GOD. 6 . BR. 7 [2022] EDUKATIVNI ČASOPIS ZA BANKARSKI I FINANSIJSKI SEKTOR U BiH

ISSN 2566-3100

FRAUDinfo

UDRUŽENJE PROFESIONALNIH RIZIK MENADŽERA U BOSNI I HERCEGOVINI

9 772566 631000 8

UPRMBiH

Udruženje profesionalnih rizik menadžera


FRAUD ALERT
CONFIRM
Click here for more information

UPRMBiH
Udruženje profesionalnih rizik menadžera

FRAUDinfo

Udruženje profesionalnih rizik menadžera u BiH

Fra Anđela Zvizdovića 1
71 000 Sarajevo - BiH

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,

tim eksperata ispred **Fraud foruma** pripremio je sedmo izdanje ***Fraud Info*** časopisa koje sadrži dosta zanimljivih tema s prijedlozima i praktičnim primjerima za unapređenje poslovanja te s prijedlozima mjera za prevenciju i detekciju *fraud* trendova, zahvaljujući pokroviteljstvu i podršci Udruženja profesionalnih rizik menadžera u BiH.

Fraud Info časopis je prvi stručni časopis koji se bavi vrstama, tehnikama, prevencijom i posljedicama prevarnih radnji i *cyber* rizika koji su usmjereni prema finansijskim institucijama i njihovim klijentima. Svojim stručnim i istraživačkim člancima pokušava pomoći finansijskim institucijama u Bosni i Hercegovini da bolje razumiju *cyber* rizike i prevare i da se adekvatno zaštite od istih.

Kriza izazvana pandemijom COVID-19 podstakla je bankarski sektor na povećanje primjene umjetne inteligencije (*Artificial Intelligence* - AI). Kako računala *uče* i donose pametnije *odluke*, vrijeme odgovora postaje brže, a učinkovitost i produktivnost se povećavaju. U svijetu kibernetičke sigurnosti umjetna inteligencija igra aktivniju ulogu u otkrivanju kibernetičkih napada. S razlogom se postavlja pitanje može li ova vrsta tehnologije, ako se nađe u pogrešnim rukama, donijeti više štete nego koristi. U sedmom izdanju ***Fraud Info*** časopisa možete pročitati osvrt u kojem autorica predstavlja benefite umjetne inteligencije, ali i moguće rizike.

Upoznajte se detaljnije s novom industrijom FinTech koja koristi digitalnu tehnologiju. Autorica teksta predstavila nam je koji su globalni trendovi - korporacija ili konkurencija između FinTecha i tradicionalnih banaka, FinTech – rizici i izazovi cyber sigurnosti i još mnogo toga.

Jedna od najbrže rastućih kriminalnih grana je krađa identiteta. Da li su digitalni tragovi *zlatni rudnik*? Koji su tipovi krađe identiteta? Kako se koriste ukradeni identiteti i kako se zaštititi od krađe identiteta? Odgovore na ova pitanja možete pronaći u našem sedmom izdanju ***Fraud Info*** časopisa.

Govorimo i o tome kako se sačuvati od kreditnih prevara i upotreba tuđih ličnih podataka, kao i njihove kreditne sposobnosti ili korištenje ličnih podataka uz falsifikovanje dokumentacije potrebne za kredit ili kreditne kartice, za pozajmljivanje novca od banaka ili drugih finansijskih institucija s ciljem kupovine dobara ili usluga bez namjere otplate duga.

Bavili smo se i KYE procedurama te njihovim benefitima za prevenciju internog *frauda*. Poznavanje ljudi znači i poznavanje organizacije. Službenici zaduženi za prevenciju *frauda* moraju izuzetno dobro poznavati i ljude i

Sadržaj

organizaciju i sve procese u organizaciji kako bi adekvatno identifikovali *slabe tačke* i poduzimali odgovarajuće aktivnosti na prevenciji. *Know-Your-Emplyoee* procedure su neizostavan paket mjera prevencije prevara.

Zanimljiv stručni rad *Osvrt na Nacrt zakona o izmjenama i dopunama Zakona o izvršnom postupku FBiH* govori o značaju ovog zakona za bankarski sektor i o njegovim izmjenama koje će imati višestruke posljedice na efikasnost naplate potraživanja svih povjerilaca, ne samo banaka. U ovom radu dat je kratki osvrt na najznačajnije izmjene koje se predviđaju prema Nacrtu. U tekstu je, uz komentar autora, izložen pregled najznačajnijih izmjena uz uporedbu s rješenjima koja trenutno važeći zakon sadržava u odnosu na efekte koje takva izmjena sa sobom donosi. Komenatar autora, iako po prirodi stvari prije svega obuhvata aspekte povjerilac/tražilac/izvršilac, je nepristrasan uvažavajući opravdane i zakonite interese svih strana u postupku.

Pripremili smo i zanimljivu ekspertizu o novinama koje donosi *Nacrt Smjernica za politike i procedure za upravljanje usklađenošću i ulozi i odgovornostima AML/CFT službenika* prema članu 8. iz poglavlja IV EU Direktive 2015/849.

Donosimo osvrt na *Odluku o sistemu internog upravljanja u banci*, koja je na snazi od 31.12.2021. godine, i određene izmjene koje sadrži u odnosu na prethodnu *Odluku o kontrolnim funkcijama banke*.

Bankomati su neizostavni dio naše svakodnevnice. U ovom broju donosimo vam zanimljiv tekst o vrstama napada i prevara na bankomatima te kako se od njih sačuvati.

Vjerujemo da novo, sedmo izdanje ***Fraud Info*** časopisa donosi dosta zanimljivih tema i aktuelnosti. ■

Igor Jokić
Predsjednik Udruženja profesionalnih rizik menadžera u Bosni i Hercegovini

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

Pored pokroviteljstva i podrške Fraud Info časopisu, u toku 2022. godine Udruženje profesionalnih rizik menadžera u BiH planira nastaviti održavanje stručnih edukacija sa temama koje su trenutno najaktuelnije za finansijski sektor. Jedna od ključnih aktivnosti u ovoj godini će također biti finaliziranje i organizacija programa certifikacije u saradnji sa GARP-om (eng. *Global Association of Risk Professionals*).

Artificial Intelligence

UMJETNA INTELIGENCIJA I KIBERNETIČKA SIGURNOST

Umjetna inteligencija ima široku primjenu – od praćenja pandemije COVID-19 i korištenja u medicinske svrhe do upotrebe u bankarskom sektoru. Upotreba AI u cyber sigurnosti je sve neophodnija da bi se na vrijeme otkrili i prevenirali napadi cyber kriminalaca.

Autorica:
Sanela Stupar

Pandemija COVID-19 obilježava naše živote na nezapamćen način. Od izbijanja u Wuhanu u Kini 2020. godine, virus se dosljedno i kontinuirano širio diljem svijeta. Međunarodne organizacije i znanstvenici sve su više počeli primjenjivati nove tehnologije, kao što je umjetna inteligencija (*Artificial Intelligence* - AI), za praćenje pandemije, predviđanje gdje bi se virus mogao pojaviti i razvijanje učinkovite reakcije. Prvo, nekoliko institucija koristi umjetnu inteligenciju za procjenu i otkrivanje lijekova ili tretmana koji bi mogli pomoći u liječenju COVID-19 te za razvoj prototipa cjepiva. AI je također korištena za otkrivanje novih potencijalnih koronavirusa na ljudima identificiranjem vizualnih znakova COVID-19 na slikama sa skeniranja pluća[1]. U ranoj fazi pandemije, **DeepMind** je koristio svoj *AlphaFold AI* sustav za predviđanje i objavljivanje proteinskih struktura povezanih s koronavirusom[2]. Sada kada se cjepiva Pfizer, Moderna i AstraZeneca primjenjuju diljem svijeta, AI i druge nove tehnologije primjenjuju se kako bi se upravljalo ovim monumentalnim naporom.Naprimjer, Regulatorna agencija za lijekove i zdravstvene proizvode Ujedinjenog Kraljevstva (MHRA), u partnerstvu s britanskom

[1] Evropska parlamentarna istraživačka služba, *Što ako bismo se mogli boriti protiv koronavirusa umjetnom inteligencijom?*, mart 2020.

[2] DeepMind, *Računalna predviđanja proteinskih struktura povezanih s COVID-19*, avgust 2020. (https://deepmind.com/research/open-source/computational-predictions-of-protein-structures-associated-with-COVID-19)

jedinicom **Genpact**, globalnom tvrtkom za profesionalne usluge specijaliziranom za digitalnu transformaciju, koristi umjetnu inteligenciju za praćenje mogućih štetnih učinaka cjepiva na različite segmente stanovništva.

AI se također koristi u drugim aplikacijama osim medicinskih. Pomogla je u borbi protiv dezinformacija rudarenjem društvenih medija, pronalaženjem riječi koje su senzacionalne ili alarmantne te identificiranjem pouzdanih i autoritativnih *online* referenci. Nekoliko zemalja diljem svijeta usvojilo je AI aplikacije kako bi podržale provedbu mjera zaključavanja, kao što su sustavi za prepoznavanje lica za prepoznavanje ljudi koji ne nose maske ili mobilne aplikacije koje prate društvene kontakte ljudi.

Vještačka inteligencija (AI) je polje aplikacija zasnovanih na algoritmima koje omogućavaju mašinama da rješavaju probleme znanja i koriste algoritme za simulaciju ljudskog donošenja odluka i kontinuirano poboljšava performanse primjenom unesenih podataka za obavljanje specifičnih zadataka. Prednosti AI se ogledaju u visokoj osjetljivosti i specifičnosti u identifikaciji objekta, brzini izvještavanja i konzistentnosti rezultata. Posljednjih godina AI je postigla značajan napredak, posebno u prediktivnim modelima mašinskog učenja za medicinsku njegu. Duboko učenje je metoda ML, zasnovana na složenoj arhitekturi umjetnih neuronskih mreža (*Artificial Neural Networks* - ANN). Duboko učenje otkriva značajne diskriminativne performanse nakon pružanja dovoljnih skupova podataka za obuku i neophodno je za predviđanje. U medicini, tehnologije zasnovane na umjetnoj inteligenciji i strojnom učenju (*Artificial intelligence and machine learning* - AI/ML) imaju za cilj poboljšati kvalitetu medicinske skrbi, povećati dijagnostičku tačnost, smanjiti potencijalne greške te predvidjeti ishode otkrivanjem novih uvida iz ogromne količine podataka proizvedenih iskustvom mnogo pacijenata.

> *U medicini, tehnologije zasnovane na umjetnoj inteligenciji i strojnom učenju imaju za cilj poboljšati kvalitetu medicinske skrbi, povećati dijagnostičku tačnost, smanjiti potencijalne greške te predvidjeti ishode otkrivanjem novih uvida iz ogromne količine podataka proizvedenih iskustvom mnogo pacijenata.*

Vještačka inteligencija u cyber sigurnosti

Prema mnogim sigurnosnim analitičarima, sigurnosni incidenti dostigli su najveći broj i stalno se povećavaju. Od krađe identiteta do *ransomwarea*, od mračne mreže kao ekonomije usluga do napada na civilnu infrastrukturu, kibernetska sigurnost uključivala je napade koji su postali sve sofisticiraniji tokom godina. Ovaj trend se nastavlja i u 2022. godini.

Cyber kriminalci su uspjeli da iskoriste pandemiju COVID-19 i rastuću *online* ovisnost pojedinca i korporacije koristeći potencijalne ranjivosti udaljenih uređaja i sigurnost propusta.

Iskorištavajući potencijal za veliki uticaj i finansijsku ko-

rist, akteri prijetnje su koristili tematske *phishing* mejlove u kojima su se lažno predstavljali kao vladini i zdravstveni predstavnici kako bi ukrali lične podatke i primijenili zlonamerni softver protiv kritične infrastrukture i zdravstvenih ustanova.

U 2022. godini težnja za sveprisutnim povezivanjem i digitalizacijom nastavlja podržavati ekonomski napredak, ali istovremeno i neizbježno stvara plodno tlo za porast obima cyber napada. Sve veći *ransomware* i raznolike taktike, sve mobilnije cyber prijetnje, sve sofisticiraniji *phishing*, cyber kriminalci i napadači ciljaju sisteme koji upravljaju našim svakodnevnim životom.

U upotrebi vještačke inteligencije u cyber sigurnosti mogu se identifikovati tri glavne kategorije: otkrivanje (51%), predviđanje (34%) i odgovor (18%)[3].

Potreba da se odgovori na cyber napade potiče kompanije da grade sisteme koji sami uče, odnosno koji su u stanju da uspostave lokalni kontekst i razlikuju odmetnuto od normalnog ponašanja.

Umjetna inteligencija za testiranje softvera (AIST) je novija oblast istraživanja umjetne inteligencije s ciljem dizajniranja softvera koji može samotestirati i samokorigovati. Samotestiranje se odnosi na *sposobnost sistema ili komponente da prati svoje dinamičko prilagodljivo ponašanje i izvrši testiranje u toku rada prije ili kao dio procesa prilagođavanja.*[4]

U cilju povećanja sigurnosnih kontrola, u toku procjene ranjivosti koriste se tehnike vještačke inteligencije.

Dok je upotreba umjetne inteligencije u cyber sigurnosti sve neophodnija, AI sistemi će i dalje zahtijevati prilično kolaborativno okruženje između AI i ljudi, barem u doglednoj budućnosti. Iako potpuno autonomni sistemi postoje, njihova upotreba je još uvijek relativno ograničena, a sistemi i dalje često zahtijevaju ljudsku

Dok je upotreba umjetne inteligencije u cyber sigurnosti sve neophodnija, AI sistemi će i dalje zahtijevati prilično kolaborativno okruženje između AI i ljudi, barem u doglednoj budućnosti.

intervenciju da bi funkcionirali kako je predviđeno.

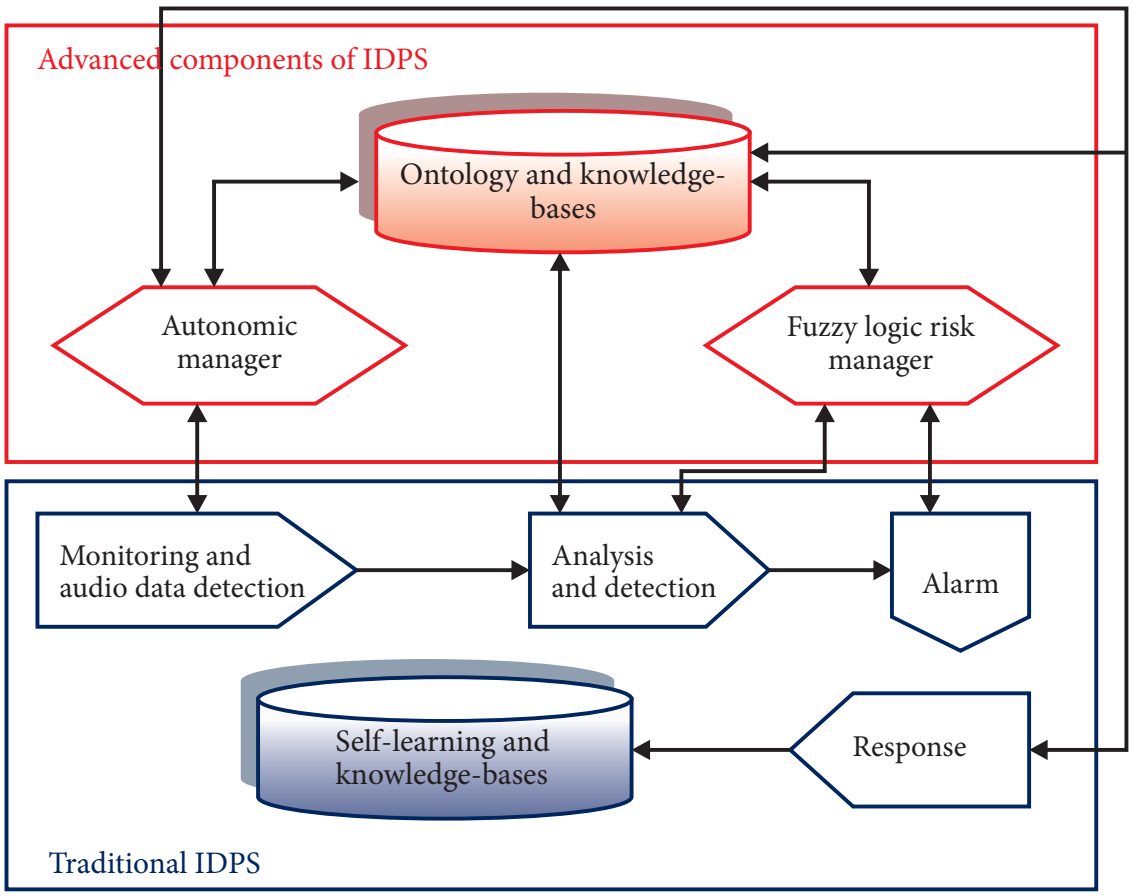
U tom smislu, ljudi koji su uključeni moraju stalno pratiti sistem (za tačnost, zahtjev za promjenu, itd.). Neki modeli se i dalje moraju obnavljati svaki dan samo da bi bili ispred napadača jer se napadi mijenjaju kao odgovor na odbranu koja se gradi. Konačno, postoje zajednice praktičara sigurnosti koje nastavljaju da rade zajedno na uspostavljanju zajedničkog razumijevanja o tome šta je zlonamjerno, a šta nije.[5]

Da bi se bolje ilustrovalo korištenje AI i ML-a za detekciju i odgovor na cyber sigurnost, Slika 1 predstavlja sistem za otkrivanje i prevenciju upa-

3 CAP Gemini, *Reinventing Cyber security with Artificial Intelligence. The new frontier in digital security*, Research Institute (2019)

4 T.M. King et. al, *AI for testing today and tomorrow: Industry Perspective*, IEEE International Conference on Artificial Intelligence Testing, IEEE, 2019, pp. 81-88.

5 This section is taken from Palo Alto Network's contribution to the fourth meeting of the CEPS Task Force



da koji kombinuje softverske i hardverske uređaje unutar mreže. Sistem može otkriti moguće upade i pokušati ih spriječiti. Sistemi za otkrivanje i prevenciju upada pružaju četiri vitalne sigurnosne funkcije: praćenje, otkrivanje, analiziranje i reagovanje na neovlaštene aktivnosti.

Sistem za detekciju i prevenciju upada[6]

Vještačke neuronske mreže

AI, koja je implementirana kao digitalna tehnologija, podložna je sigurnosnim problemima u svakom koraku svog razvoja, distribucije i upotrebe.

Većina inteligentnih sistema, koji su temelj vještačke inteligencije, funkcioniše po principu sekvencijalne (algoritamske) obrade i ograničeni su samo na određena specifična predstavljanja znanja i logike. Alternativni pristup izgradnji i funkcionisanju inteligentnih sistema je dizajniranje takve računarske arhitekture koja oponaša određene sposobnosti obrade informacija koje posjeduje ljudski mozak. Mozak obrađuje podatke na

[6] Dilek

potpuno drugačiji način od konvencionalnih digitalnih računara zasnovanih na **Fon Nojmanovim**[7] (engl. Von Neumann) principima. Rezultati primjene takvog pristupa su: otkrivanje znanja, odnosno pronalaženje skrivenih zakonitosti između podataka na bazi intenzivne (masovne) paralelne obrade, brzo dobivanje velike količine informacija upotrebljivih za odlučivanje i sposobnost prepoznavanja obrazaca zasnovanih na iskustvima koji predstavljaju temelj za prognoziranje budućeg ponašanja posmatrane pojave. Tehnologija koja ima potencijal da ostvari ove rezultate naziva se **neuronska obrada podataka na računaru** (engl. *neural computing*) ili **vještačke neuronske mreže** (engl. *artificial neural networks* - ANN). Vještačka neuronska mreža je sistem programa i struktura podataka koji simulira način funkcionisanja ljudskog mozga da bi bez ljudske pomoći ostvario makar približne rezultate u rješavanju problema koje bi inače ostvario čovjek koristeći još uvijek neprevaziđenu kreativnost i kapacitete vlastitog mozga. VNM obično obuhvata veliki broj elemenata za procesiranje podataka koji rade istovremeno na način da svaki taj elemenat ima svoj mali (ograničeni) domen znanja i pristup svim podacima u svojoj lokalnoj memoriji. VNM je najčešće na početku *obučena* za rješavanje nekog problema, odnosno u nju su ubačene velike količine podataka iz velikog broja slučajeva kao i veliki broj pravila o vezama između podataka[8].

