično, ili čak opsesivno, bili su ponosni zaljubljenici i poštovani izumitelji nove tehnologije.*

Zloupotreba hakerskog znanja

Hakiranje se nastavilo unapređivati i razvijati, a uporedo s tim razvijala se i zloupotreba hakerskog znanja. Već šezdesetih i sedamdesetih godina dvadesetog stoljeća pojam haker počinje se vezati za osobe koje bez dozvole pristupaju računarskim sistemima i mrežama. Jedan od prvih zloglasnih hakera - **John Draper**, nadimka *Cap'n Crunch*, uspio je 1971. godine hakirati telefonsku mrežu američkog telefonskog operatera AT&T i otkrio način besplatnog telefoniranja korištenjem zviždaljke iz *Cap'n Crunch* žitnih pahuljica. U proizvodnji i prodaji *plavih kutija* za hakiranje telefonskog sistema pridružuju mu se i **Steve Wozniak** i **Steve Jobs** - budući osnivači kompanije *Apple*. Početkom 1980-ih godina pojavljuju se osobni računari, a paralelno s tim dolazi do velikog rasta hakerske populacije i počinju se formirati prve hakerske grupe, između kojih će se uskoro voditi i pravi *cyber ratovi*. Prvi hakerski časopis

> *Šezdesetih i sedamdesetih godina dvadesetog stoljeća pojam haker počinje se vezati za osobe koje bez dozvole pristupaju računarskim sistemima i mrežama.*

> *Od devedesetih godina prošlog stoljeća hakeri se počinju baviti ilegalnim radnjama. Malo koji haker ostaje dobronamjeran, pa se tako i sam pojam počinje vezati za cyber kriminalca.*

The Hacker Quarterly, kojeg nazivaju *hakerskom biblijom*, počinje izlaziti 1984. godine. Godinu 1988. nazivaju *godinom Morrisovog crva*. **Robert Morris** je bio prvi optuženi haker. Tada student američkog univerziteta *Cornell*, Robert je napravio samoreproducirajući računarski virus, tzv. crv (eng. worm), i njime zarazio i srušio preko 6000 računara, a time i cijeli internet na dva dana (u to vrijeme *Arpanet* – preteča *interneta*). Od devedesetih godina prošlog stoljeća hakeri se počinju baviti ilegalnim radnjama. Malo koji haker ostaje dobronamjeran pa se tako i sam pojam počinje vezati za *cyber* kriminalca. Brojni hakeri tog doba su završili na sudu, a neki od poznatijih su: **Kevin Mitnick**, **Vladimir Levin** i **Kevin Poulsen**. Kevin Mitnick, kao najpopularniji haker tog vremena i najtraženiji *cyber* kriminalac sa FBI potjernicom, danas je, poslije više odsluženih kazni, vlasnik konsultantske kompanije i govornik na temu računarske sigurnosti. Sva navedena imena iz povijesti hakera, bez obzira na činjenicu da su neki od njih bili u sukobu sa zakonom, predstavljaju genijalce računarske ere.

Golobradi prijestupnici

Prosječna dob *cyber* kriminalaca pala je na 17 godina, a stručnjaci kažu da je svaka nova generacija vještija u korištenju tehnologije. Mladi hakeri svoj talenat otkriju još u predškolskom uzrastu. Sve počinje kao igra ili hobi – nekada se razvija u pravcu kriminala, a nekada u pravcu sigurnosti računarskih sistema. **Kristoffer Von Hassel** je kao petogodišnji dječak otkrio sigurnosni propust *Microsoft Xbox live* sistema za igranje igrica. Kanadski tinejdžer **Michael Calce**, poznatiji pod imenom *MafiaBoy*, kao četrnaestogodišnjak je u februaru 2000. godine izveo seriju DDoS napada i uspio srušiti vrhunske pretraživače i web kompanije kao što su *Yahoo*, *eBay*, *Amazon*, *CNN*. Ostao je zapamćen kao najgori maloljetni internetski kriminalac jer se šteta mjerila milionima dolara.

