GOD. 5 . BR. 6 [2021] 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


[COVID-19]
CORONAVIRUS
0034 - 234

UPRMBiH
Udruženje profesionalnih rizik menadžera

FRAUDinfo

Udruženje profesionalnih rizik menadžera u BiH

Fra Anđela Zvizdovića 1,
71 000 Sarajevo - BiH

tel.:
+387 62 393 568

e-mail:
amar.brkan@uprmbih.ba

Izdavač:
UDRUŽENJE
PROFESIONALNIH
RIZIK MENADŽERA

Design, DTP & Print:
PERFECTA, Sarajevo

perfecta

Branilaca Šipa 33

tel.:
+387 61 214 222

e-mail:
info@perfecta.ba

ISSN 2566-3100

UVODNA RIJEČ

Dragi čitaoci,

naš vrijedni tim stručnjaka ispred **Fraud Foruma** pripremio je šesto izdanje ***Fraud Info*** časopisa koji sadrži dosta zanimljivih tema s prijedlozima i praktičnim primjerima za unapređenje poslovanja te prijedloge mjera za prevenciju i detekciju *fraud* trendova. I ovaj broj izdajemo 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 pokušavamo pomoći finansijskim institucijama u BiH da bolje razumiju *cyber* rizike i prevare te da se adekvatno zaštite od istih.

Tokom 2020. i 2021. godine dominirali su naslovi o COVID-19, a uporedo se odvijao i kontinuirani trend ka digitalnoj transformaciji poslovanja društva, preduzeća i vlade.

Kako se većina zemalja širom svijeta suočava s efektima pandemije COVID-19, uloga informacione komununikacijske tehnologije postala je značajna za razvoj i nastavak ekonomske i društvene aktivnosti kao odgovor na smanjenje utjecaja pandemije.

Pred banke je stavljen težak zadatak u smislu realizacije pomoći građanima i pravnim licima. U ovom broju upoznat ćemo vas s kompleksnim problemima s kojima su banke bile suočene prilikom izmjene ugovorenih uslova s klijentima, a u cilju prevazilaženja nastalih poteškoća u otplati zaduženja uzrokovanih virusom CIVID-19.

Pandemija COVID-19 podstakla je potrošače i poduzeća da usvoje digitalne usluge i tehnologije ubrzavajući digitalnu transformaciju u ponašanju potrošača. Mnoge kompanije automatizuju svoje tradicionalno poslovanje koristeći savremenu pametnu tehnologiju pod nazivom *Četvrta industrijska revolucija* (ili *Industrija 4.0*).

U šestom izdanju ***Fraud Infa*** možete saznati da li Bosna i Hercegovina ima strateški cilj za transformaciju poslovanja u Industriju 4.0, koje sigurnosne

Sadržaj

mjere je potrebno implementirati u cilju prevencije novih globalnih *cyber* napada, koje su najbolje prakse za prevenciju neautoriziranog pristupa podacima i aplikacijama te ko je najslabija karika sigurnosti informacionih sistema.

Upoznajte se detaljnije s prednostima uvođenja sistemskog rješenja za prevenciju i detekciju prevara, a koji predstavlja jedan od veoma bitnih faktora upravljanja rizikom prevara.

Prevencija i detekcija prevare podrazumijeva otkrivanje prevare u njenom samom početku kako bi se poduzele odgovarajuće mjere i tako minimizirala prouzrokovana šteta.

Pripremili smo zanimljive ekspertize u kojima su autori dali osvrt na značaj usklađenosti poslovanja sa zakonskom regulativom, međunarodno priznatim standardima te direktivama i smjernicama Evropske unije.

Zanimljiva ekspertiza pripremljena je s aspekta postojeće zakonske regulative i praktičnih primjera u kojoj autor navodi benefite koje eksternalizacija donosi, rizike kojima je kompanija izložena u slučaju eksternalizacije te prijedloge za unapređenje upravljanja rizikom.

Usklađenost poslovanja sa standardom ISO 37001 ima za cilj pomoći organizacijama da uspostave, implementiraju, održavaju i poboljšavaju sistem upravljanja za sprečavanje podmićivanja (*anti-bribery compliance management*). Govorimo i o zaštiti "zviždača" u Evropskoj uniji.

Pripremili smo zanimljiv intervju sa Sanjom Ćatibović, oficirkom Projekta za sigurnosnu saradnju OSCE misije u Bosni i Hercegovini, u kojem ćete više saznati o poduzetim aktivnostima za uspostavu CERT-a BiH.

Udruženje profesionalnih risk menadžera u BiH ostaje posvećeno i u narednom periodu na podizanju svijesti, promovisanju najboljih praksi za upravljanje rizicima prevara, razmjeni iskustava i pokretanju relevantnih inicijativa sa ciljem umanjenja rizika. Vjerujemo da šesto 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

Uticaj pandemije COVID-19 na otplatu zaduženja

IZMJENE UGOVORENIH USLOVA IZMEĐU BANAKA I KLIJENATA UZROKOVANE PANDEMIJOM COVID-19

Govorimo o kompleksnosti problema s kojima su banke bile suočene prilikom izmjene ugovorenih uslova s klijentima i težnjama za iznalaženje što povoljnijih rješenja za klijente koja ujedno osiguravaju zakonito postupanje banke

Autor:
Muris Bešić

Pandemija koja je nastala usljed pojave virusa COVID-19 imala je veliki uticaj na sve segmente života uključujući i cjelokupnu privredu na globalnom nivou, a čega ni Bosna i Hercegovina još uvijek nije pošteđena.

S eskaliranjem pandemije pojavile su se i potrebe za ublažavanjem posljedica koje ista ima na privredne aktivnosti usljed čijeg smanjenja neminovno dolazi i do pogoršavanja sposobnosti fizičkih i pravnih lica za urednom ot-

platom zaduženja koje imaju kod subjekata finansijskog sektora. Imajući u vidu da se najveći broj zaduženja nalazi kod banaka, posmatrat ćemo navedenu problematiku s aspekta bankarskog sektora.

Na samom početku pandemije, prilikom govora o mogućim mjerama, kod određenog broja stanovništva došlo je do stvaranja pogrešne predstave o mjerama koje će nadležne institucije usvojiti kao mjere za ublažavanje posljedica pandemije. Kao najočitiji primjer navedenog, banke su se susretale sa zahtjevima da odmah prestanu s bilo kakvim daljim naplatama dugovanja od klijenata što svakako da nije bilo moguće jer kao mjera nisu ponuđeni alternativni načini otplate postojećih zakonitih dugovanja.

Preduslovi za realizaciju

Kako je i bilo za očekivati, od strane nadležnih organa usvojene su *Odluke*[1] u kojima se propisuju mogućnosti koje stoje na raspolaganju bankama i korisnicima njihovih usluga, a u cilju omogućavanja prevazilaženja teškoća u otplati kredita.

Kao mogućnosti modifikacije kredita u skladu s *Odlukama* predviđeni su:

a) moratorij, odnosno odgoda u otplati kreditnih obaveza od najduže 6 mjeseci,
b) uvođenje *grace* perioda za otplatu glavnice kreditnih obaveza u slučaju kredita koji se otplaćuju anuitetno na period od najduže 12 mjeseci,
c) produženje krajnjeg roka za otplatu kredita koji se otplaćuju anuitetno,
d) produženje roka dospijeća kredita s jednokratnim dospijećem, uključujući i *revolving* kredite i prekoračenja po transakcijskim računima na period od najduže 12 mjeseci pri čemu bi klijent banke tokom tog perioda mogao koristiti i dio izloženosti koji je bio neiskorišten na dan modifikacije,
e) odobravanje dodatnog iznosa izloženosti za potrebe prevazilaženja klijentovih trenutnih poteškoća s likvidnošću,
f) prilagođavanje plana otplate srazmjerno smanjenju prihoda ili nekom drugom relevantnom parametru koji određuje banka i
g) druge mjere koje banka poduzima u cilju olakšanja servisiranja kreditnih obaveza klijenta i uspostave održivog poslovanja klijenta.

Sve navedene mogućnosti za cilj imaju omogućavanje korisnicima bankarskih usluga prevazilaženje poteškoća u otplati kredita koje su uzrokovane pandemijom COVID-19.

> *U skladu s donesenim odlukama od strane nadležnih agencija za bankarstvo, banke su mogle navedene mjere provoditi temeljem zahtjeva fizičkih ili pravnih lica ili te mjere pokrenuti samoinicijativno uzimajući u obzir nepovoljne ekonomske posljedice (direktine ili indirektne) uzrokovane pojavom virusnog oboljenja COVID-19.*

[1] *Odluka o privremenim mjerama koje banka primjenjuje za ublažavanje negativnih ekonomskih posljedica uzrokovanih virusnim oboljenjem „COVID-19“* („Službene novine FBiH“, br. 22/20) koju je donijela Agencija za bankarstvo FBiH i *Odluka o privremenim mjerama bankama za ublažavanje negativnih ekonomskih posljedica uzrokovanih virisnim oboljenjem „COVID 19“* (Sl. glasnik RS 27/20).

U skladu s donesenim odlukama od strane nadležnih agencija za bankarstvo, banke su mogle navedene mjere provoditi temeljem zahtjeva fizičkih ili pravnih lica ili te mjere pokrenuti samoinicijativno uzimajući u obzir nepovoljne ekonomske posljedice (direktine ili indirektne) uzrokovane pojavom virusnog oboljenja COVID-19. Ujedno, imajući u vidu da odluke izričito naglašavaju da je potrebno voditi računa o dokumentovanosti kreditnih aktivnosti banke, svakako da je potrebno da klijent banke dostavi određenu vrstu dokaza kojim se dokazuje da su njegove mogućnosti otplate kredita smanjene.

Realizacije izmjena ugovorenih uslova

Imajuću u vidu da je usljed pandemije uzrokovane virusom COVID-19 u određenom broju slučajeva onemogućeno kretanje klijenata banke, a radi pristupanja u banku zbog dostave dokumentacije te potpisa odgovarajuće dokumentacije, odlukama su predviđena određena rješenja kojima se omogućava realizacija pravnih poslova u ovako otežanim uslovima. Kroz odluke je predviđena mogućnost korištenja pravnog instituta *Ponude* koji je detaljno definisan *Zakonom o obligacionim odnosima* (dalje: ZOO) u članovima 32-43. Banka ima obavezu da klijente upozna s mogućnošću korištenja mjera sa svim uslovima i efektima mjera, a klijenti su dužni izjasniti se o ponudi i, ako istu prihvataju, dostaviti pisani prihvat ponude. Iako je predviđena isključivo pisana forma prihvata ponude, odredbama odluke je predviđeno da se privremeno može prihvatiti i izjava o prihvatu data u elektronskoj formi, ali samo do sticanja uslova za pribavljanje originalnog dokumenta. Predmetno rješenje je sasvim ispravno, a imajući u vidu član 38. ZOO u kojem je predviđeno da prihvat mora biti dat u formi koju zakon predviđa za tu vrstu ugovora.

Iako je sama izmjena ugovorenih uslova olakšana u smislu da nije potrebno zaključivati klasični aneks na ugovor kako je to uobičajeno u bankarskoj praksi, postavlja se pitanje na koji način uskladiti sredstva osiguranja plaćanja ugovora koji su predmet modifikacije s izmjenama ugovora. Kada govorimo o usklađivanju sredstava osiguranja, ista je potrebno posmatati s aspekta dokumentacije koja je potrebna kako bi se uskladila s izmjenama ugovora koji se osigurava kao i s aspekta troškova koji postoje radi navedenog usklađivanja.

S obzirom na to da je vrlo širok spektar mogućih sredstava osiguranja naplate potraživanja koje banke koriste u praksi, dat ćemo osvrt i na najčešće korištena sredstva osiguranja potraživanja koja se koriste u bankarskoj praksi u Bosni i Hercegovini, a to su: mjenica, zapljena po pristanku dužnika, založno pravo na pokretnim stvarima, založno pravo na nepokretnim stvarima (hipoteka) i polica osiguranja.

Mjenica

Mjenica predstavlja sredstvo osiguranja i sredstvo naplate potraživanja koje daje korisnik kredita ili treće lice. U smislu usklađivanja sa promjenama osnovnog ugovora

> *Ukoliko je rok dospijeća ili iznos novčane obaveze upisan u samoj mjenici, svakako da je potrebno, ako se radi o produženju trajanja ugovora iz kojeg proizilazi potraživanje, uzeti novu mjenicu s upisanim elementima koji su izmijenjeni.*

iz kojeg proističe potraživanje koje se osigurava mjenicom, treba imati u vidu načelo pismenosti i načelo fiksnosti mjenične obaveze. Ukoliko je rok dospijeća ili iznos novčane obaveze upisan u samoj mjenici, svakako da je potrebno, ako se radi o produženju trajanja ugovora iz kojeg proizilazi potraživanje, uzeti novu mjenicu s upisanim elementima koji su izmijenjeni. U praksi se najčešće kao sredstvo osiguranja uzima bjanko mjenica uz odgovarajući alonž mjenice koji predstavlja ovlaštenje za popunu mjenice. U okviru ovlaštenja za popunjavanje mjenice dužnik daje povjeriocu ovlaštenje da sam popuni nedostajuće elemente mjenice koji nisu upisani. U navedenom slučaju postavlja se pitanje da li je potrebno ishoditi dodatno ovlaštenje za popunjavanje mjenice. Odgovor na navedeno pitanje zavisi od toga kako je glasilo ranije mjenično ovlaštenje. Ukoliko u ranije datom mjeničnom ovlaštenju nije sadržano ovlaštenje koje se odnosi na mogućnost korištenja mjenice i u slučaju izmjena uslova ugovora, svakako da je potrebno dopuniti mjenično ovlaštenje kako bi se izbjegli eventualni prigovori mjeničnog dužnika. S aspekta troškova koje eventualno klijent treba da snosi, usklađivanje mjenice s osnovnim ugovorom ne predstavlja veliki problem u praksi osim angažovanja banke na pripremi odgovarajuće dokumentacije i eventualno troškove ovjere potpisa ukoliko je neophodno.

Zapljena po pristanku dužnika

Zapljena po pristanku dužnika predstavlja sredstvo osiguranja uredne otplate zaduženja koje, u skladu sa propisima kojima je regulisan izvršni postupak, može dati sam korisnik kredita ili treće lice. Sama forma izjave o zapljeni je svakako pisana forma, ali elementi izjave nisu strogo predviđeni pozitivnim propisima. S obzirom na to da su elementi, odnosno tekst izjave, predmet sporazuma između dužnika i povjerioca, potrebna izmjena navedenog sredstva osiguranja je faktičko pitanje. Kao i kod mjenice, ukoliko tekst izdate isprave ne upućuje da je dužnik saglasan na produženje roka otplate ili na uvećanje kreditne obaveze (usljed povećanja iznosa ukupno naplaćene redovne kamate), svakako da je potrebno osigurati izmjenu teksta izjave o saglasnosti kako u praksi ne bi bilo zastoja u realizaciji naplate. Kako se predmetna izjava vrlo često koristi i u cilju redovne naplate mjesečnih anuiteta po kreditima, a što obavlja poslodavac dužnika, bitno je voditi računa o tome na koji način se poslodavcu komunicira trenutna obustava plaćanja kako ne bi došlo do gubitka prava prioriteta u naplati usljed eventualnih zahtjeva drugih povjerilaca. Svakako da je u navedenom cilju radi davanja pojašnjenja preporučljivo obaviti i direktne kontakte sa poslodavcima

radi usaglašavanja postupanja, a u interesu klijenata banke. I kod ovog sredstva osiguranja troškovi se odnose na postupanje banke i evetualnu ovjeru potpisa od strane nadležnih organa.

Založno pravo na pokretnim stvarima

Založno pravo na pokretnim stvarima zasniva se temeljem zaključenja ugovora o zalogu i registracijom zaloga u Registru zaloga pri Ministarstvu pravde Bosne i Hercegovine. Stoga je, prije svega, potrebno izvršiti uvid u zaključene ugovore o zalogu kako bi se utvrdilo postoje li ugovorena ograničenja koja se odnose na rok trajanja ugovora o zalogu. Ukoliko se navedena ograničenja predviđaju samim ugovorom, neophodno je zaključiti aneks na postojeći ugovor kako bi se osigurala usklađenost s izmijenjenim osnovnim ugovorom. Dodatno, s obzirom na to da je za pravnu valjanost potrebno izvršiti i registraciju založnog prava pri Registru zaloga BiH, vrlo je bitno provjeriti i način na koji je založno pravo upisano u registar zaloga kao i vrijeme registracije. Istekom vremena registracije založno pravo upisano u registar prestaje i nije moguće ishoditi potvrdu o registraciji koja je vrlo bitna jer predstavlja izvršnu ispravu temeljem koje se pokreće izvršni postupak. Kod navedenog sredstva osiguranja, pored troškova koji su navedeni u prethodnim sredstvima osiguranja, imamo i troškove koje naplaćuje Registar zaloga, a koje plaća banka. Obaveze klijenta na nadoknadu utrošenih sredstava je najčešće ugovorena ili ugovorom o kreditu ili samim ugovorom o zalogu.

Založno pravo na nepokretnim stvarima - hipoteka

Založno pravo na nepokretnim stvarima - hipoteka zasniva se upisom u nadležni javni registar koji se formira pri sudu (zk. ured) ili kao organ uprave (Uprava za geodetske i imovinsko-pravne poslove). Kao osnov za upis u nadležne registre koristi se notarski sačinjen i obrađen ugovor o zasnivanju založnog prava čija je forma propisana posebnim propisima o stvarnim pravima. Također, posebnim propisima kojim je definisan postupak upisa u nadležne registre propisani su i elementi koji se upisuju u odgovarajući izvod iz nadležne evedencije. Sama pravna priroda ugovora o hipoteci je takva da predstavlja strogo akcesoran pravni posao čija valjanost zavisi od usklađenosti s osnovnim poslom radi čijeg osiguranja se zasniva ugovor o hipoteci. Dakle, da bi se osiguralo pokriće za period u kojem je ugovor o kreditu produžen, stav autora je da je nephodno zaključenje aneksa na ugovor o hipoteci kako bi se u nadležnim registrima evidentirala izmjena ugovora o kreditu i na taj način se, za slučaj potrebe, osiguralo nesmetano provođenje izvršnog postupka. Kako u ovom slučaju osim troškova postupanja banke imamo

> *„Sama pravna priroda ugovora o hipoteci je takva da predstavlja strogo akcesoran pravni posao čija valjanost zavisi od usklađenosti s osnovnim poslom radi čijeg osiguranja se zasniva ugovor o hipoteci."*

i troškove koji se odnose na notarske usluge kao i usluge taksi za postupanje nadležnih organa koji vode javne registre kod ovog sredstva obezbjeđenja, troškovi usklađivanja znatno su veći od troškova kod prethodno navedenih instrumenata osiguranja. S obzirom na visinu troškova, a imajući u vidu razloge koji su uzrok promjene ugovorenih uslova, svakako su se od strane nadležnih institucija mogle poduzeti aktivnosti na olakšavanju snošenja troškova građanima i poslovnim subjektima. Ovo se, prije svega, odnosi na ukidanje, umanjenje ili refudiranje svih ili dijela troškova koji se odnose na troškove sudskih ili administrativnih taksi prilikom upisa u javne registre kao i umanjenje tarife od strane notara ili nadoknade građanima ili notarima dijela troškova koji se plaćaju za notarske usluge.

Polica osiguranja

Kao sredstvo osiguranja potraživanja mogu biti korištene različite police osiguranja. Svim policama je zajedničko to da imaju sadržan tačan datum isteka police osiguranja kao i iznos osigurane sume. U skladu sa pozitivnim propisima, nakon isteka roka na koji je zaključena polica prestaje važiti tako da, ukoliko se osigurani slučaj desi nakon proteka navedenog perioda, nije moguć zahtjev za naknadu štete prema osiguravajućoj

> *Svakako da je potrebno izvršiti prilagodbe police osiguranja izmijenjenim uslovima kredita. Imajući u vidu da se ovdje pored ugovornih strana javlja i treća strana - osiguravajuća kuća, potrebno je snositi i troškove produženja police osiguranja čija cijena zavisi od cjenovnika koji propisuju osiguravajuće kuće.*

kući. Također, ukoliko je policom predviđen maksimalni iznos osigurane sume, svaki iznos koji prelazi navedeni iznos osiguravajuća kuća nije obavezna nadoknaditi. Svakako da je potrebno izvršiti prilagodbe police osiguranja izmijenjenim uslovima kredita. Imajući u vidu da se ovdje pored ugovornih strana javlja i treća strana - osiguravajuća kuća, potrebno je snositi i troškove produženja police osiguranja čija cijena zavisi od cjenovnika koji propisuju osiguravajuće kuće.

Zajedničko za sve instrumente osiguranja je utvrditi faktičku potrebu za usklađivanjem instrumenata osiguranja s nastalim izmjenama osnovnog ugovora. Potrebno je adekvatno procijeniti moguće gubitke usljed određene neusklađnosti s troškovima samog provođenja usklađenja kao i opravdanosti pokretanja određenih postupaka naplate, a u odnosu na visinu dugovanja koje može ostati nepokrivano usljed načinjene modifikacije ugovora.

Zaključak

Usljed pandemije uzrokovane virusom COVID-19 pred banke je stavljen težak zadatak u smislu realizacije pomoći građanima i pravnim licima u cilju prevazilaženja nastalih poteškoća u otplati zaduženja. Bilo je potrebno uložiti dodatni napor kako bi se osiguralo adekvatno provođenje odluka nadležnih organa koje se odnose na olakšanje otplate zaduženja. Ujedno, imajući u vidu specifičnost svakog pojedinog slučaja, skoro da i nije bilo moguće zauzeti generalni stav u pogledu provođenja modifikacije kreditnih zaduženja. Svaki slučaj je posmatran pojedinačno kako bi se za svakog klijenta osigurala najadekvatnija mjera za postupanje i partnerski odnos s ciljem prevalizilaženja svih nastalih poteškoća. ■

I kompanije iz BiH mogu postati ozbiljni igrači na svjetskom tržištu

ISO 37001: KAKO USKLAĐENOST MOŽE POMOĆI IZVOZNU PRIVREDU

Certifikacija kompanije po ovom standardu pokazuje da kompanija vrlo ozbiljno i posvećeno shvata svoju ulogu društveno odgovornog poslovanja te na taj način pristupa i pitanjima mita i korupcije, a učešćem na međunarodnom tržištu nudi svoj dobar image i pozitivnu, usklađenu poslovnu kulturu.

Autor:
Mujo Vilašević

Prema podacima Agencije za statistiku, BiH je u 2020. godini izvezla robu u vrijednosti od 10.515.296.000,00 KM, a uvezla je robu u vrijednosti 16.886.250.000,00 KM. Strateški partneri u izvozu ostaju Austrija, Njemačka, Italija, Turska, Švicarska i zemlje regije na čelu sa Srbijom. Sjedinjene Američke Države, iako značajan trgovinski partner BiH, u pravilu su u skupini zemalja u koje BiH manje izvozi, zaključno s podacima za 2020. godinu. Naravno, podaci za 2020. godinu moraju se posmatrati i u kontekstu COVID-19 i svih privrednih poremećaja koji su se dogodili usljed pandemije, kao i predviđanja onih koji će se tek dogoditi, a što je u cjelini uticalo na „raspoloženje“ potrošača, poslovnih partnera i trgovinsku razmjenu.