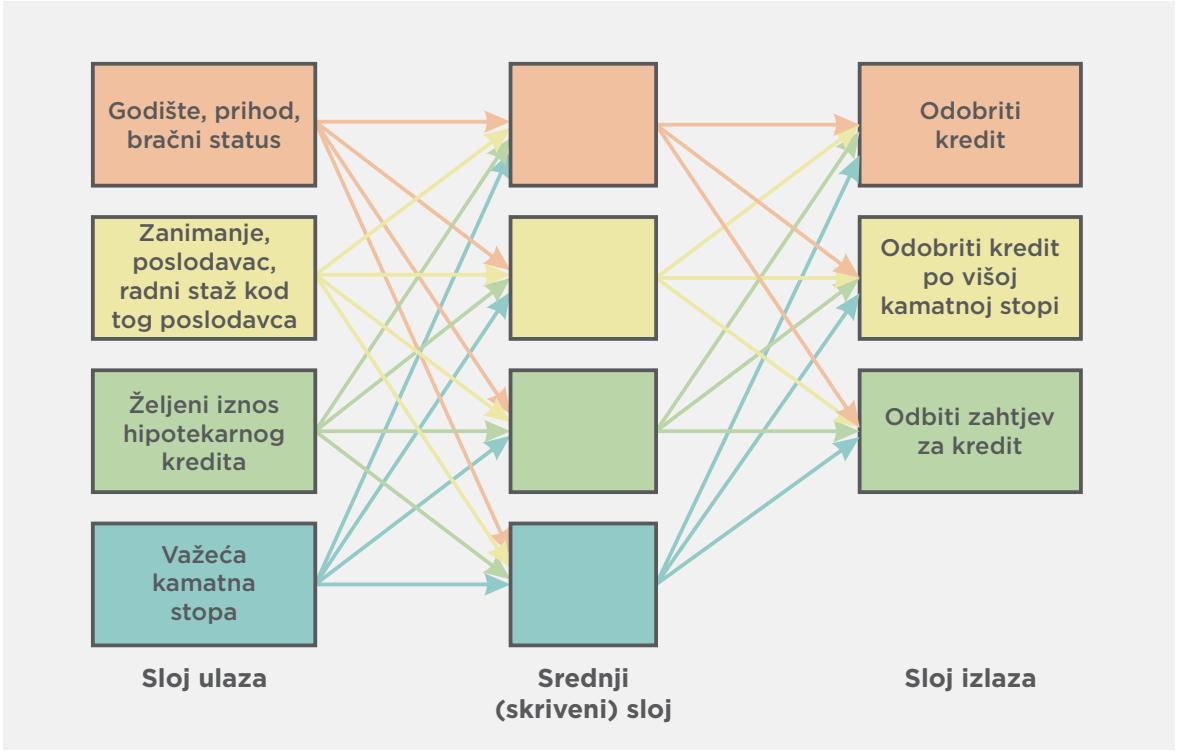
> *Neuronske mreže su postale standard u borbi protiv prevara korištenjem kreditnih kartica, prevara u zdravstvu i telekomunikacijskoj industriji i igraju veliku ulogu u savremenim međunarodnim naporima da se spriječi pranje novca.*

Neuronske mreže naročito dobro prepoznaju suptilne, skrivene i nove obrasce u složenim podacima i tumače nepotpune ulaze. Korisnicima mogu pomoći da riješe širok spektar problema, od bezbjednosti na aerodromu do kontrole zaraznih bolesti. One su postale standard u borbi protiv prevara korištenjem kreditnih kartica, prevara u zdravstvu i telekomunikacijskoj industriji i igraju veliku ulogu u savremenim međunarodnim naporima da se spriječi pranje novca.

Na primjeru prijave za hipotekarni kredit (prikazan na slici) pokazat ćemo kako se neuronska mreža koristi protiv prevara. Na slici je prikazana neuronska mreža koja ima tri vrste povezanih čvorova (slično kao ljudski mozak): sloj čvorova ulaza, srednji ili skriveni sloj čvorova i sloj čvorova izlaza. Zavisno od obuke neuronske mreže, jačina (ili tačnije veza) među čvorovima se mijenja. Naprimjer, ulazni čvorovi su godište, zanimanje,

[7] Fon Njumanov pristup izgradnji arhitekture računara opisan je u djelu *Preliminary Discussion of the Logical Design of an Electronic Computing Instrument* autora Arthura W. Burksa, Hermana H. Goldstinea i Johna von Neumanna, objavljenog 1946. godine.

[8] R. Kelly Rainer, *Efraim Turban Introduction to Information Systems Supporting and Transforming Business.*



bračni status, poslodavac, dužina staža kod tog poslodavca, željeni iznos kredita, kamatna stopa i mnogi drugi podaci. Neuronska mreža je već obučena mnogim ulaznim podacima iz uspješnih i neuspješnih zahtjeva za hipotekarni kredit. Drugim riječima, neuronska mreža je već uspostavila obrazac koji pokazuje kakve su varijable ulaza neophodne da bi rješenje za kredit bilo pozitivno. Osim toga, neuronska mreža može da se podešava prema povećavanju ili smanjivanju iznosa željenog kredita i kamata.

Neuronska mreža[9]

Prednosti i aplikacije neuronskih mreža

Vrijednost tehnologija neuronskih mreža uključuje njenu korist za prepoznavanje obrazaca, učenje i interpretaciju nekompletnih ulaza i ulaza u prisustvu jakog šuma. Neuronske mreže imaju potencijal da obezbijede neke od ljudskih karakteristika rješavanja problema koje su teške za simuliranje korištenjem logičkih, analitičkih tehnika DSS ili čak ekspertnih sistema. Jedna od ovih karakteristika je prepoznavanje obrasca. Neuronske mreže mogu analizirati velike količine podataka da bi uspostavile obrasce i karakteristike u situacijama u kojima logika ili pravila nisu poznati. Primjer bi mogli biti zahtjevi za pozajmicom. Pregledom mnogih historijskih slučajeva upitnika podnosilaca zahtje-

[9] Turban, *Uvod u informacione sisteme*, 2009.

va i donesenih odluka (da ili ne), VNM može da kreira *obrasce* i *profile* zahtjeva koje treba odobriti ili odbiti. Novi zahtjev se ravna prema obrascu. Ako priđe dovoljno blizu, računar ga klasifikuje kao *da* ili *ne*, u protivnom se dostavlja čovjeku da on donese odluku. Neuronske mreže su posebno korisne za finansijske aplikacije, kao što je određivanje kada da se kupuju ili prodaju akcije.

Neuronske mreže pružaju nekoliko drugih pogodnosti, kao što su:

- ***Tolerancija greške.*** Ako ima mnogo procesnih čvorova, šteta koja se načini na nekoliko čvorova ili na vezama ne dovodi do zastoja sistema.
- ***Generalizacija.*** Kada neuronska mreža dobije nekompletan ulazni podatak ili podatak kakav nikada *nije vidjela*, ona može da generalizuje da bi proizvela razuman odgovor.
- ***Adaptibilnost.*** Mreža uči u novim okruženjima. Novi slučajevi se trenutno koriste da se program koriguje i očuva aktuelnost.
- ***Mogućnost predviđanja.*** Slično statistici, ovdje se, također, predviđanje vrši na bazi ranijih podataka (tj. na osnovu prethistorije).

VNM ne obavlja dobro poslove koje ljudi nisu dobro uradili. Naprimjer, brze aritmetičke operacije, kao i poslovi obrade transakcija, nisu podesni za VNM i najbolje se obavljaju pomoću konvencionalnih računarskih programa. Specifične oblasti biznisa podesne za asistenciju VNM su:

- ***Otkrivanje modela podataka:*** pronalaženje podataka u velikim i kompleksnim bazama podataka i na web lokacijama;
- ***Utaje poreza:*** identifikovanje, poboljšanje i otkrivanje nepravilnosti;
- ***Finansijske usluge:*** identifikovanje obrazaca u podacima s berze i asistiranje pri prometu akcija i obveznica; izbor i prodaja robe; osiguranje hipoteke; određivanje cijena IPO-a (*Initial Public Offering* ili početna cijena ponude); prognoza kursa razmjene deviza;
- ***Procjena zahtjeva za kredit:*** procjena vrijednosti zahtjeva za pozajmicu zasnovanog na obrascu iz prethodno datih informacija u zahtjevu (kreditno bodovanje klijenata);
- ***Predviđanje solventnosti:*** procjena snage i slabosti korporacija i predviđanje mogućeg bankrotstva;
- ***Analize novih proizvoda:*** prognoziranje prodaje i ciljani marketing;
- ***Upravljanje cijenom avionskih kompanija:*** potražnja sjedišta i red letenja posada;
- ***Procjena personala i kandidata za posao:*** uparivanje podataka osoblja sa zahtjevima posla i radnim kriterijima;
- ***Distribucija resursa zasnovana na prethodnim, eksperimentalnim podacima:*** pronalaženje distribucionih šema koje će maksimizirati izlaze;
- ***Identifikovanje firmi koje će biti kandidati za preuzimanje:*** predviđanje koje će kompanije najverovatnije biti preuzete od drugih kompanija;
- ***Verifikacija potpisa:*** uparivanje potpisa s onima koji su u datoteci deponovani kao pravi;
- ***Predviđanje:*** predviđanje učinka i ponašanja zaposlenih, kao i kadrovskih uslova;

- ***Otkrivanje prevara u vezi s osiguranjem:*** otkrivanje obrazaca prevara;
- ***Otkrivanje falsifikovanih kreditnih kartica:*** analizirajući obrasce kupovanja za brzo otkrivanje prevare.

Neuronska obrada na računaru se pojavljuje kao efikasna tehnologija u prepoznavanju oblika. Ova sposobnost se prevodi u mnoge aplikacije i ponekad je integrisana s *fuzzy* logikom.

Unapređenje vještačkih neuronskih mreža zavisi od novih spoznaja o funkcionisanju ljudskog mozga i od razvoja tehnologije.

Nove cyber prijetnje

Kao i postojeće prijetnje koje se šire u obimu i opsegu, napredak u AI znači da bi se mogle uvesti potpuno nove prijetnje. Karakteristike AI neograničenosti ljudskim sposobnostima mogu omogućiti akterima da izvrše napade koji inače ne bi bili izvodljivi.

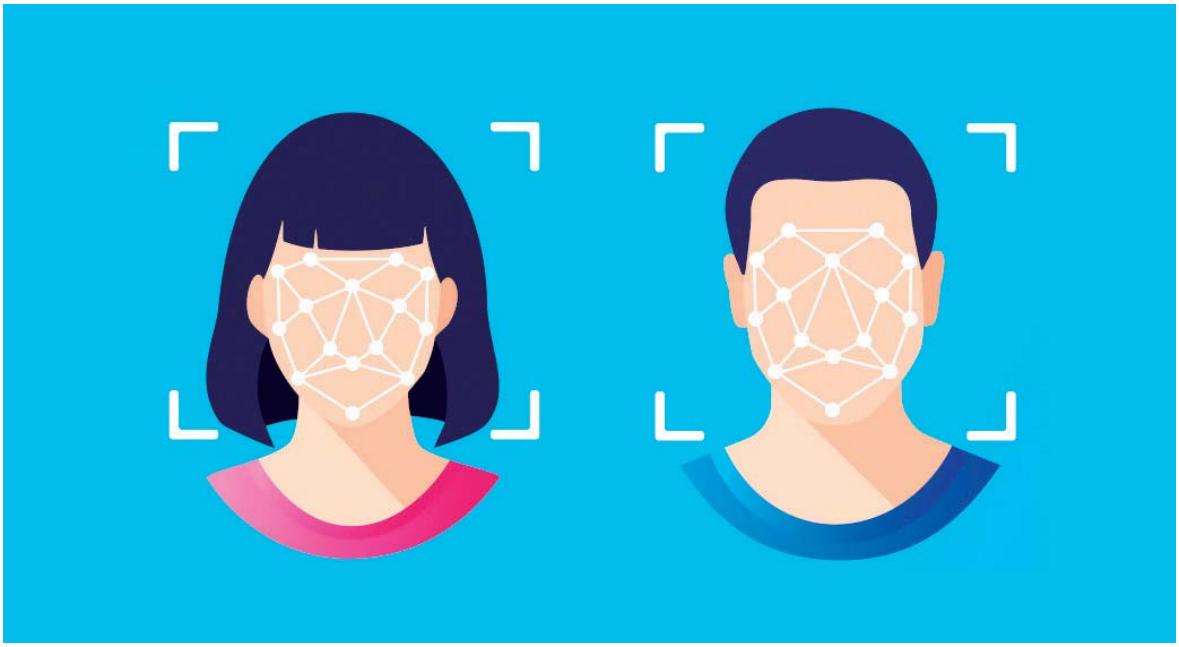
Deepfakes

Upotreba *deepfakesa* u stalnom je porastu. *Deepfakes* je tehnologija u razvoju koja koristi duboko učenje za pravljenje slika, videozapisa ili tekstova lažnih događaja. Postoje dvije glavne metode za pravljenje *deepfakesa*. Prva se obično koristi za *zamjenu lica* (tj. postavljanje lica jedne osobe na glavu ili tijelo druge) i zahtijeva hiljade snimaka lica dvoje ljudi koji trebaju proći kroz AI algoritam koji se zove *enkoder*. Koder zatim pronalazi i uči sličnosti između ova dva lica i svodi ih na njihove zajedničke karakteristike komprimirajući slike u procesu. Drugi AI algoritam nazvan *dekoder* se zatim uči da povrati lica iz komprimiranih slika: jedan dekoder oporavlja lice prve osobe, a drugi oporavlja lice druge osobe. Zatim, davanjem kodiranih slika *pogrešnom* dekoderu, zamjena lica se izvodi na što je moguće više kadrova videa kako bi se napravio uvjerljiv *deepfake*[10].
Druga i vrlo važna metoda za pravljenje *deepfakesa* naziva se ***Generative Adversarial Network*** (GAN). GAN suprotstavlja dva AI algoritma jedan protiv drugog kako bi kreirao potpuno nove slike. Jedan algoritam, generator, hrani se slučajnim podacima i generiše novu sliku. Drugi algoritam, diskriminator, provjerava sliku i podatke da vidi da li odgovaraju poznatim podacima, tj. poznatim slikama ili licima. Ova bitka između dva algoritma se u suštini završava prisiljavanjem generatora da kreira izuzetno realistične slike (npr. slavnih ličnosti) koje pokušavaju da zavaraju diskriminatora[11].

Ove slike su korištene za stvaranje lažnih, ali realističnih slika ljudi, s često štetnim posljedicama. Naprimjer, **McAfee** tim je koristio GAN da zavara sistem za prepoznavanje lica poput onih koji se trenutno koriste za verifikaciju pasoša na aerodromima. McAfee se oslanjao na najsavremenije algoritme za prepoznavanje lica otvorenog koda, koji su obično prilično slični jedni drugima, što je izazvalo značajnu

[10] I. Sample (2020), *What are deepfakes and how can you spot them, The Guardian*, 13 January (www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them).

[11] K. Vyas (2019), *Generative Adversarial Networks: The Tech Behind DeepFake and FaceApp*, Interesting Engineering, 12 August (https://interestingengineering.com/generative-adversarial-networks-the-tech-behind-deepfake-and-faceapp).



zabrinutost u pogledu sigurnosti sistema za prepoznavanje lica.[12]

Posljednjih godina kriminalci su zlonamjerno koristili *deepfake* tehnologiju za finansijsku dobit. Prema **Deeptraceu**, *deepfakes zaista predstavljaju rizik za politiku u smislu da lažni mediji izgledaju stvarni, ali trenutno je opipljivija prijetnja kako se ideja deepfakes može prizvati kako bi se pravi činio lažnim. Navijanje i prilično senzacionalno izvještavanje o spekulaciji o političkom utjecaju dubokih lažnjaka zasjenilo je stvarne slučajeve u kojima su deepfakes imali utjecaja*, kao što je kibernetički kriminal. Iako su internet i e-mail prevare prisutne decenijama, napredak tehnologije *deepfake* u zvuku, a i video formatu, omogućio je još zamršenije i teže uočljive lažne kriminalne aktivnosti.

Ove vrste zločina mogu se kretati od osnovnog nivoa aktivista koji daju lažne tvrdnje i izjave da potkopaju i destabilizuju kompaniju do ozbiljnijih napora kao što su viši rukovodioci koji priznaju finansijske zločine ili druge prekršaje. *Deepfakes*, također, može koristiti društveni inženjering kako bi prevare učinio vjerodostojnijim korištenjem videozapisa ili zvuka, naprimjer člana ciljane organizacije, čime se povećavaju šanse da napad uspije. Kompanija za istraživanje tržišta **Forrester** tvrdi da bi *deepfakes* na kraju mogao koštati kompanije čak 250 miliona dolara u 2020. godini. Razvijaju se softverski alati koji mogu uočiti kriminalni *deepfakes*, ali je potreban samo jedan pojedinac u kompaniji da vjeruje u modificirani audio ili vizuelni izvor da bi se napravila velika šteta. ■

[12] K. Hao and P. Howell O'Neill (2020), *The hack that could make face recognition think someone else is you, MIT Technology Review*, 5 August (www.technologyreview.com/2020/08/05/1006008/ai-face-recognition-hack-misidentifies-person/).

FinTech - pojava ogromnog potencijala

FINTECH - RIZICI I IZAZOVI CYBER SIGURNOSTI

Nove tehnologije omogućavaju nam i nove, jednostavnije i brže finansijske usluge. Otvaramo bankarski račun bez odlaska na šalter banke; predajemo dokumentaciju digitalnim kanalima; mobitel se pretvara u digitalni novčanik; uz pomoć aplikacije vršimo plaćanje koristeći novac sa svog računa. Svjedočimo dobu intenzivne tehnološke promjene. Pandemija COVID-19 doprinosi na svoj način te mijenja naš život i navike. Možemo samo zamisliti revoluciju finansijskih usluga u godinama koje dolaze.

Autorica:
Sanela Vrana

Digitalna transformacija potpomognuta primjenom tehnologije u cilju unaprjeđenja postojećih ili stvaranja novih finansijskih usluga dovodi nas do pojma FinTech. FinTech, kao kombinacija riječi finansije i tehnologija, relativno je nova industrija koja koristi digitalnu tehnologiju, a odnosi se na različite proizvode, aplikacije, usluge i poslovne modele koji transformišu tradicionalni način pružanja bankarskih i finansijskih usluga. FinTech kompanije popunjavaju specifičnu prazninu na tržištu koja je nastala usljed sporih promjena u tradicionalnom bankarstvu. Njihovo poslovanje je u potpunosti digitalno. Primjenjujući složena softverska rješenja koja koriste vještačku inteligenciju i tehnologiju velikih podataka, algoritmima analiziraju i prepoznaju vrijednosti, uzorke i trendove povezane s ponašanjem i interakcijama među korisnicima.

Primjena tehnologije u finansijama nije nova. Bankarstvo se desetljećima prilagođavalo tehnološkim trendovima, ali u posljednje vrijeme, pod pritiskom pojave konkurentnih, izvorno-tehnoloških, neban-

> *„FinTech, kao kombinacija riječi finansije i tehnologija, relativno je nova industrija koja koristi digitalnu tehnologiju, a odnosi se na različite proizvode, aplikacije, usluge i poslovne modele koji transformišu tradicionalni način pružanja bankarskih i finansijskih usluga."*

karskih kompanija, tzv. *FinTech startupa*, tempo ulaganja u bankarske inovacije se ubrzava. Kao rezultat ovakve digitalne transformacije razlika između FinTech industrije i tradicionalnog bankarstva se postepeno smanjuje.

Globalni trendovi - korporacija ili konkurencija između FinTecha i tradicionalnih banaka

U ovom trenutku FinTech predstavlja brzo rastuću pojavu ogromnog potencijala. Premda postoji mišljenje da je budućnost u FinTech kompanijama, možemo reći da sinergija FinTecha s tradicionalnim bankama na zajedničkom kreiranju novih proizvoda te promjeni postojećih načina poslovanja otvara više mogućnosti za klijente. Neke banke preuzimaju FinTech startupe da bi proširile set svojih usluga. Uz inovativne ideje i smanjenje troškova, tradicionalno bankarsko poslovanje se mijenja, a poslovni modeli banaka prilagođavaju se novom okruženju. Postoje i drugačiji primjeri gdje velike nebankarske FinTech kompanije sklapaju partnerstva s bankama, preuzimaju ih i ulaze u bankarstvo, tj. apliciraju za bankarske licence. Izgleda da komplementarnost u kojoj banke daju reputaciju i sigurnost, a FinTech dinamiku i kreativnost daje najbolja rješenja.

> *Premda postoji mišljenje da je budućnost u FinTech kompanijama, možemo reći da sinergija FinTecha s tradicionalnim bankama na zajedničkom kreiranju novih proizvoda te promjeni postojećih načina poslovanja otvara više mogućnosti za klijente.*

Finansijske usluge koje nastaju na ovakav način raznovrsnije su, transparentnije, dostupnije, jeftinije i lako razumljive, a od toga najviše profitiraju klijenti čije se potrebe prepoznaju i zadovoljavaju.

Ravnoteža pogodnosti i sigurnosti u FinTechu

Cyber sigurnost u bankarstvu obezbijeđena je zakonskim propisima koji zahtijevaju od banaka da pružaju pouzdane i sigurne usluge. U okruženju, koje pridaje veliku

> *Bez uravnoteženog pristupa koji uzima u obzir strateški rast i temeljne koncepte cyber sigurnosti dolazi do stvaranja funkcionalnih, ali slabo osiguranih proizvoda koji u budućnosti mogu generisati značajne sigurnosne troškove.*

važnost zaštiti podataka i informacijskoj sigurnosti, banke testiraju i provode robusne sigurnosne procedure jer ne žele rizikovati gubitak reputacije, kazne, a time i gubitak klijenata.

FinTech kompanije su često mali, brzo rastući startupi koji, u pogledu sigurnosti, nisu strogo regulisani, te imaju veću fleksibilnost u prilagođavanju zahtjevima klijenata. Oni rijetko provode takve sigurnosne mjere kao tradicionalne banke te najčešće stavljaju pogodnost ispred sigurnosti. Povećanje regulatornih zahtjeva primorat će FinTech industriju da uravnoteži to dvoje. Bez uravnoteženog pristupa koji uzima u obzir strateški rast i temeljne koncepte cyber sigurnosti dolazi do stvaranja funkcionalnih, ali slabo osiguranih proizvoda koji u budućnosti mogu generisati značajne sigurnosne troškove. Primjenjivati sigurnosne mjere retroaktivno na postojeće platforme je teško, a ponekad i nemoguće zbog postavki ili konfiguracija koje se nakon puštanja proizvoda u opticaj ne mogu lako mijenjati. Iako bi sama infrastruktura FinTech kompanija, zbog potencijalnog brzog rasta, trebala biti visoko skalabilna, njeno naknadno osiguravanje može vrlo brzo postati veoma skupo.