Za tinejdžere je hakiranje najčešće zabava jer žele vidjeti mogu li oni to učiniti, a ponekad vrsta otpora ili borbe. Zarada i novac im nisu važni, motivacija im je dokazivanje pred prijateljima te rješavanje

> *Za tinejdžere je hakiranje najčešće zabava jer žele vidjeti mogu li oni to učiniti, a ponekad vrsta otpora ili borbe. Zarada i novac im nisu važni, motivacija im je dokazivanje pred prijateljima te rješavanje tehničkih problema. Oni malo stariji bore se protiv špijunaže i kontrole interneta. Jedno im je zajedničko: ne razmišljaju o mogućim posljedicama svog djelovanja i nisu svjesni štete koju mogu prouzročiti dok se ne suoče sa pravosudnim organima.*

> *Nije rijedak slučaj da se po odsluženju kazne mladi prestupnici preorjentišu na tzv. etičko hakiranje. Shvate da su stručnjaci za računarsku sigurnost izuzetno traženi te da danas postoje brojne legalne mogućnosti za dokazivanje i zaradu.*

tehničkih problema. Oni malo stariji bore se protiv špijunaže i kontrole interneta. Jedno im je zajedničko: ne razmišljaju o mogućim posljedicama svog djelovanja i nisu svjesni štete koju mogu prouzročiti dok se ne suoče sa pravosudnim organima.

Prvi maloljetnik koji je odslužio kaznu za *cyber* kriminal u SAD-u bio je **Jonathan James**. Sa samo 15 godina provalio je u računarski sistem NASA-e i prouzrokovao tronedjeljnu blokadu računara povezanih sa Međunarodnom svemirskom stanicom. Kao da to nije bilo dovoljno, upao je i u Pentagonov sistem zaštite od nuklearnog, biološkog, hemijskog i drugih vidova napada na SAD te instalirao *trojanskog konja*, čitao mailove i otkrio korisnička imena i lozinke službenika. Današnji hakeri su sve mlađi, a njihovi postupci sve opasniji. Nije rijedak slučaj da se po odsluženju kazne mladi prestupnici preorijentišu na tzv. *etičko hakiranje*. Shvate da su stručnjaci za računarsku sigurnost izuzetno traženi te da danas postoje brojne legalne mogućnosti za dokazivanje i zaradu.

Školovanje i zarada etičkih hakera

Treba li etičko hakiranje učiti u školama i na fakultetima? Da li je maliciozno učiti mlade ljude ovakvim vještinama? Nije teško dati odgovor na ovo pitanje. Pošto se radi o etičkom hakiranju, kojim se spašavaju mnogi pojedinci i organizacije od propusta i pogrešaka u računarskom sistemu, uz dozvolu vlasnika i bez pričinjene štete – etičko hakiranje je korisno za naučiti. Škola bi trebala pružiti isplativu vještinu, a svako ponaosob treba da se ponaša u skladu sa zakonom. Ukoliko neko i napravi nešto ilegalno, isključivi krivac je sama osoba. Izazovimo djecu da budu hakeri u svom pozitivnom značenju te riječi: da nijedan posao za njih ne bude težak i dosadan, nego da ga rade sa entuzijazmom, da to bude njihova strast, istraživanje, igra i kreativnost.

Velike kompanije traže etičke hakere, daju im dopuštenje da probaju razne vrste napada kako bi probili sigurnosnu zaštitu računarskog sistema te za takve upade i otkrivanje ranjivosti plaćaju ozbiljne svote novca, a kompanija spozna ranjivosti sistema i tim lakše ih može popraviti. Raspisuju se i nagrade za otkrivanje *bagova* u kodovima programa. Pronaći *bag* koji do sada nije uočen velika je rijetkost i može da dovede do isplate velikih iznosa (u stotinama hiljada dolara) što služi kao podstrek za mlade. Postoje kompanije koje

> *Izazovimo djecu da budu hakeri u svom pozitivnom značenju te riječi: da nijedan posao za njih ne bude težak i dosadan, nego da ga rade sa entuzijazmom, da to bude njihova strast, istraživanje, igra i kreativnost.*

funkcionišu kao agenti za provjerene etičke hakere. Povezuju etičke hakere sa kompanijama koje žele da otkriju svoje sigurnosne propuste, verifikuju obavljeni posao te se staraju se o povjerljivosti klijenata. *HackerOne*, jedna od najvećih kompanija za lov na *bagove*, u evidenciji ima više od 600.000 tzv. *bijelih hakera* i do sada je isplatila više od 100 miliona dolara u svrhu nagrada.

