GOD. 7 . BR. 8 [2023] EDUKATIVNI ČASOPIS ZA BANKARSKI I FINANSIJSKI SEKTOR U BiH ISSN 2566-3100

FRAUDinfo

UDRUŽENJE PROFESIONALNIH RIZIK MENADŽERA U BOSNI I HERCEGOVINI

9 772566 310008

UPRMBiH
Udruženje profesionalnih rizik menadžera

Igor Jokić
Predsjednik Udruženja
profesionalnih rizik menadžera
u Bosni i Hercegovini

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

UVODNA RIJEČ UDRUŽENJE PROFESIONALNIH RIZIK MENADŽERA U BIH

Dragi čitaoci,

"Ekspertni tim Fraud Foruma kao i u dosadašnjim izdanjima Fraud Info magazine u 8. izdanju obrađuje najaktuelnije teme iz oblasti upravljanja operativnim rizicima, usklađenosti i informacijske sigurnosti.

U ovom izdanju magazina možete pronaći korisne informacije o online prevarama, veoma kvalitetan edukativni vodič za kriptovalute, te više interesantnih članaka iz oblasti usklađenosti, kreditnih prevara i informacijske sigurnosti.

Udruženje profesionalnih rizik menadžera u Bosni I Hercegovini, zajedno sa stručnjacima iz Fraud Foruma, u narednom periodu će pored redovne publikacije Fraud Info magazina koordinirati i dodatne seminare, edukacije i slične aktivnosti sa ciljem podizanja svijesti o važnosti usklađenosti, kvalitetnijeg upravljanja rizicima prevara i standardima upravljanja informacijskom sigurnosti."

UPRMBiH
Udruženje profesionalnih rizik menadžera

FRAUDinfo

Udruženje profesionalnih rizik menadžera u BiH

Fra Anđela Zvizdovića 1
71 000 Sarajevo - BiH

e-mail:
amar.brkan@uprmbih.ba

Izdavač:
UDRUŽENJE
PROFESIONALNIH
RIZIK MENADŽERA

Design, DTP & Print:
PERFECTA, Sarajevo

perfecta

Branilaca Šipa 33

tel.:
+387 61 214 222

e-mail:
info@perfecta.ba

ISSN 2566-3100

UVODNA RIJEČ

Dragi čitaoci,

Pred Vama je osmo (VIII) izdanje Fraud Info časopisa kao produkta kontinuirane saradnje finansijskih institucija u domeni prevara (fraud), uz podršku i pokroviteljstvo Udruženja profesionalnih rizik menadžera BiH.

Pandemija COVID-19 je dovela do promjene navika življenja i drastične promjene u ekonomijama širom svijeta. Online način kupovine i poslovanja je značajno porastao, a samim time su povećane i prevarne radnje, posebno u domeni cyber prevara. Finansijske institucije kontinuirano prate fraud trendove te unapređuju i jačaju monitoring i prevenciju istih primjenom adekvatnih mjera i alata.

Tim eksperata ispred Fraud foruma, pored redovnih diskusija iz domene prevara kao i praćenja usklađenosti, nastoji kroz časopis Fraud Info dati osvrt na posljednje fraud trendove, kao i kako ih prepoznati i prevenirati. Tim ujedno prati i zakonske i ekonomske promjene na tržištu koje također mogu uticati na redovno poslovanje finansijskog sektora, posebno u domeni sprečavanja prevara, te s tim u vezi obrađuje aktuelne teme ukazujući na eventualnu problematiku i potencijalna unapređenja.

S obzirom na to da su cyber prevare posebno u fokusu od početka pandemije, autori pišu o trendovima istih uz preporuku kako se pojedinci i poslovni subjekti mogu zaštititi, ali i kako dolazi do phishinga uzimajući u vidu psihološki aspekt. Što se tiče kreditnih prevara, uposlenici finansijskih institucija su prva linija odbrane od potencijalnih kreditnih prevara, te u u ovom broju ukazujemo na nužnost kontinuirane i kvalitetne

Sadržaj

edukacije poput Studije slučaja. Nadalje, ističe se važnost uloge samog fraud menadžera u procesu sprečavanja prevara i koje bi trebale biti odgovornosti istog.

Pored eksternih prevara, finansijske institucije su svjesne i rizika internih prevara, te rade na jačanju i primjeni alata za pravovremenu detekciju istih. Na stranicama ovog izdanja donosimo i članke o insajderskim prijetnjama i kako se zaštititi.