S druge strane, FinTech kompanije rukuju novcem i ličnim podacima klijenta. Jedinstvena kombinacija ličnih i finansijskih podataka na tehnološkoj platformi čini FinTech privlačnom metom za cyber kriminalce. Brzina pružanja personalizovane usluge u konkurentskom okruženju pomaže FinTech kompaniji da se istakne i natječe s tradicionalnim ili digitalnim bankama, ali ne bi trebala biti na štetu sigurnosti. Ulaganje u cyber sigurnost FinTech kompanija jednako je važno

kao i ulaganje u inovacije. Primjenjivanje sigurnosnih mjera u svrhu izgradnje stabilnog i sigurnog rješenja koje zadovoljava specifične poslovne potrebe ne treba shvatiti kao prepreku za rast i razvoj nego kao zaštitu održivosti poslovanja.

FinTech – rizici i izazovi cyber sigurnosti

Rizici cyber sigurnosti, već veliki u bankarskoj industriji, u slučaju potpune digitalizacije finansijskih usluga i dalje se usložnjavaju. Sve FinTech

kompanije dijele slične rizike cyber sigurnosti bez obzira na to kojoj djelatnosti pripadaju. Koji su to rizici i kako ih eliminisati?

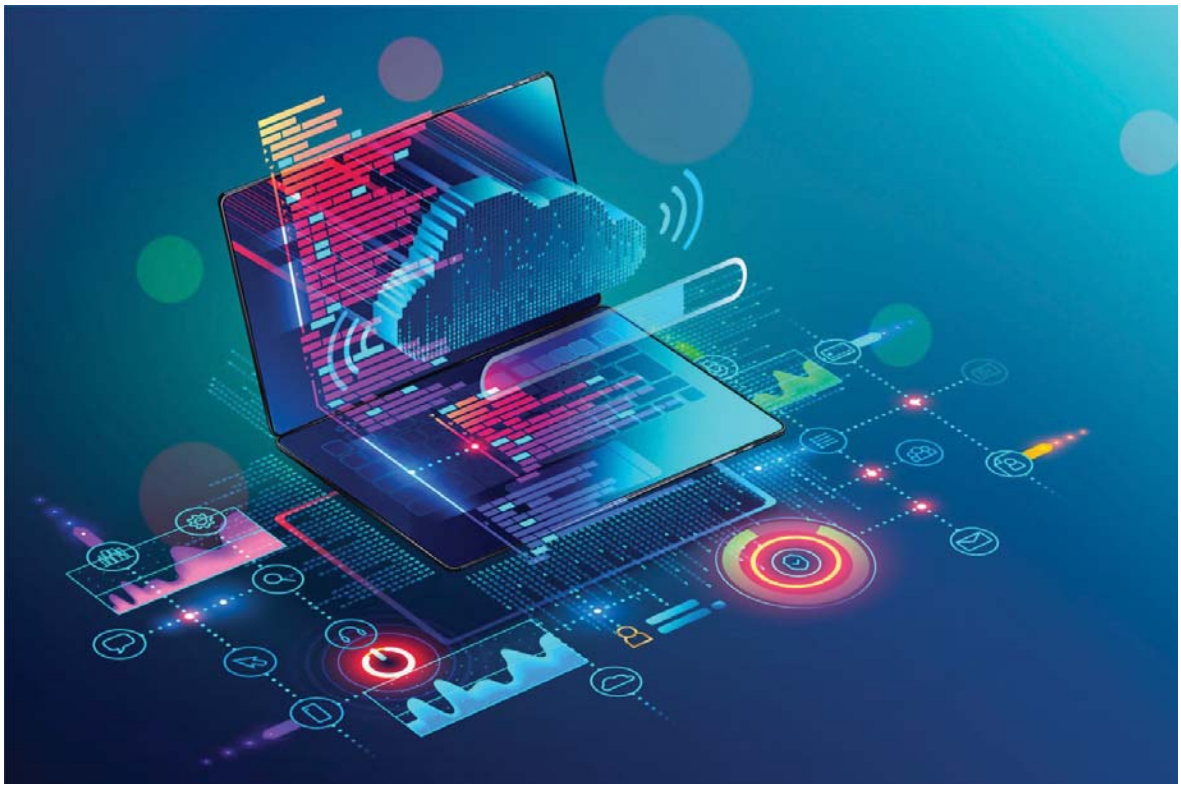
Težište FinTech poslovanja su aplikacije. One obezbjeđuju FinTechu veći broj klijenata te veći raspon usluga, ali su također ranjive i na napade. Preko aplikacije cyber napadači mogu pokušati doći i do mreže čitave kompanije. FinTech aplikacije omogućavaju korisnicima da popune osjetljive lične podatke i jednostavnim dodirom zaslona koriste novac sa svog računa. Oslanjanje na različite mobilne uređaje pri obavljanju ovakvih transakcija obezbjeđuje korisniku pristup bilo kada i bilo gdje. Jedini problem je što to isto potencijalno imaju i hakeri. Oni će pokušati pristupiti takvim računima, ukrasti novac korisnika ili njegove lične podatke te ih dalje koristiti u nizu kriminalnih aktivnosti kao što su krađa identiteta, finansijska prevara, ucjena i sl. Što se više uređaja koristi za pristup određenom računu, veće su šanse da taj račun bude kompromitovan. Gubitak povjerenja koji nastaje kao posljedica komprovitovanja računa korisnika ili podataka o korisniku, kršenje regulative o zaštiti ličnih podataka koje podliježe visokim kaznama i može izazvati pokretanje tužbi - u konačnici, sve to se pretvara u finansijske gubitke.
Cyber napad može imati katastrofalan učinak na FinTech kompaniju, naštetiti aktivnostima, prihodima i reputaciji. Napade s ciljem uskraćivanja usluga, *phishing* i *ransomware* napade često srećemo u tradicionalnom bankarstvu, a ni FinTech kompanije nisu imune na njih. Opasnost od

> *Opasnost od cyber kriminala povezanog s pranjem novca i finansiranjem terorizma čak se povećava u slučaju FinTech poslovanja, naročito ukoliko se radi o kriptovalutama.*

cyber kriminala povezanog s pranjem novca i finansiranjem terorizma čak se povećava u slučaju FinTech poslovanja, naročito ukoliko se radi o kriptovalutama. Iz svega navedenog slijedi da je i u FinTech kompanijama neophodno obezbijediti učinkovitu cyber sigurnost. Kako?

FinTech – najbolje prakse cyber sigurnosti

Jedinstveni program cyber sigurnosti - Priprema jedinstvenog programa cyber sigurnosti prilagođenog FinTech industriji te razrađenog u pojedinačne planove i operativne aktivnosti, uključujući potpuno razvijen i uvježban plan odgovora na incidente najbolji je način organizovanja zaštitnih mjera cyber sigurnosti.



Prepoznavanje najvrjednije imovine - Nemoguće je zaštititi ono što se ne poznaje. Potrebno je prepoznati najvrjedniju imovinu kompanije i omogućiti nesmetano izvođenje promjena osiguravajući pri tom da ta imovina nikada ne bude izložena.

Zaštita mreže - Zaštita mreže od upada cyber napadača prva je linija odbrane cyber sigurnosti. Rano otkrivanje problema ključ je i za njegovo rano rješavanje. Uz kvalitetan nadzor i praćenje mogu se otkloniti potencijalne ranjivosti i prije nego što nanesu štetu.

Odbrana od napada zlonamjernim softverom – Iako se noviji FinTechovi orijentišu prema protokolima plaćanja temeljenim na *blockchainu*, napadi zlonamjernim softverom i dalje predstavljaju rizik. Zlonamjerni softver može koristiti više ulaznih tačaka iz različitih izvora; njegova brzina prenosa je vrlo visoka, a može uzrokovati i rušenje cijele mreže. Automatizovano otkrivanje zlonamjernog softvera u realnom vremenu, redovni pregled ranjivosti, penetraciono testiranje i ažuriranje postojeće zaštite neophodni su koraci u izgradnji učinkovitih zaštitnih mjera.

Aplikacija kao vektor cyber napada - Aplikacija okrenuta korisnicima često se koristi kao vektor napada na FinTech kompaniju. Napadačima je obično lakše pristupiti aplikaciji nego mreži kompanije, a ukoliko dobiju pristup aplikaciji, pitanje je (kratkog) vremena kada će dobiti pri-

stup cijeloj mreži. Osim redovnog pregleda ranjivosti i testiranja penetracije, najbolji način zaštite je izrada sigurne aplikacije. Sigurnost same aplikacije u fazi dizajna uključuje praćenje najboljih praksi sigurnog razvoja aplikacija, preglede koda i penetracijska testiranja prije puštanja aplikacije u opticaj. Specifične sigurnosne tehnike potrebno je primjenjivati u svakoj životnoj fazi ciklusa razvoja softvera: od analize, preko dizajna, implementacije i testiranja, do održavanja i nadzora, ali integrisanje sigurnosti s finansijskim proizvodom od njegovog nastanka stvorit će jaču i učinkovitiju zaštitu.

Zaštita korisničkih identiteta - Zaštita korisničkih identiteta i računa provodi se implementacijom snažnih procesa provjere autentičnosti, uključujući zahtjeve za jake lozinke i multifaktorsku autentifikaciju.

Pouzdani pružatelj cloud usluga - Mnoge FinTech aplikacije su smještene u oblaku kroz koji protiče veliki broj podataka koji napadačima može poslužiti kao 'dimna zavjesa'. Zbog toga je bitno odabrati pouzdanog pružatelja usluga čiji je pristup cyber sigurnosti ažuran i proaktivan.

Rizik koji nose kriptovalute - Kriptovalute posljednjih godina stiču popularnost, ali su i veliki sigurnosni izazov za FinTech. Budući da porijeklo novca može biti anonimno, kriptovaluta se može koristiti za pranje novca. Također, anonimne transakcije kriptovaluta, kojima je veoma teško ući u trag, rado koriste hakeri kod naplate otkupnina za krađu podataka. FinTech kompanije koje se bave kriptovalutama trebale bi koristiti samo sigurne platforme za trgovanje i držati se *mainstream* kriptovaluta koje su univerzalno priznate.

Standardi sigurnosti i privatnosti - Najbolje prakse cyber sigurnosti podrazumijevaju i poštivanje ili certificiranje prema standardima koji se odnose na sigurnost i privatnost podataka. Neispunjavanje zahtjeva za usklađenost može rezultirati velikim kaznama, ali, što je još važnije, i velikim sigurnosnim propustima. Certificiranje samo po sebi neće odvratiti napadača, ali će dovesti u red upravljanje rizicima cyber sigurnosti te time obezbijediti sveobuhvatno prepoznavanje rizika i upravljanje ranjivostima.

Kultura odgovornosti pojedinca - Ojačavajući svijest i potičući internu komunikaciju između zaposlenika, stvara se kultura odgovornosti svakog pojedinca da učini svoj dio u obezbjeđenju cyber sigurnosti.

Cikličnost procesa - Cikličnost u procesu održavanja programa cyber sigurnosti obezbjeđuje uvijek ažuran pristup. Kako cyber kriminalci usavršavaju svoje tehnike, tako je potrebno da se i aktivnosti procesa cyber sigurnosti prilagođavaju novim potencijalnim prijetnjama i ranjivostima koje se svakodnevno pojavljuju.

Statistika i primjeri povrede podataka FinTech kompanija

Prema istraživanjima vodeće istraživačke organizacije za analizu sigurnosti, otkrivanje ranjivosti i usklađenost, ***Imperva Research Labs***, napadi na web aplikacije koje nude finansijske usluge u

prvoj polovini 2021. godine (u odnosu na prvu polovinu 2020. godine) povećali su se za 38%. Apetit cyber kriminalaca za ličnim podacima i dalje je visok, a 74% svih podataka ukradenih u posljednjih nekoliko godina može se iskoristiti za identifikaciju, kontaktiranje ili lociranje pojedinaca. Imperva je čak izvijestila da je samo u januaru 2021. godine kompromitovano više od 870 miliona zapisa osjetljivih podataka – više od ukupnog broja kompromitovanih podataka u cijeloj 2017. godini.

Jedan od poznatih slučajeva neovlaštenog pristupa ličnim podacima FinTech kompanije desio se sredinom 2020. godine kada su, hakiranjem vanjskog pružatelja usluga *Waydev*, zlonamjerni akteri dobili pristup cjelokupnoj korisničkoj bazi kompanije *Dave*, američkog pružatelja finansijskih usluga izvan tradicionalnog bankarskog sistema. Lične informacije 7,5 miliona korisnika FinTech Dave aplikacije bile su izložene ovoj povredi podataka. FinTech Dave riješio je sigurnosni problem tvrdeći da finansijske informacije, kao što su brojevi bankarskih računa, kreditnih kartica, kao i evidencija finansijskih transakcija, nisu bile ugrožene.

Finansijske usluge, prema brojnim izvještajima, nose najveći procenat štete od cyber kriminala. Među brojnim primjerima možemo izdvojiti jednu od najvećih povreda podataka u novije vrijeme, incident *Equifaxa* koji je 2017. godine razotkrio lične podatke 147 miliona ljudi. Equifax je potrošio 1,4 milijarde dolara samo na sigurnosne nadogradnje nakon incidenta, ne uključujući naknade osobama čiji su podaci otkriveni.

> *Finansijske usluge, prema brojnim izvještajima, nose najveći procenat štete od cyber kriminala.*

Dugoročno, za očekivati je da će sve više FinTech kompanija biti meta cyber napada. S druge strane, industrija koja se razvija jednako brzo kao FinTech je i cyber sigurnost. Za finansijske institucije cyber sigurnost je velika briga i veliki trošak, ali također i jedini način da budu korak ispred napadača. ■

Nacrt Smjernica za politike i procedure za upravljanje usklađenošću i ulozi i odgovornostima AML/CFT službenika

UNAPREĐENJE FUNKCIJE SPREČAVANJA PRANJA NOVCA I FINANSIRANJA TERORISTIČKIH AKTIVNOSTI U KONTEKSTU NACRTA EBA SMJERNICA ZA POLITIKE I PROCEDURE ZA UPRAVLJANJE USKLAĐENOŠĆU I ULOZI I ODGOVORNOSTIMA SLUŽBENIKA ZA SPREČAVANJE PRANJA NOVCA

Podnošenjem izvještaja Evropske komisije o potrebi implementacije boljeg okvira za sprečavanje pranja novca i finansiranja terorističkih aktivnosti, koji je utvrdio da je ogromna količina novčanih sredstava uključena direktno ili je vezana za aktivnosti koje imaju prefiks sumnjivih, zaključeno je da utvrđeni nedostaci predstavljaju značajnu prijetnju sigurnosti EU i njenim građanima i da AML/CFT okvir EU mora biti poboljšan bez odgađanja.

Autor:
Nermin Ibradžić

Izvještaj Evropske komisije - poziv na buđenje

Dana 24. jula 2019. godine Evropska komisija je prema Evropskom parlamentu i Vijeću Evrope usvojila i komunicirala izvještaj o potrebi implementacije boljeg okvira za sprečavanje pranja novca (dalje: AML) i finansiranja terorističkih aktivnosti (dalje: CFT).

Iako su u navedenom području zabilježeni pozitivni pomaci, izvještaj je ukazao da u pojedinim slučajevima i kod pojedinih grupacija banaka ili zemalja članica još uvijek postoje nedostaci koji generišu značajne rizike u AML/CFT području.

Jedan od okidača za kontrolu Evropske komisije i podnošenje izvještaja bila je projekcija da je čak do 1,28% GDP-a EU vezano za *sumnjive finansijske aktivnosti* (prema izvještaju Europola iz 2017. godine). Ukoliko se uzme u obzir da se GDP EU u godinama od 2017. do 2020. kreće u rasponu od 13,07 do čak 13,97 triliona EUR[1], jasno je koliko je novčanih sredstava uključeno direktno ili je vezano za aktivnosti koje imaju prefiks sumnjivih. Stoga je i pomenuti izvještaj Evropske komisije shvaćen prilično ozbiljno.

Prilikom sačinjavanja izvještaja Evropska komisija se rukovodila i standardima definiranim četvrtom, petom i šestom AML/CFT EU Direktivom.

> *Jedan od okidača za kontrolu Evropske komisije i podnošenje izvještaja bila je projekcija da je čak do 1,28% GDP-a EU vezano za sumnjive finansijske aktivnosti (prema izvještaju Europola iz 2017. godine).*

U četiri posebna dijela izvještaj je prikazao osnovne nedostatke[2].

U dijelu Izvještaja o slučajevima pranja novca i finansiranja terorizma prisutnim u finansijskim institucijama u EU, Komisija je identificirala:

- neadekvatnu prioretizaciju AML/CFT izazova u politikama banaka;
- nedostatak resursa u jedinicama koje se bave AML/CFT pitanjima;
- AML/CFT sistem internih kontrola uspostavljen formalno, bez stvarnih efekata;
- identifikovani su i nedostaci u *tri linije odbrane* pri čemu u pojedinim slučajevima prva linija odbrane nije uopće postojala, druga linija odbrane nije bila adekvatna, a interna revizija, kao treća linija odbrane, nije pridavala potreban značaj AML/CFT području;

- komunikacija AML/CFT pitanja prema višem i visokom rukovodstvu nije bila adekvatna, a u pojedinim slučajevima nije niti postojala;
- u pojedinim slučajevima agresivne metode uspostavljanja poslovnih odnosa s novim klijentima i transakcije nisu praćene zadovoljavajućom dubinskom analizom klijenata i transakcija;
- supervizorski timovi, koji treba da vrše kontrolu finansijskih institucija, u određenim slučajevima

[1] Izvor: www.statista.com

[2] Izvor: *Towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework*, Harold Koster Leiden University, Leiden, The Netherlands and Erasmus University Rotterdam, Rotterdam, The Netherlands

nisu imali dostatne ljudske potencijale, dok postojeći potencijali nisu bili dovoljno educirani i na *visini zadatka*;
– sankcije supervizora za učinjene AML/CFT prekršaje nisu bile adekvatne.

U dijelu izvještaja izvannacionalne procjene AML/CFT rizika i uticaja na EU, Komisija je identifikovala:
– 47 proizvoda finansijskih institucija koji su podložni AML riziku;
– evidentan rizik korištenja komplikovanih šema organizacije pravnih lica u *trećim zemljama*;
– nedostatke ili izostanak postojanja registara stvarnih vlasnika pravnih lica.

U dijelu međusobne saradnje obavještajno-finansijskih odjela (dalje: FIU) pojedinih zemalja, identifikovano je:
– izostanak saradnje FIU na nivou EU u pojedinim slučajevima;
– u pojedinim slučajevima nedostatak IT alata na strani FIU.

U dijelu izvještaja koji obuhvata procjene centralnih banaka vezano za adekvatnost sistema prikupljanja, obrade i razmjene podataka o računima, Komisija je procijenila da u osnovi svaka članica EU ima određeni sistem koji sadrži potrebne i korisne informacije, ali je ove sisteme potrebno dalje unapređivati i uvezivati na jedinstvenu EU platformu.

Zaključak utvrđenih nedostataka jeste da isti predstavljaju značajnu prijetnju sigurnosti EU i njenim građanima i da AML/CFT okvir EU mora biti poboljšan bez odgađanja.

Rezultat zaključaka jeste Nacrt Smjernica za politike i procedure za upravljanje usklađenošću i ulozi i odgovornostima AML/CFT službenika prema članu 8. iz poglavlja IV EU Direktive 2015/849 (dalje: Nacrt Smjernica)[3].

Nacrt Smjernica je publikovan 29.07.2021. godine, s 02.11.2021. kao rokom za dostavu komentara.

Stari problemi, nova rješenja

Kao većina pitanja vezanih za AML/CFT područje, i Nacrt Smjernica u BiH je prošao gotovo nezapaženo, što je u najmanju ruku čudno za zemlju koja zauzima visoko i nezavidno 111. mjesto od 180 zemalja po indeksu percepcije korupcije prema izvještaju *Transparency Internationala* za 2020. godinu.

Potrebno je naglasiti da Nacrt Smjernica predstavlja prvi i jedinstven dokument takve vrste u EU koji bi na sveobuhvatan način trebao uspostaviti osnovne standarde vezane za ulogu i odgovornosti

[3] Za detalje vidi: Consultation Paper, Draft Guidelines On policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849

AML/CFT službenika, ali i ulogu i odgovornosti višeg i visokog rukovodstva finansijskih institucija vezano za ovo pitanje.

Koje to novine donosi Nacrt Smjernica?

Prije svega, kod međunarodnih bankarskih grupa, gdje se banka *majka* nalazi u EU, nastaje obaveza imenovanja Grupnog AML/CFT službenika. Kroz izvještaj koji je podnijela Evropska komisija jasno je vidljivo da je kod pojedinih banaka članica većih grupacija postupanje po AML/CFT standardima bilo neujednačeno, od implementacije standarda do raportiranja. Ovo je dovelo do situacije u kojoj više rukovodstvo na nivou bankarske grupe nije raspolagalo dostatnim informacijama o stanju AML/CFT-a, te je propustilo poduzeti adekvatne mjere upravljanja AML/CFT rizikom. Predmetno se navodi kao jedan od osnovnih razloga AML/CFT afera u pojedinim bankarskim grupacijama. Jedan od osnovnih zadataka grupnog AML/CFT službenika bi bio da se pobrine da su AML/CFT standardi implementirani u bankarskoj grupaciji na adekvatan način i jednako. Dalji zadatak Grupnog AML/CFT službenika jeste da više rukovodstvo izvještava o stepenu usaglašenosti, poduzetim mjerama i utvrđenim nedostacima.