Kako kompanije postaju svjesnije da rizik od nedovoljnog rada na pronalaženjima ranjivosti može dovesti do potencijalnog hakerskog napada, tako i nagrade za *bagove* postaju sve veće. *Google* je potrošio rekordne sume na nagrade za etičke hakere. Tokom 2019. godine na nagrade je potrošeno čak 6,5 miliona dolara, što je duplo više od 3,4 miliona u 2018. godini. Ovaj primjer slijede i druge kompanije, kao što su *Microsoft*, *Facebook*, *Apple*, *Tesla*, itd. Profesija etičkog hakera je u ekspanziji i oni mogu veoma dobro zarađivati za život.

Hakeri danas

Stvorivši tehnologiju, stvorili smo i jedan posve novi virtuelni svijet – *cyber space*. Vještina i znanje o upotrebi tehnologije, koja je posrednik između fizičkog i virtuelnog svijeta, razlikuje se od čovjeka do čovjeka. Hakeri su ti genijalci računarske revolucije koji vladaju *cyber spaceom*. Kao što je današnja civilizacija nezamisliva bez računara i interneta, tako je nezamisliva i bez hakera. Hakera i hakerskih napada ima više nego ikad. Danas postoje i legalne kompanije koje javno nude hakerske usluge. Italijanska kompanija *Hacking Team* legalno prodaje usluge informatičke špijunaže korporacijama, obavještajnim službama, policiji i vladinim agencijama širom svijeta. U julu 2015. godine i ovakva kompanija biva hakirana. Šta nam to govori? Niko nije imun na hakerski napad.

> *Kao što je današnja civilizacija nezamisliva bez računara i interneta, tako je nezamisliva i bez hakera.*

Unatoč ovakvoj današnjici, ukoliko hakerima nazovemo sve inovatore, umjetnike, naučnike koji stvaraju nove društvene i kulturne prakse i bore se za slobodan i neograničen pristup informacijama, znanju i stvaralaštvu, onda se možemo nadati da će saradnja, otvorenost i kreativnost kojima su hakeri obilježili ranu povijest informatičke revolucije ostati kao općenite vrijednosti društva i za buduće generacije. ■

PHISHING U DOBA PANDEMIJE:

KAKO PREPOZNATI I ZAŠTITITI SE?

Poduzimanje adekvatnih mjera zaštite protiv cyber napada treba postati dio naše svakodnevnice, a njihovo nepoznavanje je luksuz koji sebi ne smijemo priuštiti

Autorica:
Selma Bušatlić

Tokom pandemije koronavirusa zabilježen je značajan porast svih oblika *cyber* kriminala pa tako i *phishing* napada. Brojni su primjeri hakera koji koriste kriznu situaciju te lažnim predstavljanjem putem elektronske pošte pokušavaju prikupiti lične podatke građana i/ili podatke o njihovom elektronskom identitetu i pripadajućim lozinkama.

Pandemija je sa sobom donijela i dodatne sigurnosne probleme u području informacionih tehnologija. Povećana komunikacija putem elektronske pošte stvorila je savršene uslove za *phishing* napade. Statistike pokazuju da su se napadi krađe identiteta putem e-pošte povećali za više od 600% od kraja februara 2020.

I dok statistike ne zvuče ohrabrujuće, važno je upoznati se sa najčešćim metodama *phishing* napada, savjetima kako se zaštiti kao i šta učiniti ukoliko ipak postanete žrtva *cyber* kriminala.