Niz je razloga zašto bilo koja država može imati veću ili manju vanjskotrgovinsku razmjenu, a kada je u pitanju Bosna i Hercegovina, onda je sasvim sigurno u prvom redu složena politička i pravna struktura, složene procedure i administrativni zahtjevi te, svakako, nedovoljan ili nezadovoljavajući nivo standardizacije usluga, kako u kontekstu Evropske unije tako i međunarodnih standarda.

Usklađenost i privredna aktivnost

Analizirajući ovu temu s aspekta usklađenosti, dolazimo do teze da usklađenost

> *Lice kompanije je ono što danas u velikoj mjeri prodaje kompaniju u globalnim razmjerama. Marketing bilo koje kompanije u svijetu dostupan je na samo jedan klik pa je sasvim realno očekivati da međunarodni poslovni partneri očekuju da znaju s kim rade i da njihov poslovni partner uvažava i primjenjuje međunarodne standarde poslovanja.*

kompanija, privrednih društava s određenim međunarodno priznatim standardima poslovanja može pomoći u njihovom prepoznavanju na međunarodnom tržištu, umrežavanju i zaključivanju poslovnih poduhvata u međunarodnoj robnoj razmjeni, a time i do rasta izvoza.

Zašto?

Zato što je *lice kompanije* neusmnjivo ono što danas u velikoj mjeri prodaje kompaniju u globalnim razmjerama. Marketing bilo koje kompanije u svijetu dostupan je na samo jedan klik pa je sasvim realno očekivati da međunarodni poslovni partneri očekuju da znaju s kim rade i da njihov poslovni partner uvažava i primjenjuje međunarodne standarde poslovanja. Amerikanci imaju poseban koncept *good corporate citizen* koji, ustvari, oslikava težnju društva da kompanije na određeni način „vraćaju društvu" ne samo kroz odgovorno društveno poslovanje nego, prije svega, kroz poslovanje u skladu sa propisima i dobrim tržišnim praksama. Tema na koju su posebno osjetljivi u Sjedinjenim Američkim Državama su mito i korupcija, a u prilog tome govori tzv. *Zakon o koruptivnim radnjama s elementom inozemstva* (*The Foreign Corrupt Practices Act, FCPA*) iz 1977. godine koji se u dobroj mjeri može smatrati jednim od temelja koncepta usklađenosti (*compliance*), a s vremenom se proširio na ostatak svijeta i postao primjer dobre (i često mandatorne) poslovne prakse. Ukratko, FCPA sadrži odredbe kojim se zabranjuju mito i korupcija stranim državnim službenicima u svrhu uspostavljanja ili zadržavanja poslovnog odnosa, odnosno radnje koje uključuju plaćanje, obećanje plaćanja, odobrenje plaćanja u novcu ili bilo kojoj drugoj vrijednosti

bilo kojoj osobi sa svijesti da će takva plaćanja ili vrijednosti uticati na strane državne službenike pri olakšanju uspostavljanja ili zadržavanja poslovnog odnosa ili uticati na drugi način na takve službenike u cilju osiguranja neprimjerene prednosti na tržištu. Amandmanima iz 1998. godine odredbe o mitu i korupciji FCPA primjenjuju se i na strane kompanije i fizička lica koji direktno ili putem agenta djeluju s ciljem opisanih koruptivnih radnji na teritoriji SAD-a. Dakle, cilj FCPA je uspostavljanje antikorupcijskih mjera i mjera protiv mita državnih službenika u dva pravca: i za državljane SAD-a koji to pokušavaju u inostranstvu i za strane državljane koji to pokušavaju u SAD-u (ili putem kompanija koje pripadaju SAD-u).

Imajući ovo na umu, zaključak se izvodi sam po sebi – „strane" kompanije, među njima i kompanije bosansko-hercegovačkog tržišta, mogu ostvariti značajnu komparativnu prednost u poslovanju na tržištu SAD-a ako uspostave, implementiraju i dokažu postojanje i poštivanje sistema protiv mita i korupcije. Posmatrano u kontekstu Evrope, jednak je zaključak kada govorimo i o standardima koje vrednuje globalno poznati britanski *Anti-Bribery Act*.

Vrednovanje takvog sistema je u prvom redu kroz međunarodno priznate standarde kao što je ISO 37001.

ISO 37001:2016

ISO 37001:2016 je standard objavljen od strane Međunarodne organizacije za standardizaciju (ISO) u oktobru 2016. godine i odnosi se na sistem upravljanja za sprečavanje podmićivanja. U Bosni i Hercegovini je preveden kao **BAS 37001:2019** i osnovne informacije o standardu mogu se dobiti putem Instituta za standardizaciju Bosne i Hercegovine (www.isbih.ba.gov). Ovaj standard treba pomoći organizacijama da uspostave, implementiraju, održavaju i poboljšavaju sistem upravljanja za sprečavanje podmićivanja (*anti-bribery compliance management*). Standard uključuje niz mjera i kontrola koje predstavljaju svjetske prakse protiv podmićivanja, a koje bi certificirane organizacije trebale uspostaviti. Standard mogu primjenjivati velika privredna društva, mala i srednja društva (SME), javni sektor i nevladine organizacije.

ISO 37001 pokriva mito u organizaciji ili od strane njenih zaposlenika ili vanjskih saradnika koji rade za račun organizacije, kao i mito od strane organizacije ili njenih zaposlenika ili vanjskih saradnika u vezi s aktivnostima organizacije, a prema trećim stranama i subjektima javne vlasti.

> *„ISO 37001 pokriva mito u organizaciji ili od strane njenih zaposlenika ili vanjskih saradnika koji rade za račun organizacije, kao i mito od strane organizacije ili njenih zaposlenika ili vanjskih saradnika u vezi s aktivnostima organizacije, a prema trećim stranama i subjektima javne vlasti."*

ISO 37001 definiše mito generički te pretpostavlja ovisnost definicije od nacionalnog zakonodavstva, ali daje vrlo značajan okvir za organizacije kako bi se uspostavio ovaj sistem upravljanja. Taj okvir se može podijeliti u sljedeće cijeline:

1) kultura,
2) upravljanje i nadzor,
3) procjena rizika,
4) politike i procedure,
5) trening, edukacije i komunikacije,
6) prijavljivanje (*whistleblowing*),
7) istrage,
8) monitoring i revizija,
9) procjena rizika treće strane i
10) kontinuirano unaprijeđenje.

Iako pojedini autori naglašavaju da ovaj standard nije uspostavio ništa naročito novo u odnosu na standard ISO 19600:2014 (sistemi upravljanja usklađenosti - *compliance*), ipak je važno naglasiti da je svojim sadržajem ISO 37001 otišao korak dalje i u odnosu na pomenuti američki FCPA, ali i britanski *Anti-Bribery Act* i OECD Smjernice o dobrom upravljanju, etici i usklađenosti (https://www.oecd.org/daf/anti-bribery/44884389.pdf). Ipak se radi o međunarodnom standardu protiv mita koji je samo u draftu podržalo 50 zemalja članica ISO, a koji od njegove objave može implementirati i na taj način harmonizirati borbu protiv mita u više od 160 zemalja svijeta. Kako to navodi Crescenzi M. u svom radu *ISO 37001 Certification: Understanding and navigating the process* (objavljeno u*: Compliance &*

Ethics Professionals, SCCE, USA, 2018.), ISO 37001 uspostavlja zajednički, globalni pristup upravljanju zabranom podmićivanja i rizika korupcije, neovisno gdje se kompanija nalazi, posluje ili gdje je njeno sjedište. U tome je možda i najveća vrijednost ovog standarda.

Certifikacija kompanije po ovom standardu pokazuje najmanje sljedeće: kompanija vrlo ozbiljno i posvećeno shvata svoju ulogu društveno odgovornog poslovanja te na taj način pristupa i pitanjima mita i korupcije; kompanija učestvuje u globalnim tokovima i trendovima te razumijeva potrebu stalnog unaprijeđivanja svog poslovanja; kompanija izražava težnju ka učešću na međunarodnom tržištu nudeći svoj dobar *image* i pozitivnu, usklađenu poslovnu kulturu. Osim učešća u vanjskotrgovinskoj razmjeni, certificiranim kompanijama otvaraju se i mnogo veće mogućnosti međunarodnog sufinansiranja, grantova i fondova pomoći razvoja privrede koje nude međunarodne finansijske organizacije i Evropska unija, a koje među svojim prioritetima postavljaju upravo nultu toleranciju na mito i korupciju.

> *Osim učešća u vanjskotrgovinskoj razmjeni, certificiranim kompanijama otvaraju se i mnogo veće mogućnosti međunarodnog sufinansiranja, grantova i fondova pomoći razvoja privrede koje nude međunarodne finansijske organizacije i Evropska unija, a koje među svojim prioritetima postavljaju upravo nultu toleranciju na mito i korupciju.*

Nisu li nabrojani razlozi dovoljni za certificiranje kompanija u BiH sa ISO 37001 (prije svega kompanije sa više od 50 zaposlenih) kako bi i na ovaj način pokušale ući u trku s igračima na svjetskom tržištu?

Certifikacija

Iako ISO izdaje standarde, ISO ne vrši certifikaciju organizacije. Certifikaciju vrše akreditovane organizacije za ISO standardizaciju. Certifikacija ISO 37001 može biti individualna i za organizaciju. Procijenjeni troškovi certifikacije su prosječni i u Bosni i Hercegovini. Trenutno u BiH ne postoje pouzdani podaci o broju privrednih društava koji su se odlučili za ovaj vid certificiranja. U svijetu su među prvima ISO 37001 implementirali *Microsoft* i *Walmart* (SAD), *Robert Bosch* (UAE), *Terna Group* (Italija), ali i značajan broj javnih institucija u SAD-u i svijetu, od Kine, Azerbejdžana, Malezije i Indije do zemalja Evropske unije.

Na kraju, može li usklađenost pomoći izvozno orijentiranu privredu u Bosni i Hercegovini? Nesumnjivo da može. ISO 37001 nije magični alat i ne znači da će ovom certifikacijom kompanija automatski postati relevantan međunarodni tržišni igrač, ali je ovaj standard jedan od (vrlo pouzdanih) alata kako se približiti tome. Osim toga, ISO 37001 otvara vrata i uopće *compliance* sistemima upravljanja koji bi neminovno morali postati dio agende kompanija koje žele poslovati i izvan okvira Bosne i Hercegovine. ■

Culture Eats Strategy For Breakfast

KORPORATIVNA KULTURA I ETIČKI KODEKS KAO MJERE PREVENCIJE OD INTERNIH PREVARA

Visoke standarde kulture i integriteta nije dovoljno samo imati propisane ili istaknute kao postere na zidovima hodnika organizacije, oni se moraju živjeti. Oni se moraju primjenjivati od strane svakog pojedinca u organizaciji i kada niko ne gleda.

Autor:
Nermin Ibradžić

Korporativna kultura ili koliko smo spremni da slušamo

Afera velikog proizvođača automobila s lažnim rezultatima mjerenja ispušnih plinova, pad *Lehman Brothers*, propast koncepta *BlackBerry* uređaja, skori bankrot *Delta Airlines* i *IBM-a*, pad *Motorole*[1]...

Šta je zajedničko za sve ove slučajeve?

Zajednička im je neadekvatna korporativna kultura. Jedni nisu čuli šta zaposlenici i saradnici imaju da kažu, drugi nisu slušali šta klijenti govore, treći nisu poslušali regulatora.

Riječ je o fenomenu poznatom pod nazivom ***Culture of blindness***.

Šta je to korporativna kultura i da li je ima svaka organizacija?

Iako ne postoji univerzalna definicija, korporativna kultura je dominantan način ponašanja, rada i komuniciranja zaposlenika u jednoj organizaciji. Dominantan iz razloga što se radi o ponašanju koje potiče i smatra poželjnim

[1] *Izvor: https://www.livemint.com/Sundayapp/ygKc14yXwom3yLOkkDBgIL/When-corporate-culture-goes-toxic-from-Lehman-to-Volkswagen.html*

upravo ta organizacija u kojoj se takvo ponašanje dešava.

Ona može biti formalizovana kroz standard i ciljeve organizacije ili neformalna u vidu ponašanja i načina rada koji organizacija prešutno ili otvoreno podržava.

Dakle, svaka organizacija ima određenu korporativnu kulturu pa čak i ako ona nije normirana i formalizovana kao dokument. Ono što je bitno za našu temu jeste da damo odgovore na pitanja da li je ta korporativna kultura adekvatna ili ne, da li ona podržava osnovne i proklamovane ciljeve organizacije te da li je prihvaćena u društvu u kojem organizacija djeluje.

Adekvatna korporativna kultura će, u pravilu, promicati dugoročne i pozitivne vrijednosti: etično postupanje, integritet, pomoć drugima, ekološke standarde, zaštitu zaposlenika te zadovoljstvo klijenata ispred bezobrazno visoke dobiti. Upravo te pozitivne, dugoročne i društveno korisne vrijednosti su jedan od osnova prevencije od neželjenih i prevarnih postupanja. Ukoliko su standardi poželjnog ponašanja, kao i posljedice nepoželjnog ponašanja, kodificirani i formalizirani, tada govorimo o etičkom kodeksu organizacije. Etički kodeks je alat i bitan dio korporativne kulture kao šireg pojma.

Neadekvatna korporativna kultura kao generator prevarnog ponašanja

Interne prevare su u teoriji još od 50-ih godina prošlog stoljeća definisane s tri osnovna elementa: pritisak (motiv za prevaru), prilika za prevaru i racionalizacija (opravdanje prevarnog postupanja). Navedeni elementi čine tzv. ***Trokut prevara***.

> *Adekvatna korporativna kultura će, u pravilu, promicati dugoročne i pozitivne vrijednosti: etično postupanje, integritet, pomoć drugima, ekološke standarde, zaštitu zaposlenika te zadovoljstvo klijenata ispred bezobrazno visoke dobiti. Upravo te pozitivne, dugoročne i društveno korisne vrijednosti su jedan od osnova prevencije od neželjenih i prevarnih postupanja.*

> *Adekvatan sistem internih kontrola će prilično umanjiti mogućnost prevare.*

U novijoj teoriji se pominje i četvrti element, odnosno postojećim elementima se dodaje i element sposobnosti ili mogućnosti/prilike da neko lice učini prevaru.

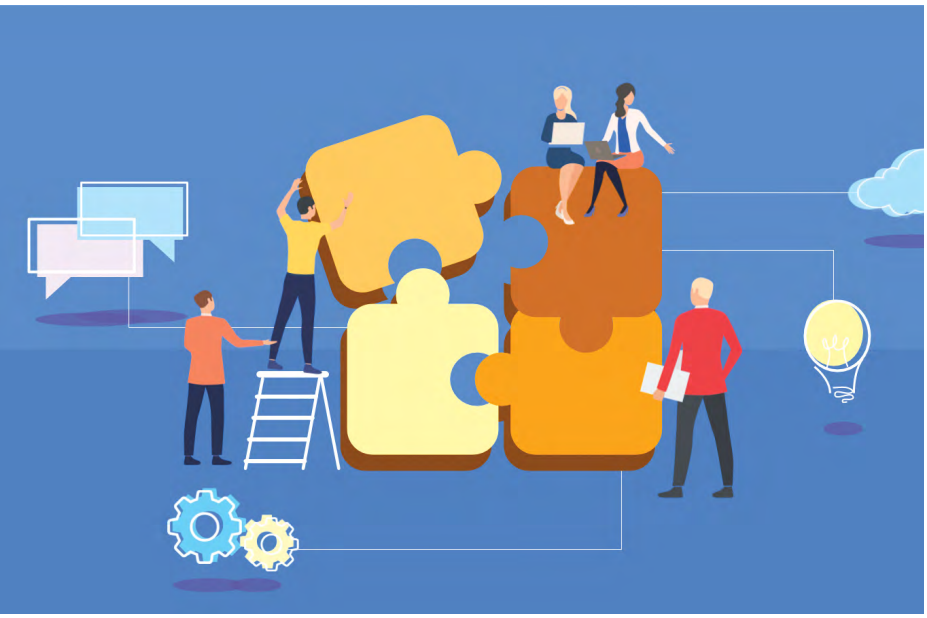
Kada generalno govorimo o prevenciji prevara, prvo na što pomislimo jeste adekvatan sistem internih kontrola kojim će se spriječiti da se svi elementi prevare ostvare i uvežu. Nesporno je da interne kontrole imaju značajnu ulogu u prevenciji neželjenog ponašanja. Adekvatan sistem internih kontrola će prilično umanjiti mogućnost prevare. Ipak, ukoliko se organizacija u sprečavanju prevara ograniči samo i isključivo na

[2] *Izvor: https://www.vanityfair.com/news/2017/05/wells-fargo-corporate-culture-fraud*

formalizovane interne kontrole, a zanemari ostale alate prevencije, izgledno je da će uspjeh biti ograničen ili će u cjelosti izostati.

Jedan od primjera je slučaj **Wels Fargo[2],** koji je preko 5 godina koristeći se prevarnim praksama koje su prihvaćene kao korporativna kultura organizacije, bez saglasnosti klijenata otvorio na ime klijenata preko 1,5 miliona računa i izdao preko 500.000 kreditnih kartica. Radi se o konzervativnoj procjeni, a prema nekim procjenama ekonomskih stručnjaka na ovaj način je bez saglasnosti klijenta otvoreno preko 3,5 miliona računa. Kako je provedena ova prevara koja je postala dio kulture same organizacije WelsFargo i koja je snažno podržana od rukovodstva? Ciljevi za zaposlenike u prodaji bili su postavljeni na takav način da je svaki zaposlenik morao dnevno prodati po *cross sell* principu minimalno 8 proizvoda klijentu. Broj osam je bio određen od strane visokog rukovodstva zato što se 8 na engleskom jeziku rimuje sa sjajno, odnosno odlično (*eight rimes with great/ Gr8*).

Pod takvim pritiskom zaposlenici su otvarali račune klijentima bez saglasnosti klijenata tako da su klijenti imali i do osam različitih računa za koje nisu ni znali. Da bi se sa ovih osam računa naplaćivale naknade, sredstva sa *glavnog* računa (za koji je klijent znao) su bez saglasnosti klijenta raspoređivali na ostale račune. To nije bilo dovoljno pa su u sistemu kod podataka klijenta mijenjali e-*mail* adrese i adrese stanovanja kako klijenti ne bi dobili na adresu izvode u kojima bi vidjeli da nešto nije uredu. Posebno su bile ranjive grupe starijih klijenata i grupe imigranata u SAD (Hispanjolci, Kinezi i sl.). Tako su zabilježeni slučajevi gdje su klijentima starosti i preko 80 godina, koji se nisu znali koristiti računarom, prodavane elektronske usluge, u sistemu su se mijenjali matični brojevi klijenata kako se provjerom ne bi moglo identificirati da se radi o jednom te istom klijentu koji koristi više proizvoda nego što mu treba, mijenjani su podaci o brojevima telefona klijenata kako se nakon upućivanja žalbe klijent ne bi mogao kontaktirati. U jednom slučaju je starijoj klijentici bez njenog pristanka ili zahtjeva izdana kreditna kartica uz obrazloženje da se radi o kartici koja sadrži potvrdu nove adrese klijentice. Što je zaposlenik bio maštovitiji u prevari i prikrivanju tragova, više je prodavao, što je više prodavao, više se uspinjao na hijerarhijskoj ljestvici. A kada se jednom popneš dovoljno visoko, nastaviš podržavati sistem koji te tamo doveo. Zaposlenici koji su shvatili sistem rada i koji se nisu osjećali ugodno ili nisu željeli da rade na takav način, brzo su napuštali organizaciju svojom voljom ili prinudno zbog neostvarenih "rezultata". Zaposlenici koji bi interno prijavili nepoštenu i prevarnu praksu brzo bi dobili nove i više ciljeve te bi dobijali otkaz "zbog neispunjenja ciljeva". Sistem je funkcionisao sve do onog momenta kada su žalbe klijenata i zaposlenika postale toliko brojne da se više nisu mogle sakriti ili ignorirati. Kompletna situacija je dospjela u medije, a ostalo je historija. WelsFargo je na ime odšteta i kazni do kraja 2018. godine platio 2,7 milijardi USD. Navedeni iznos je bez iznosa ostalih sudskih i drugih troškova koji su milionski. Pored



toga, preko 1000 zaposlenika ostalo je bez posla, a reputacija organizacije je trajno narušena. I danas, nakon 6 godina od slučaja, organizacija je pod budnim okom regulatora.

Ono što je vezano direktno za ovu temu jeste da je WelsFargo imao propisane standarde korporativne kulture i Kodeks ponašanja. I jedno i drugo, barem formalno, nisu dopuštali nedozvoljene i nepoštene prakse radi ostvarenja rezultata. Međutim, visoko rukovodstvo nije mislilo tako. Zaposlenici koji su na nepošten način stvarali rezultat slavljeni su kao heroji, a oni koji bi se pobunili brzo bi ostajali bez posla. Interne kontrole su postojale i otkrile su neke od ovih slučajeva, ali su takvi slučajevi ocijenjeni kao "sporadični", a ne kao pravilo u organizaciji te nisu ozbiljnije ispitani.

Na ovom primjeru najbolje vidimo koliko je bitno da su korporativna kultura i etički kodeks adekvatni, ali i koliko je bitno da se provode u praksi. Da su u naprijed navedenom primjeru poželjni standardi korporativne kulture adekvatno implementirani i vrednovani, da je nepoželjno ponašanje na vrijeme sankcionisano, da je etički kodeks implementiran onako kako glasi, da su standardi etičnog postupanja i očuvanja integriteta te interesi i zaštita klijenata stavljeni ispred interesa pojedinca i visokih bonusa rukovodilaca, slučaj WelsFargo ne bi se ni desio. Organizacija bi uštedjela milijarde USD, a reputacija bi rasla umjesto njenog strmoglavog pada. Iz navedenog primjera možemo zaključiti da su adekvatna korporativna kultura i etički kodeks možda i bolja prevencija prevarnih postupanja nego solidan sistem internih

> *Ako organizacija kao cjelina ima visok nivo pozitivne korporativne kulture, ako su pravilni principi ugrađeni u sve procese, u organizaciju kao grupu i u svakog pojedinca koji pripada grupi, mala je šansa da će pojedinac, i pored poznavanja nedostataka internih kontrola, ostvariti svoj naum prevare.*

kontrola. Sistem internih kontrola može imati nedostatke i „zaposlenici loših namjera" te nedostatke mogu iskoristiti na štetu organizacije i klijenata, a

na svoju ličnu dobrobit. Međutim, ako organizacija kao cjelina ima visok nivo pozitivne korporativne kulture, ako su pravilni principi ugrađeni u sve procese, u organizaciju kao grupu i u svakog pojedinca koji pripada grupi, mala je šansa da će pojedinac, i pored poznavanja nedostataka internih kontrola, ostvariti svoj naum prevare. Jednostavno, takav pojedinac neće za takvo postupanje imati ni podršku ni razumijevanje kolega i rukovodioca. Valja naglasiti da visoke standarde kulture i integriteta nije dovoljno samo imati propisane ili istaknute kao postere na zidovima hodnika organizacije, oni se moraju živjeti. Oni se moraju primjenjivati od strane svakog pojedinca u organizaciji i kada niko ne gleda. U tom smislu možda bi se svaki *compliance* službenik zadužen za etiku i integritet trebao zapitati: Da li sam zaista pristupio svakoj prijavi s dužnom pažnjom? Da li mi sistem "zviždača" zaista funkcionira, da li "zviždače" štitim na odgovarajući način? Da li sam održao dovoljno edukacija i dao dovoljno primjera? Da li je svakom zaposleniku pojedinačno jasno šta treba da radi ako se sretne sa neetičnim postupcima? Ako je samo jedan odgovor na navedena pitanja NE, možda je sad pravo vrijeme da unaprijedite svoj sistem praćenja korporativne kulture i etike.