> *Kroz izvještaj koji je podnijela Evropska komisija jasno je vidljivo da je kod pojedinih banaka članica većih grupacija postupanje po AML/CFT standardima bilo neujednačeno, od implementacije standarda do raportiranja.*

Drugi standard Nacrta Smjernica koji treba biti naglašen jeste uloga *tijela upravljanja* finansijske institucije u djelu AML/CFT aktivnosti. Iz definicije pojma *tijela upravljanja* iz Nacrta Smjernica proizilazi da se radi o ekvivalentu lokalne uprave banke ili nadležnog člana uprave banke koji bi u dijelu AML/CFT trebali imati dvojnu funkciju - funkciju upravljanja i funkciju nadgledanja. U dijelu funkcije nadgledanja uprava banke/nadležni član uprave treba imati nesmetan pristup svim informacijama vezanim za AML/CFT područje, dok u dijelu upravljanja treba osigurati sve uslove za efikasnu implementaciju AML/CFT funkcije, uključivo ljudske resurse i tehničke uslove. Uprava banke bi bila direktno odgovorna i za stvaranje uslova za implementaciju relevantnih AML/CFT standarda, ali bi bila obavezna i da razmatra i procjenjuje izvještaje AML/CFT službenika. Nacrt Smjernica definira i posebne uslove za nadležnog člana uprave banke koji se odnose na adekvatno iskustvo i poznavanje AML/CFT materije. Nacrt Smjernica propisuje i jasne kriterije za odgo-

> *Nacrt Smjernica propisuje i jasne kriterije za odgovornosti, ovlaštenja i profil AML/CFT službenika. Prvenstveno je naglašeno da AML/CFT službenik ne može biti podređen članu upravljačkog tijela (uprave) koji u svojim ovlaštenjima ima aktivnosti koje AML/CFT službenik treba nadgledati.*

vornosti, ovlaštenja i profil AML/CFT službenika. Prvenstveno je naglašeno da AML/CFT službenik ne može biti podređen članu upravljačkog tijela (uprave) koji u svojim ovlaštenjima ima aktivnosti koje AML/CFT službenik treba nadgledati. Tako je unaprijed isključeno da AML/CFT službenik može biti podređen članu uprave koji je odgovoran za prodaju, platne transakcije, korespondentsko bankarstvo i sl. Pored obaveze da AML/CFT službenik ima pristup svoj dokumentaciji i informacijama finansijske institucije, jasno je naglašeno da je isključivo AML/CFT službenik osoba koja će odlučiti koje informacije su mu potrebne i u kom obliku. Na ovaj način se evidentno izbjegavaju situacije u kojima se, pod okriljem povjerljivosti, AML/CFT službeniku ograničava pristup pojedinim informacijama ili su mu proslijeđivane *zamjenske* informacije umjesto onih koje su tražene iz razloga što finansijska institucija nije raspolagala tehničkim mogućnostima ili možda voljom da dostavi set podataka koji su inicijalno traženi.

Uloga AML/CFT službenika prema Nacrtu Smjernica jasno je naglašena i u dijelu edukacija koji, zbog značaja, dobija jedno posebno poglavlje. Pored obaveze obuke iz područja AML/CFT za nove zaposlenike, i to neposredno nakon njihovog prijema, AML/CFT službenik bi imao obavezu da pripremi adekvatne programe edukacije ne samo za stranu prodaje/mreže/poslovnica, nego i za druge funkcije koje se dotiču pitanja AML/CFT-a te za zaposlenike koji direktno, pored ili zajedno s AML/CFT službenikom, rade na implementaciji standarda kao i za vanjske pružaoce usluga. Edukacije i treninzi, pored teorijskog, treba da sadrže i praktični dio, a dodatna uloga AML/CFT službenika je da razvije indikatore temeljem kojih će moći procijeniti da li je i u kojoj mjeri edukacija/trening uspio.

Nacrt Smjernica sada propisuje i jedinstvenu formu izvještaja AML/CFT službenika. U zavisnosti od kompleksnosti i veličine finansijske institucije, izvještaji AML/CTF službenika će obuhvatiti do 27 raznih tačaka, od broja sumnjivih transakcija do procjene AML/CFT službenika o raspoloživosti ljudskih i tehničkih resursa potrebnih za adekvatno upravljanje AML/CFT rizicima. Sam izvještaj sadrži veliki broj statistički obrađenih i podataka agregiranih iz centralnog sistema banke, što će svakako uticati i na dorade u smislu novih aplikativnih zahtjeva u postojećem IT okruženju.

Imajući u vidu da aktivnosti AML/CFT službenika u Nacrtu Smjernica dobijaju na intezitetu i kompleksnosti, kroz Nacrt Smjernica je prepoznata i potreba definiranja kriterija za AML/CFT službenike s ciljem kako bi isti na adekvatan način odgovorili budućim izazovima. Pored kriterija reputacije, poštenja i integriteta, od kandidata za AML/CFT službenika će biti tražen i zadovoljavajući nivo vještina i ekspertize u dijelu pravne regulative, razumijevanja AML/CFT standarda i identifikacije rizika kao i vremenska raspoloživost kandidata za obavljanje ove bitne funkcije. Već u ovom momentu je izgledno da će za budući izbor AML/CFT službenika biti potrebna *fit& proper* procjena koja se

> *Pored kriterija reputacije, poštenja i integriteta, od kandidata za AML/CFT službenika će biti tražen i zadovoljavajući nivo vještina i ekspertize u dijelu pravne regulative, razumijevanja AML/CFT standarda i identifikacije rizika kao i vremenska raspoloživost kandidata za obavljanje ove bitne funkcije.*

primjenjuje za ključne i kontrolne funkcije ili za kandidate višeg rukovodstva banke.

Posljednje, ali ne i manje bitno, Nacrt Smjernica propisuje obavezu učešća AML/CFT funkcije u realizaciji plana kontinuiteta poslovanja (BCP) kroz dva segmenta: kroz obavezu uvrštavanja u BCP situacije nedostupnosti AML/CFT službenika i situaciju kada je AML/CFT službenik u nemogućnosti obavljanja funkcije na koju je imenovan uslijed toga što je njegov/njen integritet doveden u pitanje. Prilikom kreiranja BCP-a, AML/CFT službenik je u obavezi da identificira područja ili aktivnosti za koje bi bilo potrebno osigurati kontinuitet provođenja u svim okolnostima.

Rezime

Kroz Nacrt Smjernica EU regulator pokazuje odlučnost da područje upravljanja rizicima, izvještavanja i uslova za rad AML/CFT funkcije definira na jedinstven način, ne samo za finansijske institucije na području jurisdikcije EU, nego i za finansijske institucije van tog okvira, a koje su članice grupe koja matičnu finansijsku instituciju ima na području EU.

Upravo zbog tog elementa grupne usklađenosti, evidentno je da će nove EBA smjernice, jednom kad stupe na snagu, imati efekte i na banke u BiH čije matične banke imaju sjedište u EU.

Način na koji Nacrt Smjernica vidi AML/CFT funkciju u budućnosti ne može se nazvati izmjenom koja će izazvati tektonske promjene u finansijskom sektoru. Veliki broj standarda iz Nacrta Smjernica lokalne banke primjenjuju, prema nalozima grupe banaka kojoj pripadaju ili prema nalozima lokalnog regulatora. Međutim, stepen zahtijevanih unapređenja onog što već postoji nije zanemarljiv, a posebno u područjima:

- znanja i vještina AML/CFT službenika;
- uslova za rad AML/CFT funkcije;
- izvještavanja;
- odgovornosti višeg rukovodstva (prvenstveno uprave banke) i
- edukacija i treninga.

Svi procesi, koje će biti potrebno unaprijediti, zahtijevat će multidisciplinaran pristup kroz aplikativne dorade, selekcijski proces za zaposlenike, dodatne edukacije, moguću izmjenu organizacijske šeme i sl.

Dosadašnje iskustvo je pokazalo da se EU standardi i zahtjevi u lokalno zakonodavstvo prenose *u zadnji čas* s izuzetno kratkim rokovima za implementaciju i usklađivanje. Stoga bi na mjestu bila sugestija da AML/CFT funkcija kao minimum u ovom momentu već pokrene aktivnosti kako bi više rukovodstvo upoznala s potencijalnim dodatnim zahtjevima u pogledu AML/CFT kao i resursima koji će biti prijeko potrebni da se to ostvari. ■

Jedna od najbrže rastućih kriminalnih grana

KRAĐA IDENTITETA

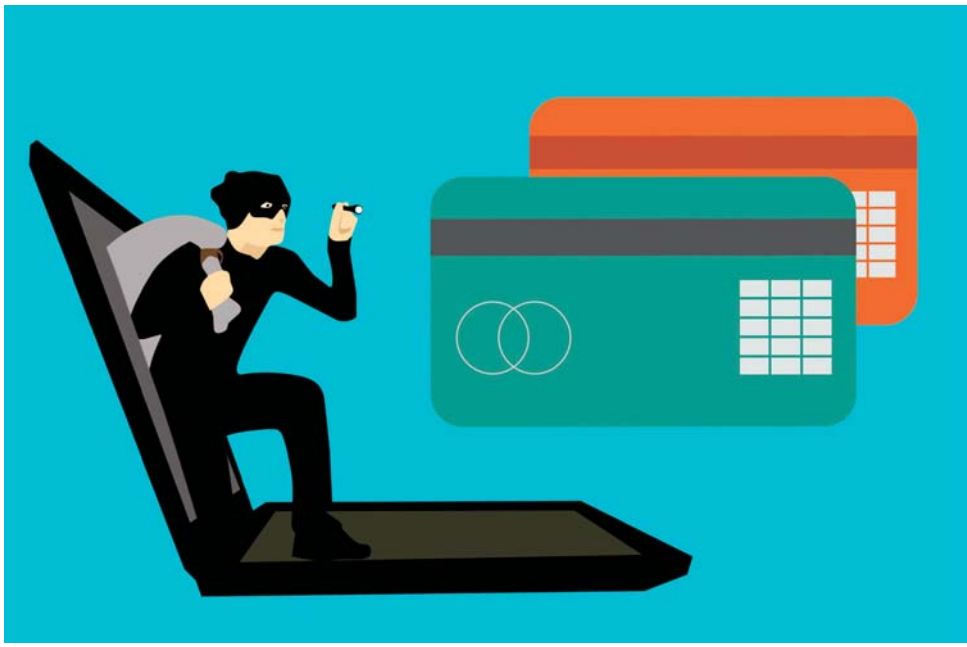
Razvoj tehnologije omogućava nam nove načine komuniciranja, informisanja, obrazovanja, rada i zabave. Nismo ni svjesni količine ličnih informacija koje pri tome ostavljamo na internetu te na taj način olakšavamo kriminalcima njihovu zloupotrebu. Ni kriminalci nisu više oni stari. Različite vrste krađa i prevara dešavaju se bez upotrebe sile, maski na licu ili oružja. Krađa identiteta jedan je od najčešćih oblika računarskog kriminala. Ona ne poznaje granice - žrtva i prijestupnik mogu biti na dvije različite strane svijeta.

Autorica:
Sanela Vrana

Informacije koje nas mogu identifikovati (PII – *Personally Identifiable Information*)

Da bismo počeli priču o krađi identiteta, moramo krenuti od onoga čime je naš identitet jednoznačno određen. Podaci uz pomoć kojih možemo jedinstveno identifikovati određenu osobu smatraju se osjetljivim i spadaju u jedinstvene identifikatore, a to su matični broj, broj lične karte, vozačke dozvole, broj računa u banci i druge finansijske informacije, kao i broj

pasoša i sl. Ostali lični podaci, kao što su ime i prezime, adresa, datum rođenja, broj telefona, e-mail adrese, lozinke, pa čak i lokacija, IP adresa ili fotografija, u kombinaciji jedni s drugima mogu poslužiti u identifikaciji pojedinca te su na jednak način privlačni prevarantima. Sve navedene informacije opisuju naš jedinstveni identitet. Uz pomoć identiteta mi obavljamo radnje u svakodnevnom životu.



Krađa identiteta

Za identifikacijske podatke povezuju se različiti rizici. Oni mogu biti kopirani, preneseni, viđeni, objavljeni, ukradeni ili korišteni od strane neovlaštenih pojedinaca. Kada dođe do otuđenja i neovlaštenog korištenja tuđih identifikacijskih podataka, tada govorimo o krađi identiteta kao obliku kriminalne radnje lažnog predstavljanja, a u svrhu sticanja materijalne koristi ili prikrivanja nekog djela.

> *Kada dođe do otuđenja i neovlaštenog korištenja tuđih identifikacijskih podataka, tada govorimo o krađi identiteta kao obliku kriminalne radnje lažnog predstavljanja, a u svrhu sticanja materijalne koristi ili prikrivanja nekog djela.*

Krađa identiteta jedan je od najčešćih oblika računarskog kriminala. Ova kriminalna grana postala je vrlo unosan posao zbog sve veće dostupnosti naših informacija na internetu. Globalna pandemija imala je dramatičan uticaj na ponašanje ljudi u njihovom poslovnom i privatnom životu. Stvorila je mnogo više tačaka ranjivosti za pojedince i kompanije. Ljudi sve više vremena provode online, kako zbog posla i online trgovine tako i zbog društvenih mreža, te namjerno ili nenamjerno dijele informacije o sebi. Cyber kriminalcima ovakve promjene, nažalost, pogoduju. Što je više informacija koje su o nekom pojedincu dostupne

> *Što je više informacija koje su o nekom pojedincu dostupne online, to je lakše preuzeti njegov identitet.*

online, to je lakše preuzeti njegov identitet.

Iako krađa identiteta nije tako zastrašujuća kao nasilni zločini u fizičkom svijetu, ipak je riječ o vrlo ozbiljnoj, invazivnoj i uznemirujućoj vrsti zločina jer ovaj oblik kriminala gotovo uvijek ostaje neotkriven sve dok se ne uoče njegove posljedice. Krađa identiteta, kao kriminalna aktivnost, danas već dostiže epidemijske razmjere. Mnoge druge vrste cyber kriminala u osnovi imaju krađu identiteta kao polaznu tačku za izvršavanje kriminalnih djela.

Digitalni tragovi – *zlatni rudnik*

Današnje vrijeme karakteriše obrada ogromnih količina podataka. Lični podaci u svemu tome postaju veoma vrijedni. Za cyber kriminalce lični podaci su *zlatni rudnik*, ali i u mnogim legalnim poslovima lične podatke nazivaju i po vrijednosti smatraju *novom naftom*.

Digitalni tragovi, tj. podaci o određenom korisniku koji su dostupni online, čine njegov jedinstveni digitalni otisak, a

> *Za cyber kriminalce lični podaci su zlatni rudnik, ali i u mnogim legalnim poslovima lične podatke nazivaju i po vrijednosti smatraju novom naftom.*

možemo ih grupisati u dvije kategorije:

- aktivni digitalni tragovi su podaci koje sami korisnici namjerno dijele ili svjesno ostavljaju koristeći internet,
- pasivni digitalni tragovi se prikupljaju o korisnicima, a da oni toga nisu ni svjesni (lokacija, IP adresa i sl.).

Ukoliko zamislimo sve moguće kombinacije gore navedenih kategorija, uz primjenu analize i različitih algoritama, vidjet ćemo da je naš digitalni otisak mnogo veći nego

> *Podaci su osnova nove industrijske revolucije, ali njihova neadekvatna upotreba može nanijeti ozbiljnu štetu.*

što smo mislili. Digitalni tragovi imaju i nekih prednosti, npr. omogućavaju praćenje zlonamjernih aktivnosti te poboljšanje i personalizaciju usluga na internetu, ali su za našu analizu daleko značajniji njihovi negativni aspekti, kao što su gubitak privatnosti te različite mogućnosti krađe identiteta i kriminalnih radnji koje se na tome zasnivaju. Krađa identiteta predstavlja tešku povredu privatnosti. Podaci su osnova nove industrijske revolucije, ali njihova neadekvatna upotreba može nanijeti ozbiljnu štetu.

Tipovi krađe identiteta

Nije se krađa identiteta uvijek dešavala putem interneta. Nekada su kradljivci pretraživali smeće u potrazi za bankovnim izvodima, gledali preko ramena ili nastojali ukrasti lične stvari (novčanike) i u takvim slučajevima bismo mogli reći da se radi o krađi identiteta fizičke prirode. Danas češće govorimo o krađi identiteta elektronske prirode gdje kradljivci koriste napredne tehnološke metode te dolaze u posjed cijelih baza podataka ličnih ili povjerljivih informacija; koriste

maliciozni kod, metode socijalnog inžinjeringa, presretanje ili preusmjeravanje mrežnog saobraćaja.

Krađa podataka ne podrazumijeva samo krađu ličnih podataka iz organizacija koje pohranjuju podatke. Često se događa da napadač dobija informacije direktno ili na prevaru od same žrtve. Žrtva u većini slučajeva nije svjesna kriminalne radnje sve dok se ne uoče njene posljedice. Elektronska krađa identiteta ne poznaje geografske granice – žrtve i prijestupnici mogu biti na suprotnim stranama svijeta.

Prema podacima koji se otuđuju, krađa podataka može uključivati krađu finansijskih podataka, matičnih ili čak medicinskih podataka, a postoji i takozvana **sintetička** krađa podataka. Kod sintetičke krađe podataka, kriminalac kombinuje stvarne i lažne informacije (najčešće stvarni jedinstveni indentifikator, npr. matični broj s izmišljenim ličnim podacima, npr. imenom ili adresom) i stvara novi identitet koji onda koristi u svrhu prevare. Nije rijetka ni krađa identiteta preminulih, a sve češća je krađa identiteta djece.

Kako se koriste ukradeni identiteti

Postoje razni maliciozni načini na koji kriminalci mogu iskoristiti nečiji identitet. Ukradeni identiteti služe širokom spektru kriminalnih radnji, kao što su prevare, krivotvorenje i narušavanje privatnosti te kriminalne radnje pronevjere, iznude, ucjene i sl.

Kada cyber kriminalci dođu u posjed ličnih identifikacijskih podataka, oni mogu otvoriti nove *online* ili bankovne račune, podići kreditne kartice i/ili vršiti kupovinu uz pomoć njih, aplicirati za kredit ili počiniti bilo kakav kriminal u tuđe ime. Ovakve zlonamerne radnje stvaraju velike probleme za žrtvu, čak i onda kada se počinilac uhvati, jer mogu usloviti narušavanje ugleda ili kreditnog rejtinga, a za otklanjanje posljedica nekada je potrebno potrošiti mnogo novca i vremena.

> *Ukradeni identiteti služe širokom spektru kriminalnih radnji, kao što su prevare, krivotvorenje i narušavanje privatnosti te kriminalne radnje pronevjere, iznude, ucjene i sl.*

Tuđi identitet počinitelj može iskoristiti i kako bi dobio pristup osjetljivim informacijama, npr. povjerljivim poslovnim dokumentima, a jedan od malicioznih načina

korištenja ukradenog identiteta je i njegova prodaja na ***Dark Webu***, sakrivenom dijelu interneta čiji je skoro sav sadržaj ilegalan, a koji nazivamo i podzemljem ili mračnom stranom interneta. Tako su se na Dark Webu u aprilu 2021. godine našli na prodaju više od milijardu *Facebook* i *LinkedIn* računa, uključujući imena, lokacije, datume rođenja, e-mail adrese, te u slučaju LinkedIna i sve ostale poslovne podatke korisnika. Uz pomoć ukradenih informacija mogli su se identifikovati pojedinci iz 106 različitih zemalja. Nešto malo ranije, početkom 2021. godine, dogodilo se curenje preko dvjesto dvadeset miliona veoma osjetljivih ličnih podataka Brazilaca, čak više od trenutne populacije Brazila jer su podaci obuhvatali i preminule osobe. Baze podataka koje su postale dostupne besplatno ili uz naknadu uključivale su imena, jedinstvene poreske identifikatore, slike lica, adrese, brojeve telefona, e-mail adrese, kreditne bilanse, plate i više od toga.
Kao primjer najopasnijeg načina iskorištavanja krađe identiteta možemo navesti iskorištavanje ukradenih podataka od strane osoba koje su u prošlosti imale problema sa zakonom te nastoje iskoristiti tuđi identitet kako bi izbjegle posljedice.

> *Ono što je zastrašujuće je broj pokušaja i brzina kojom kriminalci dolaze do izloženih podataka, što pokazuje njihovo veliko interesovanje za lične podatke i njihovu spremnost da ih promptno ukradu ukoliko im se otvori put.*

Ono što je zastrašujuće je broj pokušaja i brzina kojom kriminalci dolaze do izloženih podataka, što pokazuje njihovo veliko interesovanje za lične podatke i njihovu spremnost da ih promptno ukradu ukoliko im se otvori put.

Nemojte biti dio statistike

Globalna pandemija je obezbijedila plodno tlo za sve vrste cyber kriminala, a naročito za krađu identiteta.

Prema izvještajima FTC-a (*Federal Trade Commission* – američka nezavisna agencija čiji je cilj zaštita potrošača) broj slučajeva krađe identiteta se više nego udvostručio u 2020. godini. Za razliku od 2019. godine, kada je ukupni gubitak od krađe identiteta u SAD-u iznosio blizu 17 milijardi, u 2020. godini ova je brojka dostigla iznos od 56 milijardi dolara, a 49 miliona potrošača su postali žrtvom krađe identiteta (*2021 Identity Fraud Study by Javelin Strategy & Research*).

Krivični zakon Bosne i Hercegovine ne poznaje direktno materiju krađe identiteta kao krivično djelo te se na slične situacije primjenjuju odredbe vezane za nedozvoljeno korištenje ličnih podataka, falsifikovanje isprava ili lažno predstavljanje. Cyber kriminal u našem regionu još uvijek nije uznapredovao, ali sa sve većim brojem osoba koje koriste online plaćanje i koje svoje podatke nepromišljeno ostavljaju širom interneta za očekivati je da broj prevara svake godine bude sve veći. Krađa ličnih podataka i krivotvorenje podataka ne događa se samo u filmovima. Kazne za takva djela nisu bezazlene. U Bosni i Hercegovini se za nedozvoljeno korištenje ličnih podataka može dobiti novčana kazna ili kazna zatvora (*Krivični zakon Bosne i Hercegovine*).