Najčešće korištene metode *phishinga*

– ***Zahtjev za odavanje ličnih podataka primaoca*** poput jedinstvenog matičnog broja, broja lične karte, transakcijskog računa i sl. prilikom čega se pošiljalac lažno predstavlja kao administrator web servisa kojem su ti podaci potrebni radi provjere podataka, nadogradnje sigurnosnog softvera i sl.;

– ***Obavijest primaocu da je njegov račun kod banke ili PayPal kompromitovan*** i da je potrebno hitno se prijaviti putem linka koji se nalazi u sadržaju e-maila kako bi se spriječio pokušaj prevare. Otvaranjem linka u poruci, žrtva se usmjerava na malicioznu web stranicu;

– ***Obavijest primaocu da je osvojio nagradu u nagradnoj igri u kojoj nije učestvovao***. Čest je slučaj i da korisnik dobije obavijest da je primio značajnu sumu novca, ali da je za podizanje iste nužno uplatiti dodatne troškove;

– ***Lažni linkovi u e-mail porukama koji vode korisnika na malicioznu web stranicu*** gdje se od njega traži da upiše svoje korisničko ime i lozinku ili druge osjetljive podatke.

Ipak, postoje jednostavni koraci koje možete poduzeti kako ne biste postali žrtva krađe identiteta:

- Ne odajite bilo kakve lične ili finansijske podatke niti lozinke putem e-pošte!

- Ne otvarajte e-poštu koja insistira na tome da primalac djeluje odmah. Lažne poruke često pokušavaju stvoriti osjećaj hitnosti ili zahtijevaju trenutnu akciju.

- Provjerite da li adresa (URL) na koju se unose povjerljivi podaci odgovara legitimnoj (adresa krivotvorene web stranice može se razlikovati u jednom slovu od legitimne). Nepodudaranje sa originalnom domenom smatra se znakom upozorenja.

- Provjerite da li web stranica preko koje se unose povjerljivi podaci koristi HTTPS protokol – web adresa finansijskih institucija trebala bi počinjati s https:// umjesto sa http://.

- Obratite pažnju na pravopisne i gramatičke greške! Ako adresa ili sadržaj e-maila sadrži pravopisne, interpunkcijske i/ili gramatičke greške, moguće je da je u pitanju phishing e-pošta.

- Obavezno provjerite digitalni certifikat web poslužitelja prije unosa bilo kakvih podataka!

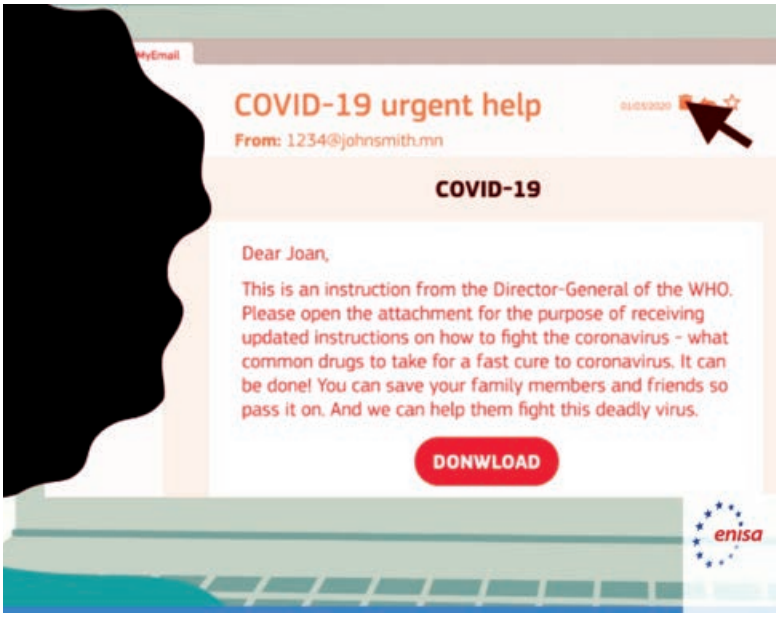
- Ne slijedite linkove koji se nalaze unutar sumnjivih i neočekivanih e-mail poruka!

- Koristite jake lozinke i često ih mijenjajte! Dobre lozinke sastoje se od kombinacije velikih i malih slova, brojeva i simbola što ih čini vrlo teškim za probijanje.