Tips and tricks

U praksi postoje razne metode i mjerila koja vam mogu pomoći da identificirate da li je korporativna kultura na željenom nivou i da ih dodatno ispitate:

- neprijateljsko natjecanje između zaposlenika,
- ogovaranja kao "normalan" način ponašanja zaposlenika,
- česta bolovanja većeg broja zaposlenika,
- česta fluktuacija zaposlenika izvan organizacije (korisne informacije može dati izlazni razgovor),
- velik broj anonimnih prijava na neželjena postupanja,
- potpuni nedostatak empatije,
- brojevi i dobit kao jedini i isključivi cilj,
- loše ocjene zaposlenika za rukovodioce,
- mikromenadžiranje i sl.[3]

Na kraju, umjesto zaključka, spomenut ćemo korisnu misao velikana i jednog od utemeljitelja pojma modernog upravljanja kompanijama. U pitanju je **Peter Ferdinand Drucker** (19.11.1909-11.11.2005.). Radi se o konsultantu, edukatoru i autoru mnogih djela i članaka, čovjeku koji je izrekao tezu da zaposlenike ne treba gledati kao *liabilitie* (obavezu) nego kao *asset*, a znanje zaposlenika kao ključni sastojak moderne ekonomije.

Njegova izreka "Kultura (korporativna, nap.a.) može pojesti strategiju za doručak" (eng. *Culture Eats Strategy For Breakfast)*[4] trebala bi se uvažiti u svakom slučaju kada se strateški ciljevi, bonusi i dobit stavljaju daleko ispred korporativne kulture. ■

[3] *Izvor: https://builtin.com/company-culture/bad-company-culture*
[4] *Izvor: https://inside.6q.io/10-warning-signs-negative-corporate-culture/*

Evropsko zakonodavstvo

DIREKTIVA 2019/1937 O ZAŠTITI "ZVIŽDAČA" U EVROPSKOJ UNIJI

Bosanskohercegovačko društvo suočava se s prevarama, korupcijom, krivičnim djelima u privrednom sektoru, nedovoljnom zaštitom javnih sredstava te s netransparentnom potrošnjom budžetskih sredstava. Prijavljivanje ovakvih negativnih pojava od izuzetne je važnosti za njihovu prevenciju.

Autor:
Mujo Vilašević

Dana 26.11.2019. godine u *Službenom glasniku* Evropske unije br. L305/46 objavljena je ***Direktiva 2019/1937*** Evropskog Parlamenta i Vijeća od 23. oktobra 2019. godine o zaštiti osoba koje prijavljuju povredu prava Unije (dalje u tekstu: Direktiva). Radi se o prvom unijskom dokumentu koji nastoji harmonizirati prava država članica u pogledu zaštite "zviždača". Evropski zakonodavac opredijelio se za harmonizirajući instrument, direktivu, imajući u vidu da bi neposredno primjenjujući instrument (uredba) ipak naišao na otpor u državama članicama, imajući u vidu različitosti pravnih sistema i razumijevanja "kulture prijavljivanja povrede prava".

Razlozi za usvajanje

Prijavljivanje povrede prava, propisa ili internog pravila od izuzetne je važnosti za prevenciju prevara, korupcije, krivičnih djela u privrednom sektoru, ali i zaštite javnih sredstava te transparentnosti budžetske potrošnje. Ključna ideja normiranja prijavljivanja povrede prava ("zviždača") podrazumijeva odsustvo straha zbog prijave, jasne, precizne i implementirane politike zaštite "zviždača" od osvete, bilo da se radi o privatnom ili javnom sektoru. Zaštita prava radnika, radno-pravna pitanja i povezani procesi (koji su najčešće pogrešno sinonim i percepcija

za zaštitu "zviždača") mogu, ali ne moraju biti, dio ovog koncepta i politika zaštite "zviždača". Jasne, precizne i implementirane politike zaštite od "zlonamjernih i neosnovanih lažnih (i više nego često, ličnih) informacija" drugi su dio ovog koncepta bez kojeg uopće nije ozbiljno razgovarati o implementaciji "zaštite zviždača".

> *"Zdrav ekonomski prostor za Uniju u prvom redu, bez sumnje, znači prostor u kome su javna sredstva, prikupljanje i potrošnja transparentni, a uvjeti rada, zaštite sigurnosti i zaštite potrošača na izuzetno visokim standardima."*

Iako često zanemarena činjenica, Evropska unija je vrlo vjerovatno najveći i najproduktivniji zakonodavac u svijetu. Jedinstveno evropsko tržište postoji i ovisi od odgovarajuće implementacije unijskog prava, a naročito u segmentima koji su ključni za "zdrav ekonomski prostor" kao što su javne nabavke, zaštita od mita i korupcije, sigurnost proizvoda i usluga i slično. Zdrav ekonomski prostor za Uniju u prvom redu, bez sumnje, znači prostor u kome su javna sredstva, prikupljanje i potrošnja transparentni, a uvjeti rada, zaštite sigurnosti i zaštite potrošača na izuzetno visokim standardima (ovdje možemo čitati i jedan od razloga opstojnosti Unije).

Međutim, unijski *decision-makeri* došli su do zaključka da je prijavljivanje kršenja prava Unije na izrazito niskom nivou iako su slučajevi poput *Panama Papers*, *Wikileaks* i slično pokazali da stvarnost ipak ne odgovara nivou prijavljenih slučajeva

kršenja prava. Prema istraživanju *Eurobarometra* iz 2017. godine, 81% Evropljana koji su iskusili ili bili svjedoci korupcije nisu je prijavili. Prema istim istraživanjima, jedno od troje Evropljana (29%) mišljenja su da ljudi ne prijavljuju korupciju jer odgovarajuća zaštita ne postoji.

Svakako se već u prvoj tački preambule Direktive daje i odgovor zašto baš ovaj unijski akt, a nastavno na prethodno pomenutu težnju zaštite unijskog prava i ekonomskog prostora: *"... potencijalni zviždači često se zbog straha od osvete boje prijaviti ono što ih zabrinjava ili na što sumnjaju. U tom se kontekstu sve više prepoznaje važnost pružanja uravnotežene i učinkovite zaštite zviždača kako na nivou Unije tako i na međunarodnom nivou"*.

Na šta i koga se odnosi Direktiva?

Direktivom se utvrđuju zajednički minimalni standardi za zaštitu osoba koje prijavljuju povrede prava Unije u sljedećim oblastima (čl. 2.):

- javne nabavke,
- finansijske usluge, proizvodi i tržišta te sprečavanje pranja novca i finansiranje terorizma,
- sigurnost proizvoda,
- sigurnost prometa,
- zaštita okoline,
- zaštita od zračenja i nuklearna sigurnost,
- sigurnost hrane i hrane za životinje, zdravlje i dobrobit životinja,
- javno zdravlje,
- zaštita potrošača i
- zaštita privatnosti i ličnih podataka te sigurnost mrežnih i informacijskih sistema.

Dodatno, Direktiva se odnosi i na povrede prava koje utiču na finansijske interese Unije, povrede koje se odnose na unutrašnje tržište uključujući povrede pravila o tržišnoj konkurenciji kao i povrede koje se odnose na kršenje pravila o porezu na dobit ili aranžmani čija je svrha ostvariti poresku prednost u suprotnosti s ciljem i svrhom poreskog zakonodavstva.

Navedeno nisu konačne liste, države članice mogu proširiti obim zaštite. Također, države članice mogu propisati i da se pravila uspostavljena ovom Direktivom odnose i na privredna društva s manje od 50 zaposlenih radnika.

Ad personam, Direktiva se primjenjuje na prijavitelje zaposlene u privatnom ili javnom sektoru i stekli su informacije o povredama u javnom okruženju, a što najmanje uključuje sljedeće osobe (čl. 4., ko uživa zaštitu):

- radnici,
- samozaposleni radnici (*freelanceri*),
- dioničari i članovi organa upravljanja privrednih društava, uključujući neizvršne članove, volontere, plaćene ili neplaćene pripravnike,
- izvršioci ugovora ili podugovora o djelu ili ugovora o nalogu,
- osobe koje su prestale s angažanom u bilo kojem naprijed navedenom svojstvu, a povreda prava se desila u toku trajanja angažmana,
- osobe koje tek trebaju zasnovati neki angažman ili posao, a informacije o povredi prava stekli su prilikom postupka zapošljavanja ili pregovora prije sklapanja ugovora,

- osobe pomagači prijavitelja, treće osobe povezane s prijaviteljem, a koje bi mogle pretrpjeti osvetu zbog prijave (kolege ili srodnici) te pravna lica u vlasništvu prijavitelja, lica za koje upravitelj radi ili su na drugi način povezani u radnom okruženju s prijaviteljem.

Uslovi zaštite prijavitelja - "zviždača" su kumulativni:

- da su imali opravdan razlog vjerovati da su prijavljene informacije o povredama istinite u trenutku prijave i da su te informacije obuhvaćene područjem primjene Direktive te
- da su podnijeli prijavu unutrašnjim ili vanjskim kanalima u skladu s Direktivom ili su javno otkrili informacije (čl. 7, 10. i 15. Direktive).

> *"Direktiva daje mogućnost državama članicama da odluče svojim propisima o pravilima vezanim za anonimne prijave, ali i nalaže da se prijaviteljima, nakon što je otkriven njihov identitet, osigura odgovarajući stepen zaštite."*

Direktiva daje mogućnost državama članicama da odluče svojim propisima o pravilima vezanim za anonimne prijave, ali i nalaže da se prijaviteljima, nakon što je otkriven njihov identitet, osigura odgovarajući stepen zaštite.

Direktiva nadalje detaljno propisuje proces unutrašnje i vanjske prijave te uslove javnog otkrivanja informacija kao i zaštitu povjerljivosti i identiteta prijavitelja te zaštitu ličnih podataka koji se obrađuju kroz proces obrade prijave.

Zabrana osvete (*non-retaliation policy*), mjere zaštite, sankcije „lažnim zviždačima"

Možda i ključne odredbe, koje bi trebale ohrabriti buduće prijavitelje, su odredbe Direktive o zabrani osvete "zviždačima". Da bi bilo koji sistem prijavljivanja, u privatnom ili javnom sektoru, mogao i pokušati da bude efikasan, *non-retaliation policy* mora biti jasna, transparentna, primjenjiva i svima poznata.

Članom 19. Direktive propisuje se da će države članice poduzeti potrebne mjere zabrane svih oblika osvete nad "zviždačima", uključujući prijetnje i pokušaje osvetom, između ostalih posebno u obliku (neiscrpna lista):

- privremenog udaljenja, otpuštanja, razrješenja ili sličnih mjera,
- nazadovanja ili uskraćivanja mogućnosti za napredovanje,
- prijenosa dužnosti, promjene radnog mjesta, smanjenja plate, promjene radnog vremena,
- uskraćivanja mogućnosti za osposobljavanje,
- negativne ocjene rada ili preporuke za zapošljavanje,
- nametanja ili određivanja kazne, opomene ili druge sankcije uključujući finansijsku sankciju,
- prisile, zastrašivanja, uznemiravanja ili izoliranja,
- diskriminacije, stavljanja u nepovoljni položaj ili nepravednog tretmana,
- nepretvaranja ugovora o radu na određeno vrijeme u ugovor o radu na neodređeno vrijeme ako je radnik imao legitimno očekivanje da će mu se ponuditi stalno zaposlenje,
- neproduženje ugovora o radu na određeno vrijeme ili njegov prijevremeni raskid,
- šteta, uključujući štetu na ugled osobe, posebno na društvenim mrežama ili finansijski gubitak, uključujući gubitak poslovanja i gubitak prihoda,
- stavljanje na crnu listu na osnovu neformalnog ili formalnog sektorskog sporazuma ili sporazuma koji se primjenjuje u cijeloj industriji, što u budućnosti može značiti da oso-

ba neće moći naći posao u tom sektoru ili industriji,

- prijevremenog raskida ugovora o nabavci robe ili usluge ili njegovog poništenja,
- poništenje licence ili dozvole te
- psihijatrijskih liječenja ili upućivanja doktoru.

Nadalje, Direktiva propisuje i mjere podrške za zaštitu "zviždača" koje se naročito odnose na: sveobuhvatne i nezavisne informacije i savjete lako dostupne i besplatne u javnosti, a odnose se na dostupne postupke i pravna sredstva za zaštitu od osvete i prava prijavljene osobe; efikasnu pomoć nadležnih tijela pred bilo kojim relevantnim tijelom koje učestvuje u zaštiti od osvete, uključujući i potvrdu činjenice da „zviždač" ima pravo zaštite u skladu s Direktivom i pravnu pomoć u krivičnim i prekograničnim građanskim postupcima te pravnu pomoć u daljim postupcima i pravno savjetovanje ili neku drugu pravnu pomoć. Države članice mogu, temeljem Direktive, u okviru sudskog postupka predvidjeti i finansijsku pomoć i podršku za „zviždače", uključujući i psihološku podršku.

Mjere za zaštitu od osvete (čl. 21.) uključuju posebno

> *„Zviždači" su zaštićeni i od odgovornosti u postupcima klevete, povrede autorskog prava, poslovne tajne, pravila o zaštiti podataka ili zahtjeva za naknadu na osnovu privatnog, javnog ili kolektivnog radnog prava, a koji su pokrenuti zbog prijava ili javnih razotkrivanja.*

> *„Zviždači" ne snose odgovornost u pogledu sticanja prijavljenjenih ili javno razotkrivenih informacija ili pristupa njima pod uslovom da takvo sticanje ili pristup nisu sami po sebi krivično djelo, a svaka druga potencijalna odgovornost „zviždača" utvrđuje se odredbama nacionalnog prava ili prava Unije.*

zaštitu „zviždača" koji javno otkriju informacije, u smislu Direktive, da ni na koji način ne snose odgovornost u vezi takve prijave ili javnog razotkrivanja pod uslovom da su imale opravdan razlog vjerovati da su prijava ili javno razotkrivanje bili nužni radi otkrivanja povrede prava. „Zviždači" ne snose odgovornost u pogledu sticanja prijavljenjenih ili javno razotkrivenih informacija ili pristupa njima pod uslovom da takvo sticanje ili pristup nisu sami po sebi krivično djelo, a svaka druga potencijalna odgovornost „zviždača" utvrđuje se odredbama nacionalnog prava ili prava Unije.

Dodatna mjera je i „obrnuti teret dokazivanja" pa je tako u postupcima pred sudom ili drugim tijelom zbog štete koju je pretrpio „zviždač", koji dokaže da je prijavitelj ili da je javno otkrio informaciju i zbog toga pretrpio štetu, teret dokazivanja da šteta nije nanesena, tj. „primjerenosti radnje i utemeljenosti na va-

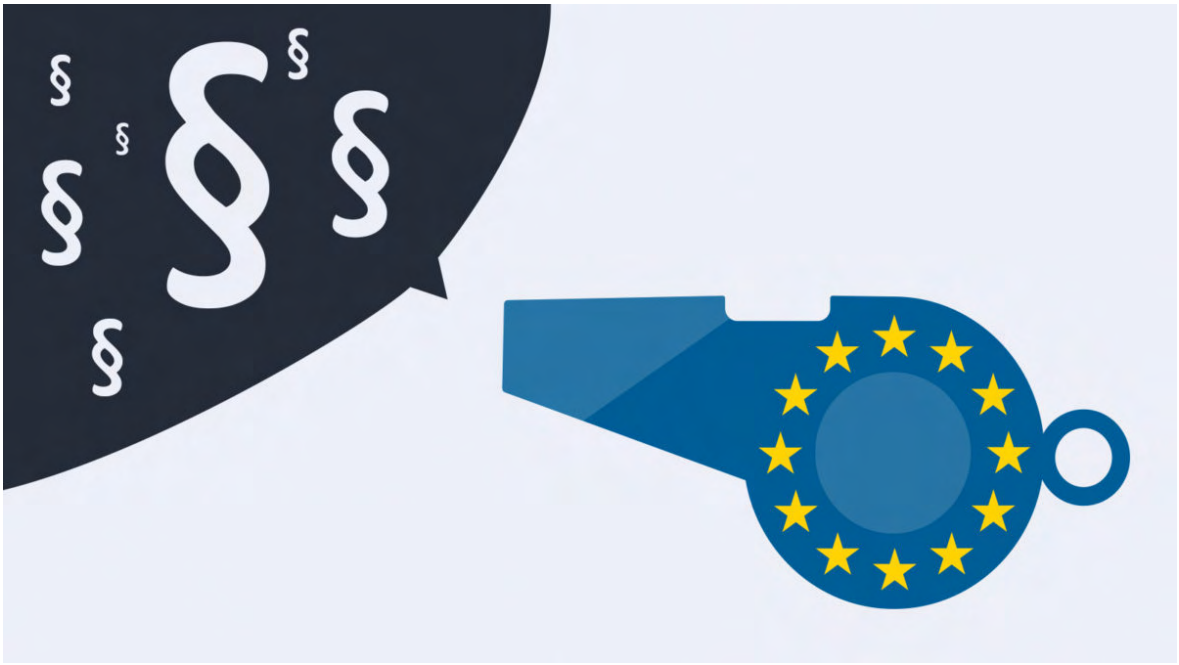
ljano opravdanim razlozima“ na tuženoj strani, s obzirom na to da se, shodno odredbama Direktive, šteta nanesena „zviždaču“ pretpostavlja. „Zviždači“ su zaštićeni i od odgovornosti u postupcima klevete, povrede autorskog prava, poslovne tajne, pravila o zaštiti podataka ili zahtjeva za naknadu na osnovu privatnog, javnog ili kolektivnog radnog prava, a koji su pokrenuti zbog prijava ili javnih razotkrivanja na osnovu Direktive te imaju pravo tražiti odbacivanje takvih predmeta, ali pod uslovom da su imali opravdan razlog vjerovati da su prijava ili javno razotkrivanje nužni radi otkrivanja povrede prava u skladu s Direktivom.

Članom 22. Direktive propisuje se i zaštita prijavljenih osoba na način da države članice osiguravaju da prijavljene osobe imaju potpuno pravo na efikasan pravni lijek i pravično suđenje te na pretpostavku nevinosti, pravo na odbranu, uključujući pravo na saslušanje i pravo na pristup predmetu. Nacionalna tijela dužna su svojim propisima osigurati zaštitu identiteta prijavljenih osoba tokom istrage pokrenute prijavom ili javnim razotkrivanjem, a prijavljena osoba mora uživati zaštitu identiteta kakvu uživa i „zviždač“. Istovremeno, Direktiva u članu 23. propisuje i obavezu država članica da definišu učinkovite, proporcionalne i odvraćajuće sankcije za „zviždače“ za koje je utvrđeno da su svjesno prijavili ili javno otkrili lažne informacije, kao i da propisima definišu mjere za naknadu štete nastale iz takvih prijava ili javnih otkrivanja u skladu s nacionalnim zakonodavstvom.

Države članice obavezne su propisati i učinkovite, proporcionalne i odvraćajuće sankcije za fizičke ili pravne osobe koje sprečavaju ili pokušaju spriječiti podnošenje prijave, osvećuju se protiv „zviždača“, pokreću zlonamjerne postupke protiv njih ili krše dužnost čuvanja povjerljivosti identiteta „zviždača“.

Usklađivanje s Direktivom

Direktiva je stupila na snagu dvadesetog dana od objave u *Službenom glasniku* Evropske unije, a države članice dužne su uskladiti se sa Direktivom do 17. decembra 2021. Izuzetak je za privredna društva koja imaju između 50 i 249 zaposlenih radnika, a za koje je obaveza usklađivanja odgođena do decembra 2023.



Države članice dužne su voditi evidencije o prijavama „zviždača“, pokrenutim istragama, ishodima i mjerama. Evropska komisija će u decembru 2023. podnijeti prvi izvještaj o provedbi ove Direktive Evropskom Parlamentu i Vijeću.

Direktiva o zaštiti „zviždača“ nesumnjivo je značajan *milestone* na nivou Evropske unije u pogledu borbe protiv mita i korupcije, zaštite privatnog kapitala i transparentnosti javne potrošnje. Harmonizacija unijskog prava u tom smislu može pospješiti procenat prijave i otkrivanja kršenja prava Unije, ali će stvarnu efikasnost ovog unijskog instrumenta tek pokazati prvi izvještaji Komisije, posebno u svjetlu svih okolnosti COVID-19, a koje su neminovno vezane za proces javnih nabavki, složene procedure prioritiziranja vakcinacije, ali i nove faktore tržišne utakmice privatnog kapitala poslije vanrednih gubitaka profita te, na koncu, i nove dinamike radno-pravnih odnosa, „rada od kuće“ i povratka na posao.

U Bosni i Hercegovini složena političko-administrativna struktura uvjetovala je postojanje dva različita zakona: ***Zakon o zaštiti lica koja prijavljuju korupciju u institucijama Bosne i Hercegovine*** – odnosi se samo na javne institucije (*Sl. glasnik BiH* br. 100/13), ***Zakon o zaštiti lica koja prijavljuju korupciju RS*** – odnosi se i na javne institucije i privatni sektor (*Sl. glasnik RS* br. 62/17) i jedan nacrt zakona koji i dalje nije usvojen (februar 2021.), a radi se o ***Nacrtu Zakona o zaštiti uzbunjivača FBiH***, koji je 2021. odbijen od strane Predstavničkog doma Parlamenta FBiH uz zaključak Parlamenta prema Ministarstvu pravde da pripremi novi nacrt „u skladu s evropskim normama“. ■

Upravljanje rizikom prevara

ULOGA SISTEMSKIH RJEŠENJA U AKTIVNOSTIMA PREVENCIJA I DETEKCIJA PREVARA

Kako osigurati osjećaj sigurnosti i povjerenje klijenata

Autori:
Vedran Vinšalek
Mirzad Topić

U vremenu kada banke digitalizuju sve veći broj svojih procesa, neophodno je da osiguraju osjećaj sigurnosti i povjerenje klijenata u takve procese. Isto se jednim dijelom može postići uvođenjem sistemskog rješenja za prevenciju i detekciju prevara koji predstavlja jedan od veoma bitnih faktora upravljanja rizikom prevara.

Osnovne tri teme koje je potrebno obraditi kako bi se smanjile prevare su:

- Zaštita klijenta,
- Prevencija prevare i
- Odgovor na prevaru.

Prevencija i detekcija prevare podrazumijeva otkrivanje prevare u njenom samom početku kako bi se poduzele odgovarajuće mjere i na taj način minimizirala prouzrokovana šteta.

Srećom, postoji nekoliko taktika osmišljenih za otkrivanje i sprečavanje prevara, uključujući sistemsko praćenje aktivnosti s više lokacija u svrhu otkrivanja sumnjivog ponašanja.