Kako se zaštititi od krađe identiteta

Pravo na zaštitu ličnih podataka i privatnosti jeste jedno od osnovnih ljudskih prava. S naglim razvojem digitalne tehnologije i interneta, ovo pravo dovedeno je u pitanje. Srećom, postoje i preventivne mjere koje se mogu poduzeti, kako online tako i offline, da bi se zaštitile informacije čije otkrivanje bi moglo dovesti do krađe određenog identiteta.

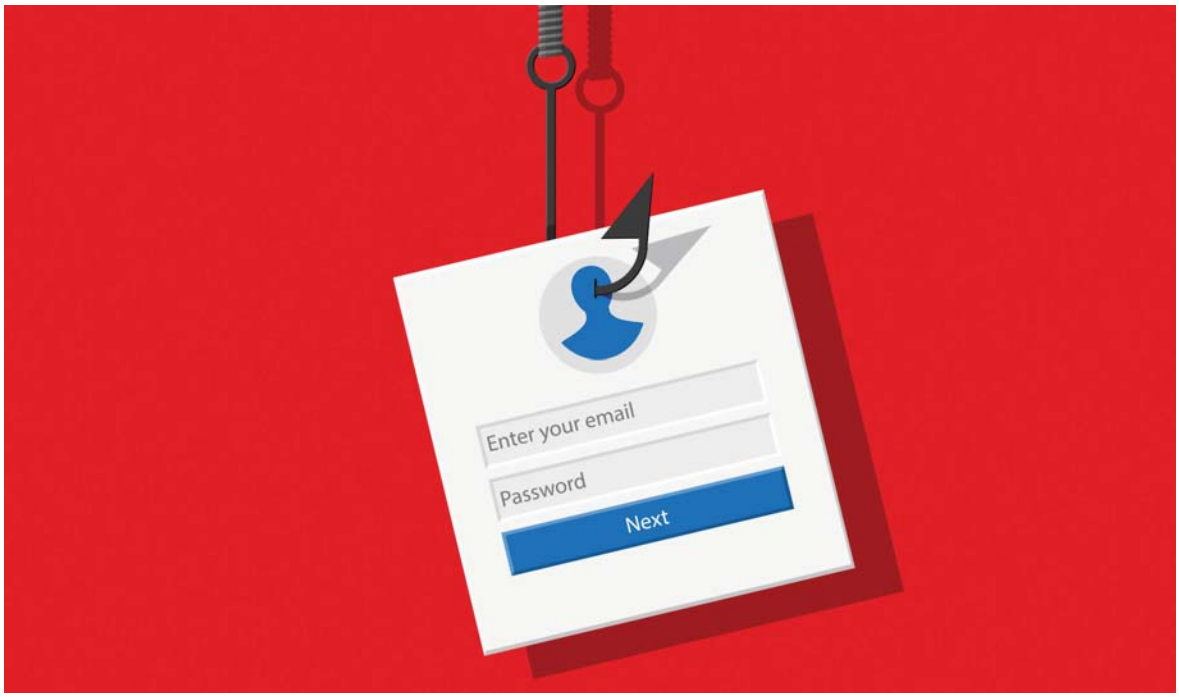
Online:

– ne dijelite svoje lične podatke ukoliko niste sigurni da je riječ o provjerenoj osobi ili organizaciji - za dostavu ličnih podataka treba da postoji osnovan razlog; budite naročito oprezni kada ostavljate

svoje lične podatke na javno dostupnim web stranicama;
– dobro osmislite, ali i redovno mijenjate lozinke na korisničkim računima; koristite *firewall* i antivirusni program; ažurirajte softver na svim vašim uređajima;
– nemojte držati skenirane dokumente s ličnim podacima na računarima;
– budite svjesni lažnih poruka u kojima se od vas traži da potvrdite podatke o vašem računu; prijavite takve pokušaje i pomozite razotkrivanju prevaranata - banke od svojih korisnika nikada ne traže potvrdu putem e-maila;
– pratite svoje bankovne izvode, obratite pažnju na nepoznate transakcije te odmah prijavite bilo kakva neslaganja ili neovlaštene aktivnosti vašoj banci;
– zaštitite svoju elektronsku poštu kao što biste zaštitili sadržaj svog novčanika ili torbe.

Offline:

– količinu dokumenata koje svakodnevno nosite sa sobom svedite na minimum; ne nosite lične dokumente u novčaniku i pokazujte ih samo kada je neophodno;
– nikada ne zapisujte PIN-ove za svoje platne kartice na samim karticama ili na bilo kojem dokumentu u novčaniku;
– budite svjesni pogleda ljudi koji vam 'vire preko ramena' kada unosite svoj PIN na bankomatu ili čekate u redu za blagajnu; kada karticu predate blagajniku, ne ispuštajte je iz vida;
– ne koristite bankomat ako primijetite da ga je neko neovlašteno dirao ili otvarao te prijavite svoje sumnje banci;



– budite oprezni s telefonskim pozivima iz navodno legitimnih kompanija koje zahtijevaju lične, finansijske i/ili *login* kredencijale; nikada nemojte telefonom davati svoje finansijske podatke;
– odložite bankovne izvode, račune i povjerljivu korespondenciju na sigurno mjesto, baš kao što biste uradili i s drugim vrijednim predmetima, te uništite sve dokumente koje više ne trebate.

Ukoliko je došlo do krađe identiteta

Rano otkrivanje krađe identiteta je veoma važno. Prilikom pokušaja krađe identiteta, ključno je brzo djelovati i sve prijaviti nadležnim službama. Što se prije otkrije krađa identiteta, to će se prije poduzeti mjere u cilju sprečavanja daljnje štete.

Ukoliko su vaši lični podaci kompromitovani, imate saznanje da prevarant posjeduje podatke o vašem bankovnom računu ili da je vašem računu na internetu neko nezakonito pristupao, potrebno je da hitno kontaktirate nadležne (banku, policiju, web stranicu...).

Prilikom pokušaja krađe identiteta, ključno je brzo djelovati i sve prijaviti nadležnim službama.

Što se prije otkrije krađa identiteta, to će se prije poduzeti mjere u cilju sprečavanja daljnje štete.

Ukoliko se radi o elektronskoj krađi identiteta, prisjetite se i zapišite sve detalje o napadu kojih se možete sjetiti: korisnička imena, brojevi računa ili lozinke koje ste eventualno podijelili. Odmah promijenite lozinke na zahvaćenim računima, kao i na bilo kojim drugim ukoliko koristite istu lozinku. Dodajte višestruku provjeru autentičnosti za svaki račun za koji možete. Obavijestite svoje kontakte o mogućem napadu s vašeg kompromitovanog računa.

Catch Me if You Can

Završit ćemo priču o krađi identiteta prenoseći savjete vodećeg sigurnosnog stručnjaka iz oblasti krađe identiteta, a nekada zloglasnog svjetskog krivotvoritelja i prevaranta **Franka Abagnalea** (po njegovom životu je snimljen film *Catch Me if You Can*). Vjeruje se da je u svojoj kratkoj kriminalnoj karijeri on preuzeo najmanje osam identiteta i napravio malverzaciju u vrijednosti od 4 miliona dolara u 26 zemalja. Frank Abagnale danas pomaže u hvatanju prevaranata kakav je i on nekada bio i piše knjige o metodama kojima se služe prevaranti kako bi ukrali nečiji identitet ili novac. U svojim nastupima i knjigama naglašava da ljudi trebaju biti svjesniji opasnosti od krađe identiteta, pametniji u svojim postupcima, a ne bi bilo loše da budu i sumnjičavi i skeptični jer prevare koje je on učinio u svojoj mladosti danas je, uz pomoć tehnologije, daleko lakše učiniti.

Tehnologija rađa kriminal, a ljudi konstantno pokušavaju razviti tehnologiju koja će biti korak ispred kriminala.

Borba se nastavlja! ■

Kako prepoznati kriminalce i zaštititi se od prevara

KREDITNE PREVARE

Kradljivci identiteta koriste razne tehnike kako bi se domogli naših ličnih podataka i korisničkih računa. Banke konstantno rade na unaprijeđenju sistema zaštite od kreditnih prevara. Da bismo se zaštitili od kriminalaca koji žele da se domognu naših ličnih podataka, trebamo biti oprezni i svakodnevno poduzimati mjere zaštite o kojima govorimo u ovom tekstu.

Autori:
Mirzad Topić
Vedran Vinšalek

Kreditna prevara je nezakonita upotreba tuđih ličnih podataka, kao i njihove kreditne sposobnosti, ili korištenje ličnih podataka uz falsifikovanje dokumentacije potrebne za kredit ili kreditne kartice, za pozajmljivanje novca od banaka ili drugih finansijskih institucija s ciljem kupovine dobara ili usluga bez namjere otplate duga.
Ukoliko se radi o osobi čiji su lični podaci zloupotrijebljeni, onda ta osoba obično završi s neplaćenim dugom na svoje ime. Na svu sreću, to se na kraju može riješiti, ali proces zahtijeva vrijeme i trud i može prouzrokovati nesposobnost osobe da dobije novi kredit na neko vrijeme.

Vrste kreditnih prevara

Postoji više različitih vrsta kreditnih prevara. Većinom se odnose na krađu identiteta, a razlikuju po sljedećim kombinacijama:

- **Krađa ličnih podataka koji se koriste da bi se pretpostavio identitet žrtve**. Ukradene kreditne kartice, brojevi računa, korisnička imena i lozinke su najčešći lični podaci koji se mogu koristiti za izvršenje kreditne prevare.
- **Načini na koji se kradu lični podaci.** Kriminalci mogu doći do vaših ličnih podataka na mnogo načina, uključujući sljedeće:
  1. *Phishing*. Putem e-mailova, telefonskih poziva, tekstualnih poruka ili poruka na društvenim mrežama, kriminalci se predstavljaju kao autoritet kojem možete vjerovati i pokušavaju vas prevariti da otkrijete lične podatke. Kada ste u nedoumici, prekinite komunikaciju i kontaktirajte

> *Putem e-mailova, telefonskih poziva, tekstualnih poruka ili poruka na društvenim mrežama, kriminalci se predstavljaju kao autoritet kojem možete vjerovati i pokušavaju vas prevariti da otkrijete lične podatke.*

banku ili drugu kompaniju. Odgovaranjem na sumnjivu poruku, klikom na vezu ili otvaranjem datoteke, kradljivcu identiteta možete dati put da uđe i preuzme podatke.

2. *Preuzimanje podataka*. Hakovanjem u komercijalne baze podataka, kriminalci ponekad dobijaju gomile ličnih podataka pojedinaca u velikim količinama koje ili koriste za svoje potrebe ili prodaju drugim kriminalcima.
3. *Fizička krađa*. Ukradeni novčanici i torbice s kreditnim karticama i ličnim kartama sadrže podatke koji mogu otvoriti svijet mogućnosti za kreditne prevarante. Dobro je voditi popis predmeta koje redovno nosite i informacije o tome kome se obratiti ako su izgubljeni ili ukradeni.

- **Vrste kredita dobijenih prevarom.** Kradljivci identiteta koriste različite tehnike za otmicu kredita, uključujući:
  - otvaranje novih zajmova ili računa kreditnih kartica na vaše ime;
  - preuzimanje kontrole

nad postojećim računima kreditnih kartica promjenom poštanskih adresa i lozinki;
- trošenje s ukradenim kreditnim karticama ili brojevima računa;
- otvaranje jednog ili više računa na ime vaše maloljetne djece koja inače ne bi imala lične kreditne izvještaje.

Kako se zaštititi od kreditnih prevara?

Komercijalne banke konstantno rade na unapređenju sistema zaštite od kreditnih prevara, kao i svakog drugog oblika prevara. Sistem zaštite od prevara je regulisan kroz:

- bankarske procedure,
- edukacije zaposlenika,
- interne kontrole,
- različita softverska rješenja i
- zaposlenike čiji je glavni zadatak sprečavanje i prevencija prevara.

Raširenost kreditne prevare i metoda koje kriminalci neprestano koriste za krađu ličnih podataka čine kritičnim čuvanje vaših kreditnih podataka, uključujući brojeve kreditnih kartica, korisnička imena i lozinke računa.
Mjere koje možete poduzeti da zaštitite svoje podatke uključuju:

- **Ostanite skeptični**: Budite oprezni kad god se od vas zatraži da dostavite bilo koju osjetljivu informaciju putem e-maila, telefonskog poziva ili tekstualne poruke. Komunikacija može izgledati kao da dolazi iz pouzdanog izvora, ali banke već znaju brojeve vaših računa tako da nema smisla da traže od vas podatke o istima, čak i ako pokušavaju da potvrde vaš identitet. Ako ste u nedoumici, sami kontaktirajte svoju banku telefonom kako biste provjerili da li vas je pozivao neko iz banke.

- **Sigurno pregledavanje**: Prilikom kupovine na internetu provjerite da li je veza vašeg pretraživača s trgovcem sigurna i šifrirana (potražite *https* na početku web adrese) i izbjegavajte korištenje otvorenih javnih Wi-Fi mreža (onih bez lozinki) koje lopovi mogu lako pratiti tražeći važne podatke.

- **Zaštitite se od znatiželjnih očiju**: Vodite računa da zaštitite tastaturu kada unosite PIN na bankomatima.

Čuvanje vaših podataka je ključno, ali budući da kriminalci ponekad mogu dobiti lične podatke hakiranjem velikih baza podataka koje utiču na hiljade potrošača odjednom, važno je i da stalno pazite na znakove neovlaštene aktivnosti na vašim kreditnim i drugim finansijskim računima:

- **Svakog mjeseca pažljivo provjerite izvode svoje kreditne kartice.** Pratite sve svoje račune, čak i one koje ne koristite redovno. Provjerite jeste li prepoznali sve transakcije, a ako niste sigurni u bilo koju, kontaktirajte svoju banku kako biste saznali više.

- **Pregledajte svoje kreditne izvještaje za nepoznate kreditne provjere i nove račune.** Ako vidite unose koje ne razumijete, kontaktirajte banku kako biste se raspitali o tome šta se događa. ■

Know-Your-Emplyoee procedure su neizostavan paket mjera prevencije prevara

KYE I PREVENCIJA FRAUDA

Integritet zaposlenika je presudni faktor u vlastitoj, individualnoj odluci da li će se poslovi obavljati u skladu s propisima, pravilima i procedurama ili će prevagnuti lični, vlastiti interesi, što je u konačnici savršena formula za *fraud*.

Autor:
Mujo Vilašević

Zašto KYE?

Kada se govori o prevenciji *frauda*, vrlo često se diskusija vodi u pravcu izazova savremenih tehnologija, *cyber* sigurnosti i prevara u kontekstu digitalne imovine, zapostavljajući nepravedno jedan od osnovnih uzroka prevara - zaposlenika.

Istraživanja pokazuju da je otprilike 20% svih prevara, koje su zabilježene u bankarskom sektoru Evropske unije do 2019. godine, zapravo interni *fraud*, a da su banke uspjele nadoknaditi tek 25% štete nastale takvim internim prevarama. Zbog toga, a imajući u vidu i da se eksterni *fraud* u konačnici svodi na postupke koje će poduzeti ljudi, zaposlenici banke prilikom rješavanja slučaja *frauda*, provjere zaposlenika, odnosno, *Know-Your-Emplyoee* procedure su neizostavan paket mjera prevencije prevara.

Šta podrazumijeva KYE?

Lokalna bankarska regulativa u Bosni i Hercegovini nažalost ne tretira naročito detaljno KYE procedure, ova obaveza striktno je propisana tek članom 32. *Odluke o sistemu internog upravljanja u banci* (*Službene novine Federacije BiH*, br. 39/21) gdje se navodi da je „banka dužna da sačini procedure za zaštitu aktive koje kao minimum moraju da uključe ... f) procedure za zapošljavanje osoblja koje, posebno za specifična radna mjesta u banci, moraju da uključe obaveznu prethodnu provjeru pouzdanosti i stručnosti". Dakle, s aspekta

> *Banka svakako mora imati procedure za specifična radna mjesta, u kontekstu zaštite svoje aktive, što će reći – radna mjesta uključena u kreditni proces i platne transakcije.*

regulative provjera svih zaposlenika, kao ni mandatorni elementi takve provjere, još uvijek nisu dovoljno precizno propisani. To, međutim, ne znači da obaveza provjere zaposlenika nije jedna od primarnih obaveza banke u kontekstu prevencije prevara.

Oslanjajući se na naprijed citirane odredbe, da se zaključiti da banka svakako mora imati procedure za specifična radna mjesta, u kontekstu zaštite svoje aktive, što će reći – radna mjesta uključena u kreditni proces i platne transakcije. Na osnovu toga, banka bi trebala procedurama obuhvatiti cjelokupan set mjera i pravila temeljem kojih se provjeravaju njeni zaposlenici, prije i tokom zaposlenja.

U ovisnosti od pristupa svake banke pojedinačno te vlastite procjene izloženosti rizicima, uključujući pri tome i rizik internih prevara, KYE procedure će biti manje ili više granulirane, odnosno inkorporirati manje ili više *in* i *out* kriterija. Važno je napomenuti da je za ovaj proces ključna najbliža saradnja službe za ljudske resurse i *compliance* službe (ili druge organizacijske jedinice zadužene za *fraud* i provjeru zaposlenika). U tom kontekstu, KYE procedure trebalo bi kao minimum da uključuju:

- provjere koje provodi služba za ljudske resurse prilikom selekcijskog procesa svakog zaposlenika banke,
- provjere koje provodi *compliance* (ili druga nadležna jedinica za prevenciju *frauda*) te
- kontrolne aktivnosti koje provodi interna revizija.

Način na koji će banka definisati interni proces provjere, a naročito u dijelu *compliance* provjera, ovisit će, kako je i navedeno, od rizičnog profila banke, ali i od prioritizacije *compliance* relevantnih pitanja. Dakle, banka, kao i bilo koja druga organizacija koja uspostavlja svoje poslovanje na principima poslovne etike i integriteta, postavit će *compliance* provjere svih potencijalnih zaposlenika, kao i eksternih saradnika, vrlo visoko na listi svojih prioriteta. Zašto? Zato što će u proteku vremena i radnog angažmana bilo kojeg zaposlenika, neovisno od njegove funkcije, uloge ili moći u lancu odlučivanja, integritet ipak biti presudni faktor u vlastitoj, individualnoj odluci da li će se poslovi obavljati u skladu s propisima, pravilima i procedurama ili će prevagnuti lični, vlastiti interesi, što je u konačnici savršena formula za *fraud*. Zbog toga je insistiranje na uspostavljanju adekvatnih procedura provjere integriteta, ličnosti, obrazaca ponašanja, navika i sklonosti izuzetno važan indikator *compliance* provjera zaposlenika, a koji se nužno provodi u saradnji sa službom zaduženom za ljudske resurse.

Obim KYE procedura također ovisi od vlastite *compliance* procjene u svakoj banci, ali bi nesumnjivo isti trebalo kao minimum da uključuje:

- provjere stručnosti i sposobnosti neophodnih za konkretno radno mjesto (primarno obavlja služba ljudskih resursa),
- provjere iz evidencija krivičnih postupaka,
- provjere potencijalnih sukoba interesa prema evidencijama poslovnih subjekata i

– provjere javno dostupnih podataka na društvenim mrežama i slično.

Naravno, imajući u vidu prirodu podataka koji se obrađuju u procesu provjere zaposlenika, neizostavna je prethodna pisana saglasnost potencijalnih zaposlenika ili zaposlenika u toku trajanja radnog angažmana, a za obradu ličnih podataka temeljem propisa o zaštiti ličnih podataka i/ili GDPR. Jedan od korisnih *out* indikatora može biti i odbijanje potencijalnog zaposlenika na davanje takve saglasnosti banci. U svakom slučaju, banka je dužna KYE procedurama definisati proces, uloge i odgovornosti svih uključenih učesnika, kao i postupanje u slučaju različitih rezultata provjera, a prije svega kako bi se uspostavila jednoobrazna matrica prihvatljivih i neprihvatljivih indikatora kod angažmana zaposlenika.

> *Banka je dužna KYE procedurama definisati proces, uloge i odgovornosti svih uključenih učesnika, kao i postupanje u slučaju različitih rezultata provjera, a prije svega kako bi se uspostavila jednoobrazna matrica prihvatljivih i neprihvatljivih indikatora kod angažmana zaposlenika.*

Konačni benefit KYE

Poznavanje ljudi znači i poznavanje organizacije. Službenici zaduženi za prevenciju *frauda* moraju izuzetno dobro poznavati i ljude i organizaciju i sve procese u organizaciji kako bi adekvatno identifikovali *slabe tačke* i poduzimali odgovarajuće aktivnosti na prevenciji. Adekvatne provjere zaposlenika, s odgovarajuće postavljenim kriterijima, metodama i procesima, proporcionalno mogu uticati na smanjenje internog *frauda*, a time ostvariti i značajne uspjehe na troškovnoj strani budžeta svake organizacije te dugoročno očuvati imovinu i reputaciju.