Praćenje usklađenosti (compliance) dobija sve više na značaju u svim domenama poslovanja, posebno finansijskim. U ovom broju donosimo nekoliko zanimljivih ekspertiza, od značaja compliancea za biznis i šta je potrebno da bi bio efikasan, kao i može li se izmjeriti „trošak" praćenja usklađenosti. Također, jako zanimljiva aktuelnost je i efikasnost Procjene primjerenosti, popularno fit&proper procjena, koja je jedna od relativno novijih aktivnosti koje su banke dužne provoditi u odnosu na članove organa banke te u odnosu na ključne funkcije.

Kriptovalute su uvijek zanimljiva tema te je ovaj put među tekstove uključen i Vodič za kriptovalute sa osnovnim informacijama o ovoj vrsti digitalnog novca.

Vjerujemo da će vam novo, osmo izdanje Fraud Info časopisa donijeti dosta zanimljivih tema i aktuelnosti. Cilj eksperata okupljenih u okviru Fraud foruma nastoji da ukaže na posebne oblike prevara i predlože mjere prevencije primjenjive čak na nivou pojedinca, kao i da prate relevantne tržišne i zakonodavne promjene koje utiču na poslovanje finansijskog sektora. Sa sve većim značajem funkcije usklađenosti u poslovanju, članovi također podižu svijest o radu i aktivnostima iste.

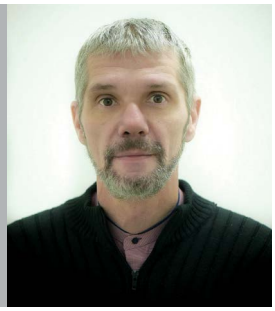
Djelovanje finansijskih institucija kroz ovakvu vrstu saradnje primarno doprinosi zajedničkoj borbi protiv prevara koje će uvijek predstavljati rizik po poslovanje.

UREDNIČKI TIM ČASOPISA

Negativni savremeni trendovi

SOCIJALNI INŽENJERING KROZ PRIZMU INFORMACIJSKE SIGURNOSTI

Dobili ste ponudu da kupite luksuzni proizvod po nerealno niskoj cijeni, e-mail s linkom na nepoznatu stranicu ili je neko nepoznat od vas tražio lične podatke? Ako je vaš odgovor da, sigurno ste bili žrtva socijalnog inženjeringa koji je sve više prisutan online. U ovom tekstu saznajte više o metodama online psihološke manipulacije i šta možete učiniti da zaštite sebe i svoju kompaniju.



Autor:
Eldin Mulić

Socijalni inženjering, tema koja je sve više u trendu s povećanom digitalizacijom i sveukupnom informatizacijom društva, je, zapravo, psihološka manipulacija ljudima s ciljem otkrivanja povjerljivih informacija te izvlačenjem materijalne ili druge koristi. Kraća definicija bi bila da je to djelovanje koji utiče na potencijalnu žrtvu da uradi nešto što može biti na štetu te osobe.

Metode i tehnike socijalnog inženjeringa zasnivaju se na psihologiji ljudskih osobina i načinu donošenja odluka, a što se bazira na kognitivnim predrasudama. U novije doba najčešća vrsta socijalnog inženjeringa dešava se *online*, a u manjem obimu i preko telefona. Socijalni inženjering nije jednokratna aktivnost, nego se radi o nizu koraka koji dovode do neke posljedice. Posljedice, bilo pozitivne ili negativne, zavise od ciljeva koji stoje iza njega.

Socijalni inženjering se u velikoj mjeri oslanja na sljedećih 6 principa koje je uspostavio **Robert Cialdini**. Cialdinijeva teorija uticaja zasniva se na šest ključnih principa: reciprocitet, posvećenost i dosljednost, društveni dokaz, autoritet, sklonost i nestašica.

Reciprocitet - Ljudi imaju tendenciju da uzvrate uslugu što je razlog mnogih besplatnih uzoraka u marketingu.

Posvećenost i dosljednost - Ako se ljudi posvete cilju, veća je vjerovatnoća da će ispuniti tu obavezu jer su izjavili da ta ideja ili cilj odgovara njihovoj slici o sebi. Primjer su marketinški stručnjaci koji prave pop up prozore na internetu s porukama kao što su: "Ja ću se kasnije prijaviti" ili "Ne, hvala, ne želim da zarađujem novac".

Društveni dokaz - Ljudi će raditi stvari koje vide drugi ljudi. Naprimjer, u jednom eksperimentu jedan ili više saučesnika bi gledali u nebo; ostali posmatrači bi onda pogledali u nebo da vide ima li nešto na nebu što su oni promašili. U jednom trenutku ovaj eksperiment je prekinut jer je toliko ljudi gledalo gore da su zaustavili saobraćaj.

Autoritet - Ljudi teže tome da poštuju autoritetske figure, čak i ako se od njih traži da izvrše nepoželjne radnje.

Sklonost - Ljudi će prije povjerovati drugim ljudima koje vole. Cialdini citira marketing *Tupperwarea*, što se kasnije može prepoznati kao viralni marketing. Ljudi su bili skloniji kupovini ako im se dopada osoba koja prodaje.