Osnovne prednosti sistemskog načina otkrivanja sumnjivih aktivnosti su:

- brzo otkrivanje prevara u svrhu sprečavanja gubitaka,
- monitoring miliona transakcija s više kanala u stvarnom vremenu,
- prepoznavanje obrazaca neobičnog ponašanja kombiniranjem podataka o transakcijama u stvarnom vremenu i povijesne analize ponašanja klijenata/uposlenika,

- brzo prilagođavanje novim trendovima prevara i primjenom novih pravila,
- ažuriranje pravila u stvarnom vremenu,
- optimizacija procesa i
- zadovoljstvo i osjećaj sigurnosti kod klijenata.

Navedena rješenja mogu funkcionisati na 3 načina:

1. Rule Based Solutions

Sistemska rješenja bazirana na pravilima kao osnovu rješenja sadrže unaprijed definisana pravila koja sprečavaju nastanak prevare. Unaprijed definisana pravila kreirana su na osnovu prethodnih iskustava i prevara koje su se desile nekad u prošlosti. Navedena pravila moraju se stalno dorađivati i nadograđivati, kao i kreirati nova s obzirom na to da se obrasci prevara često mijenjaju.

Unaprijed definisana pravila kreirana su na osnovu prethodnih iskustava i prevara koje su se desile nekad u prošlosti. Navedena pravila se moraju stalno dorađivati i nadograđivati, kao i kreirati nova s obzirom na to da se obrasci prevara često mijenjaju.

Mana navedenog je to što su pravila reaktivna i nisu proaktivna. Pravila se ne uče sama od sebe i sporo reagiraju na promjene u obrascima prevare. Zbog toga ne prepoznaju prevaru sve dok se pravila ne dorade u skladu s novim obrascima sumnjivog ponašanja.

2. Machine learning rješenja

Velika prednost *Machine learning rješenja* je sposobnost kategorizacije i analize mnogo podataka s više izvora na mnogo koherentniji i efikasniji način od ljudskog mozga. Navedena rješenja su proaktivnija i dizajnirana su za učenje na vlastitim greškama tako da mogu poboljšati svoje performanse i tačnost čak i bez ikakve ljudske intervencije.

Veoma je komplikovano napraviti adekvatno rješenje koje će se oslanjati na *machine learning* s obzirom na to da kvalitet podataka i performanse sistema koji se koriste u navedenom moraju biti na visokom nivou kako bi rješenje adekvatno funkcionisalo.

3. Scoring rješenja

Scoring rješenje funkcioniše na način da za zaprimljenu transakciju na osnovu različitih parametara (vrijeme realizacije, iznos transakcije, geolokacija i sl.) šalje preporuku u obliku bodovanja. U zavisnosti od ocjene koju je postavilo rješenje, odgovorne osobe donose konačnu odluku o tome da li transakciju treba odobriti ili odbiti. ■

Prevencija je mnogo jeftinija od tretmana? A možda i učinkovitija. (*Debbie Adair*)

ULOGA SISTEMA INTERNIH KONTROLA U PREVENCIJI PREVARA

Adekvatno upravljanje sistemom internih kontrola, uz odgovarajuću metodologiju i alate, donosi niz prednosti za finansijske institucije u smislu unapređenja kontrola u poslovnim procesima čime se ublažavaju rizici, preveniraju potencijalne prevare, smanjuju troškovi i poboljšava kvalitet usluga.

Autori:
Azra Beriša
Haris Buturović

PREVARE

Čin obmane koji ima za cilj sticanje finansijske koristi na nezakonit način, a na štetu drugih strana.

Prevara se definiše kao svaka nečasna/nepoštena aktivnost podnositelja zahtjeva, klijenta, zaposlenika ili bilo koje treće strane koja rezultira gubitkom za finansijske institucije, njihove klijente i/ili treće strane korištenjem obmane u ličnu korist ili korist treće strane, koja se provodi u vezi s aktivnostima i uslugama finansijske institucije, a u cilju sticanja nepravične ili nezakonite koristi.

> *Prevara se definiše kao svaka nečasna/nepoštena aktivnost podnositelja zahtjeva, klijenta, zaposlenika ili bilo koje treće strane koja rezultira gubitkom za finansijske institucije, njihove klijente i/ili treće strane korištenjem obmane u ličnu korist ili korist treće strane.*

VRSTE PREVARA

Prema izvoru počinitelja prevare se mogu podijeliti na interne i eksterne.

Interna prevara podrazumijeva prevare počinjene interno, od strane uposlenika, s namjerom sticanja koristi, te za posljedicu ima nanošenje štete finansijskoj instituciji i/ili njenim klijentima (npr. nelegalno prisvajanje novca/imovine, namjerno nepravilno vrednovanje transakcija, zloupotreba povjerljivih informacija, malverzacije s kreditnim karticama, pronevjera, povreda zakonskih propisa, itd.).

Eksterna prevara je prevara počinjena od strane trećeg lica s namjerom da prevari finansijsku instituciju ili njene klijente, ošteti ili zloupotrijebi njenu imovinu (npr. krivotvorenje, ispravka ili izmjena dokumenata, prezentiranje lažnih informacija, krivotvorenje novčanica, pljačke, provale i krađe, probijanje IT sistema, krađa informacija, itd.).

Prevare se prema direktnoj povezanosti s jednim ili više proizvoda/usluga mogu podijeliti na kreditne, nekreditne, kartične i ostale vrste prevara koje nisu povezane s proizvodom finansijske institucije (računovodstvene prevare, prevare u procesu nabavke, itd.).

KAKO SE ZAŠTITITI?

Sprečavanje i otkrivanje prevara obuhvata preduzimanje onih akcija kojima se obeshrabruju potencijalni počinioci prevare. Osnovni mehanizam za sprečavanje prevare je interna kontrola. Primarnu odgovornost za uspostavljanje i održavanje interne kontrole treba da ima rukovodstvo. Također, interni revizori imaju značajnu ulogu u otkrivanju i sprečavanju prevare jer oni vrše pregled internih kontrola. Oni treba da budu svjesni svih scenarija prevare i da svoje programe revizije baziraju na riziku od prevare.

> *Osnovni mehanizam za sprečavanje prevare je interna kontrola. Primarnu odgovornost za uspostavljanje i održavanje interne kontrole treba da ima rukovodstvo.*

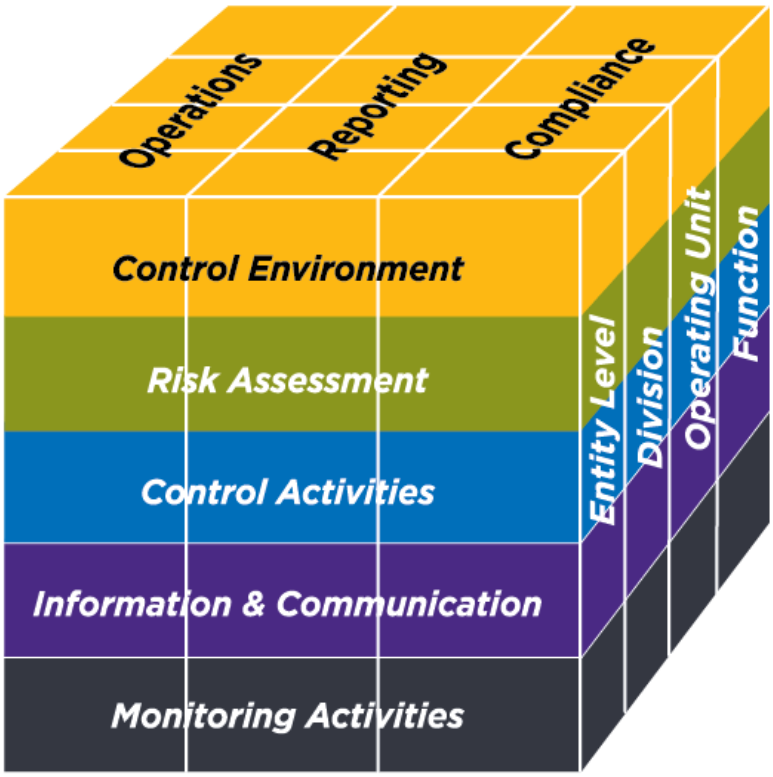
Kako istraga i otkrivanje prevara ponekad nije dovoljno, potrebno je kreirati kvalitetan program prevencije prevarnih radnji kako bismo spriječili njihov nastanak.

Polazna tačka je pristup koji uključuje sljedeće komponente:

- adekvatna korporativna kultura i kultura upravljanja rizicima,
- uspostavljanje politike zviždača (*whistleblowers*),
- podizanje svijesti o mogućim rizicima,
- sistem upravljanja rizicima,
- monitoring sumnjivih transakcija,
- zapošljavanje adekvatnih saradnika te
- efikasan i efektivan sistem internih kontrola (SIK).

Globalizacija i tehnološki napredak imaju tendenciju povećanja rizika poslovanja usljed pojave različitih mogućnosti i prilika počinjenja prevare, što posebno dovodi do potrebe da finansijske institucije uvedu i provedu učinkovite mjere interne kontrole.

Kako je ranije navedeno, jedan od ključnih načina za prevenciju prevara je uspostavljanje efikasnog sistema internih kontrola za adekvatnu kontrolu rizika, praćenje učinkovitosti



Slika 1. *COSO Internal Control - Integrisani okvirni principi*

i djelotvornosti poslovanja koji je kao takav sve više u fokusu kako finansijskih institucija tako i regulatora.

Metodologija koja se najčešće koristi u praksi jeste međunarodni COSO okvir (*Committee of Sponsoring Organizations of the Treadway Commission*) koji definiše interne kontrole kao proces koji sprovodi top menadžment zajedno sa svim uposlenicima kako bi se osiguralo ispunjenje sljedećih ciljeva:

- učinkovitost i efikasnost poslovnih procesa,
- pouzdanost izvještavanja i
- usklađenost s važećim zakonima i propisima.

Sistem internih kontrola provodi se putem pet međusobno povezanih komponenti internih kontrola koje obuhvataju:

1. Kontrolno okruženje – Koji je nivo rizika koji se pojavljuje u internom i eksternom okruženju?

- Integritet i etičke vrijednosti
- Nadzor
- Struktura, autoritet i odgovornost
- Nadležnost
- Poticanje odgovornosti

2. Procjena rizika – Da li je uložen učinkovit napor na identifikaciji rizičnih područja koja bi omogućila pojavu materijalno značajnih grešaka?

- Prikladnost ciljeva
- Identifikacija i analiza rizika
- Procjena rizika prevara
- Identifikacija i analiza značajnih promjena

3. Kontrolne aktivnosti – Da li postoje adekvatne kontrole da u potpunosti učinkovito mitigiraju rizik na prihvatljiv nivo?

- Selekcija i razvoj kontrolnih aktivnosti
- Selekcija i razvoj opštih kontrola nad tehnologijom
- Primjena putem politika i procedura

4. Informacije i komunikacija – Da li postoje kontrole

koje osiguravaju blagovremeno i odgovarajuće obavještavanje o materijalno značajnim greškama, ako i kada se dogode?

- Korištenje relevantnih informacija
- Interna komunikacija
- Eksterna komunikacija

5. Praćenje aktivnosti – Da li postoji sistem praćenja aktivnosti kako bi se kontinuirano vrednovala i poboljšavala učinkovitost internih kontrola?

> *U cilju postizanja kvalitetnog korporativnog upravljanja, a samim tim i upravljanja rizicima, neophodno je dobro razumijevanje sistema internih kontrola i načina na koji one funkcionišu u praksi.*

- Tekuće i/ili pojedinačno ocjenjivanje
- Evaluacija i komuniciranje identifikovanih nedostataka

U cilju postizanja kvalitetnog korporativnog upravljanja, a samim tim i upravljanja rizicima, neophodno je dobro razumijevanje sistema internih kontrola i načina na koji one funkcionišu u praksi. Razlog tome leži u činjenici da način upravljanja rizicima zavisi od učinkovitosti sistema internih kontrola, odnosno od sposobnosti organizacije da spozna rizike koji utiču ili bi mogli uticati na njeno poslovanje, a od čega zavisi i kvalitet korporativnog upravljanja.

KONTROLE vs. MJERE

Interne kontrole su ciljne/stvarne usporedbe kako bi se provjerilo da li se upute o radu poštuju u izvršenju definisanog radnog koraka. Ključne kontrole služe za sprečavanje, smanjenje ili otkrivanje značajnih rizika. Ključne kontrole mogu se sastojati od niza pojedinačnih kontrola za postizanje kontrolnih ciljeva višeg nivoa.

U SIK-u se mogu u obzir uzeti i mjere ublažavanja rizika. To su druge korektivne i preventivne aktivnosti za smanjenje nivoa rizika koje mogu biti procesno integrisane ili procesno neovisne.

PRIMJENA SIK-a U PRAKSI

Standardni SIK proces generalno obuhvata sljedeće korake:

- definisanje SIK relevantnih procesa i njihovo dokumentovanje,
- analiza i procjena ključnih inherentnih rizika,
- definisanje kontrola za mitigaciju identifikovanih ključnih rizika,
- procjena ključnih rezidualnih rizika,
- upravljanje ključnim kontrolama te
- praćenje i izvještavanje.

Vrste kontrola koje se najčešće primjenjuju u praksi su:

- **Manuelna kontrola** - kontrola koju obavlja jedan ili više uposlenika bez pomoći IT sistema ili posebno programiranih aplikacija;
- **Sistemska kontrola** - kontrola koja se obavlja automatizirano u IT sistemima ili posebno programiranim aplikacijama;
- **Preventivna kontrola** - kontrola koja bi trebala spriječiti pogreške ili ne-

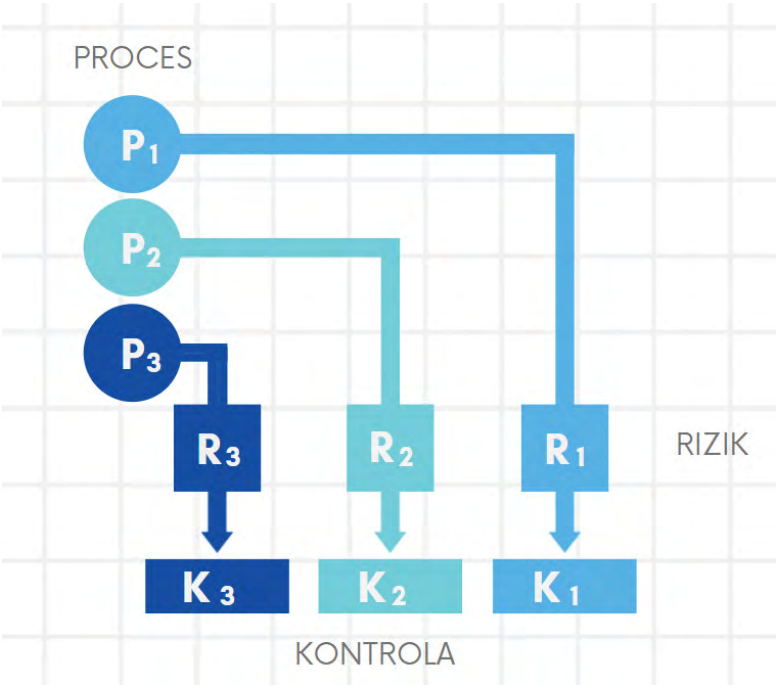
pravilnosti *a priori* (npr. razdvajanje funkcija, šifri i pristupnih pravila i sl.)
- **Detektivna kontrola** - kontrola dizajnirana za otkrivanje pogrešaka i nepravilnosti (npr. kontrolne karte).

Alati koji se koriste i njihova svrha

Alati za upravljanje rizicima se upotrebljavaju u cilju povećanja efikasnosti, pružajući optimalno korisničko iskustvo, sveobuhvatnu podršku u svim domenama upravljanja rizicima, ispunjavajući regulatorne smjernice i zahtjeve. Ovi alati trebaju da posjeduju i automatizirano upravljanje, unaprijed definisane obrasce, izvještavanje, centralizirano povezivanje procesa, rizika i kontrola, procjenu rizika, monitoring i dokumentovanje izvršenja zadanih kontrolnih aktivnosti.

Primjeri SIK alata/modula:

- SAI Global - Bwise GRC,
- Optimiso Group - Optimiso Suite ICS,
- GBTEC Software AG - BIC GRC,
- ServiceNow Governance, Risk and Compliance,
- SAP Process Control, SAP Business Objects,
- MetricStream CCM,
- OneTrust GRC i
- HighBond by Galvanize.



ZAKLJUČAK

Evidentno je da adekvatno upravljanje sistemom internih kontrola, uz odgovarajuću metodologiju i alate, donosi niz prednosti za finansijske institucije u smislu unapređenja kontrola u poslovnim procesima čime se ublažavaju rizici, preveniraju potencijalne prevare, smanjuju troškovi i poboljšava kvalitet usluga.

Navedene prednosti omogućavaju banci fokusiranje na glavne poslovne aktivnosti, veću fleksibilnost i bolje upravljanje, a što u konačnici direktno utiče na povećanje efikasnosti i efektivnosti cjelokupnog poslovanja. To je ujedno i strateški cilj svake finasijske institucije. ■

Povjeravanje obavljanja poslova ili usluga jedne kompanije trećim licima

RIZICI EKSTERNALIZACIJE U POSLOVANJU BANAKA

Zbog čega jedna kompanija (ili banka) želi poslove ili usluge koje obavlja povjeriti trećem licu?
Koji su rizici i kako izvršiti njihovu procjenu?
Kako predvidjeti intenzitet i efekte rizika?
Koje mjere banka može odrediti i provesti?

Autor:
Nermin Ibradžić

Eksternalizacija kao poslovni model

Eksternalizacija je, možemo slobodno reći, jedan globalni fenomen koji je uzeo učešće u svim sektorima poslovanja. Izuzetak od tog fenomena nisu ni banke, ali ni druge finansijske institucije.

U širem smislu, eksternalizacija podrazumijeva povjeravanja obavljanja nekih poslova ili usluga jedne kompanije trećim licima - pružaocima usluga.

U kontekstu poslovanja banaka u BiH, definicija eksternalizacije (*outsourcinga*) proizilazi iz *Odluke o upravljanju eksternalizacijom u banci*[1], koju je donijela Agencija za bankarstvo Federacije Bosne i Hercegovine, i *Odluke o upravljanju eksternalizacijom*[2], koju je donijela Agencija za bankarstvo Republike Srpske. Ovim odlukama ona je definirana kao ugovorno povjeravanje obavljanja

[1] *Objavljeno u Službenim novinama F BiH , broj 81/17.*
[2] *Objavljeno u Službenom glasniku RS, broj 114/20.*

> *Odlukom o upravljanju eksternalizacijom u banci, koju je donijela FBA, i Odlukom o upravljanju eksternalizacijom, koju je donijela ABRS, eksternalizacija je definirana kao ugovorno povjeravanje obavljanja aktivnosti banke pružaocima usluga koje bi inače banka obavljala sama.*

aktivnosti banke pružaocima usluga koje bi inače banka obavljala sama.

Kada govorimo o eksternalizaciji, nameću se pitanja: šta je pokretač postupka eksternalizacije, šta je razlog zbog čega jedna kompanija (ili banka) želi poslove ili usluge koje obavlja povjeriti trećem licu?

Prema istraživanju **Deloittea** iz 2020. godine (*Deloitte Global Outsourcing Survey 2020 godine*[3]), glavni cilj i razlog eksternalizacije su troškovi, tačnije redukcija/smanjenje troškova.

Drugi razlog jeste to što eksternalizacija kompanijama omogućava određeni stepen fleksibilnosti.
Valja naglasiti da razlozi kao što su agilnost/brzina usluge i činjenica da eksternalizacija omogućava pristup potrebnim alatima i procesima zauzimaju tek nešto više od 10% odgovora.

Prema istom istraživanju, područje u kojem je eksternalizacija najdominantnija je poslovanje „u oblaku" *(cloud*) bez obzira na vrstu oblaka (javni, privatni zajednički, hibridni). Vezano za poslovanje u oblaku, najviše zabrinutosti kod ispitanika je izazvalo pitanje sigurnosti i to: sigurnost informacija, podataka, dokumenata, mogućnost neovlaštenih izmjena i sl. Situacija nije puno drugačija ni u finansijskom sektoru u BiH gdje su pitanja poslovanja u oblaku sve aktuelnija, prvenstveno zbog procesa digitalizacije i automatizacije.

Deloitte istraživanje je rađeno na globalnom nivou i segmentacija po djelatnostima nije dostupna tako da nije moguće izdvojiti podatke koji se odnose samo na finansijski sektor. Međutim, možemo se složiti da je optimizacija troškova jedan od glavnih razloga zašto se i finansijske institucije odlučuju za postupke eksternalizacije. Kao drugi razlog možemo navesti i fokus na *core* poslovne aktivnosti jer eksternalizacija omogućava da se posvetite onom što najbolje znate da radite, a poslove za koje su potrebna druga specifična znanja povjerite stručnjacima van vaše kompanije.

Eksternalizacija i regulativa

Kada govorimo o eksternalizaciji, pored benefita koje ona donosi potrebno je cijeniti i rizike kojima je kompanija (u našem slučaju banka) izložena u slučaju eksternalizacije. Ne tako davno primarno je bilo procijeniti šta se eksternalizira (aktivnost koju se eksternalizira) dok je pitanje kome se aktivnost eksternalizira često bilo sekundarno. Svakako da je u prošlosti bilo i manje

[3] *Dostupno na https://www2.deloitte.com/global/en/pages/operations/articles/gx-global-outsourcing-survey.html*

postupaka eksternalizacije pa je manji broj pružalaca ove usluge bilo moguće lakše kontrolirati.

Međutim, kako je eksternalizacija uzimala veći zamah tako su se otvarala pitanja i u odnosu na kompanije koje pružaju usluge eksternalizacije.
Kakva je kompanija koja vam pruža uslugu eksternalizacije? Koliko dugo i kako posluje? Koje standarde primjenjuje i na koji način? Ko ju kontroliše i kako? Koliko je transparentno i etično njeno poslovanje? Kome sve pruža usluge, na koji način i u kojem kapacitetu? Kakvo je njeno upravljanje finansijama? Kako i na koji način ulaže svoja sredstva? Ko su stvarni vlasnici kompanije? Da li je kompanija samoodrživa ili se finansira isključivo iz kredita i naplaćenih avansa? Kakve su izlazne strategije u konkretnom slučaju? Da li postoje i kakvi su planovi kontinuiteta poslovanja, kako na strani pružaoca usluga tako i na strani banke? Koliko se često provode penetracijska testiranja i da li su scenariji za testiranja i kontinuitet poslovanja realni?

Dakle, pored predmeta eksternalizacije u jednakom fokusu su i pružalac usluga eksternalizacije, ali i mjesto pružanja usluga eksternalizacije.

U poslovanju banaka eksternalizacija nije više izuzetak. Radi se o procesu koji će povećati prihode, smanjiti troškove i poboljšati učinkovitost. S druge strane, eksternalizacija nije jednostavan proces. Ona danas zahtijeva holistički pristup, učešće više funkcija banke u procjeni, praćenju i kontroli rizika eksternalizovane aktivnosti i pružaoca usluga (npr. učešće funkcije rizika, IT funkcije, funkcije informacione sigurnosti, funkcije sprečavanja pranja novca, *antifraud* funkcija, funkcija praćenja usklađenosti, interna revizija, pravna funkcija, itd.).