Osim toga, zdrava organizacija ne može ni u teoriji funkcionisati bez odgovarajućih ljudskih resursa koji su posvećeni integritetu, poštenim poslovnim praksama i najboljem interesu organizacije. Konačno, u doba ESG modela poslovanja samo organizacije koje su *dobri korporativni građani* će pronaći svoje odgovarajuće mjesto na tržištu te sačuvati komparativnu prednost tek ukoliko prepoznaju priliku u izgradnji vlastitog integriteta njegujući kulturu integriteta svojih zaposlenika. ■

Interno upravljanje

FUNKCIJA PRAĆENJA USKLAĐENOSTI U SVJETLU ODLUKE O SISTEMU INTERNOG UPRAVLJANJA U BANCI

Donosimo osvrt na Odluku o sistemu internog upravljanja u banci, koja je na snazi od 31.12.2021. godine, i određene izmjene koje sadrži u odnosu na prethodnu Odluku o kontrolnim funkcijama banke.

Autor:
Nermin Ibradžić

Agencija za bankarstvo Federacije Bosne i Hercegovine donijela je 12.05.2021. godine *Odluku o sistemu internog upravljanja u banci* (dalje: Odluka) koja je objavljena u *Službenim Novinama Federacije BiH*, broj 39/21.

Odluka se primjenjuje od 31.12.2021. godine, a početkom njene primjene prestaje važiti *Odluka o kontrolnim funkcijama banke* (*Službene Novine Federacije BiH*, broj 81/17) koja je bila osnov za implementiranje i rad funkcije praćenja usklađenosti kao jedne od kontrolnih funkcija.

Sama Odluka nije iznenađenje s obzirom na to da sadrži odredbe koje su uglavnom usklađene s ***Europian Banking Authority*** (EBA) *Smjernicama za interno upravljanje* koje su donesene 2017. godine i revidirane 2021. godine.

Ipak, u odnosu na kontrolnu funkciju praćenja usklađenosti (dalje: FPU), postoje određene izmjene u odnosu na Odluku o kontrolnim funkcijama banke.

Plan rada FPU

Prije svega, regulator u Odluci apostrofira potrebu da Plan rada funkcije praćenja usklađenosti usvaja nadzorni odbor banke što do sad nije bilo

eksplicitno propisano, iako se u praksi primjenjivalo.

Navedena dopuna je i razumljiva imajući u vidu ulogu nadzornog odbora u formiranju sistema internih kontrola banke, ali i zbog činjenice što FPU u osnovi direktno odgovara nadzornom odboru banke.

Plan obuke zaposlenika

Sljedeća novina je obaveza FPU da sačini plan obuke zaposlenika angažiranih u kontrolnoj funkciji FPU. Apostrofirano je da je banka u obavezi da osigura sve kadrovske i finansijske resurse za implementaciju ovakvih planova. U ovom dijelu bi se rukovodilac FPU mogao susresti s jednim praktičnim problemom, a to je na koji način predvidjeti i implementirati potrebne i planirane edukacije.

> *Banka je u obavezi da osigura sve kadrovske i finansijske resurse za implementaciju ovakvih planova. Rukovodilac FPU bi se mogao susresti s jednim praktičnim problemom, a to je na koji način predvidjeti i implementirati potrebne i planirane edukacije.*

Bosna i Hercegovina je zemlja u kojoj je FPU faktični tek *u povojima*, što znači i izostanak potrebnih edukacija iz razloga što iste nisu toliko zastupljene u Bosni i Hercegovini. Naravno, uvijek postoji mogućnost da se takvi vidovi edukacije osiguraju i van BiH, što će svakako uticati i na troškove edukacija koje je unaprijed potrebno planirati i budžetirati na dostatan način.

Ljudski i drugi resursi

Iako Odluka ne propisuje minimalan broj članova/zaposlenika FPU, jasno apostrofira da taj broj mora biti adekvatan veličini banke te njenoj organizaciji i poslovnom modelu/poslovima koje obavlja prema načelu proporcionalnosti. Iako se dopuna u ovom dijelu ne čini krucijalnom, ipak predstavlja alat svim onim rukovodiocima FPU koji su do sada posao obavljali bez adekvatnih kadrova ili su čak bili *one man show* kao rukovodilac FPU i njen jedini član/zaposlenik.

> *Prošlost nas uči da je FPU efikasna u onoj mjeri u kojoj ima podršku prvenstveno nadzornog odbora pa onda i uprave banke za svoj rad.*

Dodatno, regulator je propisao i jasne uslove razrješenja FPU. Tako će se, u slučaju da razrješenje FPU zahtijeva uprava banke, morati provesti postupak razrješenja pred nadzornim odborom, pri čemu se objema stranama daje prilika da argumentirano definišu svoje *pro/contra* razloge. Navedeni princip svakako ide u korist stabilnosti i sigurnosti FPU i njenoj adekvatnoj neovisnosti.

Imajući u vidu prethodnu odredbu koja efekat ima u jačanju FPU kao kontrolne funkcije, pomalo iznenađuje odredba stava 8. člana 39. Odluke koja garantuje izvještavanje FPU prema nadzornom odboru banke i neometan pristup nadzornom odboru, dok ujedno definiše i

da je navedeni uslov zadovoljen ukoliko FPU odgovara upravi banke, odnosno nadležnom članu uprave banke. Treba vjerovati da ovakva formulacija neće onemogućiti FPU da u slučaju potrebe ostvari direktan kanal komunikacije prema nadzornom odboru, a posebno ukoliko je predmet izvještaja FPU uprava banke ili pojedini član uprave. Prošlost nas uči da je FPU efikasna u onoj mjeri u kojoj ima podršku prvenstveno nadzornog odbora pa onda i uprave banke za svoj rad.

Opis aktivnosti FPU

Iako opis poslova FPU Odlukom nije značajnije dopunjen, u dijelu procjene reputacijskog rizika definiran je dodatni zahtjev prema FPU. Naime, ukoliko reputacijski rizik FPU procijeni kao značajan, dužan je osigurati da je navedeni rizik uključen u ICAAP.

Umjesto zaključka

Kako je prethodno navedeno, pomenuta Odluka u odnosu na FPU i Odluku o kontrolnim funkcijama u banci ne donosi značajne izmjene. Ipak, naprijed su navedene odredbe koje mogu imati uticaja na dosadašnji rad FPU, a svakako bi ih bilo potrebno iskoristiti radi daljeg jačanja FPU kao čuvara integriteta i usklađenosti svake banke.

U konačnici, valja napomenuti da ovaj tekst ne treba čitati kao priručnik za implementaciju izmjena vezanih za FPU, nego isključivo kao materijal koji će ponukati svaku FPU da revidira svoju ulogu u odnosu na Odluku na najprihvatljiviji način. ■

Pregled najznačajnijih izmjena uz uporedbu s rješenjima koja trenutno važeći zakon sadržava

OSVRT NA NACRT ZAKONA O IZMJENAMA I DOPUNAMA ZAKONA O IZVRŠNOM POSTUPKU FBIH

Imajući u vidu da je Zakon o izvršnom postupku vrlo značajan za bankarski sektor te da će njegove izmjene imati višestruke posljedice na efikasnost naplate potraživanja svih povjerilaca, ne samo banaka, dajemo kratki osvrt na najznačajnije izmjene koje se predviđaju prema Nacrtu.

Autor:
Muris Bešić

Tokom juna 2021. godine Vlada FBIH je u parlamentarnu proceduru uputila Nacrt Zakona o izmjenama i dopunama zakona o izvršnom postupku FBiH (u nastavku: NZIDZIP). Nakon provedene parlamentarne procedure, Predsjedavajući Predstavničkog doma Parlamenta FBIH je aktom broj: 01-02-1334/21 od 30.07.2021. godine dostavio nacrt navedenog propisa Domu naroda Parlamenta FBIH. Predsjedavajući Doma naroda Parlamena FBiH je aktom broj: 02-02-1334/21 od 14.10.2021. godine Predsjedniku i Potpredsjedniku Zastupničkog doma Parlamenta FBIH uputio Zaključak u skladu s kojim se navodi da Dom naroda PSFBIH prihvata nacrt zakona te da isti može poslužiti kao temelj za izradu Prijedloga zakona.

Imajući u vidu da je Zakon o izvršnom postupku vrlo značajan za bankarski sektor te da će njegove izmjene imati višestruke posljedice na efikasnost naplate potraživanja svih povjerilaca, ne samo banaka, u ovom radu će biti dat kratki osvrt na najznačajnije izmjene koje se predviđaju Nacrtom.

Trenutno važeći Zakon o izvršnom postupku FBIH[1] (u

[1] Zakon o izvršnom postupku i njegove izmjene su objavljeni je u Službenim novinama Federacije BiH, br. 32/2003, 52/2003 - ispr., 33/2006, 39/2006 - ispravka, 39/2009, 35/2012 i 46/2016 i Službenom glasniku BiH, br. 42/2018 - odluka Ustavnog Suda.

daljem tekstu: ZIP) je objavljen 2003. godine i već je pretrpio izmjene 2006, 2009, 2012, 2016. i 2018. godine. Sada predložene izmjene predstavljaju najobimnije i suštinski najzačajanije izmjene i dopune. Kao što je navedeno, u nastavku teksta će biti izložen pregled najznačajnijih izmjena uz uporedbu s rješenjima koja trenutno važeći zakon sadržava, te po potrebi komentar autora, u odnosu na efekte koje takva izmjena sa sobom donosi. Komentar autora, iako po prirodi stvari prije svega obuhvata aspekte povjerilac/tražilac/izvršilac, bit će nepristrasan uvažavajući opravdane i zakonite interese svih strana u postupku. Izmjene koje, prema mišljenju autora, nisu od velikog značaja za sam postupak neće biti prikazane i analizirane u ovom pregledu te svakako da upućujem na detaljniji pregled NZIDZIP-a u cilju upoznavanja sa svim izmjenama zakona.

Pregled najznačajnijih izmjena i dopuna NZIDZIP-a

Prva izmjena se odnosi na izmjenu stava 3. člana 8. ZIP-a u skladu s kojom se u slučajevima u kojima se izvršno rješenje o izvršenju na određenom predmetu ili sredstvu ne može provesti, pravo tražioca izvršenja na predlaganje novog predmeta ili sredstva izvršenja ograničava rokom od 15 dana. Prema trenutno važećem zakonskom rješenju ovaj rok uopšte nije definisan. Izmjena predložena kroz NZIDZIP u smislu određivanja roka za postupanje tražioca izvršenja svakako da predstavlja pozitivan prijedlog jer će tražioca izvršenje disciplinirati na brže postupanje i spriječiti gomilanje u sudu predmeta koji nemaju perspektive. S druge strane, utvrđeni rok od 15 dana je prekratak i ne omogućava dovoljno vremena tražiocu izvršenja da obavi sve potrebne radnje kako bi utvrdio i sudu predložio novo sredstvo i predmet izvršenja te bi navedeni rok svakako trebao biti duži i određen na minimalno 60 dana.

Izmjena je i u članu 15. ZIP-a u skladu s kojom se rokovi za postupanje suda za donošenje odluke po pravnim lijekovima produžavaju. Rok za postupanje za donošenje odluke o prigovoru se s 8 dana produžava na 15 dana dok se rok za odlučivanje po žalbi produžava s 15 na 30 dana. Navedena izmjena, osim kraćeg produžavanja rokova za postupanje, ne bi trebala imati značajniji uticaj na sam postupak, naravno pod uslovom da se postupanja odvijaju u rokovima koji su definisani.

Nadalje, kroz NZIDZIP je predviđena izmjena u dijelu zakona koji se odnosi na definisanje isprava koje se smatraju vjerodostojnim, član 29. stav 2. Vjerodostojne isprave su isprave temeljem kojih je moguće bez obaveze provođenja parničnog postupka predložiti provođenje izvršnog postupka radi naplate dugovanja koje se navodi u samoj ispravi. Prema

> *Prema predviđenoj izmjeni povećan je broj isprava koje se smatraju vjerodostojnim, a to su: račun za isporuku električne energije, račun za uslugu telefonskih operatera, naplate javnog parkinga i naknade za održavanje zajedničkih prostorija.*

predviđenoj izmjeni povećan je broj isprava koje se smatraju vjerodostojnim, a to su: račun za isporuku električne energije, račun za uslugu telefonskih operatera, naplate javnog parkinga i naknade za održavanje zajedničkih prostorija. Svakako da se predmetna izmjena može smatrati pozitivnom jer će isporučiocima usluga omogućiti efikasniju prinudnu naplatu naplaćenih dugovanja.

Vrlo značajna izmjena koja je predložena u NZIDZIP-u se odnosi na izmjenu člana 37. (Provjera imovine izvršenika). Kroz predloženo zakonsko rješenje u cjelosti je izmijenjen koncept provjere imovine izvršenika. Dosadašnji koncept u kojem je sud imao obavezu provjere imovine izvršenika je u cjelosti napušten. Novi koncept daje mogućnost tražiocu izvršenja da sam izvrši provjeru imovine izvršenika, a nadležnim organima koji su navedeni u zakonu se predviđa rok i obaveza u kojem moraju dati odgovor na zahtjev za dostavu podataka koje je uputio tražilac izvršenja. Obaveza dostavljanja podataka o izvršenicima se odnosi na sljedeće subjekte: Federalni zavod za zdravstveno i penziono osiguranje, Porezna uprava FBIH, Kantonalni MUP, banke i druge finansijske institucije ili organizacije zadužene za vođenje računa poslovnih subjekata, ovlaštene institucije za vođenje podataka o prebivalištu, zemljišno-knjižni uredi i Katastar. Navedene institucije imaju pravo na podmirivanje troškova za poduzimanje navedenih radnji i predviđena je naročita zabrana da vrše obavještavanje izvršenika o zaprimljenim zahtjevima. Ukoliko tražilac izvršenja pretrpi štetu zbog nepostupanja po njegovom zahtjevu, predviđa se pravo na nadoknadu štete zbog propuštanja poduzimanja dužnih radnji. Zaprimljeni podaci se ne smiju koristiti u drugu svrhu osim u svrhu pokretanja i vođenja izvršnog postupka, a lica koja su ih tražila dužna su ih tretirati kao službenu tajnu. Vrlo je bitno navesti da je putem NZIDZIP-a predviđeno da se u slučaju kolizije odredbi drugih zakona s odredbama izmijenjenog člana 37. primjenjuju odredbe NZIDZIP-a. Predmetna izmjena svakako da predstavlja pozitivno rješenje jer će tražioci izvršenja sigurno puno efikasnije provesti postupke provjere dužnikove imovine radi pokretanja izvršnog postupka. Ono što bi u praksi moglo uzrokovati nedostatke ovog rješenja su moguće visoke naknade koje pružaoci podataka mogu tražiti za dostavu navedenih podataka te da se usljed takvog pristupa ovo rješenje u praksi pokaže kao nedjelotvorno. U ovom dijelu korisna bi bila dopuna zakona na način da se utvrdi da pružaoci usluga, naročito državni, entitetski i kantonalni, pa i drugi koji su u obavezi uraditi dostavu, ne smiju kao cijenu za usluge odrediti veće cijene nego što stvarno imaju povodom dostave podataka. Postoji opasnost da se kroz naplatu vidi i mogućnost

„Korisna bi bila dopuna zakona na način da se utvrdi da pružaoci usluga, naročito državni, entitetski i kantonalni, pa i drugi koji su u obavezi uraditi dostavu, ne smiju kao cijenu za usluge odrediti veće cijene nego što stvarno imaju povodom dostave podataka.“

zarade kroz uvođenje previsokih cijena za dostavu podataka usljed čega će potencijalni tražioci izvršenja odustajati od traženja podataka. S druge strane, kako bi se spriječili suvišni zahtjevi kao i to da poslovi pružalaca usluga ne bi bili dovedeni u pitanje usljed prevelikog broja zahtjeva zainteresovanih lica, svakako da je potrebno imati primjerenu naknadu za pruženu uslugu kojom će biti pokriveni troškovi pružalaca usluga.

U okviru člana 50. predviđeno je dodavanje novog stava 6. u skladu s kojim se, prilikom okončanja parnice na koju je tražilac izvršenja upućen po prigovoru na Rješenje o izvršenju donijeto temeljem vjerodostojne isprave, propisuje rok za predlaganje nastavka izvršnog postupka u roku od 30 dana od dana izvršnosti odluke parničnog suda. U protivnom će sud obustaviti izvršni postupak.

Uočava se da je propisani rok prekratak za adekvatno poduzimanje radnji na provjeri imovine dužnika kao i poduzimanje radnji na ponovnom predlaganju provođenje postupka, stoga rok za navedeno postupanje ne bi smio biti kraći od 60 ili 90 dana, dok je samo utvrđivanje roka za postupanje pod prijetnjom obustave svakako pozitivno rješenje koje će osigurati efikasnije postupanje u izvršnim postupcima.

Predložena je i izmjena NZIDZIP-a kojom se putem izmjene člana 60. kroz dodavanje novog stava 4. predviđa da se samo jednom u toku postupka može tražiti odlaganje izvršenja, dok u trenutno važećem zakonskom rješenju nema takvog ograničenja. S navedenom dopunom kao cjelinu treba posmatrati i i izmjene člana 61. kojim se definiše vrijeme odlaganja izvršenja. Tako se predviđa da vrijeme na koje se izvršenje odlaže ne može biti duže od 6 mjeseci, izuzetno može i duže ako je zaključen pisani sporazum o načinu izmirenja potraživanja. Posmatrajući kroz praksu, navedeno rješenje u cjelini nije adekvatno i vrlo je ograničavajuće kako za tražioca izvršenja tako i za izvršenika. Naime, kroz praksu se vrlo često i dešava zaključenje sporazuma o izmirenju dugovanja što je svakako najbolje rješenje za sve učesnike, i za stranke u postupku i za sud. U tim slučajevima se izvršni postupak odgađa za određeni period. Također, vrlo često se događa da izvršenik prestane s izvršenjem obaveza te je tražilac izvršenja prinuđen nastaviti izvršni postupak kako bi se izvršenik prinudio na plaćanje dužne obaveze. Ograničenjem na mogućnost samo jedne odgode izvršnog postupka, tražioci izvršenja će biti prinuđeni provoditi izvršne postupke bez mogućnosti daljeg zaključenja ili nastavka postupanja po pisanim sporazumima s izvršenicima. Stoga, ovo rješenje nije adekvatno jer ograničava mogućnosti disponiranja s procesnim pitanjima koje su stranke do sada imale na raspolaganju, a napominjem da sud u ovim slučajevima nema nikakvo postupanje osim čiste evidencije predmeta.

Značajne izmjene su predviđene u dijelu zakona koji se odnosi na napokretnost kao predmet izvršenja. Izmjena koju predviđa NZIDZIP se ogleda i u izmjeni člana 69. (Nepokretnost kao predmet izvršenja). Prilikom provođenja izvršnog postupka na suvlasničkom dijelu nekretnine predviđa se potreba pribavljanja izričite saglasnosti svih suvlasnika za provođenje izvršnog postupka na cijeloj nekretnini. Suvlasnici koji nisu izvršenici imaju pravo na namirenje u visini svojih suvlasničkih dijelova prije namirenja ostalih troškova koji se namiruju u izvršnom postupku. Isto postupanje se predviđa i u slučaju pokretenja izvršnog postupka na nekretnini koja predstavlja zajedničku imovinu.

Član 70. predviđa da, u slučaju da je nekretnina u zemljišnoj knjizi upisana na neko drugo lice koje nije izvršenik, prijedlogu za izvršenje se može udovoljiti samo ako su ispunjeni uslovi za promjenu zemljišno-knjižnog stanja te je u skladu s izmjenom člana 37. brisana obaveza utvrđivanja dužnikove imovine od strane suda kakva je ranije bila propisana.

Član 79. odnosi se na izuzimanje od izvršenja nekretnina. Shodno navedenom, novina je da ne može biti predmet izvršenja nekretnina koja predstavlja jedini dom izvršenika. Pojam *jedini dom izvršenika* je kroz nacrt zakona djelimično određen. Jedini dom izvršenika se propisuje kao nekretnina ili drugi objekat koji služi isključivo za stanovanje izvršenika i članova njegove uže porodice, a obim i površina nekretnine koja predstavlja jedini dom

> *Novina je da ne može biti predmet izvršenja nekretnina koja predstavlja jedini dom izvršenika. Jedini dom izvršenika se propisuje kao nekretnina ili drugi objekat koji služi isključivo za stanovanje izvršenika i članova njegove uže porodice.*

izvršenika utvrđuje u svakom konkretnom slučaju. Dodatno, kao novina propisano je da nekretnina ne može biti predmet izvršenja ako je vrijednost potraživanja manja od 1/3 tržišne vrijednosti nekretnine. Princip da se izuzeća ne primjenjuju na nekretninama na kojima je zasnovano založno pravo je zadržan u nacrtu zakona.

Članom 87. određeno je da će se ročište za javno nadmetanje održati ako sud utvrdi da su ispunjene zakonske pretpostavke za njegovo održavanje u smislu člana 82. Zakona, a zahtjev za odgodu ročišta za javnu prodaju je moguće tražiti samo jednom u toku postupka. Ukoliko na ročište ne dođe niti jedan ponuđač, prodaja će se smatrati neuspjelom i novo ročište za prodaju nekretnine će biti zakazano u roku od 30 dana.

Član 89. stav 5. se mijenja i prema istom, ako nepokretnost ne bude prodana ni na drugom ročištu, sud će na prijedlog tražioca izvršenja donijeti rješenje kojim se utvrđuje pravo vlasništva tražioca izvršenja srazmjerno njegovom potraživanju u odnosu na utvrđenu vrijednost nepokretnosti. Vrlo bitna novina u skladu s navedenom odredbom je ukidanje treće prodaje koje je do sada bila predviđena.