- Pratite aktuelne informacije o *cyber* kriminalu na internetu! Sigurnosna edukacija je najefikasnija odbrana od pokušaja *phishinga*.

- U situaciji trenutne pandemije neophodan je dodatni oprez u slučaju primanja e-pošte koja u predmetu sadrži informacije o COVID-19. Lažni e-mailovi mogu izgledati kao da dolaze iz prave organizacije, ali legitimne vladine agencije i zdravstvene ustanove nikada ne koriste e-poštu za slanje aktuelnih informacija.

-Instalirajte *anti-spam*, *anti-spyware* i antivirusni softver uz njihovo redovno ažuriranje.



Šta učiniti ako primalac e-maila ipak postane žrtva *phishing* napada?

- Ukoliko su za pristup informacijama već uneseni korisnički podaci za prijavu (korisničko ime i lozinka), potrebno ih je odmah promijeniti.

- Ukoliko je otvaranjem linka u sadržaju e-maila preuzet štetni softver, potrebno je ažurirati sigurnosni softver na računaru i pokrenuti skeniranje.

- Ako su navedeni lični i bankovni podaci žrtve *phishing* napada, odmah je potrebno obratiti se banci ili kompaniji za izdavanje kreditnih kartica.

Relativno je jednostavno izbjeći *phishing* napade ako se upoznaju njihove metode. Za razliku od kompjuterskih virusa, *phishing* se oslanja isključivo na primaoca maila. Stoga možemo zaključiti da kontinuirana edukacija korisnika o opasnostima koje vrebaju iza ovakvih poruka i poduzimanje adekvatnih mjera zaštite treba postati neophodan dio ljudske svakodnevnice, a njihovo nepoznavanje luksuz koji danas niko ne smije sebi priuštiti. ■

Sigurnost na internetu

POČINIOCI PREVARA PROFITIRAJU NA PANDEMIJI COVID-19

Oni ne sjede skrštenih ruku. Svoje prevarne radnje organizovali su u skladu sa situacijom u kojoj imamo smanjeno kretanje i strah ljudi, pojačanu potrebu za zaštitnim sredstvima te daleko veće oslanjanje na digitalna rješenja. Kako ih prepoznati i kako se zaštititi?

Autorica:
Berina Kapa

Pandemija COVID-19 nesumnjivo je preobrazila živote zajednica širom svijeta. Ljudi se moraju prilagoditi novim ograničenjima u pogledu svakodnevne slobode kretanja i novim radnim navikama, odnosno okruženju, dok se vlade i međunarodne organizacije suočavaju sa izazovima provođenja javnih zdravstvenih mjera i minimiziranja ekonomske štete.

Pandemija COVID-19 ima snažne posljedice na društvo i ekonomiju, ali i negativne posljedice u smislu povećanja kriminalnih i prevarnih radnji. Počinioci prevara ne sjede skrštenih ruku te su svoje prevarne radnje organizovali u skladu sa situacijom u kojoj imamo smanjeno kretanje i općenito strah ljudi, pojačanu potrebu za zaštitnim sredstvima te daleko veće oslanjanje na digitalna rješenja.

Imajući u vidu navedeno, pored borbe protiv globalnog širenja koronavirusa, podrške zdravstvenim sistemima i zaštite ekonomije, vlade širom svijeta suočavaju se i sa potrebom osiguranja sigurnosti i donošenja mjera protiv kriminalnih aktivnosti za vrijeme pandemije koronavirusa.

U nastavku donosimo neke od najčešćih oblika prevara na globalnom nivou proizašlih iz pandemije.