> *Eksternalizacija nije jednostavan proces. Ona danas zahtijeva holistički pristup, učešće više funkcija banke u procjeni, praćenju i kontroli rizika eksternalizovane aktivnosti i pružaoca usluga (npr. učešće funkcije rizika, IT funkcije, funkcije informacione sigurnosti, funkcije sprečavanja pranja novca, antifraud funkcija, funkcija praćenja usklađenosti, interna revizija, pravna funkcija, itd.).*

Kada govorimo o regulatornom okviru, osim zakonima o bankama, područje eksternalizacije aktivnosti banaka definirano je kroz već ranije pomenutu *Odluku o upravljanju eksternalizacijom u banci*, koju je donijela Agencija za bankarstvo FBiH (dalje: Odluka FBA), i *Odluku o upravljanju eksternalizacijom*, koju je donijela Agencija za bankarstvo Republike Srpske (dalje: Odluka ABRS).

Za banke, koje su članice bankarskih grupacija koje imaju glavno sjedište u zemljama Evropske unije, u primjeni su i *Smjernice za eksternalizaciju* (broj EBA/GL/2019/02 od 25.02.2019. godine) koje je donijela Evropska asocijacija banaka/*European Banking Association* (dalje označene kao: EBA smjernice). Konkretno, Glava IV, tačka 2. član 21. u vezi sa članom 23. i 24.

EBA Smjernica referiše na primjenu istih za kompletne bankarske grupacije na konsolidovanoj osnovi, a izuzeća od primjene moraju biti posebno odobrena.

Pored navedenih zakona, podzakonskih akata i međunarodnih standarda, postoji još niz drugih odluka lokalnog regulatora i EU tijela koje, posredno ili neposredno, referišu na područje eksternalizacije. Dublja analiza te regulative i standarda bi u ovom slučaju zauzela puno prostora, a ne bi dala proporcijalno istu dodatnu vrijednost ovom članku pa ćemo se njima baviti možda nekom drugom prilikom.

Kako nam je lokalna regulativa manje-više poznata, na ovom mjestu ćemo ukratko predstaviti EBA smjernice i novine koje one donose.
EBA smjernice sadrže više poglavlja koja se u osnovi mogu podijeliti na: procjenu eksternalizacije i procjenu pružaoca usluga eksternalizacije u prethodnom postupku, odobravanje eksternalizacije, ugovoranje eksternalizacije, praćenje eksternalizovanih aktivnosti i kontrola pružaoca usluga, kontinuitet poslovanja i izlazne strategije.

Ono što je posebno naglašeno u EBA smjernicama je:
– pristup temeljen na procjeni rizika (RBA-*Risk Based Approach*);
– primjena načela proporcionalnosti - usklađenost si-

stema upravljanja rizicima eksternalizacije sa profilom rizičnosti, veličinom i poslovnim modelom banke;
- primjena smjernica i principa internog upravljanja eksternalizacijom na konsolidovanoj i podkonsolidovanoj osnovi (primjena na kompanije "kćerke" i izvan područja EU);
- inkorporiranje odredbi koje se odnose na eksternalizaciju poslovanja "u oblaku" u smjernice bez naglašavanja da je poslovanje "u oblaku" nužno ključna ili značajna eksternalizacija/funkcija;
- rizik koncentracije;
- kontinuitet poslovanja i značaj izlazne strategije.

Bitno je napomenuti da je nova *Odluka* ABRS u međuvremenu velikim dijelom usaglašena sa EBA smjernicama, a u FBiH taj proces je u toku. S druge strane, Agencija za bankarstvo FBiH u proteklom periodu formirala je nove setove izvještaja o eksternalizovanim aktivnostima koji su prilagođeni EBA smjernicama. U kojem pravcu će lokalni regulatori dalje djelovati u području eksternalizacije i koliki uticaj će imati na sam proces, ostaje da se vidi.

(Pr)ocjena rizika eksternalizacije

Pod pojmom "rizik eksternalizacije" podrazumijevamo skup rizika koji nastaju ili potencijalno mogu nastati kada banka aktivnosti, koje bi inače vršila sama, povjerava trećem licu, odnosno pružatelju usluga.
Kada govorimo o riziku eksternalizacije, ne govorimo o jednom riziku, nego o više povezanih i neovisnih vrsta i kategorija rizika koji mogu nastati, ne samo u odnosu na eksternalizovanu aktivnost nego i u odnosu na pružaoca usluga, u odnosu na klijente, poslovno okruženje, političku ili situaciju u društvu i sl.

Ukoliko konsultujemo naprijed navedene regulative na lokalnom i nivou EU, zaključit ćemo da ne postoji katalog rizika eksternalizacije kao numerus clausus[4] rizika koje je potrebno cijeniti u svakom pojedinačnom slučaju. Nije moguće objektivno definirati koje tačno rizike, na koji način i u kojem obimu banka treba da procijeni za svaki konkretan slučaj da bi zadovoljila osnovne principe kvalitetne procjene eksternalizacije i pružaoca usluga.
Svaka eksternalizacija je postupak za sebe i svaka ima određene specifičnosti. Ovo vrijedi čak i u slučaju kada više raznih banaka radi sa istim pružaocem usluge i kada se radi o istom predmetu eksternalizacije. Predmet

"Nije moguće objektivno definirati koje tačno rizike, na koji način i u kojem obimu banka treba da procijeni za svaki konkretan slučaj da bi zadovoljila osnovne principe kvalitetne procjene eksternalizacije i pružaoca usluga.

Svaka eksternalizacija je postupak za sebe i svaka ima određene specifičnosti."

[4] *lat. zatvoren ili konačan broj*

eksternalizacije i pružalac usluga nisu jedini elementi u jednačini procjene rizika. Tu su još veličina banke, njen apetit za rizik, način na koji je sistem internih kontrola uspostavljen (ili nije uspostavljen), pripadnost grupi banaka, metodologije koje se koriste za procjenu rizika, prihvaćene mjere mitigacije rizika i sl. To svaku eksternalizaciju čini unikatnom.

Bez obzira na navedeno, banke su u mogućnosti na osnovu dosadašnjih, kako vlastitih tako i dostupnih iskustava drugih subjekata, procijeniti koji rizici bi imali značajan uticaj kod svakog pojedinog postupka eksternalizacije, koji intezitet i efekti rizika se mogu očekivati/predvidjeti te koje mjere banka može odrediti i na kraju provesti.

Operativni rizik nije novina u poslovanju banaka i podrazumijeva rizik gubitaka nastalih kao rezultat neodgovarajućih ili loših procedura, ljudskih pogrešaka, grešaka sistema/procesa ili nepredvidivih vanjskih događaja, uključujući i rizik neusklađenosti sa zakonskom regulativom. Stoga procjena ovog rizika ne bi trebala biti poseban izazov. Da li pružalac usluga ima odgovarajuće procedure, koliko ih često revidira, da li postoje dostupni podaci o greškama ili eventualno izrečenim kaznama, da li pružalac usluga ima adekvatno osiguranje za pričinjenu štetu trećim licima, odnosno osiguranje od profesionalne odgovornosti, da li postoje zabilježeni slučajevi kršenja zakonskih propisa od strane pružaoca usluga, samo su neka od pitanja na koja bi trebalo odgovoriti kod procjene ove vrste rizika.

Strateški rizik se može manifestirati u onim slučajevima kada se strateška opredjeljenja pružaoca usluga bitno razlikuju od strategije banke. Ukoliko banka traži dugoročno stabilnog pružaoca usluga, a pružaocu usluga eksternalizovana aktivnost nije *core* djelatnost nego sporedni posao, teško da postoji usaglašenost strateških ciljeva banke i pružaoca usluga. Dodatno, ako je banka opredijeljenja na rad s klijentima i poslovnim partnerima koji ispunjavaju više/visoke ekološke i socijalne standarde i ako to proklamuje kao jedan od svojih strateških ciljeva i vrijednosti, a pružalac usluga ne odgovara navedenom profilu, vrlo lako je moguće da postoje velike razlike u strategiji banke i pružaoca usluga.

Kreditni rizik (na strani pružaoca usluga) manifestira se u mogućnosti pružaoca usluga da ispunjava svoje kreditne/finansijske obaveze. Kreditna zaduženost nije nužno odlika lošeg poslovanja, ona može biti i pokazatelj visokog stepena investicija u razvoj novih tehnologija, širenja tržišta, opravdanih investicionih ulaganja. Međutim, ako elementi i struktura kreditne i finansijske zaduženosti pružaoca usluga ukazuju na problem sa solventnošću, ako je izmirenje obaveza neuredno, to svakako treba da bude poziv na oprez i dubinsku analizu. Pružalac usluga koji je suočen s finansijskim kolapsom vrlo vjerovatno neće biti u mogućnosti da ispunjava svoje obaveze iz osnova eksternalizacije, a što za banku može generisati reputacijski rizik, operativni rizik i rizik od finansijskih gubitaka.

Pravni rizik na strani banke i pružaoca usluga postoji

ukoliko jedna od ugovornih strana nije u mogućnosti da ispuni svoje ugovorne obaveze, odnosno da ih provede u praksi. Dodatno, o pravnom riziku govorimo i u slučaju da određene obaveze, po sili zakona, jednostavno nisu provodive u jurisdikciji pružaoca usluga koja je različita od jurisdikcije banke. Upravo iz navedenog razloga, osim što ugovorne klauzule moraju zadovoljiti minimum propisan odlukama regulatora, potrebno je da su iste jasne i provodive kako na strani banke tako i na strani pružaoca usluga. U slučaju strane jurisdikcije svakako je potrebno dodatno ispitati da li postoje smetnje za provođenje ugovora i da li je obaveze iz osnova ugovora moguće prinudno ostvariti u jurisdikciji pružatelja usluga.

Rizik ugleda/reputacijski rizik procjenjuje se u odnosu na ugled/reputaciju pružaoca usluga i efekte koje reputacija pružaoca usluga može imati u odnosu na poslovanje banke. Negativni medijski natpisi i afere na strani pružaoca usluga vrlo vjerovatno će imati uticaja na kvalitet usluge, ali i na povjerenje klijenata prema banci ili na vanrednu reviziju od strane regulatora, a što u konačnici može imati negativne finansijske efekte, potencijalne regulatorne kazne, gubitak klijenata i uticaj na ocjenu strateškog i operativnog rizika.

Rizik koncentracije, kao relativno nova kategorija rizika, podrazumijeva više aspekata. Jedna od njih je procjena rizika u odnosu na pružaoca usluga koji je "dominantan" na tržištu kao pružalac određene usluge ili određene kategorije usluga. Drugi aspekt je koliko je usluga banka (ili bankarska grupa na konsolidovanoj osnovi) eksternalizovala na jednog pružaoca usluga ili na više pružalaca usluga koji su usko povezani (vlasništvom, ekonomski i sl). Ukoliko je u jednom ili drugom slučaju koncentracija u odnosu na istog ili povezane pružaoce usluga visoka, banka pored procjene rizika (ukoliko ostaje kod eksternalizacije) treba odrediti i adekvatne mjere. U ovom slučaju takve mjere treba da osiguraju kontinuitet usluge u slučaju prekida eksternalizacije, a što uključuje i efikasne izlazne strategije i mogućnost povrata eksternalizovane usluge u banku. Banke neće uvijek biti u mogućnosti da procijene pružaoca usluga na tzv. makro nivou, odnosno da ocijene da li je neki pružalac usluga dominantan na cijelom tržištu ili ne. Otkrivanje drugih poslovnih partnera/banaka, kojima pružalac usluga pruža iste ili slične usluge, uvijek može biti opravdano čuvanjem poslovne tajne tako da u ovom dijelu i sam regulator mora dati svoj doprinos.

Rizik dostupnosti/lokacije pružaoca usluga i lokacije pružanja usluge podrazumijeva prvenstveno mogućnost da banka, njeni interni i eksterni revizori ili regulator imaju pravovremen i neograničen pristup podacima, dokumentaciji, zaposlenicima i procesima vezanim za eksternalizovanu uslugu na strani pružaoca usluga. Ukoliko su banka i pružalac usluge iz područja iste jurisdikcije, to ne bi trebao biti problem. Međutim, ukoliko se jurisdikcija banke, sjedište pružaoca usluge i mjesto pružanja usluge razlikuju, banka mora biti oprezna i provesti dublju analizu mogućnosti

pristupa. Rizik dostupnosti je dodatno potrebno cijeniti i s obzirom na političku i sigurnosnu situaciju na lokaciji sjedišta pružaoca usluge ili lokaciji pružanja usluge (to mogu biti dvije različite lokacije). Cijena pružanja eksternalizovanih usluga u trećim zemljama koje su slabije razvijene može biti ekonomski opravdana i prihvatljiva, ali takve zemlje u pravilu nisu politički i/ili sigurnosno stabilne. Potencijalni gubitak u tom slučaju može biti znatno veći od ostvarene uštede.

Rizik otkrivanja povjerljivih informacija/rizik informacione sigurnosti uvjetuje procjenu pružaoca usluge i lokacije pružanja usluge s aspekta čuvanja povjerljivosti, integriteta i dostupnosti informacija. Da li pružalac usluga primjenjuje adekvatne tehničke i druge mjere zaštite informacija, da li usluge pruža sukladno međunarodno priznatim standardima (npr. ISO 27001:2013, PCI DSS i sl.), da li ima adekvatne procedure, da li postoji dvofaktorska autentifikacija za ključne procese/radnje, ima li razvijen i funkcionalan sistem internih kontrola, da li postoje nalazi regulatora ili revizora na strani pružaoca usluga koji ukazuju na propuste u domenu povjerljivosti informacija ili informacione sigurnosti, da li su na lokaciji pružanja usluge primijenjene sve adekvatne mjere, samo su neka od pitanja na koja je potrebno odgovoriti u dijelu dubinske analize ove vrste rizika. Metode neovlaštenog pristupa povjerljivim informacijama ili neovlaštene izmjene povjerljivih informacija su sve sofisticiranije tako da i pružalac usluga mora imati zaštitu od takvih postupaka na odgovarajućem nivou.

Rizik finansijske intervencije podrazumijeva rizik u kojem bi banka bila primorana da dodatno finansijski ili na drugi sličan način interveniše kod pružaoca usluga kako bi isti nastavio pružati ugovoreni nivo i kvalitetu eksternalizovane usluge. Navedeno može podrazumijevati i zahtjeve pružaoca usluga za visokim avansnim uplatama, ali i zahtjeve za isplatu cijene prije ugovorenog roka dospijeća i sl.

Rizik sukoba interesa manifestuje se kroz situacije u kojima pojedinac (učesnik postupka eksternalizacije) ima istovremeno suprotstavljene profesionalne i privatne interese. Sukob interesa u pravilu nije smetnja za postupak eksternalizacije sve dok postoje adekvatne mjere koje sprečavaju da se isti realizuje. U ovu kategoriju mogu spadati i mjere koje se odnose na sprečavanje koruptivnih radnji.

Kako proizilazi iz prethodnog teksta, rizici eksternalizacije predstavljaju složen skup međusobno povezanih ili zasebnih kategorija više rizika. Iz navedenog razloga je na samom početku ovog teksta naglašeno da procjena rizika eksternalizacije zahtijeva holistički pristup. Takav pristup

> *„Procjena rizika eksternalizacije zahtijeva holistički pristup. Takav pristup podrazumijeva učešće više organizacionih jedinica u procjeni rizika eksternalizacije, odnosno više eksperata iz ovog područja koji će „govoriti istim jezikom".*

podrazumijeva učešće više organizacionih jedinica u procjeni rizika eksternalizacije, odnosno više eksperata iz ovog područja koji će „govoriti istim jezikom".

Na tragu navedenog su i EBA smjernice gdje se u Glavi III, tačka 6, član 38. navodi obaveza finansijskih institucija da uspostave funkciju odgovornu za eksternalizaciju ili odrede člana višeg rukovodstva koji bi bio nadležan za područje upravljanja rizicima eksternalizacije. Možemo reći da navedeni princip u praksi već funkcioniše kod većine banaka u BiH koje već imaju formirane komisije ili odbore za upravljanje rizicima eksternalizacije i čiji članovi su eksperti iz raznih područja (pravo, usklađenost, operativni rizici, informaciona sigurnost, IT tehnologije i sl.).

Naposljetku...

Svaki postupak eksternalizacije je složen postupak kojeg je moguće pojednostaviti na način da se isti posmatra kao skup posebnih cjelina koje su međusobno povezane i imaju određeni slijed:

- Proces planiranja eksternalizacije (identifikacija potrebe za eksternalizacijom, procjena materijalne značajnosti eksternalizacije, procjena potencijalnih rizika eksternalizacije, određivanje mjera, donošenje odluke o nastavku procesa eksternalizacije ili prekidu postupka);
- Proces odabira pružaoca usluga (procjena rizika na strani pružaoca usluga i njegovih podizvođača - ako postoje, dubinska analiza pružaoca usluga i njegovog poslovanja, priprema prijedloga ugovora, usaglašavanje ugovora, definiranje mjera za kontinuitet poslovanja i definiranje izlazne strategije, obavještavanje regulatora u skladu s lokalnim propisima);
- Nadzor i kontrola eksternalizacije (praćenje kvaliteta isporučene usluge, praćenje vremena odziva pružaoca usluga, revidiranje inicijalno utvrđenih rizika, predlaganje novih mjera za upravljanje rizicima, definiranje mjera za korigovanje postupanja koje je suprotno ugovoru - ako takva postupanja postoje);
- Prekid ugovora/eksternalizacije (procjena uslova za prekid eksternalizacije, procjena rizika prekida eksternalizacije, ažuriranje izlazne strategije, ažuriranje planova kontinuiteta poslovanja, obavještavanje regulatora, aktiviranje izlazne strategije i mjera kontinuiteta poslovanja, pronalaženje novog pružaoca usluga ili povratak eksternalizovane usluge u banku).

U postupku procjene rizika eksternalizacije potrebno je:

- identificirati sve relevantne rizike na strani pružaoca usluga i eksternalizovane aktivnosti;
- ocijeniti uticaj rizika na poslovanje banke (mjerenje rizika), definisati scenarija i provesti testiranja (npr. uključiti scenarija u testiranja kontinuiteta poslovanja);
- odrediti mjere mitigacije i/ili praćenja rizika;
- vršiti nadzor, pratiti rizike, vršiti redovnu reprocjenu rizika i određivanje novih mjera (ako su potrebne).

Ono što je potrebno dodatno zapamtiti jeste da se prenosom eksternalizovane aktivnosti na pružaoca usluga

banka ni na koji način ne oslobađa odgovornosti za upravljanje rizicima eksternalizacije. Banka i dalje ostaje vlasnik svih rizika i kao takva je nosilac i benefita i negativnih posljedica za kvalitetno ili loše upravljanje rizicima. Pružalac usluge ostaje odgovoran banci za ispunjenje ili neispunjenje ugovorenih obaveza i naknadu štete koja time može nastati, ali obaveza upravljanja rizicima i odgovornost za eventualne posljedice trećim stranama i dalje ostaje u okviru banke. Zbog kompleksnosti materije veoma je moguće da će različite banke primijeniti različite metodologije i standarde kod upravljanja rizicima eksternalizacije. Tako se ne mogu isključiti situacije u kojima će određena aktivnost u jednoj banci biti procijenjena kao materijalno značajna eksternalizovana aktivnost, a u drugoj banci kao „obična" eksternalizacija. U dijelu ujednačavanja praksi ključnu ulogu imaju regulatori koji prvenstveno kroz mišljenja, pojašnjenja, prezentacije i edukacije mogu imati značajan uticaj na ujednačavanje postupanja banaka u ovom području. Dodatno, imajući u vidu da je u pitanju materija koja je sklona brzim promjenama, da su očekivanja klijenata banaka svake godine sve viša, da je digitalizacija i poslovanje "u oblaku" nešto što se dešava svakodnevno, postupci eksternalizacije, osim što treba da budu ujednačeni, treba da budu i dovoljno efikasni kako na strani banaka tako i na strani regulatora. ■

> *Prenosom eksternalizovane aktivnosti na pružaoca usluga banka se ni na koji način ne oslobađa odgovornosti za upravljanje rizicima eksternalizacije. Banka i dalje ostaje vlasnik svih rizika i kao takva je nosilac i benefita i negativnih posljedica za kvalitetno ili loše upravljanje rizicima.*

Ostali korišteni izvori:

„Top 10 risks of outsourcing and how to mitigate them, autor Pavlo Zinchenko, dostupno na: https://www.mindk.com/blog/risks-of-outsourcing/
„Concentration risk and the EBA's outsourcing guidelines", autor Luke Scanlon, dostupno na: https://www.pinsentmasons.com/out-law/analysis/concentration-risk-eba-outsourcing-guidelines
„The 10 most important changes in the EBA's revised outsourcing guidelines", autor Luke Scanlon, dostupno na: https://www.pinsentmasons.com/out-law/analysis/the-10-most-important-changes-in-the-ebas-revised-outsourcing-guidelines

***Cyber* napadi**

SIGURNOST KRITIČNE INFRASTRUKTURE U BOSNI I HERCEGOVINI

Cyber napadi na kritičnu infrastrukturu ostavljaju velike posljedice na stanovništvo, kompanije, ekonomiju, zdravstvo, energetiku i druge grane privrede. U ovom tekstu spomenut ćemo primjere _cyber_ napada na kritičnu infrastrukturu koji su zabilježeni u 2021. godini s ciljem da istaknemo važnost donošenja strategije _cyber_ sigurnosti na državnom nivou.

Autorica:
Sanela Stupar

U proteklom periodu zabilježeni su *cyber* napadi na kritičnu infrastrukturu u svijetu koji su imali posljedice na stanovništvo, kompanije, ekonomiju, zdravstvo, energetiku i druge grane privrede.

Da li Bosna i Hercegovina ima strategiju sigurnosti za kritičnu infrastrukturu? Da li su vlasnici kritične infrastrukture izvršili procjenu rizika koja se odnosi na *cyber* sigurnost? Da li se provodi revizija ključne infrastrukture za *cyber* sigurnost? Ovo su samo neka od pitanja na koja još uvijek nemamo odgovore.

Kritična infrastruktura

Kritična infrastruktura predstavlja imovinu, sistem ili njegov dio koji se nalazi na teritoriji zemlje članice i koji je neophodan za održavanje ključnih društvenih funkcija, zdravstva, bezbjednosti, sigurnosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na zemlju.[1]

Vlasnici kritične infrastrukture trebali bi kreirati sigur-

[1] *Council Directive 2008/114/EC of 8 Decembar 2008 on the identification and designation of European critical Infrastructures and the ssessment of the need to improve their protection" Official Journal of the European Union, 2008., str. 345.*

> *Kritična infrastruktura predstavlja imovinu, sistem ili njegov dio koji se nalazi na teritoriji zemlje članice i koji je neophodan za održavanje ključnih društvenih funkcija, zdravstva, bezbjednosti, sigurnosti, ekonomskog ili socijalnog blagostanja, a čije bi ometanje ili uništenje imalo značajan uticaj na zemlju.*

nosni plan na osnovu procjene nivoa informacionih rizika.

Informacioni rizici predstavljaju vjerovatnost nastanka nekog nepoželjnog događaja (prijetnje) koja u datim okolnostima može uzrokovati štetu, zastoj ili umanjeni intezitet rada informacionog sistema ili štetu nad informacijama koje su u njemu pohranjene. Primjer takvog neželjenog događaja (prijetnje) koji predstavlja informatički rizik su kompjuterski virusi.