Nedostatak - Percipirani nedostatak nečega stvara potražnju. Naprimjer, kada kažu da su ponude dostupne samo za neko *ograničeno vrijeme*, podstiče se prodaja.

Najčešći vektori napada metodama socijalnog inženjeringa

Vishing

Vishing, poznatiji kao *glasovni phishing*, je kriminalna praksa korištenja socijalnog inženjeringa preko telefona kako bi se dobio pristup privatnim i finansijskim informacijama. Napadači također to koriste i za izviđanje kako bi prikupili detaljnije informacije o ciljanoj osobi ili kompaniji.

Phishing

Phishing je tehnika prevare u pribavljanju privatnih informacija. Obično prevarant šalje e-mail koji izgleda kao da dolazi iz legitimnog biznisa - banke ili kompanije za izdavanje kreditnih kartica - tražeći *verifikaciju* informacija i upozoravajući na neke teške

posljedice ako se ne poduzmu tražene radnje.

Baiting

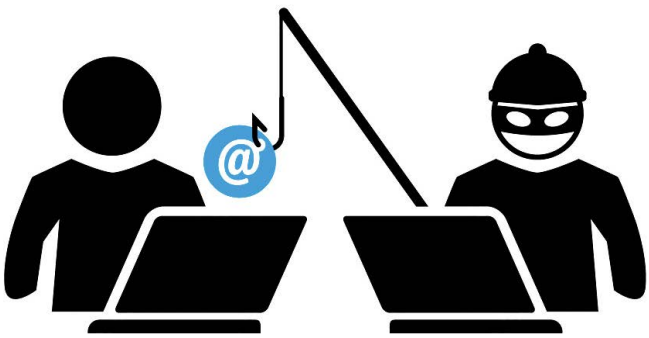
Ljudi su radoznali, a što je osnovna permisa za ovaj scenario napada. *Cyber* kriminalac na javnom mjestu ostavi uređaj (npr. USB) koji je zaražen *malverom*. Žrtva pronađe USB, poveže ga sa svojim kompjuterom iz radoznalosti i *pokupi malver* ili sličan zlonamjerni *software*.

Hakiranje e-maila i spam kontakata

Ljudi prirodno vjeruju u tačnost i valjanost poruka koje im stiže od poznatog pošiljaoca. Naprimjer, od poznatog e-mail kontakta dobijete poruku s nekim linkom na vama nepoznatu stranicu, ali uz obrazloženje da je to nešto super. To je razlog za krađu e-mail adresa i *passworda*. Kada dođu do tih podataka, otvara se mogućnost za *spamovanje* svih kontakata iz adresara čime se postiže širenje *malvera* i obmana žrtve da bi se došlo do ličnih, poslovnih ili drugih povjerljivih informacija.

Pretexting

Kod ove vrste socijalnog inženjeringa napadač pravi detaljan scenario kojim pokušava da *upeca* žrtve. Nekada je to tužna priča o tome kako se našao sam u stranoj zemlji bez novca, nekada je u pitanju *princ* kome je nedavno otac preminuo i kome treba par stotina dolara da postane kralj. Kod ovakvih prevara napadač računa da će ljudi iz socijalne osjetljivosti pomoći osobi koja je u nevolji, a, s druge strane, računaju i na pohlepu i mogućnost brze zarade. Ova tehnika često se kombinuje s drugim tehnikama jer je kod ovakvih scenarija potrebno osmisliti priču koja će privući pažnju žrtve, a nekada napadač mora da se pretvara da je neko drugi i u e-mail komunikaciji i preko telefona.



Quid pro Quo

Nešto za nešto. Ovdje se korisnicima nude nagrade ili popusti na skupe proizvode, ali tek nakon što popune formu u kojoj ostavljaju gomilu ličnih informacija. Zatim se prikupljeni podaci koriste za krađu identiteta.

Spear Phishing

Spear phishing je ciljana *phishing* kampanja u kojoj su meta zaposleni u tačno određenoj kompaniji ili organizaciji iz koje *cyber* kriminalci pokušavaju da ukradu podatke i/ili novac. Napadači izaberu metu u datoj organizaciji, a zatim obave *online* istraživanje o njoj (prikupljaju lične informacije sa društvenih mreža, itd.). Kada upoznaju metu, započinju slanje e-mail poruka čiji je sadržaj prilagođen upravo njoj. U poruci se nalazi maliciozni link ili fajl za preuzimanje. Kada korisnik klikne na link ili preuzme

zaraženi fajl, *malver* ulazi u sistem i lako se širi.