Cyber kriminal

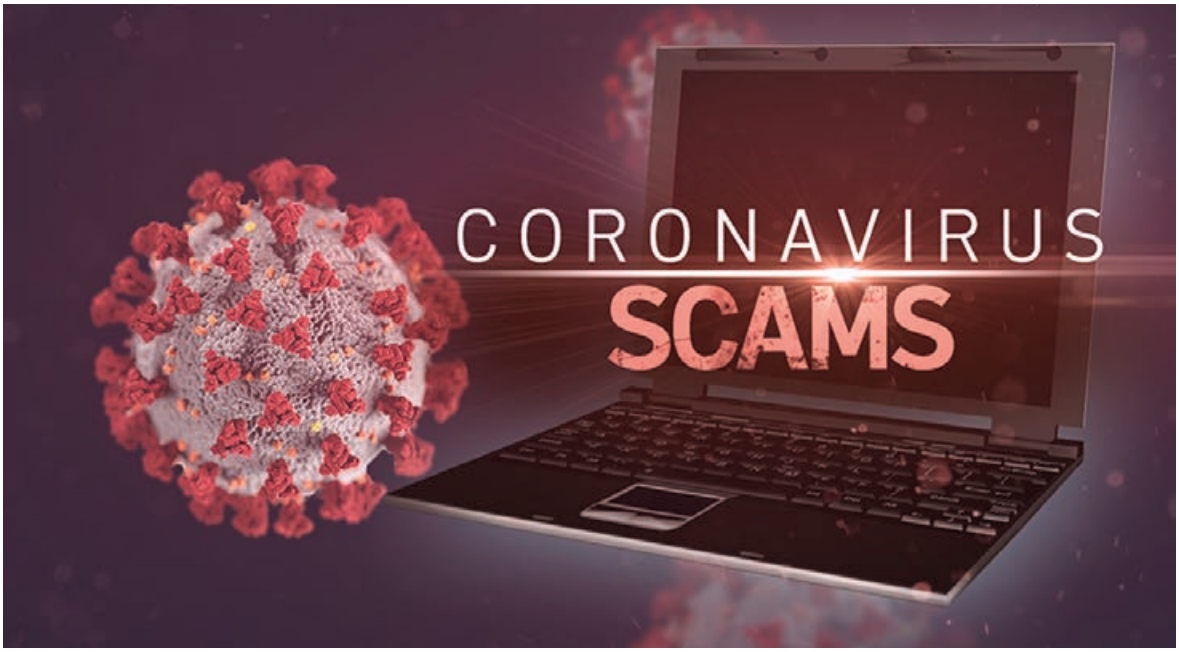
Uporedo sa širenjem COVID-19 u svijetu, raste i razina *cyber* kriminala. *Cyber* kriminalci iskorištavaju strah i neizvjesnost u vezi pandemije koronavirusa, kao i povećano vrijeme provedeno online tokom društvenog distanciranja kako bi ljude prevarili u objavljivanju osjetljivih informacija. *Phis-*

> *Cyber kriminalci iskorištavaju strah i neizvjesnost u vezi pandemije koronavirusa, kao i povećano vrijeme provedeno online tokom društvenog distanciranja kako bi ljude prevarili u objavljivanju osjetljivih informacija.*

hing je u porastu i to oblik sa COVID-19 tematskim prevarama gdje kriminalci šalju e-mail poruke za koje se čini da dolaze iz bolnica ili vladinih agencija kako bi ljude naveli na preuzimanje priloga ili odavanje ličnih identifikacijskih podataka. Svjetska zdravstvena organizacija nedavno je upozorila na kriminalce koji šalju e-mailove predstavljajući se kao WHO (*World Health Organization*). Popularna je i upotreba mračnih web stranica (tzv. *Dark web*) na kojima prevaranti nude posebnu robu za zaštitu od koronavirusa uz popuste, a ustvari je riječ o tzv. *scam* robi. Inače, termin *scam* predstavlja shemu za brzo ostvarivanje profita u kojoj neka osoba, grupa ljudi ili organizacija vara druge osobe ili grupe tako da im pruža lažne podatke prilikom davanja ponude ili nuđenja dogovora.