BiH je i dalje jedina zemlja u Jugoistočnoj Europi koja nema strategiju cyber sigurnosti na državnom nivou, kao ni CERT.

BiH je izrazila odlučnost da će primjenjivati mjere za visoki nivo sigurnosti mrežnih i informacionih sistema širom Unije (NIS Direktiva [EU] 2016/1148 Evropskog parlamenta i Vijeća) i ispuniti Opštu direktivu o zaštiti podataka (Direktiva[EU] 2016/679). BiH ima za cilj i implementirati Konvenciju Vijeća Evrope o *cyber kriminalu* koja služi kao smjernica za bilo koju zemlju koja razvija državno zakonodavstvo i saradnju u borbi protiv *cyber kriminala* (tj. Budimpeštanska konvencija). Na-

> *BiH nema službeni i dogovoreni strateški pristup i okvir za reagovanje na prijetnje cyber sigurnosti. Iako se neke strategije dijelom bave cyber sigurnošću, BiH je i dalje jedina zemlja u Jugoistočnoj Europi koja nema strategiju cyber sigurnosti na državnom nivou, kao ni CERT.*

žalost, BiH nema službeni i dogovoreni strateški pristup i okvir za reagovanje na prijetnje *cyber sigurnosti*. Iako se neke strategije dijelom bave *cyber sigurnošću*, BiH je i dalje jedina zemlja u Jugoistočnoj Europi koja nema strategiju *cyber sigurnosti* na državnom nivou, kao ni CERT. Nedostatak koordinacije, nedovoljno usklađen pristup, neadekvatni kapaciteti i odsustvo strateške vizije i dalje predstavljaju pitanja koja treba riješiti. Postojeće zakonodavstvo tek treba da se u potpunosti uskladi s relevantnim pravnim tekovinama EU, a ne postoji ni sveobuhvatni zakon o sigurnosti informacija. Odluka Vijeća ministara BiH o dodjeljivanju CERT-a za institucije BiH iz 2017. godine još uvijek zahtijeva institucionalnu operacionalizaciju. Također, ključni nacionalni prioriteti sadržani u *Politici upravljanja informacijskom sigurnošću za razdoblje od 2017. do 2022. godine za institucije BiH* tek treba da budu operacionalizovani, što je uspostava mehanizama za adekvatno reagiranje na savremene izazove digitalnog doba.

Sve ovo ostavlja javni i privatni sektor u BiH, kao i pojedine građane, visoko ranjivim na rastuće prijetnje u cyber prostoru, uključujući cybernapade i terorizam koji ciljaju kritičnu infrastrukturu.[2]

Četvrta industrijska revolucija (ili Industrija 4.0)

Mnoge kompanije automatizuju svoje tradicionalno poslovanje koristeći savremenu pametnu tehnologiju pod nazivom Četvrta industrijska revolucija (ili Industrija 4.0). Karakteristika Industrije 4.0 odnosi se na automatizacije i razmjene podataka koristeći nove tehnološke inovacije koje su povezane i koje čine osnovu za njezinu primjenu i razvoj, a to su:

- Cyber-Physical Systems (CPS),
- Internet of Things (IoT or IioT),
- Industrijski internet stvari (IIoT),
- Umjetna inteligencija (UI),
- Horizonalna i vertikalna integracija,
- Robotika,
- Blockchain tehnologija,
- 3D tehnologija,
- Kibernetički sistemi (CPS),
- Big Data & Analytic,
- Pametna proizvodnja,
- Pametne tvornice,
- Cloud Computing i
- Kognitivno računanje.

U odnosu na druge razvijene zemlje BiH je vrlo malo započela transformaciju poslovanja „Industrija 4.0“.

Danas kao nikada ranije vrijedi sintagma da „mali mogu biti veliki“ pa u konačnici ne pobjeđuju veliki male, nego brzi i prilagodljivi spore i neodlučne.

Strateški cilj razvoja BiH trebao bi biti transformacija poslovanja u Industriju 4.0 uz implementaciju zakonodavstva Evropske unije koje se odnosi i na *cyber sigurnost*. Na taj način bismo podržali razvoj i rad domaćih kompanija.

> *Strateški cilj razvoja BiH trebao bi biti transformacija poslovanja u Industriju 4.0 uz implementaciju zakonodavstva Evropske unije koje se odnosi i na cyber sigurnost. Na taj način bismo podržali razvoj i rad domaćih kompanija.*

Jedino bankarski sektor ima zakonske propise, kontrole te uspostavljene adekvatne sigurnosne standarde dok ostali sektori usljed cyber napada mogu biti van funkcije i na nekoliko dana, a zbog nedostataka sigurnosnih mjera i procedura, plana kontinuiranog poslovanja i edukacije.

Cyber napad na kritičnu infrastrukturu

Mnogo je lakše razumjeti uticaj kibernetičkog napada ako izravno utječe na vaš svakodnevni život. (Marty Edwards) Predstavljamo vam primjere *cyber napada* na kritičnu infrastrukturu koji su zabilježeni u 2021. godini.

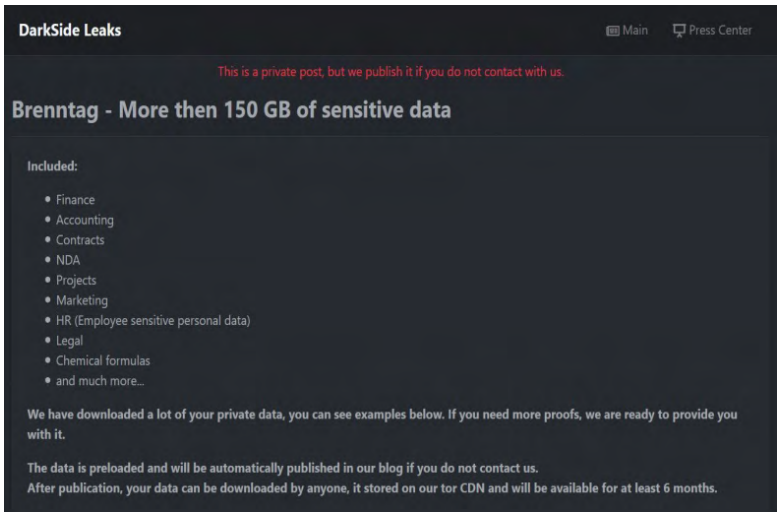
Hakerska grupa pod nazivom **DarkSide** izvršila je 7. maja *ransomware cyber napad* prisilno isključivši dio sistema van mreže te je time nedelju dana onemogućila rad kompanije **Colonial Pipelin**, najveće kompanije naftovoda u SAD koja dnevno prenosi 100 milijuna galona benzina, dizela i goriva za vazduhoplovstvo za velika američka tržišta. *Cyber napad* na Colonial Pipelin je okarakterisan kao najznačajniji napad na kritičnu nacionalnu infrastrukturu SAD u povijesti. Colonial je 19. maja priznao da je platio 4,4 miliona dolara u bitcoinu.

Colonial Pipeline zatvorio je 5.500 milja cijevi za gorivo kao odgovor na ransomware incident. ***Slika:*** *colpipe.com*

Brenntag, kompanija za distribuciju hemikalija, 11. maja platila je 4,4 miliona dolara otkupnine u bitcoinu za *ransomware cyber napad* DarkSide kako bi otključala kriptovane datoteke i spriječila da se javno ne objavi 150 GB ukradenih podataka. Brenntag je vodeća svjetska kompanija za distribuciju hemikalija sa sjedištem u Njemačkoj, ali sa preko 17 000 zaposlenih širom svijeta na preko 670 lokacija.

DarkSide, da bi dokazala svoje tvrdnje za *ransomware*, kreirala je privatnu stranicu za objavu podataka koja sadrži opis i vrstu podataka koji su ukradeni te snimke zaslona nekih datoteka.

Obično se, u toku pregovara o uplati otkupnine za *ransomware*, traži da hakerska grupa otkrije na koji način je izvršila upad ili napad na kompaniju u cilju identifikacije ranjivosti infomacionog



sistema. Informacije se dobiju obično u obliku izvještaja, pasusa ili sa ekrana *chat Tor*. U Brenntagovom slučaju, iz DarkSidea su naveli da su pristup mreži dobili nakon što su kupili ukradene informacije, ali za početak nisu znali kako su pribavljeni kredincijali.

Hakerska grupa DarkSide kreirala je model na pretplatu Ransomware kao usluga (*Ransomware as a service - RaaS*) koji podružnicama hakerskih grupa omogućava korištenje već razvijenih *ransomware* alata za izvršavanje *ransomware* napada. Podružnice su hakerske grupe koje su angažovane od strane DarkSidea putem oglasa koji objavljuju na svojoj web stranici te tako zarađuju postotke za svaku uspješnu isplatu otkupnine.

Većina modernih *ransomware* napada zahtijeva tim *cyber* kriminalaca u kojem je svakom članu dodijeljena određena uloga. Jedan od načina na koji tim može nabaviti zlonamjerni softver je kupnja izvornog koda od drugih *cyber* kriminalaca, a zatim njegovo modificiranje za svoje potrebe.

DarkSide bira svoje ciljeve i određuju odgovarajuću otkupninu na osnovu finansijskih prihoda organizacije.

Hakerska grupa DarkSidea prilagođava izvršnu datoteku *ransomwarea* za određenu kompaniju koju napada ukazujući da svaki napad prilagođavaja radi maksimalne efikasnosti. *Ransomware* izvršava *PowerShell* naredbu koja briše *Shadow Volume Copies* na sistemu. Zatim DarkSide nastavlja s ukidanjem različitih baza podataka, aplikacija i klijenata pošte kako bi se pripremio za šifriranje. Prosječno vrijeme je oko 45 dana od početnog pristupa i primjene *ransomwarea*.

Neophodno je da kompanije odgovorne za kritičnu infrastrukturu shvate da nesigurni sistemi predstavljaju sočan ransomware cilj kibernetičkog kriminala, a proaktivna odbrana u velikoj će mjeri spriječiti buduće incidente poput onoga što se dogodilo s kolonijalnim cjevovodom, prema sigurnosnoj tvrtki Intel 471 .

Istrage za digitalne otkupnine

Radna grupe za *ransomware* i digitalno iznuđivanje koja pripada Ministarstvu pravde Sjedinjenih Američkih Država (*United States Department of Justice, DOJ*) i FBA uspjeli su izvršiti povrat oko 20% do

30% od bitcoina isplaćenih od strane Colonial Pipelin napadačima *prateći novac* - iako se novac nalazio u kriptovaluti kojoj je teško ući u trag.

Elliptic softver za provjeru transakcija identificirao je *bitcoin* novčanik koji koristi DarkSide *ransomware* grupa za uplatu otkupnina od svojih žrtava na osnovu prikupljanja obavještajnih podataka i analize *blockchain* transakcija. *Bitcoin* novčanik primio je uplatu od 75 BTC (vrijednu 4,4 miliona američkih dolara u trenutku transakcije) koju je uplatila Colonial Pipelin 8. maja, nakon *cyber-napada* na njegovo poslovanje, što je dovelo do nestašice goriva u SAD-u.

Analizom *bitcoin* novčanika utvrđeno je da je digitalni novčanik bio aktivan od 4. marta 2021. godine te da je preko njega izvršeno pedeset sedam (57) uplata iz dvadeset jednog (21) različitog digitalnog novčanika. Neke od uplata direktno su se podudarale s otkupninama za koje je poznato da su ih druge žrtve platile DarkSideu, poput 78,29 BTC (također vrijednosti 4,4 miliona dolara u trenutku transakcije) koje je kompanija za distribuciju hemikalija Brenntag uplatila 11.5.2021. godine.

Intel 471, *Fortinet*, *Sophos*, *Kaspersky* i druge sigurnosne kopmanije izvršile su analizu *cyber napada* od strane DarkSidea i otkrile detalje kao i okvirne prijedloge sigurnosnih mjera. ■

Opšta procjena rizika za ključnu infrastrukturu BiH	
Ranjivost	Ključna infrastruktura ekonomija, zdravstva, vodovoda, energetike, telekomunikacije...
Ocjena nivoa rizika	**Kritičan/Visok**
Vjerovatnost (vjerovatnost nastanka neželjenog događaja, ranjivost sistema)	• Srednja - teroristički napad • Niska - *cyber grupe* u posljednje vrijeme napadaju firme za koje smatraju da će platiti otkupninu
Sigurnosne mjere	• Implementacija sigurnosnih mjera za operativne sisteme i mrežne uređaje u skladu sa standardima sigurnosti informacionih sistema; • Pravovremeno ažuriranje operativnih sistema i mrežnih uređaja; • Korištenje dvofaktorske autentifikacije; • Redovno izvođenje penetracijskih testova; • Implementacija sigurnosnih alata; • Osiguravanje rezervne kopije podataka; • Implementiranje plana kontinuiranog poslovanja (BCP), • Antivirus; • IPS; • Edukacija zaposlenika...

Najslabija karika može prekinuti i najjači lanac

LJUDSKI FAKTOR – NAJSLABIJA KARIKA SIGURNOSTI INFORMACIONIH SISTEMA

Prema raznim statistikama oko 40% slučajeva narušavanja podataka nastaje zbog djelovanja ljudskog faktora. Bilo nenamjernim ili namjernim djelovanjem radi zadovoljstva, lične koristi ili iz nekog drugog razloga, ljudi čine veliku prijetnju informacionom sistemu.

Autorica:
Sanela Vrana

Lanac sigurnosnih mjera

Davne 1785. godine škotski filozof **Thomas Reid** (1710-1796.), jedan od utemeljitelja filozofske škole zdravog razuma, u svom djelu *Eseji o intelektualnim silama čovjeka* istakao je da je svaki lanac onoliko jak koliko je jaka njegova najslabija karika.

Lanac sigurnosnih mjera kojima nastojimo zaštititi informacioni sistem sastoji se od niza implementiranih mehanizama, aktivnosti, postupaka i procedura. Tehničke, administrativne i fizičke mjere zaštite nadopunjuju jedna drugu i samo tako objedinjene mogu zaštititi svu informatičku imovinu (računarsku, mrežnu komunikacionu

Lanac sigurnosnih mjera kojima nastojimo zaštititi informacioni sistem sastoji se od niza implementiranih mehanizama, aktivnosti, postupaka i procedura. Tehničke, administrativne i fizičke mjere zaštite nadopunjuju jedna drugu i samo tako objedinjene mogu zaštititi svu informatičku imovinu.

opremu, softverske pakete te informacionu imovinu u vidu baza podataka, datoteka, dokumentacije, akata, ugovora i sl.).

Sigurnost je postala značajan faktor u funkcionisanju informacionih sistema te se svakodnevno razvijaju različiti sigurnosni mehanizmi kojima se nastoji osigurati efikasna zaštita.

Apsolutna sigurnost ne postoji

Prije nego što počnemo razmatrati mjere zaštite, moramo biti svjesni da apsolutna sigurnost ne postoji. Prema riječima američkog profesora informatike, **Eugenea H. Spaffordа**, eksperta u polju sigurnosti: "Jedini informacioni sistem koji je zaista siguran je onaj koji je isključen s napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru te okružen naoružanim čuvarima, pa čak ni tada se ne bismo trebali baš kladiti na njega".

> *"Jedini informacioni sistem koji je zaista siguran je onaj koji je isključen s napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru te okružen naoružanim čuvarima, pa čak ni tada se ne bismo trebali baš kladiti na njega."*
>
> *(Eugene H. Spafford)*

Sigurnosne mjere, kao što su *firewalli*, antivirusni softveri i VPN-ovi, veoma su moćno oružje za odbranu sigurnosti informacionih sistema. One su dizajnirane, razvijene, testirane i rade u svrhu održavanja sigurnosti, ali i takve mjere su podložne propustima - unatoč svemu, greške se javljaju. Čak bismo mogli reći da su za propuste u tehničkim mjerama sigurnosti informacionih sistema često odgovorni ljudi. Računari sami po sebi ne implementiraju sigurnosne politike i

procedure - potrebni su ljudi da nabavljaju i konfigurišu sisteme, pokreću kontrolne funkcije, nadziru i prate alerte. Gledano sa stanovišta rizika, ljudi kreiraju prijetnje, ranjivosti i uticaj.

Prijetnje informacionim sistemima

Kako bismo sigurnosne prijetnje mogli otkloniti, prvo ih moramo znati prepoznati.
Prijetnje informacionim sistemima možemo podijeliti prema izvoru na:

- namjerne ljudske radnje,
- nenamjerne ljudske radnje,
- tehničke uzroke i
- prirodne katastrofe.

Zadržimo se na prijetnjama koje uzrokuju ljudski resursi, bilo namjernim djelovanjem (neautorizovanim pristupom, sabotažom, špijunažom, prevarom, krađom, malicioznim kodom, uništavanjem, ratnim razaranjem) ili nenamjernim djelovanjem (nepažnjom, neposlušnošću, neznanjem, kršenjem pravila, neprimjerenim programima, lošom organizacijom).
Prema mjestu nastanka, prijetnje koje uzrokuju ljudski resursi mogu biti unutrašnje (namjerne i nenamjerne radnje korisnika koji imaju direktan pristup informacionom sistemu) i vanjske (svi pokušaji nanošenja bilo kakvog oblika štete udaljenim napadima ili ubacivanjem zlonamjernih programa u informacioni sistem s udaljenih lokacija).

Lifeware

Ljudske resurse kao živu komponentu informacionog sistema, koja podrazumijeva sve ljude koji su uključeni u rad informacionog sistema

(operatori, programeri ili administratori) te sve osobe koje imaju doticaja sa imovinom i podacima organizacije (poslovne partnere, klijente, dobavljače), jednim informatičkim terminom nazivamo *lifeware*.

Čovjek je osnovna komponenta informacionog sistema - x faktor na koga se mora računati. On pretvara poslovno okruženje u podatke i informacije te uz pomoć tehnologije stiče nova znanja koja mu pomažu da donosi poslovne odluke i izvršava svoje poslovne zadatke. Međutim, ljudi su i oni koji kreiraju i šalju *malware*, oni koji nepažljivo rukuju elektronskom poštom i povjerljivim informacijama, ali i oni koji gube svoje mobilne uređaje. Ljudi, također, znaju biti i takmičarski nastrojeni, nositi posao kući, a time i iznositi podatke organizacije te na taj način izlagati organizaciju povećanom riziku. Zlonamjerne radnje malicioznih pojedinaca, nezadovoljnih, neposlušnih ili bivših zaposlenika su problem, ali je za većinu krađa podataka zaslužan nemar, nepažnja, neznanje, kršenje pravila i prezaposlenost uz kontinuirani nedostatak edukacije o sigurnosti informacionog sistema.

> *„Čovjek je osnovna komponenta informacionog sistema - x faktor na koga se mora računati. On pretvara poslovno okruženje u podatke i informacije te uz pomoć tehnologije stiče nova znanja koja mu pomažu da donosi poslovne odluke i izvršava svoje poslovne zadatke."*

Prema raznim statistikama oko 40% slučajeva narušavanja podataka nastaje zbog djelovanja ljudskog faktora. Rizik predstavljaju ne samo zaposlenici, nego i klijenti, poslovni partneri, dostavljači, te ostale osobe koje imaju doticaja s imovinom i podacima organizacije. Bilo nenamjernim ili namjernim djelovanjem radi zadovoljstva, lične koristi ili iz nekog drugog razloga, ljudi čine veliku prijetnju informacionom sistemu.

Socijalni inžinjering

Zlonamjerni korisnici služe se različitim tehnikama i iskorištavaju različite ranjivosti

> *Socijalni inžinjering je najefikasnija metoda napada protiv najranjivije komponente informacionog sistema – ljudskog faktora.*

kako bi dobili pristup informacionom sistemu, izveli nedozvoljene akcije ili otkrili povjerljive informacije. U cilju pripreme za napad često koriste razne metode socijalnog inžinjeringa. Osnovni koncept socijalnog inžinjeringa kaže da su postupci ljudi i njihove reakcije na vanjski uticaj, u većini slučajeva, predvidljivi. Susretljivog *help-desk* operatera lako je nagovoriti da oda povjerljive informacije potpunom strancu. Socijalni inžinjering je najefikasnija metoda napada protiv najranjivije komponente informacionog sistema – ljudskog faktora.

Zašto je ljudski faktor tako ranjiv? Krivac za ranjivost je sama ljudska priroda, a socijalni inžinjering predstavlja upravo vještinu manipulisanja ljudskom prirodom, tj. psihološkim osobinama čovjeka koje ga čine podložnim ovakvoj vrsti napada.

Profesor psihologije i marketinga na univerzitetima u Arizoni, Stantfordu i Kaliforniji, **Robert Cialdini**, u svojoj knjizi *Influence: The Psychology of Persuasion,* postavio je šest osnovnih principa na kojima se zasniva socijalni inženjering:

- reciprocitet (ljudi žele uzvratiti uslugu),
- dosljednost (ljudi, u želji da ispoštuju dogovor, previde štetne posljedice svog djelovanja),
- društveno dokazivanje (nesigurne osobe žele ostaviti utisak samopouzdanja ili samouvjerenosti pa u toj svojoj želji učine pogrešnu ili štetnu aktivnost),
- autoritet (ljudi su naučeni da poštuju autoritete, čak i ako se od njih traži da izvrše nepoželjne radnje),
- privlačenje (što se ljudima više sviđa osoba koja ih ubjeđuje u nešto, to su oni skloniji povjerovati joj),
- nedostatak (privid ograničene ponude stvara potražnju).

Karakteristike ljudskog ponašanja stavljaju ljudske resurse u poziciju najslabije karike sigurnosti informacionog sistema. Vidimo da je lakše hakirati osobu nego njen računar.

Popularnost društvenih mreža direktno pomaže efikasnosti socijalnog inžinjeringa. Društvene mreže i servisi nas poznaju bolje nego što poznajemo sami sebe. Interakcijama koje svakoga dana napravimo na društvenim mrežama stva-

ramo jedinstveni digitalni otisak. Prema njemu se mogu predvidjeti naše želje do te mjere da budemo uvjereni da nas prisluškuju. Oslanjajući se na podatke stalno rastućih društvenih mreža te zahvaljujući konstantnoj prijetnji koju nose ljudske pogreške, socijalni inžinjering ima zabrinjavajuće svijetlu budućnost.

Iskorištavanjem ljudskih ranjivosti omogućava se pristup informacionom sistemu bez obzira na nivo sigurnosti koji je organizacija uvela. Ljudi ostaju primarna meta napadača, kao i zadnja odbrana organizacije od napada na informacioni sistem.

Da bi se odgovorilo ovim prijetnjama, potrebno je odabrati holistički pristup odbrane te ulagati kako u sigurnosne procedure i alate tako i u edukaciju korisnika i podizanje svijesti o sigurnosti informacionog sistema.

Ključ je u edukaciji

Kevin Mitnick, danas stručnjak za računarsku sigurnost, a ranije *hacker* i *cracker*, u svojoj najpopularnijoj knjizi *The Art of Deception: Controlling the Human Element of Security* objašnjava da je najjednostavniji način za ulazak u tehnološki zaštićene informacione sisteme preko ljudi koji te sisteme koriste i njima upravljaju.