Sumarno u odnosu na nekretnine kao predmet izvršenja, može se istaći sljedeće:

- kao novine predviđaju se obavezna saglasnost suvlasnika/zajedničara ukoliko je predmet prodaje nekretnina u suvlasništvu/zajedničkom vlasništvu;
- predlaganje kao predmeta izvršenja nekretnine koja nije knjižno vlasništvo izvršenika moguće je bez obaveze utvrđenja imovine od strane suda;
- izuzimanje od izvršenja nekretnine koja predstavlja jedini dom izvršenika;
- zabrana prodaje neketnine ispod 1/3 procijenjene vrijednosti;
- ukidanje trećeg ročišta za prodaju nekretnine te
- uvođenje mogućnosti da sud, ukoliko nekretnina ne bude prodana na trećem ročištu, na zahtjev tražioca izvršenja donese rješenje u skladu s kojim se utvrđuje njegovo pravo vlasništva na nekretnini srazmjerno njegovom potraživanju u odnosu na utvrđenu vrijednost nepokretnosti.

Navedene izmjene su svakako vrlo značajne i krupne, njihov stvarni efekat u odnosu na dosadašnje rješenje s aspekta efikasnosti namirenja povjerilaca se u ovom trenutku ne može u cjelosti procijeniti. S druge strane, svakako će povećati efikasnost postupanja sudova i skratiti trajanje postupka, ali to samo sebi ne može biti svrha niti smjer kojim tre-

> *Ukoliko usljed nekog rješenja izostane efikasnost naplate, izmjene zakona nisu ispunile svoju svrhu.*

ba ići prilikom unapređenja postupka. Ukoliko usljed nekog rješenja izostane efikasnost naplate, izmjene zakona nisu ispunile svoju svrhu. Svakako da i povjerioci koji se bave kreditiranjem, naročito banke, moraju adekvatno procijeniti cjelishodnost korištenja založnih prava prilikom osiguranja kredita u odnosu na nova ponuđena rješenja.

Naredna izmjena odnosi se na postupanje prilikom provođenja izvršnog postupka na pokretnim stvarima te se predviđa izmjena člana 125. ZIP-a. Ukoliko, prilikom provođenja pljenidbe pokretnih stvari, sud ne nađe stvari koje mogu biti predmet izvršenja, pozvat će tražioca izvršenja da u roku od 8 dana dostavi tačnu adresu gdje se nalaze pokretne stvari koje mogu biti predmet pljenidbe ili da uredi prijedlog za izvršenje i predloži novo sredstvo i predmet izvršenja. Ukoliko tražilac izvršenja ne postupi u navedenom roku, sud će obustaviti postupak izvršenja. Kako se može uočiti, postavljeni rok u potpunosti onemogućava tražioca izvršenja da bilo šta učini u cilju saznanja za adresu ili imovinu izvršenika koja može biti predmet pljenidbe i prodaje. U skladu s navedenim, vrlo je jasno da bi postavljeni rok morao biti znatno duži, minimalno 60 dana, kako bi tražilac izvršenja uopšte mogao imati vrijeme potrebno za davanje adekvatnog prijedloga.

Zaključak

Analizom predloženih zakonskih rješenja može se ustanoviti da su ponuđena određena rješenja koja će svakako imati pozitivan efekat na efikasnost postupanja kao i na samu naplatu potraživanja. Određena rješenja koja su ponuđena mogu dovesti do toga da se povjerioci u većoj mjeri opredijele za druga sredstva osiguranja u odnosu na ona koja su do sada koristili kao osiguranje svojih potraživanja, a zbog predloženih rješenja u pogledu rokova za postupanje od kojih neka skoro u cjelosti onemogućavaju adekvatne procesne aktivnosti, a time i mogućnosti naplate potraživanja. Ovdje se prvenstveno misli na pokretne stvari te na ponuđena rješenja prilikom prodaje nekretnina. Također, primjećuje se tendencija značajnog skraćenja rokova za postupanje tražilaca izvršenja, čak u određenim situacijama i do mjere koja onemogućava bilo kakvu aktivnost tražioca izvršenja te bi svakako trebalo produžiti rokove za postupanje koji su predviđeni za postupanje tražilaca izvršenja. Ukoliko je namjera predlagatelja kroz skraćenje rokova bio uticaj na povećanje efikasnosti postupanja sudova, što je svakako pohvalno, ne može se izbjeći dojam da je zanemarena svrha izvršnog postupka, a to je na prvom mjestu efikasnost naplate potraživanja. Stoga, svakako da treba uvažiti sugestije javnosti i omogućiti primjerene rokove za postupanje tražilaca izvršenja. ■

> *„Ne može se izbjeći dojam da je Nacrtom zanemarena svrha izvršnog postupka, a to je na prvom mjestu efikasnost naplate potraživanja."*

Sačuvajte se od krađe

NAPADI I PREVARE NA BANKOMATIMA

Korištenje bankomata postalo je svakodnevnica. Kriminalci neprestano smišljaju nove načine kako da otuđe novac i lične podatke s kartica. Smanjite vjerovatnoću da budete žrtva prevare ili drugih opasnosti koje vas vrebaju – čitajući i slijedeći naše savjete.

Autor:
Medžid Suljić

Samim početkom korištenja bankomata, pojavili su se i izazovi o zaštiti istih s obzirom na to da je napad na bankomate, zbog načina izvršenja, definisan kao krivično djelo *teške krađe* za koju je zaprijećena zatvorska kazna.
Kao i svaki računarski uređaj, bankomati imaju ranjivosti. Jedan od načina da se shvati zašto su *loši momci* privučeni njima je razumjeti njegove komponente i način na koji komunicira s bankovnom mrežom. Bankomat se sastoji od kompjutera (i njegovih perifernih uređaja) i sefa.

Sam ormar nije posebno siguran ili čvrst zbog čega kriminalci mogu koristiti jednostavne alate i ključ za otključavanje koji se može nabaviti na internetu kako bi provalili u njega i time pristupili kompjuteru ili sefu.

Računar obično radi na *Windowsu*, verziji posebno kreiranoj za bankomate. Korisnici bankomata ne vide poznati Windows desktop interfejs jer je pristup operativnom sistemu ograničen. Ono što vidimo su aplikacije okrenute korisniku koje nam pomažu u obavljanju transakcija s mašinom.

Bitno je naglasiti da, ako je operativni sistem (dalje: OS) zastario, očekujte da će softver u njima možda trebati i nadogradnju. Međutim, kriminalci mogu sami izabrati koje eksploatacije da koriste kako bi maksimalno iskoristili ranjivosti softvera i preuzeli kontrolu udaljenim sistemom.

U nekim slučajevima, otvori poput vidljivog USB porta mogu ohrabriti korisnike s

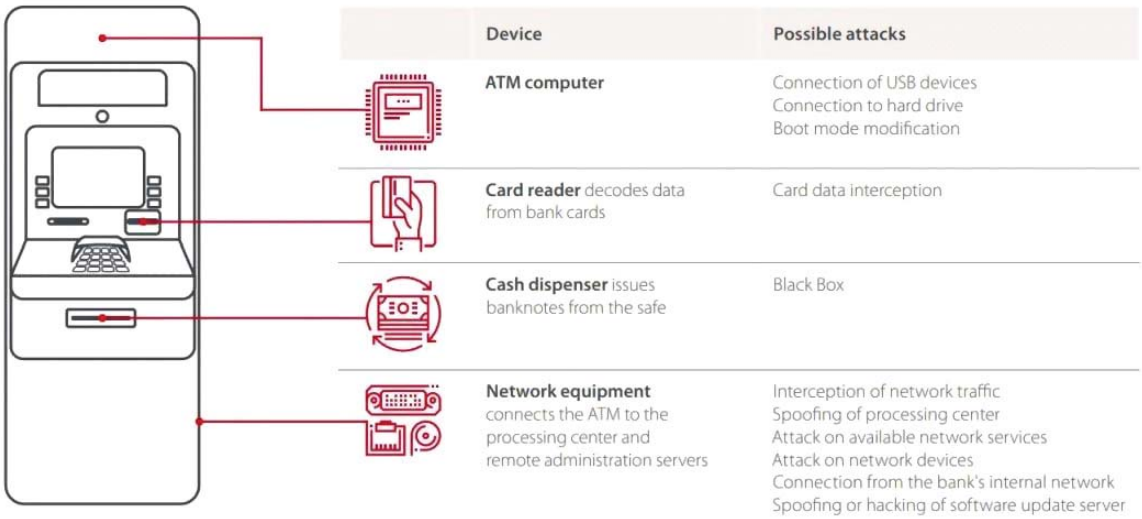
> *Ukoliko OS na bankomatu ne sadrži sigurnosne softvere ili druge elemente zaštite i potrebne zakrpe OS, put prema novcu na bankomatu je otvoren. Do danas je već otkriveno 20 vrsta poznatih bankomatskih/ATM malwarea.*

lošom namjerom da unesu zlonamjerni softver u uređaj putem USB porta preko prijenosnog uređaja koji posjeduju. Ukoliko OS na bankomatu ne sadrži sigurnosne softvere ili druge elemente zaštite i potrebne *zakrpe* OS, put prema novcu na bankomatu je otvoren. Do danas je već otkriveno 20 vrsta poznatih bankomatskih/ATM malwarea.

Bankomat je direktno pričvršćen za sef u kojem se čuva gotovina. Kompromitovani računar može lako omogućiti kriminalcima pristup interfejsu između računara i sefa kako bi mu naredili da izda gotovinu bez korištenja ukradenih podataka o kartici korisnika. Može se pri tome desiti da saobraćaj između ATM/bankomatskog računara i servera za obradu transakcija obično nije šifrovan, što hakerima omogućava da lakše presretnu prenijete podatke od klijenta do servera banke. Ukoliko pri tome bankomat ne posjeduje ili psjeduje lošu zaštitu firewalla, to ga čini naročito podložnim mrežnom napadu. Druge značajne slabosti su nedostatak ili pogrešno konfigurisan softver za kontrolu aplikacija, nedostatak enkripcije hard diska i mala ili nikakva zaštita od korisnika koji pristupaju Windows interfejsu i uvode druge hardverske uređaje u bankomat.

Vrste prevara i napada na bankomat

Hakovanje servera banke samo je jedan od mnogih poznatih načina na koje krimi-



nalci mogu doći do podataka o karticama vlasnika računa i njihovog teško zarađenog novca. Neke metode su pametne i taktičke dok su druge destruktivnije i opasnije. Bez obzira na cijenu, možemo biti sigurni da će kriminalci učiniti sve što je potrebno da izvedu uspješnu pljačku.
Ovdje ćemo istaći neke tipove napada na ATM:

ATM Skimming

Ovo je vrsta prevare u kojoj se uređaj za skimiranje, obično tandem čitača kartica (skimera) i preklapanja tastature ili kamere s rupicama, uvodi u mašinu tako što se postavlja preko otvora za karticu i tastature.

Što više liči na mašinu, to će bolje raditi (i manje je vjerovatno da će izazvati sumnju). Svrha drugog čitača je kopiranje podataka s magnetne trake i PIN-a kartice kako bi kriminalac mogao krivotvoriti karticu.

Naravno, postoji mnogo načina da se podaci o kartici i PIN-u krišom zahvate. Svi oni potpadaju pod ovu šemu. Primjeri uključuju skimming uređaje koji spajaju mrežne kablove bankomata, koji mogu presresti podatke u tranzitu.

Kriminalci mogu povećati ulog svoje kampanje skimminga tako što će kupiti polovni bankomat (po povoljnoj cijeni), a zatim ga namjestiti za snimanje podataka. Ovi bankomati ne izdaju gotovinu, nego putem prevare prikupljaju podatke s kartica, uključivo PIN. Ovo je daleko najuvjerljivija metoda jer oprezni vlasnici računa ne bi pomislili da je cijeli bankomat lažan.

Uređaji za skidanje se, također, mogu postaviti na terminale

na prodajnom mjestu (POS) u prodavnicama ili unutar benzinskih pumpi. Neki skimeri su dovoljno mali da se mogu sakriti u ruci tako da, ako nekome sa zlim namjerama uručite platnu karticu, on je može brzo provući kroz svoj skimer nakon što je provuče na POS terminalu.

Shimming

Ovo se može nazvati unapređenim oblikom skimminga. Iako još uvijek cilja na kartice, njegov fokus je snimanju ili krađi osjetljivih podataka iz njihovih ugrađenih čipova. Uređaj za podmetanje tankog papira umetnut je u slot za kartice bankomata gdje se nalazi između kartice i čitača čipova na bankomatu. Na ovaj način skimmer snima podatke s čipa kartice dok ih čitač čipova mašine čita. Za razliku od ranijih uređaja za skimiranje, novi mogu biti praktički nevidljivi ako su savršeno umetnuti, što ih čini teškim za otkrivanje. Međutim, jedan od znakova da bi bankomat mogao imati instaliran skimming uređaj je tijesan utor kada umetnete bankovnu karticu.

> *Podaci ukradeni s čipova kartica (također poznati kao EMV kartice) mogu se konvertovati u podatke s magnetnom trakom koji se zauzvrat mogu koristiti za kreiranje lažnih verzija naših tradicionalnih kartica s magnetnom trakom.*

Podaci ukradeni s čipova kartica (također poznati kao EMV kartice) mogu se konvertovati u podatke s magnetnom trakom koji se zauzvrat mogu koristiti za kreiranje lažnih verzija naših tradicionalnih kartica s magnetnom trakom.
Izdavači su jednom rekli da EMV kartice nude bolju zaštitu od prevare u odnosu na tradicionalne bankovne kartice.

S obzirom na to da sve više korisnika i trgovaca sada favoriziraju kartice s čipom zbog pogodnosti ili usklađenosti s industrijom, očekivalo se da će kriminalci na kraju pronaći način da zaobiđu sigurnost čipa i pročitaju podatke s njega. Nažalost, nisu razočarali.

Trapping kartice bankomata

Iako nije tako široko izvještavan kao druge šeme napada na bankomat, trapping kartica je aktivan i nažalost radi. Trapping kartica je metoda u kojoj kriminalci fizički hvataju debitnu ili kreditnu karticu svoje mete putem bankomata. Oni to rade uvođenjem uređaja, obično libanonske petlje, koji sprječava izbacivanje

kartice nakon što se transakcija završi. Kriminalci kradu PIN svoje mete pogledom preko ramena korinika ili upotrebom male skrivene kamere slične onima koje se koriste u skimmingu.

Cash trapping

Ovo je sistem kao hvatanje kartica, samo kriminalci hvataju gotovinu koju je njihova meta upravo podigla. Alat za trapping je nalik kandži, ogromna naprava nalik na viljušku koja drži otvor za gotovinu otvorenim nakon podizanja bankomata uvodi se u otvor za gotovinu bankomata kako bi uhvatio barem dio gotovine ili uglavnom sve.

Black box attacks

Black box je elektronički uređaj - drugi kompjuter, mobilni telefon, tablet ili čak modificirana ploča spojena na USB žicu - koji izdaje komande bankomatu na iniciranje prevara. Najvjerovatnije mete ovog napada su bankomati izvan objekata banke (dislocirani bankomati).

Napad black box mogao bi uključivati taktike socijalnog inženjeringa, poput oblačenja u tehničara bankomata, kako bi se otklonile sumnje dok akter pljačke fizički dira bankomat. Ponekad prevaranti koriste endoskop, medicinski alat koji se koristi za ispitivanje ljudskog tijela, kojim lociraju i odspoje žicu bankomata i povežu je s njihovim black boxom. Ovaj uređaj zatim izdaje komande dispenzeru da izbaci novac.

Kako ovaj tip napada ne koristi zlonamjerni softver, black box napad obično ostavlja malo ili nimalo dokaza - osim ako su prevaranti ostavili hardver koji su koristili, naravno.

Social engineering

Direktno ciljanje bankomata ugrožavanjem njihovih slabih tačaka, bilo da se nalaze na površini ili iznutra, nije jedini efikasan način za prevarante

da lako dođu do gotovine. Oni, također, mogu iskoristiti nepažnju ljudi koji koriste bankomate. Evo načina na koji korisnici mogu da predaju teško zarađeni novac kriminalcima, često bez znanja.

Defrauding the elderly (Prevara starijih osoba)

Obmanjivanje starijih osoba. Ovo je postao trend u Japanu. Prevaranti, koji se predstavljaju kao rođaci kojima je potreban novac za hitne slučajeve ili državni službenici koji prikupljaju naknade, ciljaju na starije žrtve. Zatim im *pomažu* dajući upute kako da prebace novac putem bankomata.

Assistance fraud (Pomoć kao prevara)

Nekome je u nekom trenutku u prošlosti možda prišao ljubazni stranac u istom redu bankomata pružajući mu ruku pomoći. Prevaranti koriste ovu taktiku kako bi mogli zapamtiti broj kartice i PIN svoje mete koje zatim koriste za pokretanje nezakonitih novčanih transakcija. Česte mete ovog napada su i starije osobe, kao i zbunjeni novi korisnici koji su vjerovatno prvi put vlasnici kartice.

Shoulder surfing (Pogled preko ramena)

Ovo podrazumijeva situaciju da vas neko posmatra dok ukucavate svoj PIN pomoću tastature bankomata. Ukradeni PIN kodovi su posebno zgodni za *surfere preko ramena*, posebno ako njihova meta odsutno napusti područje nakon što uzme gotovinu, ali nije u potpunosti završila sesiju. Neki korisnici bankomata odlaze prije nego što uspiju odgovoriti na upit mašine kada ih pita da li imaju još jednu transakciju.

I prije nego što sesija nestane, prevarant unosi ukradeni PIN kako bi nastavio istu.

Eavesdropping

Kao i prethodna tačka, cilj prisluškivanja je krađa PIN koda mete. Ovo se radi slušanjem i pamćenjem tonova koje tasteri bankomata daju kada neko unese svoj PIN tokom sesije transakcije.

Distraction fraud

Prevara koja odvlači pažnju. Ova taktika je zahvatila Britaniju prije nekoliko godina. A scenario ide ovako: nepoznatog korisnika bankomata ometa zvuk ispuštanja novčića iza sebe dok vadi novac. On ili ona se okreću da pomognu osobi koja je ispustila novčiće, ne znajući da neko drugi već krade gotovinu koju je bankomat upravo izbacio ili zamjenjuje lažnu karticu njegovom pravom. Korisnik bankomata se osvrće na terminal, zadovoljan da je sve izgledalo normalno, a zatim nastavlja svojim putem. S druge strane, osoba kojoj su pomogli ili daje ukradenu karticu ili svom saučesniku kaže PIN ukradene

kartice koji je zapamtila prije nego što je namjerno ispustila novčiće.

ATM Fizički napadi

Ako blaža metoda nije dovoljna za uspješnu pljačku bankomata, moguće su metode primjene sile. Koliko god grubo, nesofisticirano i aljkavo izgledali, kriminalci su postigli određeni uspjeh ovim putem.

Prevaranti, koji bi radije bili glasni nego tihi u svojim aktivnostima, odlučili su se za korištenje eksploziva - čvrstog i plinskog, podjednako, te sajlom na mašini kako bi je izvukli i odvezli. Neki koriste bager za kopanje pri čemu

> *Prevaranti, koji bi radije bili glasni nego tihi u svojim aktivnostima, odlučili su se za korištenje eksploziva - čvrstog i plinskog, podjednako, te sajlom na mašini kako bi je izvukli i odvezli. Neki koriste bager za kopanje pri čemu čupaju bankomate postavljene na zid s vanjske strane zgrade.*

čupaju bankomate postavljene na zid s vanjske strane zgrade.

Ukupni fizički napadi na bankomate nastavljaju da rastu u Evropi. Prema Evropskom udruženju za sigurne transakcije (EAST) Od 2017. do 2018. godine došlo je do povećanja ukupnih gubitaka od 16 posto (sa 34,6 miliona dolara na 40,2 miliona dolara) i povećanja prijavljenih incidenata za 27 posto (sa 3.584 na 4.549). Najveći dio gubitaka nastao je zbog eksplozivnih ili plinskih napada praćenih pljačkom.

"Stopa uspjeha eksplozivnih napada je od posebnog značaja", rekao je izvršni direktor EAST-a **Lachlan Gunn** u izvještaju. Ovakvi napadi nastavljaju da se šire geografski, a dvije zemlje su ih prvi put prijavile početkom 2019. godine.

Radna grupa za sigurnost bankomata (ATMSWG) objavila je dokument o najboljim praksama protiv fizičkih napada na bankomate na koji se finansijske institucije, banke i trgovci na bankomatima mogu pozvati i koristiti u svom planiranju da pojačaju fizičku sigurnost svojih mašina. Slično tome, ATM Industry Association (ATMIA) ima zgodan vodič o tome kako spriječiti ATM gas i eksplozivne napade.

Finansijske institucije i provajderi bankomata znaju da je pred njima dug put kako bi se u potpunosti riješili prevara

i krađe te su pronalazili i primjenjivali načine da pojačaju svoje sigurnosne mjere. Naravno, ni korisnici bankomata ne bi trebali smanjiti oprez.