Klasične prevare

U izvještaju *Europola* iz marta 2020. godine, koji je rađen na temu *Kako kriminalci iskorištavaju krizu COVID-19*, navodi se da su u nekim zemljama Evrope zabilježene razne vrste prilagođenih verzija telefonskih prevara, prevara vezanih za isporuku i slično. Primjera radi, stanovnici nekih zemalja su primali pozive od ljudi koji tvrde da rade za javnu zdravstvenu organizaciju i sugerisali da je stanovnik kojeg pozovu možda izložen COVID-19. Prevaranti bi im saopštili da moraju platiti komplet za testiranje što nije istina. Stoga se u istom



izvještaju sugeriše svima da budu oprezni sa onima koji nude ili prodaju:

- setove za testiranje virusa - to nudi samo nadležna zdravstvena organizacija,
- cjepiva ili čudesne lijekove - trenutno nema cjepiva ili lijeka,
- precijenjene ili lažne robe kako bi se zaštitili od koronavirusa poput antibakterijskih proizvoda,
- usluge kupovine ili sakupljanja lijekova.

Falsifikovanje

Pandemija virusa korona izazvala je novi trend krivotvorenih medicinskih predmeta i preparata. Novi virus pružio je priliku za brzu zaradu jer kriminalci koriste veliku potražnju na tržištu za proizvodima namijenjenim za ličnu zaštitu i higijenu.

Evropski ured za borbu protiv prevara (OLAF) otvorio je istragu o uvozu lažnih proizvoda povezanih s COVID-19, a koji su neučinkoviti ili čak štetni za zdravlje, a u to spadaju maske, sredstva za dezinfekciju i testiranje. OLAF zajedno sa državnim carinskim upravama radi na sprečavanju ulaska tih opasnih krivotvorina ili zabranjenih proizvoda u EU. Ovi krivotvoreni proizvodi ulaze u Evropu putem internetske prodaje. Stižu i u kontejnerima s lažnim certifikatima ili su deklarirani kao drugi proizvodi i pronalaze svoj put u uobičajene kanale distribucije ili se prodaju na crnom tržištu.

Evropski ured za borbu protiv prevara (OLAF) otvorio je istragu o uvozu lažnih proizvoda povezanih s COVID-19, a koji su neučinkoviti ili čak štetni za zdravlje, a u to spadaju maske, sredstva za dezinfekciju i testiranje.

Nadalje, *Europol* je podržao globalnu operaciju usmjerenu na trgovinu krivotvorenim

lijekovima. *Operacija Pangea*, kojom je koordinirao *Interpol* i koja je uključila 90 zemalja svijeta, održala se između 3. i 10. marta 2020. godine. Zanimljiv je podatak da su vlasti širom svijeta zaplijenile skoro 34.000 krivotvorenih hirurških maski, čineći ih medicinskim proizvodom koji se najčešće prodaje online. Također, službenici za provedbu zakona oborili su 2.500 linkova s proizvodima povezanim sa COVID-19 (web stranice, društvene mreže, online trgovine, oglasi).

Rezultati operacije otkrivaju i zabrinjavajući porast neovlaštenih antivirusnih lijekova i antimalarijskog klorokina. Vitamin C, poznat po svojstvima pojačavanja imuniteta, i ostali dodaci prehrani zaplijenjeni su širom svijeta. Značajan dio zapljene čine i lijekovi protiv bolova i antibiotici.

Opreza nikada dosta

Da bi se zaštitili od potencijalnih prevara, odgovornost je svakog pojedinca da preduzme minimalne mjere zaštite, posebno pri korištenju interneta i online kupovine. Dakle, ovu vrstu infekcije treba liječiti vlastitim higijenskim oblicima. Izbjegavanje klikanja na veze nepouzdanih korisnika ili nepružanje ličnih podataka nepoznatim izvorima, minimalne su mjere koje se mogu poduzeti da se izbjegne bilo kakva šteta. Pri kupovini proizvoda uvijek je potrebno izvršiti detaljniju provjeru ponuđača, web stranice i sl. Veća svijest o postojanju opasnosti od prevara i veća odgovornost pri korištenju interneta smanjuju potencijalne prilike za prevarante. ■

Dodatni izvori:
www.europol.europa.eu
www.interpol.int

UREDNIČKI TIM


UPRMBiH
Udruženje profesionalnih rizik menadžera
Hvala Vam za uspješnu suradnju
tokom 2020. godine
Sretne nadolazeće praznike i
uspješnu novu 2021. godinu želi Vam
Udruženje profesionalnih rizik menađera