> *Podizanjem svijesti o sigurnosti i edukacijom zaposlenika smanjujemo vjerovatnoću grešaka kojima se ugrožava integritet i sigurnost sistema te se najbolje pripremamo za odbranu od napada socijalnog inžinjeringa.*

Tehničke mjere sigurnosti same po sebi ne mogu biti dovoljna garancija za sigurnost informacionih sistema. Podizanjem svijesti o sigurnosti i edukacijom zaposlenika smanjujemo vjerovatnoću grešaka kojima se ugrožava integritet i sigurnost sistema te se najbolje pripremamo za odbranu od napada socijalnog inžinjeringa. Meta socijalnog inžinjeringa može biti svako i zato je važno educirati sve zaposlenike da poštuju pravila koja će učiniti sistem otporni(ji)m na napade.

Šta možete izgubiti? Skoro sve: lične informacije i povjerljive kredencijale, ali i povjerljive informacije poslodavca što može narušiti ugled organizacije i njenu prednost na tržištu. A šta bismo trebali učiniti da se zaštitimo od socijalnog inžinjeringa?

Think Before You Click, Check Before You Act

Pametno i odgovorno korištenje tehnologije koja nas okružuje rizike svodi na minimum. Bitno je biti svjestan opasnosti socijalnog inžinjeringa, sumnjičav i oprezan pri bilo kakvim zahtjevima za novcem, *passwordima*, brojevima računa ili drugim osjetljivim informacijama bez obzira od koga su upućeni. Socijalni inžinjering najčešće koristi ljude kojima najviše vjerujemo. Budite svjesni i informacija koje se o vama mogu pronaći putem društvenih mreža. Kada dobijete e-*mail*, čak i od nekoga koga poznajete ili od organizacije u koju imate povjerenja, uvijek zastanite; pogledajte još jednom; razmislite da li smijete reći nešto što se od vas traži te se ponašajte prema pravilima i prijavite svaku sumnjivu radnju, upit, e-*mail* ili zahtjev. Poštujte sigurnosne politike, pravilnike i procedure; često mijenjajte *passworde*; enkriptirajte i *patchirajte*; podesite opcije privatnosti na društvenim mrežama i uvijek provjerite prije nego što reagujete.

Oprezno i promišljeno ponašanje unutar svojih ovlaštenja, uz poštovanje politika i procedura, doprinosi sigurnosti informacionog sistema. Od velikog značaja je ulaganje u tehnološke mjere zaštite sigurnosti informacionog sistema, znanje i vještine informatičkih stručnjaka, ali i u podizanje svijesti krajnjih korisnika o sigurnosti informacionog sistema.

Svi napori u borbi da zaštitimo informacioni sistem efikasni su onoliko koliko je oprezan svaki pojedinačni korisnik informacionog sistema. Možemo s pravom reći da najslabija karika može prekinuti i najjači lanac. ■

Sigurnost za IT, jednostavnost za korisnika - manje glavobolje za sve

MULTIFAKTORSKA AUTENTIFIKACIJA – NAJBOLJA PRAKSA ZA PREVENCIJU NEAUTORIZOVANOG PRISTUPA

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

Autorica:
Sanela Vrana

MULTIFAKTORSKA AUTENTIFIKACIJA PRIZNATA JE KAO NAJSIGURNIJA METODA ZA KONTROLU PRISTUPA PODACIMA I APLIKACIJAMA

Ne ostavljajte 'ključ ispod otirača'!

Autentifikacija predstavlja proces utvrđivanja istinitosti nečije tvrdnje o svom identitetu. *Username* i *password* su primjer najjednostavnijeg načina autentifikacije – jednostruke autentifikacije (SFA – *single factor authentication*). *Password*, kao najčešće korišteni način kontrole pristupa, ujedno je i najranjivija tačka u arhitekturi sigurnosti informacionog sistema.

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

Password nam daje dodatnu sigurnost kod korištenja *online* usluge ili pristupa traženom uređaju, ali vrlo lako može biti „dvosjekli mač“ ukoliko ga ne koristimo odgovorno i oprezno te može nanijeti više štete nego koristi.

Korisnici i njihovi *passwordi* su najslabija karika u sigurnosti informacionog sistema i mogu uzrokovati da ostane nejasno ko stvarno koristi sistem i pristupa podacima i aplikacijama. Iz izvještaja o povredama podataka uzrokovanim *cyber security* napadima možemo saznati da se 80% njih odnosi na korištenje ukradenih *passworda* i slabih *passworda*, tj. onih koji se lako otkrivaju. *Cyber* kriminalci koriste metode socijalnog inžinjeringa, tj. manipulišu ljudskom prirodom: povjerenjem, radoznalošću, strahom, velikodušnošću ili čak dobrotom kako bi došli do naših kredencijala, do našeg novca ili novca poslodavca. Ranjivost *passworda* leži u činjenici da isti ne obezbjeđuje jedinstven identitet korisnika. Bilo ko da dođe u posjed *passworda* može pristupiti računu, uređaju ili usluzi. Često je sigurnost *passworda* ugrožena već od strane njegovog vlasnika izborom lako pamtljivih riječi umjesto jedinstvenih nizova brojeva, karaktera i simbola.

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

Zašto je multifaktorska autentifikacija tako važna?

Odgovor je vrlo jednostavan: jednostruka autentifikacija više nije dovoljna. Logiranje, odnosno spajanje na određenu *online* aplikaciju, servis ili nešto treće samo s korisničkim imenom i *passwordom* više nije sigurno. Sve veći poslovni zahtjevi, sve veći broj servisa koji se iz svakodnevnog života sele u digitalni svijet te svakodnevna

pojava novih prijetnji, rizika i ranjivosti upućuju na stalnu potrebu osnaživanja pristupa provjere identiteta, zadržavajući pri tom zahtjev za jednostavnim korištenjem i neometanim pružanjem usluga. Zato se uvodi dvofaktorska (dvostruka) ili multifaktorska (višestruka) autentifikacija kako bi se onemogućio neovlašteni pristup pod nečijim tuđim identitetom.

Šta je multifaktorska autentifikacija (MFA)?

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

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

Dvofaktorska autentifikacija (2FA) je najjednostavnija i najčešće korištena forma multifaktorske autentifikacije (MFA). Najobičniji primjer dvofaktorske autentifikacije je povlačenje novca sa ATM uređaja koje zahtijeva od korisnika da potvrdi svoj identitet fizičkim ubacivanjem kartice i unosom PIN-a. Najčešći primjer dvofaktorske autentifikacije u *online* uslugama je dvostruka digitalna autentifikacija uz pomoć *passworda* i koda koji je poslan korisniku na neki od njegovih uređaja u formi teksta. Dvofaktorska autentifikacija je, na neki način, podskup metoda multifaktorske autentifikacije. Multifaktorska autentifikacija je, s druge strane, autentifikacija koja

> *Multifaktorska autentifikacija priznata je kao najsigurniji metod za kontrolu pristupa podacima i aplikacijama, a predstavlja naprednu proceduru kontrole pristupa koja potvrđuje identitet korisnika kombinujući više jedinstvenih faktora.*

zahtijeva provjeru i potvrdu više parametara/faktora.

Iako dvofaktorska autentifikacija ima značajne prednosti nad jednostrukom autentifikacijom (SFA – *single factor authentication*), ona i dalje predstavlja određeni stepen ranjivosti, pogotovo zbog toga što zahtijeva prisustvo mobilnog uređaja koji može biti ukraden ili tehnički neispravan.

Kako radi multifaktorska autentifikacija?

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

> *Upotrebljavajući više nezavisnih faktora prilikom autentifikacije, praktično onemogućavamo da se neko drugi predstavi, odnosno logira umjesto nas.*

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

Upotrebljavajući više nezavisnih faktora prilikom autentifikacije, praktično onemogućavamo da se neko drugi predstavi, odnosno logira umjesto nas. Broj nezavisnih faktora je jako važan jer što ih je više to je manja vjerovatnoća da će svi biti otuđeni istovremeno, a to je ključno u konceptu multifaktorske autentifikacije.

Neki od faktora su u ***virtuelnom svijetu*** (npr. *password* koji se može ukrasti), a neki su u ***realnom svijetu*** (npr. mobilni uređaj, token i sl.) i do njih je već teže doći. U tom slučaju korisnik posjeduje nešto što nema niti onaj ko pruža određenu uslugu te se samim tim ne može ni otuđiti iz sistema i iskoristiti umjesto ili protiv korisnika. Dodatna sigurnost je kratki vremenski period za koji vrijedi generisani kod poslan na neki od

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

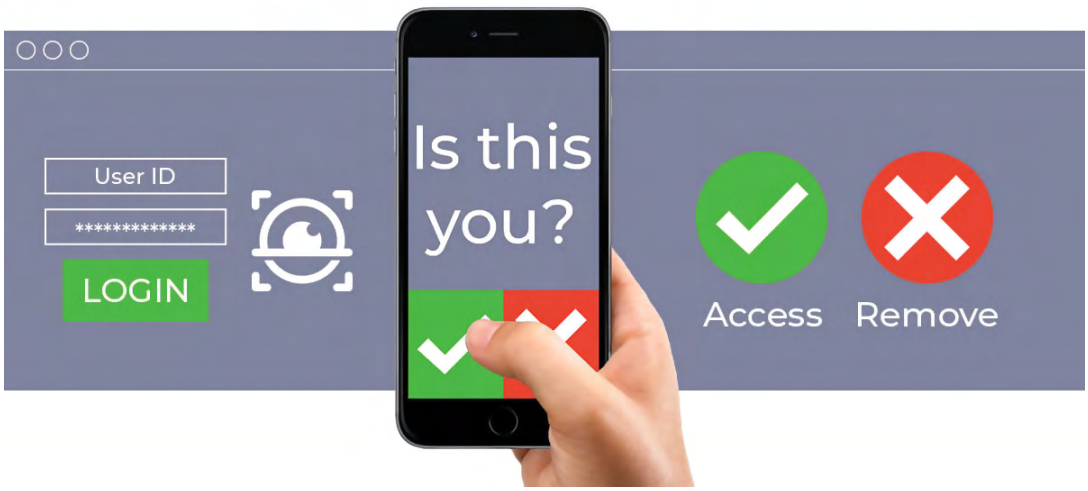
Kada je riječ o biometriji, ona se kod *online* servisa rijetko koristi (jer je teško obezbijediti da svi klijenti posjeduju čitač otiska prsta ili nešto slično), ali u velikim kompanijama i sistemima biometrija ulazi na velika vrata i koristi se često za onemogućavanje pristupa dijelovima kompanije za čiji pristup korisnici nemaju ovlaštenje. Cijene biometrijskih rješenja su u padu širom svijeta, a napredak je svakodnevan u segmentu kontaktnih i beskontaktnih rješenja. Jedno od najčešće korištenih kontaktnih rješenja su otisci prstiju. Beskontaktna biometrijska rješenja su u prvom redu skeniranje šarenice oka i prepoznavanje lica, pri čemu biometrija doživljava uspon u segmentu prepoznavanja lica, a čini se da koncept skeniranja šarenice oka ne spada više u rastuću tehnologiju.

Integracija sigurnosnih rješenja kontrole pristupa

Savršen sistem autentifikacije ne postoji jer ga kreira čovjek pa ga čovjek može i probiti. Ono što možemo učiniti jeste primijeniti snažan multifaktorski sistem autentifikacije te educirati korisnike o najnovijim opasnostima kao i najnovijim trendovima sigurnosti.

Budućnost nam donosi integraciju različitih sistema kontrole pristupa, videonadzora, kontrole perimetara, a menadžerima sigurnosti se na taj način olakšava nadzor i obezbjeđuje holistički pregled situacije.

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



Ransomware

SPREČAVANJE PRANJA NOVCA DIGITALNE VALUTE

Suočavamo se sa sve većim razmjerama i oblicima narušavanja integriteta i zlouporabe međunarodnog finansijskog sistema. Ni kriptovalute nisu pošteđene od krađe i zloupotrebe.

Autorica:
Sanela Stupar

Kako hakerske grupe unovče zaradu, a da ne budu identificirane

Ransomware je jedna od najraširenijih vrsta *cyber* kriminala. Korištenjem visoko automatizovanog i lako distribuiranog *malwarea* za kripto zaključavanje i za prisilno šifriranje sistema, napadači mogu tražiti otkupninu u *bitcoinama* u zamjenu za ključeve dešifriranja.

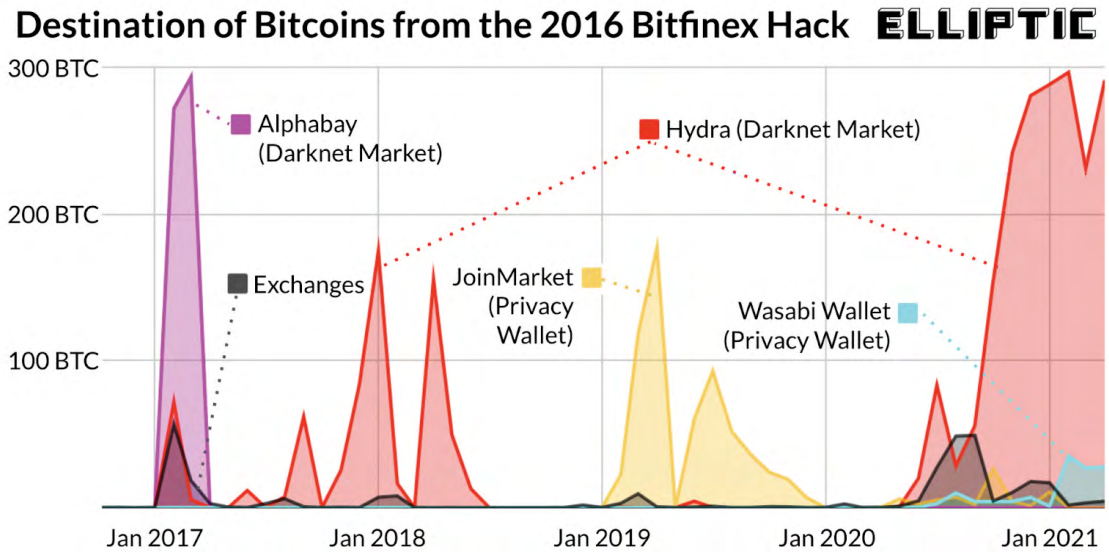
Organizacije i pojedinci, koji su žrtve hakerskih napada, uplaćuju otkupninu na jedinstvenu *bitcoin* adresu. Hakerske grupe koje vode *ransomware* kampanju obično sve uplate usmjeravaju na tri vrste aktera:

1. darknet tržišta (84%),
2. privatne novčanike (12%) i
3. razmjene (4%).

1. Darknet tržišta

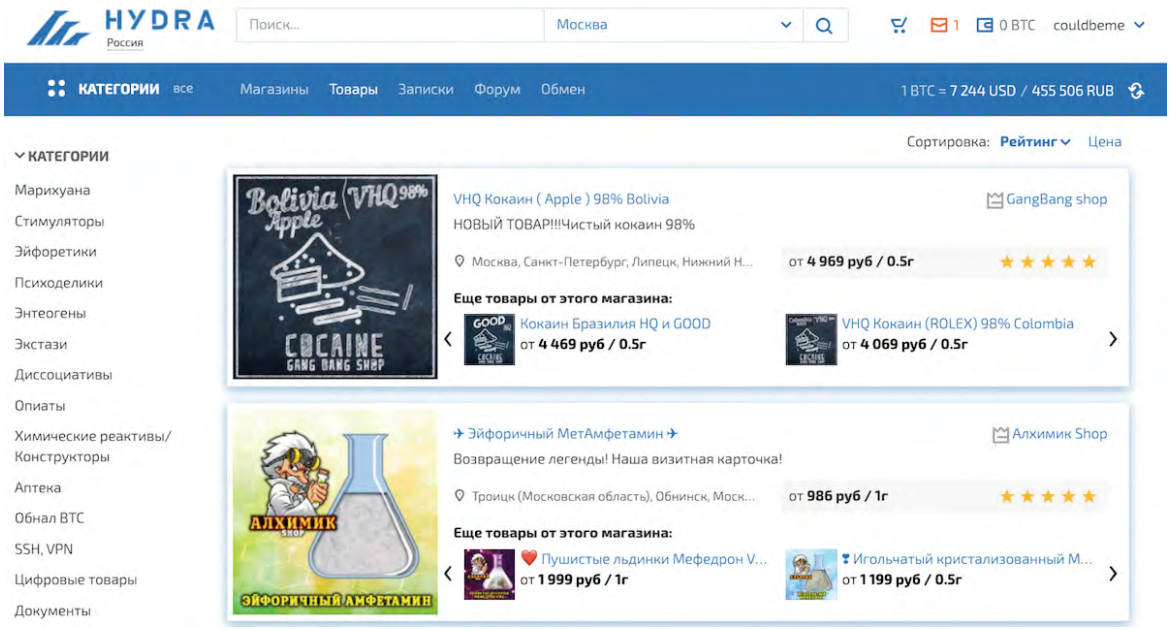
Pranje ukradenih novčanih sredstava zabilježeno je u 2017. godini na **Alphabayu**, najvećem aktivnom tržištu *darkneta*[1] u to vrijeme. Kada je Alphabay ugašena od strane regulatora, praonice su prešle na **Hydra**, najveće rusko *darknet* tržište koje danas posluje.

[1] ***Dark web*** *je dio duboke mreže (Deep Web) i čini ga sadržaj koji je namjerno sakriven i pristup mu je moguć isključivo uz korištenje određenih alata i programa. https://repozitorij.unizg.hr/islandora/object/ffzg:2638/datastream/PDF*



Hydra omogućava pretvaranje *bitcoina* u poklon-bonove, *pripejd* debitne kartice ili gotov novac. Hydra tržišta nude usluge isplate uz narkotike, alate za hakiranje, kreditne kartice, zdravstvene kartice i lažne lične karte.

Prema istraživanjima sigurnosnih kompanija, do kraja marta 2021. godine preko Hydre izvršeno je oko 720 miliona dolara transfera ukradenih bitkoina.



2. Privatni novčanici

Bitfinex bitcoina su novčanici koji štite privatnost korisnika - prvenstveno *JoinMarket* i *Wasabi* novčanik. Navedeni softverski novčanici pomažu u sprečavanju *blockchaina.*

```
0.1 BTC (Alice)        0.1 BTC (Anon set 3)
0.3 BTC (Bob)      ->  0.1 BTC (Anon set 3)
0.4 BTC (Charlie)      0.1 BTC (Anon set 3)
                       0.2 BTC (Change Coin Bob)
                       0.3 BTC (Change Coin Charlie)
```

3. Razmjene

Razmjene predstavljaju najmanju kategoriju odredišta za ukradena sredstva. *Blockchain* analitikom mogu se identifikovati depoziti proistekli iz kriminalnih aktivnosti. Iz tih razloga, razmjene koje su u posljednjih pet godina primile ukradene *Bitfinex bitcoine* uglavnom su one sa sjedištem u jurisdikcijama u kojima kripto poslovanje još uvijek nije strogo regulirano. Međutim, mali dio ukradenih sredstava otišao je na dobro regulisane berze. Te transakcije predstavljaju važne tragove za istražitelje koji žele identificirati hakerske organizacije.

Tri su glavne faze kripto pranja novca:

Plasman
Kriptovalute se mogu kupiti gotovinom (*fiat*) ili drugim kripto vrstama (*altcoin*). Tržišta (berze) internetske trgovine kriptovalutama imaju različite nivoe usklađenosti s propisima koji se odnose na finansijske transakcije.

Legitimne razmjene slijede regulatorne zahtjeve za provjeru identiteta i izvor sredstava te su u skladu s AML-om. Druge razmjene nisu u skladu s AML-om niti se trude da budu. Više su fokusirane na njihovu tekuću borbu da prekorače propise o usklađenosti sa podalatima. Ova ranjivost je mjesto gdje se odvija većina transakcija povezanih s pranjem novca od *bitcoina*. Kada su razmjene regulisane, oni moraju primijeniti KYC politike i protokole na svoje kupce. To omogućava podudaranje podataka o transakciji s odgovarajućim kupcem čime se prekida *anonimnost* za svaku transakciju. U *Ellipticu* ne pohranjujemo podatke o kupcima nego umjesto toga koristimo ID-ove kupaca (koje pružaju razmjene) kako bi se podudarali s podacima o transakcijama.

Skrivanje
Transakcije zasnovane na kriptografiji mogu se generalno pratiti putem *blockchaina*. Međutim, kad je prljava kriptovaluta u igri, kriminalci mogu koristiti uslugu anonimiziranja kako bi sakrili izvor sredstava, prekidajući veze između *bitcoin* transakcija. Često je glavni izgovor za nedozvoljene aktivnosti skrivanja argument da upotreba anonimnih pružatelja usluga štiti privatnost.

To se može postići na redovnoj kripto berzi ili sudjelovanjem u početnoj ponudi kovanica (ICO) gdje upotreba jedne vrste kovanica za plaćanje druge vrste može

zatamniti porijeklo digitalne valute.

Integracija
Tačka u kojoj više ne možete lako pratiti prljavu valutu natrag do kriminalnih radnji je tačka integracije - *završna faza pranja valute.*

Uprkos tome što valuta više nije izravno vezana za kriminal, praonice novca i dalje trebaju naći način da objasne kako su došle u posjed valute. Integracija je to objašnjenje.

Jednostavna metoda legitimisanja nezakonitog dohotka je predstavljati ga kao rezultat profitabilnog poduhvata ili druge aprecijacije valute. To je vrlo teško opovrgnuti na tržištu kada se vrijednost bilo kojeg datog *altcoina* može mijenjati svake sekunde.

Alternativno, slično onome kako se *off-shore* bankovni račun u *fiat* valuti može koristiti za pranje prljavog novca, internetska kompanija koja prihvaća *bitcoin* plaćanja može se stvoriti kako bi legitimirala prihod i transformirala prljavu kriptovalutu u čisti, legalni *bitcoin*.

Regulativa u borbi protiv pranja novca, finansiranja terorizma te finansiranja proliferacije

Suočena sa sve većim razmjerama i oblicima narušavanja integriteta i zlouporabe međunarodnog finansijskog sistema, međunarodna zajednica odlučila je ojačati aktivnosti na planu borbe protiv pranja novca, finansiranja terorizma te finansiranja proliferacije. Dana 21. juna 2019. godine **FATF**[2] je objavila ažurirane smjernice za virtualnu imovinu i pružatelje usluga virtualne imovine.

FATF-ove nove smjernice imaju za cilj pružanje pomoći regulatorima (*Virtual Asset Service Providers*).

Financial Conduct Authority (FCA) predlaže da razmjene kriptoaseta i skrbnici novčanika koji posluju u zemlji preuzimaju dodatne obaveze izvještavanja i pružaju agenciji više informacija o rizicima pranja novca za njihovo poslovanje. Konkretno, svi pružatelji usluga virtualne imovine (VASP - *Virtual Asset Service Providers*, izraz koji uključuje razmjene

kriptovaluta, pružatelje skrbničkih novčanika, itd.) moraju FCA-u dostaviti izvještaj o svom riziku od finansijskog kriminala bez obzira na njihov ukupni godišnji prihod. Prema FCA-ovom prijedlogu, izvještaj bi trebao sadržavati informacije poput segmentacije kupaca, naprimjer koliko je kupaca sa sjedištem u visoko rizičnim jurisdikcijama, broj kupaca koji su odbili uslugu ili otkazali zbog finansijskog kriminala, kao i vrste kriminala i rizike (npr. prevare) povezane s određenim novčanicima ili kupcima.