Savjeti za sigurno korištenje bankomata

Smanjite vjerovatnoću da budete žrtva prevare ili drugih opasnosti koje vas vrebaju – čitajući i slijedeći ove savjete:

- Odaberite bankomat koji se čini sigurnim za korištenje. Dobro je osvijetljen, prolaznici ga mogu vidjeti, a na njega je usmjerena nadzorna kamera. U idealnom slučaju, idite na zatvoreni bankomat koji se može naći u poslovnicama banaka, trgovačkim centrima, restoranima, trgovinama i drugima. Izbjegavajte mašine koje su bile zanemarene ili vandalizirane.
- Ako se nađete u području koje vam nije poznato, pokušajte potražiti bankomate koji ispunjavaju većinu fizičkih zahtjeva koje smo spomenuli.
- Ograničite samo odlazak na lokacije bankomata, posebno kada to radite izvan uobičajenog radnog vremena banke. Vaš prijatelj ili rođak može pomoći ako transakcija krene po zlu. Također, samo njihovo prisustvo moglo bi odbiti pljačkaša.
- Provjerite bankomat. Potražite uređaje koji možda vire iza njega ili iz bilo kojeg od njegovih perifernih uređaja. Potražite lažne prednje strane (preko utora za kartice i novac, tastature ili, još gore, preko cijele strane mašine), sitne rupe na kojima bi mogle biti postavljene kamere, pukotine, neusklađene boje

tipki, itd. Prijavite bilo koji od ovih znakova banci i onda potražite drugi bankomat.
- Na kraju, uočite svakoga za koga mislite da luta u vašoj blizini ili se ponaša sumnjivo. Ne suprotstavljajte im se. Umjesto toga, ako je njihovo ponašanje dovoljno uznemirujuće, prijavite ih policiji.
- Odložite sve što će vam odvratiti pažnju dok koristite bankomat. Da, mislimo na vaš telefon i vaš Nintendo Switch. Zbog toga bi čovjek lako mogao prestati biti svjestan svog okruženja, što kriminalci mogu iskoristiti u svoju korist.
- Povucite čitač kartica i bankomat kako biste bili sigurni da nema priključenih dodatnih uređaja.
- Isplati se pokriti tastaturu prilikom unosa PIN-a, bez obzira da li ste sami u redu čekanja ili ne. Možda ste na bankomatu provjerili ima li znakova fizičkog neovlaštenog pristupa, ali uvijek je moguće nešto propustiti. Također, ako je sljedeća osoba u redu preblizu, podsjetite je da se pomjeri dalje ili pokrijte PIN polje koliko god možete.
- Uvijek odštampajte kopiju računa za bankomat i odložite je radi sigurnosti. Na ovaj način imate nešto na šta možete da se osvrnete i uporedite s izvodom iz banke.
- Brzo i diskretno odložite svoju karticu, gotovinu i račun.
- Ako bankomat nije vratio vašu karticu, ostanite pored aparata i nazovite broj podrške vaše banke 24/7 da ukinete vašu karticu tako da, kada kriminalci pokušaju da je koriste, neće uspjeti. Recite drugima iza vas u redu da se vaša kartica zaglavila i da neće moći koristiti mašinu dok je ne izvadite.
- Ako bankomat nije izdao novac, zabilježite tačan datum, vrijeme i lokaciju bankomata gdje se to dogodilo i nazovite broj podrške banke 24/7. Snimite nekoliko slika i pomoću telefona pošaljite kopiju sebi (bilo putem SMS-a ili e-pošte) kako biste imali digitalni zapis.
- Također pozovite izdavatelja kartice ili banku da podnesete zahtjev, saopštite im da bankomat koji koristite nije izdao gotovinu. Podnošenje zahtjeva bilo bi mnogo lakše i brže da koristite bankomat svoje banke u zgradi banke.
- Ako se to dogodilo u trgovini, odmah obavijestite nekog od zaposlenih. Možda imaju proces da ubrzaju stvari. Oni mogu spriječiti druge kupce u trgovini da koriste problematičnu mašinu.
- Redovno provjeravajte svoj bankovni izvod za potencijalna povlačenja i/ili korištenje kartice koje niste sami učinili. Prijavite prevaru svojoj banci ako je uočite. Koristite usluge SMS dojave transakcije.

Razmislite o drugim načinima plaćanja

Ne morate uvijek podizati novac s bankomata. Ako postoje načini na koji potrošači mogu platiti robu bez upotrebe gotovine na bankomatu, trebali bi barem razmotriti ove opcije.

Mnogi tvrde da je korištenje beskontaktne ili *dodirni i plati* funkcije vaše kartice ili pametnog telefona efikasan način za borbu protiv prevara računa (i bankomata) u potpunosti. ■

Kao i uvijek, čuvajte se!!!

***Svakog minuta 2.900.000 dolara se izgubi zbog cyber kriminala*. (Forbes)**

VEKTORI *CYBER* NAPADA U 2021. GODINI

Cyber kriminalci stalno mjenjaju svoje taktike. Prije 10 godina čest vektor napad bile su zlonamjerne web stranice koje su pokušavale instalirati zlonamjerni softver na uređaj.

Autorica:
Sanela Stupar

Vektor napada je sredstvo pomoću kojeg haker može provaliti u kompjuterski sistem ili mrežu kako bi pokrenuo napad.

Cyber napad je namjerna radnja koju provode jedan ili više cyber kriminalaca kako bi ukrali podatke, izmislili informacije ili onemogućili digitalne sisteme. Da bi se izborile s ovim višestrukim vrstama cyber napada, organizacijama su potrebni IT stručnjaci i stručnjaci za cyber sigurnost.

Putem cyber sigurnosnih napada cyber kriminalci dobijaju nezakonit i neovlašten pristup jednom ili više računara koje koriste u skladu sa svojim pogodnostima. Postoje različite vrste cyber napada koji pogađaju pojedince širom svijeta.

Izdvajamo najčešće tipove cyber napada koji su zabilježeni u 2021. godini i koji se nastavljaju i u 2022. godini.

To su:

1. *phishing*,
2. *malware*,
3. *ransomware*,
4. napadi uskraćivanja usluge (DDoS),
5. kompromitovani kredencijali,
6. zlonamjerni insajderi,
7. pogrešna konfiguracija,
8. nedostatak enkripcije,
9. napadi na web aplikacije i
10. udaljeni pristup zaposlenika.

Vektor napad	Opis	Prijedlog opštih mjera
Phishing	*Phishing* napadi su jedan od najčešćih tipova cyber napada. Koristeći ove napade, napadači pokušavaju doći do ličnih podataka ili podataka poput korisničkog imena, lozinke i podataka o kreditnoj kartici, maskirajući se u subjekte od povjerenja. *Phishing* se uglavnom provodi putem elektronskih medija, e-pošte ili telefonskih poziva.	Možete izbjeći prevaru tako što ćete obučiti svoje osoblje da uoči znakove prevare, kao što je odgovor za unosom određenih informacija odmah. Educirajte osoblje da provjere s navodnim pošiljaocem potencijalne poruke putem drugog načina komunikacije prije nego što odgovore.
Malware	U *malware* napadu napadači kreiraju kod koji se zove *malware*, a koji služi za hakiranje digitalnih uređaja, uključujući prijenosna računala, računare i mobilne uređaje kako bi dobili neovlašteni pristup. Često se isporučuje na računar ili mrežu putem *phishing* e-pošte na koju je kliknut, ali se ponekad greškom preuzme sa zlonamjerne web stranice.	Zlonamjerni softver možete izbjeći praćenjem korisničkog prometa na mreži, ponašanjem korisnika putem e-pošte i korištenjem antivirusnih rješenja.
Ransomware	Ransomware je vrsta zlonamjernog softvera koji zaključava korisnike iz njihovih sistema i podataka. Da bi dobili ključ za šifriranje, moraju platiti otkupninu. Ako to ne urade, prijete posljedice. To može varirati od objavljivanja vlasničkih informacija na javnoj web stranici do jednostavnog nevraćanja njihovih podataka. To ne znači da kriminalci uvijek drže svoju riječ kada se otkupi plaća – oni su ipak kriminalci.	Izbjegnite napade *ransomwarea* tako što nećete kliknuti na sumnjive veze, skenirajte e-poštu u potrazi za zlonamjernim softverom i čuvajte sigurnosnu kopiju svih podataka. Ako ste na meti, ali imate sigurnosnu kopiju podataka i sistema, moći ćete nastaviti poslovati uprkos napadu.
Napadi uskraćivanja usluge (DDoS)	Napadi uskraćivanja usluge su jedan od najčešćih vektora napada; prema **Dark Readingu**, DDoS napadi u prvom kvartalu 2021. porasli su za 31% u odnosu na isti period 2020. godine. DDoS napad je jedan od uobičajenih tipova cyber napada koji ima za cilj da preplavi sistem na takav način da ne odgovori na zahtjeve svojih klijenata ili kupaca zbog čega se može izgubiti ogroman broj klijanata ili kupaca u kratkom roku.	Možete ublažiti DDoS napad praćenjem mrežnog saobraćaja i filtriranjem dolaznog saobraćaja.
Kompromitovani kredencijali	U ovim vrstama napada napadači pokušavaju da hakuju različite naloge žrtava hakirajući njihove profile	Razmislite o dvofaktorskoj autentifikaciji ili uklonite

Kompromitovani kredencijali	i njihove lozinke, što im daje nezakonit pristup svim informacijama žrtve koje na kraju koriste napadači u skladu sa svojim prednostima.	lozinke korištenjem autentifikacije bez lozinke za svoje korisnike.
Zlonamjerni insajderi	Mnoge vrste cyber napada dešavaju se svakodnevno, a najšokantnija činjenica je da većinu vremena postoji insajder uključen u proces koji pomaže cyber kriminalcima da dođu do informacija o njihovoj organizaciji. Insajderi ciljnih organizacija na kraju postaju ti koji svakodnevno dovode do ovakvih cyber napada. Oni pomažu vanjskim napadačima dajući im sve potrebne informacije, što dovodi do daljnjih posljedica. Ove vrste hakerskih napada mogu se odvijati u korporativnim okruženjima. To je također jedan od uobičajenih tipova napada na banke i druge finansijske institucije.	Nadgledajte podatke i pristup mreži radi čudnog ponašanja i utvrdite koji su zaposlenici nezadovoljni.
Pogrešna konfiguracija	Greške u konfiguraciji mogu ostaviti organizaciju otvorenom za prijetnje i rizike. Ako je korpa Amazon Web Services pogrešno konfigurirana, to može ostaviti vrijedne podatke otvorenim za javni internet, a vaša organizacija nikada neće znati ko je vidio te podatke.	Uspostavite procese kako biste bili sigurni da je svaki dio vaše mreže ispravno konfiguriran i dosljedno nadzirite svoje mreže kako biste na vrijeme uočili anomalije na sistemu.
Nedostatak enkripcije	Enkripcija podataka prevodi vaše podatke u drugi oblik koji samo ljudi s pristupom tajnom ključu ili lozinki mogu pročitati. Svrha: zaštita vaših podataka tokom skladištenja ili prijenosa između mreža. Kada nema enkripcije ili je slaba enkripcija, haker koji je hakovao sistem će jednostavno moći da pročita vaše osetljive podatke.	Primijenite jaku enkripciju, posebno za osjetljive podatke.
Napadi na web aplikacije	Ovi napadi uključuju SQL injekciju i cross-site skriptiranje. Ove vrste napada su fokusirane na određeni cilj, kao što je prenamjena web aplikacije za distribuciju zlonamjernog softvera, na primjer.	Firewall za web aplikacije, korištenjem sigurnog razvoja i praćenje ranjivosti.
Udaljeni pristup zaposlenika	Hakeri se fokusiraju na nesigurne krajnje tačke do vašeg preduzeća. Kućne bežične mreže nisu tako sigurne kao na radnom mjestu. Prosječna kućna mreža nema zaštitne zidove, a neki radnici možda koriste svoje lične uređaje za pristup vašoj mreži.	Zaštitite svoje udaljene radnike dosljednim praćenjem sigurnosti vaše krajnje tačke i brzim reagiranjem na incidente.

Angažovanjem IT stručnjaka i stručnjaka za cyber sigurnost, implementacijom sigurnosnih standarda za informacionu tehnologiju i informacijsku sigurnost, primjenom kritičnih kontrola uz pomoć sigurnosnih alata, kao i redovnim provođenjem penetracijskog testiranja smanjiti ćete rizike od incidenata u cyber sigurnosti.

Ransomware

Cyber kriminalci stalno mjenjaju svoje taktike. Prije 10 godina čest vektor napad bile su zlonamjerne web-stranice koje su pokušavale instalirati zlonamjerni softver na uređaj. *Ransomware* je postao jedna od najpopularnijih vrsta cyber kriminala. Evoluirao je kako

Zanimljivost

Troškovi cyber osiguranja će se i dalje povećavati

"S obzirom na to da isplate osiguranja postaju sve češće i sve skuplje, cijena cyber osiguranja je već naglo porasla. Cijene su porasle za 96% u SAD-u i 73% u Velikoj Britaniji u trećem tromjesečju 2021. u poređenju sa istim kvartalom prošle godine. Očekujemo nastavak povećanja u 2022.

Štaviše, polise osiguranja će **zahtijevati implementaciju kritičnih kontrola koje smanjuju rizik od incidenata u cyber sigurnosti.** Kako napadi postaju sve češći, osiguravajuća društva će plaćati samo u izuzetnim slučajevima" - *Ilia Sotnikov, stručnjak za cyber bezbjednost i potpredsjednik Stratega korisničkog iskustva i sigurnosti u Netwrixu*

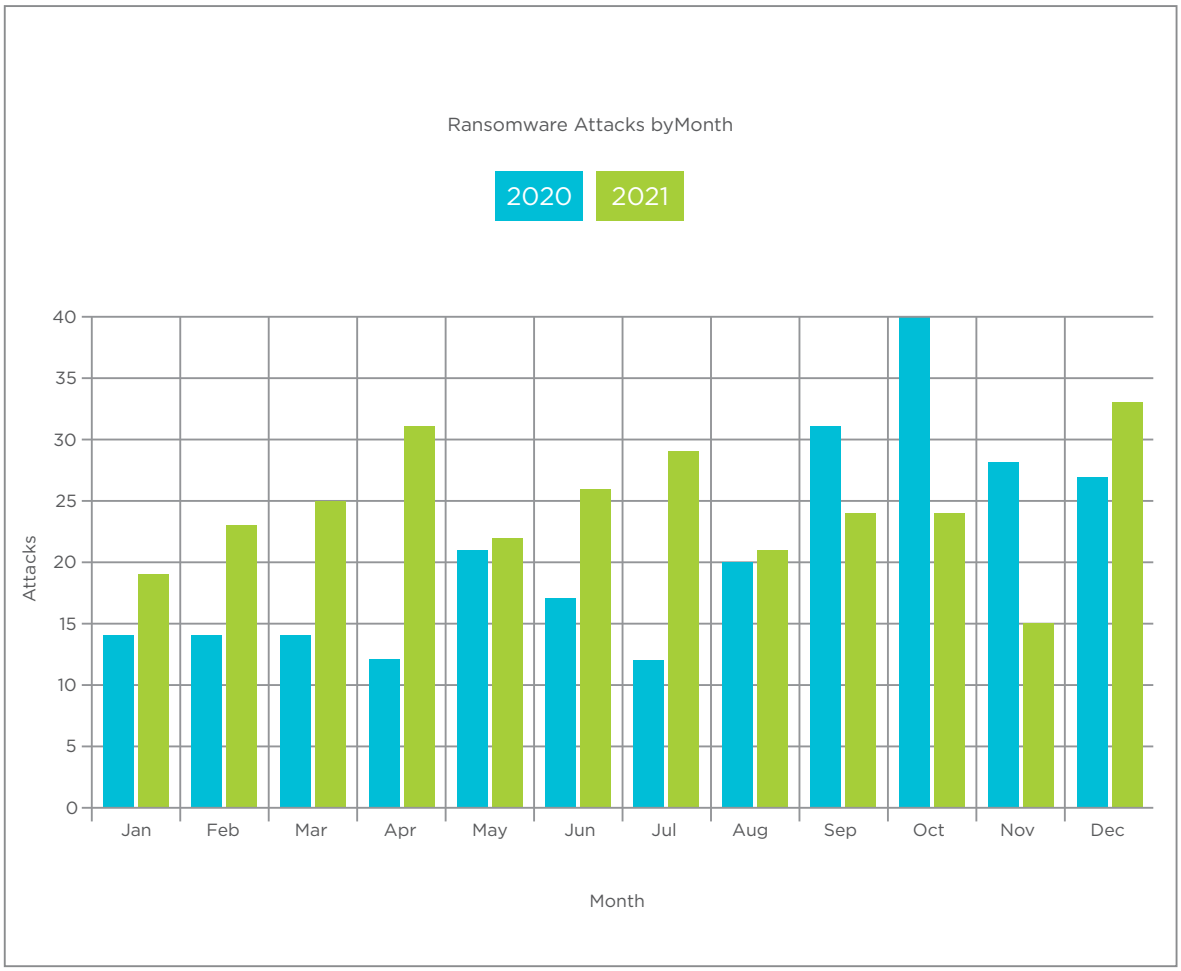
su se hakeri udaljili od automatiziranih, raspršenih *ransomware* kampanja prema ručnom ciljanju velikih organizacija. Troškovi ciljanih napada su veći, ali hakeri računaju da su velike organizacije spremnije isplatiti znatno veće otkupnine kako bi se što prije oporavile od cyber napada. Savremeni *ransomware* ovisi o nekoliko tehnologija (npr. kriptovalute) i usluga dostupnih na internetskim kriminalnim tržištima.

> *Ransomware je postao jedna od najpopularnijih vrsta cyber kriminala. Evoluirao je kako su se hakeri udaljili od automatiziranih, raspršenih ransomware kampanja prema ručnom ciljanju velikih organizacija.*

Pojava kriptovaluta, kao što je *bitcoin*, omogućila je transakcionalnu finansijsku infrastrukturu koja omogućava anonimna, brza i globalna plaćanja. Transakcije kriptovalutama su nepromjenjive (tj. transakcije se ne mogu

poništiti) i provjerljive (tj. transakcije su uvijek javne i mogu se automatski potvrditi). Ovo su kritične značajke koje osiguravaju da se isplate otkupnine ne mogu poništiti nakon dešifriranja datoteka žrtve. *Bitcoin* je postao istaknut na nekoliko internetskih tržišta na kojima se prodavala ilegalna roba od 2011. do 2013. godine, a cyber kriminalci su prihvatili *bitcoin* kao standardni oblik plaćanja otkupnine oko 2013. godine.

Prije kriptovaluta i povezanih usluga pranja novca, cyber kriminalci su se gotovo u potpunosti oslanjali na tradicionalne mehanizme pranja novca kao što su slanje ukradenog novca na posredničke račune u zemlji žrtve i angažovanje kriminalaca ili nesvjesnih lokalnih stanovnika da brzo prenesu sredstva u strane banke ili loše regulirane sisteme plaćanja na mreži. Ovi posrednici mogli su naplatiti do 60% vrijednosti transakcije. Za usporedbu, transakcije kriptovalutama obično koštaju ispod 5% vrijednosti transakcije. ■



KLJUČNE VARIJANTE I OPERATORI RANSOMWAREA[1]

CRYPTO LOCKER	*Ransomware* koji je 2013. godine kreirao ruski cyber kriminalac, Evgeniy Bogachev, smatra se prvom modernom varijantom *ransomwarea* koju distribuira malver **GameOverZeus**, čiji su operateri uključivali Bogacheva i Evil Corp.
EVIL CORP	Organizirana kibernetička kriminalna grupa sa sjedištem u Rusiji odgovorna za **Dridex** zlonamjerni softver i višestruke kampanje *ransomwarea* od 2015. U decembru 2019. SAD su optužile i sankcionirale članove *Evil Corpa* zbog njihovih tekućih cyber kriminalnih aktivnosti i pružanja pomoći ruskoj obavještajnoj službi.
FIN6	Organizirana cyber kriminalna grupa, vjerovatno ruskog govornog područja, navodno je povezana s višestrukim infekcijama **Ryukom** i **Megacortexom** od 2018. godine, a aktivna je od 2015. godine.
MAZE	Varijanta *ransomwarea* za čije je operatere poznato da propuštaju podatke o žrtvama zbog neplaćanja. Aktivan je najmanje od novembra 2019.
MEGA CORTEX	Varijanta *ransomwarea* otkrivena 2019. godine. Zapaženo je kako cilja na procese industrijskih kontrolnih sistema koji su navodno povezani s **Trickbot** i **FIN6** operacijama.
RYUK	Varijanta *ransomwarea* za koju je poznato da cilja velika preduzeća, bolnice i kritičnu infrastrukturu i zahtijeva izuzetno velike otkupnine. Aktivan je od avgusta 2018. godine. Ryuk je povezan sa više cyber kriminalaca koji govore ruski, uključujući i operatere **Trickbota**.
SAMSAM	Varijanta *ransomwarea* koju su koristili iranski cyber kriminalci i koja je ugrozila više opština, bolnica, univerziteta i preduzeća u Kanadi, SAD-u, Velikoj Britaniji i drugim zemljama, prvenstveno u periodu od 2015. do 2018. godine.
SODINOKIBI	Varijanta *ransomwarea* čiji programeri, koji govore ruski, unajmljuju druge cyber kriminalce da distribuiraju i implementiraju njihov *ransomware*.
TRICK BOT	Bankarski trojanac koji se koristi za krađu finansijskih podataka i akreditiva za *online* bankarstvo. Trickbot je povezan s više kibernetičkih kriminalaca koji govore ruski i primarni je distributer **Ryuk** *ransomwarea*.

[1] https://cyber.gc.ca/

UPRMBiH

Udruženje profesionalnih rizik menadžera

UREDNIČKI TIM

Muris Bešić
Voditelj odjela za
pravnu podršku mreži,
Direkcije pravnih poslova
Sparkasse Bank dd BiH

Nermin Ibradžić
Voditelj Odjela za usklađenost
poslovanja i sprečavanje pranja
novca i terorističkih aktivnosti
NLB Banka d.d. Sarajevo

Sanela Stupar
Specijalista za
informacionu sigurnost
Raiffeisen Bank dd BiH

Medžid Suljić
Stručni saradnik za fizičku
i tehničku sigurnost
NLB Banka dd Sarajevo

Mirzad Topić
Specijalista za detekciju
i prevenciju prevara
Sberbank BH dd

Mujo Vilašević
Rukovodilac Regulatorne
usklađenosti i suzbijanja
finansijskog kriminala
Raiffeisen Bank dd BiH

Vedran Vinšalek
Voditelj odjela
Operativni rizik
Sberbank BH dd

Sanela Vrana
Voditelj sigurnosti
informacionog sistema
Razvojna banka
Federacije BiH