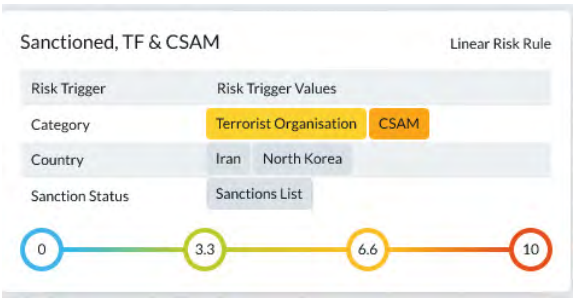
U cilju usklađenosti poslovanja i upravljanja rizikom, pružatelji usluga virtualne imovine koriste sigurnosne alate za dubinsku analizu kripto novčanika kako bi spriječili pranje novca, sankcije regulatora i prevare prije nego što se transakcija održi.

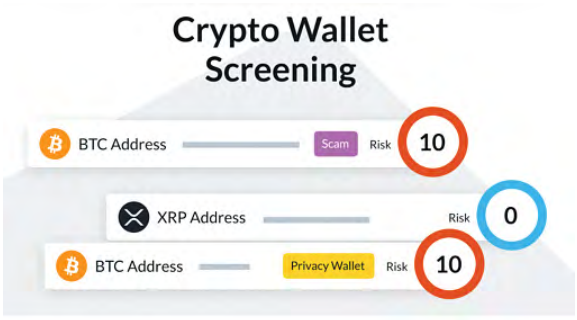
[2] ***FATF*** *– Financial Action Task Force (Projektna grupa za finansijsko postupanje) je organizacija s 36 članica i učestvovanje preko 180 zemalja kroz globalnu mrežu regionalnih tijela.*

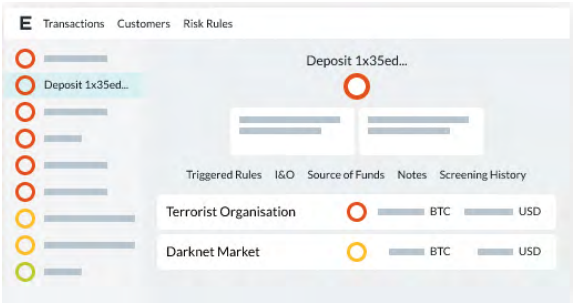
Izdvajamo kompaniju **Elliptic** koja je identificirala *bitcoin* novčanik koji koristi *DarkSide ransomware* grupa za primanje otkupnina od svojih žrtava.

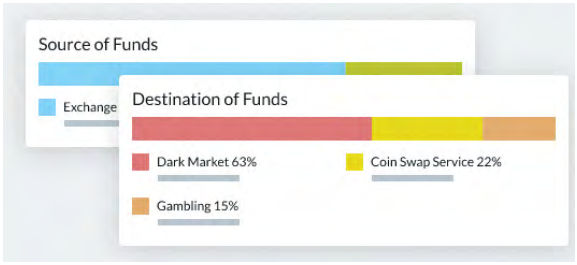
Elliptic softversko rješenje za nadgledanje transakcija *kriptoasseta* za kripto preduzeća i financijske institucije sadrži:

- otkrivanje kripto transakcija visokog rizika,
- identifikaciju visoko rizičnih kupaca,
- pregled transakcije - odakle je došla ili gdje se šalje praćenjem putem *blockchaina* kako bi se utvrdili krajnji izvor ili odredište sredstava,
- revizorski trag kripto transakcije.









Zanimljivosti

Sjevernokorejska hakerska grupa pod nazivom **Lazarus Group** optužena je za pljačku na berzi kriptovaluta **KuCoin**, nazvanu najvećom krađom kriptovaluta prošle godine s virtualnim novcem u vrijednosti od 275 miliona dolara. Ta brojka predstavlja polovinu od ukupnog broja ukradenih kriptovaluta u 2020. godini, prema podacima za praćenje kriptovaluta i dobavljača zakona *Chainalysis*.[3]

[3] ***FATF** – Financial Action Task Force (Projektna grupa za finansijsko postupanje) je organizacija s 36 članica i učestvovanje preko 180 zemalja kroz globalnu mrežu regionalnih tijela.*

Intervju

SANJA ĆATIBOVIĆ
– PROGRAMSKA SLUŽBENICA PRI ODJELU ZA SIGURNOSNU SARADNJU, MISIJA OSCE-A U BOSNI I HERCEGOVINI

Iskusna članica OSCE-a sa demonstriranom istorijom rada u vojno-političkoj dimenziji i oblasti sigurnosne saradnje. Sveobuhvatno razumijevanje vrijednosti, normi i struktura OSCE-a, stečenih tokom više od dvije decenije profesionalnog angažmana u Organizaciji. Stručno znanje u političko-vojnim aspektima sigurnosti, demokratskom nadzoru, kontroli naoružanja, mjerama izgradnje povjerenja i sigurnosti, kao i cyber sigurnosti.

Nosilac univerzitetske diplome u mašinskom, vazduhoplovnom inženjerstvu.

U toku ovog rada, stekla je značajna teorijska i praktična znanja o dimenzijama sigurnosti OSCE-a i o poštivanju međunarodnih, multilateralnih sigurnosnih obaveza.
Pohađala i stekla diplome škola, treninga i kurseva u oblasti sigurnosti, od kojih su neki:

- "Vojna doktrina", Državna akademija odbrane u Austriji;
- "Reforma sigurnosnog sektora", European Security and Defence College -Evropski koledž za odbranu i sigurnost;
- "Inicijativa razvoja sigurnosnog obrazovanja", Četverogodišnja ljetna škola Centra za sigurnosne studije;
- "Kurs o sigurnosnoj saradnji", NATO škola u Oberamergau;
- i niz drugih kurseva, inicijativa i edukativnih institucija, uključujući "Trening o diplomatskim vještinama"- The United States Institute of Peace; Evropske integracije i EU IPA fondovi i The Open University UK- Cyber sigurnost.

Aktivno uključena u podršku razvoju Strateškog okvira za cyber sigurnost u Bosni i Hercegovini, u okviru neformalne ekspertne grupe koja djeluje pod okriljem Misije OSCE-a u BiH.

Član i jedan od osnivača Međunarodne neformalne koordinacione grupe stručnjaka za IKT i cyber sigurnost u BiH.

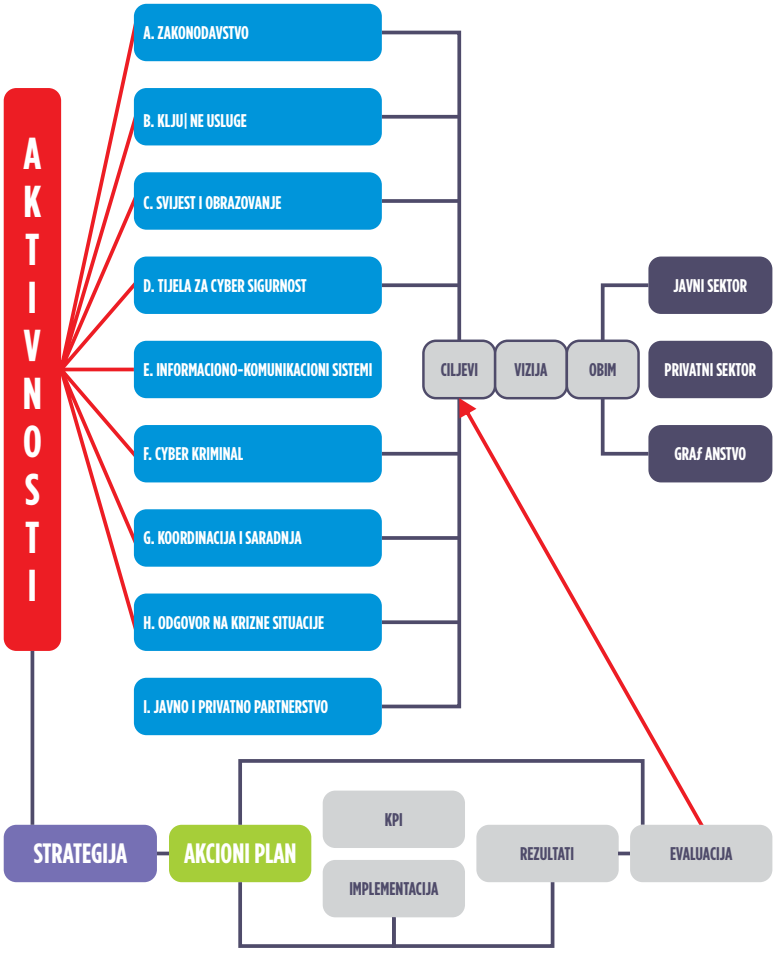
FRAUDINFO: OSCE u BiH ima misiju za oblast Cyber/ IKT sigurnosti. Da li nam možete o tome nešto više reći

Sanja: Naša podrška unapređenju cyber sigurnosti u BiH je sve sistematičnija, imajući u vidu eksponencijalni rast prijetnji iz cyber prostora i trenutno ograničeni kapacitet BiH da se pozabavi takvim prijetnjama i da na njih odgovori. Mi pomažemo BiH u izradi strateških politika djelovanja i ključnih mehanizama u oblasti cyber sigurnosti, u skladu sa relevantnim standardima i međunarodnim obavezama BiH. To, na primjer, uključuje izradu ključnih smjernica za strateški okvir cyber sigurnosti, koji sada služi kao osnova za izradu relevantnih strategija i akcionih planova na različitim nivoima vlasti.

Mi u velikoj mjeri stavljamo naglasak na poboljšanje međuagencijske i multisektorske saradnje o pitanjima cyber sigurnosti, pošto je to ključno za efektivnu implementaciju srodnih okvira politika djelovanja.

Takođe radimo na unapređenju kapaciteta za pružanje obuke u svrhu borbe protiv cyber kriminala i cyberom omogućenog kriminala, naročito kroz stručno usavršavanje praktičara i predavača iz oblasti krivičnog prava.

Nadamo se i očekujemo da će naša podrška i zastupanje stava o potrebi uspostavljanja i operacionalizacije timova za odgovor na računarske incidente (CERT) u BiH uskoro dovesti do određenih ključnih rezultata, stavljajući u funkciju kapacitete neophodne za pravovremenu i djelotvornu prevenciju i odgovor na IKT/ cyber incidente i napade.



FRAUDINFO: Koje su obaveze BiH u oblasti cyber sigurnosti?

Sanja: Bosna i Hercegovina je dio sigurnosne zajednice OSCE - a, što naravno također znači i odgovornost za provedbu obaveza OSCE-a proizašlih iz odluka Ministarskog vijeća OSCE-a o povećanju napora na smanjenju rizika od sukoba zbog korištenja IKT-a. BiH također izražava predanost poštovanju dogovorenih Mjera za izgradnju povjerenja (CBMs-a) koje se odnose na cyber sigurnost i IKT sigurnost, u cilju povećanja predvidljivosti i transparentnosti i smanjenja pogrešnih percepcija i sukoba u cyber domeni.

U svjetlu procesa pristupanja EU, BiH je također izrazila odlučnost da se primjenjuju mjere za visoki nivo sigurnosti mrežnih i informacionih sistema širom Unije (NIS Direktiva [EU] 2016/1148 Europskog parlamenta i Vijeća) i ispuni Opštu direktivu o zaštiti podataka (Direktiva[EU] 2016/679).

BiH ima za cilj i implementirati Konvenciju Vijeća Evrope o cyber-kriminalu koja služi kao smjernica za bilo koju zemlju koja razvija državno zakonodavstvo i saradnju u borbi protiv cyber-kriminala (tj. Budimpeštanska konvencija).

FRAUDINFO: Pod pokroviteljstvom Misije OSCE-a pripremljene su i usvojene Smjernice za strateški okvir cyber sigurnosti u BiH. Možete li nam nešto vise reći o Smjernicama?

Sanja: Sa zadovoljstvom i ponosom naglašavam da su Smjernice nastale kao rezultat konstruktivnih pregovora i postignutog kompromisa. Vizija Strateškog okvira za cyber sigurnost u Bosni i Hercegovini je prilagođena

da odgovori realnim potrebama i potencijalnim prijetnjama, kao i međunarodnim obavezama i standardima u oblasti cyber sigurnosti. Cilj Smjernica je da se osigura strateški i zakonski okvir, te unaprijede procedure i tehnike u cilju zaštite informaciono-komunikacionih sistema i krajnjih korisnika. Takva vizija je ključna za smanjenje rizika i poboljšanje zaštite privatnosti. Ona istovremeno pomaže promovisanju tehničke inovacije, omogućavajući lakšu komunikaciju, ekonomski razvoj i transparentnost, time unapređujući sigurnost pojedinaca, institucija i kompanija.

U Izvještaju Evropske komisije o napretku Bosne i Hercegovine već 2016. godine je naglašeno da „Bosna i Hercegovina nema sveobuhvatni strateški pristup za rješavanje pitanja prijetnji u oblasti cyber kriminala i cyber sigurnosti.“ Navodi se potreba da se ojača odgovor na takve prijetnje , pa i povećanjem kapaciteta za borbu protiv cyber kriminala, kao i kapacitete timova za prevenciju i zaštitu od cyber incidenata i prijetnji sigurnosti javnih informacijskih sistema (CERT/CSIRT)[1].

Postojeći ljudski i materijalni resursi i kapaciteti institucija, u različitim sektorima, trenutno nisu dovoljni da osiguraju potreban nivo sigurnosti u cyber prostoru u Bosni i Hercegovini. Različiti nivoi vlasti imaju različite nivoe pripremljenosti, koji su doveli do različitog pristupa u osiguranju cyber sigurnost. Kao posljedica ovog nedostatka koherentnosti, postoji nejednak i nezadovoljavajući nivo zaštite korisnika, kako u javnom, tako i u privatnom sektoru. To podriva ukupni nivo zaštite u cyber prostoru, vodeći ka većoj ranjivosti na prijetnje i napade, te nepravovremenom djelovanju. Osim nedovoljne saradnje i koordinacije sa ostalim državama u regiji i svijetu. Bosna i Hercegovina je jedina zemlja u Evropi koja nema uspostavljen sveobuhvatan CSIRT sistem, drugim riječima, sistem pomoći korisnicima interneta u Bosni i Hercegovini u primjeni proaktivnih mjera za smanjivanje rizika od kompjutersko-sigurnosnih incidenata te hvatanje u koštac sa posljedicama nastalih kompjutersko-sigurnosnih incidenata.[2]

Smjernice za strateški okvir cyber sigurnosti su primijenile iskustva i dobre prakse zemalja koje su već usvojile i primjenjuju strategije u oblasti cyber sigurnosti. Dokument definiše ciljeve i aktivnosti koji će dovesti do efikasnog i provedivog strateškog okvira, odnosno do opipljivih i mjerljivih rezultata upravljanja sistemom cyber sigurnosti. Takvo upravljanje će se ogledati u provođenju projekata i njihovih različitih faza, koje se odnose se na: izradu, evaluaciju i prilagođavanje. Time ovaj dokument predstavlja dobar strateški okvir uspostave efikasnog sistema za cyber sigurnost. On je baziran na NIS direktivi, te vodiču najboljih praksi ENISA-e, kao i na pozitivnim praksama zemalja EU,

[1] *CERT (eng. Computer Emergency Response Team) ili CSIRT (engl. Computer Security Incident Response Team)*

[2] *ENISA, CSIRTs by Country - Interactive Map, dostupno na: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.*

te zemalja iz okruženja koje su već ranije donijele strategije i uspostavile odgovarajuće mehanizme kao odgovor na cyber napade.

Smjernice daju određen broj strateških ciljeva koje treba

provesti putem zakonodavnih, regulatornih i operativnih mjera sa ciljem postizanja i osiguravanja visokog nivoa sigurnosti informaciono-komunikacionih sistema.

Svaki strateški cilj uključuje podciljeve i obrazložen je do nivoa aktivnosti.

Strateški ciljevi:

- Osiguran sistematski pristup harmonizaciji i izradi zakonodavstva u oblasti cyber sigurnosti;
- Zaštićeni informaciono-komunikacioni sistemi za pružanje ključnih usluga;
- Podizanje nivoa svijesti i znanja o cyber sigurnosti;
- Uspostavljena tijela zadužena za osiguranje, jačanje i poboljšanje cyber sigurnosti;
- Poboljšana sigurnost i otpornost informaciono-komunikacionih sistema;
- Ojačani kapaciteti za borbu protiv cyber kriminala;
- Uspostavljena efikasna saradnja u oblasti cyber sigurnosti u međunarodnim, regionalnim i domaćim okvirima;
- Izgrađeni kapaciteti za adekvatan odgovor na krizne situacije;
- Uspostavljeno javno-privatno partnerstvo.

FRAUDINFO: Pod pokroviteljstvom Misije OSCE-a osnovana je "Neretva grupa za cyber sigurnost". Možete li nam nešto vise reći o ovoj grupi.

Sanja: To je neformalna radna grupa otvorenog tipa, sa više zainteresovanih strana, koja okuplja ključne praktičare i stručnjake iz različitih sektora i sa svih nivoa vlasti u BiH. Grupa uključuje predstavnike državnih i entitetskih institucija, agencija, privatnog sektora, banaka, energetskog sektora, kao i mladih.

Ona je inkubator prijeko potrebnih politika djelovanja, alata i inicijativa iz oblasti cyber sigurnosti, uključujući razvoj platformi i modula za e-učenje. Saradnja i operativnost članova Grupe su doveli do uticajnih rezultata koji su osigurali određeni napredak u BiH bez obzira na izazovne okolnosti.

FRAUDINFO: Šta je do sad "Neretva grupa za cyber sigurnost" implementirala?

Sanja: Na primjer, prošle godine je, uz podršku Misije, Neretva Grupa za cyber sigurnost organizovala niz

webinara koji su osposobili više od 200 zaposlenih u javnom sektoru kako da osiguraju osnove cyber sigurnosti u svom radu. To je bilo od naročite važnosti u vrijeme pandemije COVID-19, koja je dovela do izuzetnog povećanja obima rada od kuće. Webinari su koristili platforme agencija za državnu službu BiH, Republike Srpske (RS) i Federacije BiH (FBiH), što je omogućilo da veliki broj državnih službenika iskoristi mogućnost učestvovanja. Takođe prošle godine, članovi Grupe iz privatnog sektora su izradili i stavili u funkciju privremenu platformu sa modulima koji pružaju osnovno znanje o cyber sigurnosti. Simbol prepoznavanja vrijednosti rada

Grupe predstavlja nedavno formiranje podgrupe za energetski sektor.

Ta grupa stručnjaka i praktičara sada radi pod pokroviteljstvom USAID na razvoju Mape puta za implementaciju EU Direktive 2016/1148 (NIS Direktiva) u BiH. To je značajan korak ka unapređenju zaštite kritične infrastrukture i energetskih sistema u BiH od cyber napada.

FRAUDINFO: Koje bi značajne aktivnosti izdvojili Misije OSCE- za cyber sigurnost?

Sanja: OSCE pruža podršku Bosni i Hercegovini u provedbi dogovorenih mjera OSCE-a na izgradnji uzajamnog povjerenja u oblasti cyber sigurnosti.

U tom cilju, na primjer, mi omogućavamo partnerstva i umrežavanje između privatnog i javnog sektora, kao i promociju mogućnosti za mlade u ostvarenju karijere u oblasti IKT cyber sigurnosti. Takođe bih željela iskoristiti ovu priliku da naglasim važnost rada neformalne međunarodne koordinacione grupe za cyber sigurnost u BiH. Grupa je formirana na inicijativu OSCE-a i rahmetli Šadija Matara iz Delegacije EU i Ureda Specijalnog predstavnika EU u BiH.

Grupa osigurava izuzetno potrebnu koordinaciju i razmjenu informacija o prioritetima, izazovima i naporima između najaktivnijih međunarodnih aktera u ovoj oblasti. To naravno vodi uticajnijoj i održivijoj pomoći BiH.

FRAUDINFO: Koje su naredne aktivnosti Misije OSCE- za cyber sigurnost?

Sanja: OSCE će nastaviti podržavati Izgradnju održivih kapaciteta za cyber sigurnost Bosne i Hercegovine, fokusirajući se na prioritetne potrebe a u skladu sa njenim obavezama kao članice OSCE-a. To će podrazumijevati podršku izradi ključnih strateških dokumenata, izgradnju ljudskih i tehničkih kapaciteta za viši nivo zrelosti cyber sigurnosti, CERT i IKT timova i njihovu integraciju u globalne okvire cyber sigurnosti. Naša podrška će takođe uključivati promociju privatno-javnog partnerstva u domenu cyber sigurnosti. Također ćemo, ostati odlučni da promovišemo i omogućimo veću i svrsishodniju ulogu za mlade ljude i žene u radu na poboljšanju cyber sigurnosnih kapaciteta i otpornosti. Veća digitalna pismenost žena i veća rodna raznolikost stručnjaka u ovoj oblasti će dati značajan doprinos smanjenju ranjivosti u cyber prostoru.

FRAUDINFO: Kada možemo očekivati da se uspostavi CERT u BiH?

Sanja: Operativni CERT već postoji u RS, ali još ne u FBiH. Takođe, u skladu sa odlukom Vijeća ministara BiH iz 2017. godine, CERT za institucije BiH treba da bude uspostavljen u Ministarstvu sigurnosti BiH. Međutim, to tek treba da se dogodi, uglavnom zbog administrativnih pitanja koja se odnose na političku volju i proaktivnost. Sigurno je krajnje vrijeme da CERT-ovi za institucije BiH i za FBiH budu uspostavljeni, operacionalizovani i potom međusobno umreženi.

Paralelno sa tim, postoje indikacije da će CERT-ovi možda biti formirani na drugim nivoima i za druge segmente, moguće u privatnom i akademskom sektoru. ■

UPRMBiH

Udruženje profesionalnih rizik menadžera

Udruženje profesionalnih rizik menadžera u BiH (UPRMBiH) Vas poziva da uzmete učešće na specijalističkom jednodnevnom seminaru kojeg UPRMBiH organizuje u saradnji sa Deloitte d.o.o. Sarajevo a koji će se održati 20. septembra, 2021. g. na temu "Minimalnih zahtjeva za regulatorni kapital i prihvatljive obaveze" (eng. *Minimum Requirement for Own Funds and Eligible Liabilities - MREL*).

Pozivnice za ovaj seminar će biti distribuirane početkom septembra na adrese Vaših institucija.

UREDNIČKI TIM

Azra Beriša
Saradnik upravljanja rizikom finansijskog kriminala
Sparkasse Bank dd BiH

Muris Bešić
Voditelj odjela za pravnu podršku mreži - Direkcija pravnih poslova
Sparkasse Bank d.d. BiH

Haris Buturović
Direktor Direkcije za sprječavanje pranja novca, operativne rizike i informacijsku sigurnost
Sparkasse Bank dd BiH

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

Sanela Stupar
Stručni saradnik za sigurnost informacionog sistema

Mirzad Topić
Specijalista za detekciju i prevenciju prevara
Sberbank BH dd

Mujo Vilašević
Sekretar Društva i Compliance Oficir Raiffeisen Invest Društvo za upravljanje fondovima dd

Vedran Vinšalek
Voditelj odjela Operativni rizik
Sberbank BH dd

Sanela Vrana
Voditelj sigurnosti informacionog sistema
Razvojna Banka FBiH