Smishing

To je čin korištenja SMS tekstualnih poruka kako bi se žrtve namamile na određeni način djelovanja. Kao i *phishing*, možete kliknuti na zlonamjerni link ili otkriti informacije.

Pretvaranje

Ovaj način djelovanja podrazumijeva pretvaranje ili stvaranje izgovora da je druga osoba s ciljem fizičkog pristupa sistemu ili zgradi. Napadači se često služe ovom tehnikom jer im za uspješan napad nije potrebno probijanje sigurnosnih šifri i zaštita, korištenje ranjivosti njegovog softvera i sl. Pojam socijalnog inženjeringa je popularizirao poznati i osuđeni haker **Kevin Mitnick** koji tvrdi kako je mnogo lakše nekoga prevariti služeći se socijalnim inženjeringom nego probiti njegov informacijski sustav.

Napadač se trudi da ostavi utisak legalnosti, odnosno povjerljivosti. U e-mail porukama obično se navodi neki poznati podatak o korisniku (najčešće njegovo ime ili zanimanje, a što je dostupno iz nekog javnog izvora ili s društvenih mreža). Treba napomenuti kako se napadač može usmjeriti na prikupljanje detaljnih informacija o ciljanom korisniku umjesto masovnog prikupljanja osnovnih informacija o velikom broju korisnika čime otvara sebi mogućnost slanja puno osobnijeg e-maila, a koja može biti vezana uz specifično zanimanje korisnika, privatne, poslovne informacije ili slične detalje. Tako se umanjuje broj poslanih poruka, ali se povećava utisak legalnosti e-mail-a što povećava šansu uspješnog ostvarivanja kontakta sa žrtvom i ostvarenje cilja.

„Rezultat kvalitetnog napada može biti višestruk, a uobičajeno je to materijalna dobit, gubitak privatnih ili poslovnih povjerljivih informacija, gubitak ugleda, korištenje prikupljenih podataka za daljnje napade te emocionalni pritisak koji žrtva osjeća."

Rezultat kvalitetnog napada može biti višestruk, a uobičajeno je to materijalna dobit, gubitak privatnih ili poslovnih povjerljivih informacija, gubitak ugleda, korištenje prikupljenih podataka za daljnje napade te emocionalni pritisak koji žrtva osjeća.

Svijest i zaštita

Kada govorimo o zaštiti od napada metodama socijalnog inženjeringa i *cyber* napada povezanih s metodama socijalnog inženjeringa, na prvom mjestu treba naglasiti svijest. Kada krećemo u proces organizovanja zaštite, krećemo od permise da smo svjesni da možemo postati meta napada. „Neće nas niko napadati, mi nemamo šta kriti“ je prvi korak u postajanju žrtve napada, bilo svjesno ili nesvjeno. Vođeni sviješću da možemo postati meta napada u svakom trenutku, radimo analizu i procjenu rizika te na osnovu toga i gradimo sistem zaštite, a s naglaskom na one vrste napada za koje smo ustanovili da su *risk analizom* u „crvenom“.

> *„Neće nas niko napadati, mi nemamo šta kriti“ je prvi korak u postajanju žrtve napada, bilo svjesno ili nesvjeno.*

Zaštitne mjere od napada socijalnog inženjeringa primjenjujemo na način da se upoznamo s vrijednostima podataka, provjeravamo identitet osoba s kojima stupamo u *online* kontakt, s povjerljivim podacima postupamo odgovorno i promišljeno. Pogotovo je važno osvijestiti činjenicu kako se tehnike napada usavršavaju svakodnevno i kako ne postoji univerzalna zaštita za sve oblike napada. Mjere zaštite, kad se jednom postave, moraju se redovno usavršavati i unapređivati u skladu s trendovima, a što znači da se mora redovno pratiti dešavanje u ovoj oblasti. Bitno je kritički posmatrati *online* okolinu, služiti se internetom odgovorno i savjesno kako bi se umanjila mogućnost napada, a samim tim i omogućilo pravovremeno i adekvatno reagovanje.

Prilikom rada na zaštiti od ove vrste napada treba posebnu pažnju posvetiti tome da svi korisnici interneta na vrijeme dobiju informacije o mogućim propustima, prijetnjama i modusima napada što automatski podiže razinu svijesti i ima uticaj na povećanje nivoa sigurnosti.

Osnovne mjere zaštite

Pored svega gore navedenog, efikasne mjere koje je potrebno poduzeti u jednoj kompaniji mogu se svrstati u sljedeće kategorije:

- **Obuka zaposlenih** u sigurnosnim situacijama relevantnim za njihovu poziciju;
- **Standardni okviri** - uspostavljanje okvira rada unutar kompanije (definisati koji zaposlenik ima pristup kojoj vrsti podataka na osnovu potreba posla te uspostaviti pravilnike i procedure za zaštitu i klasifikaciju informacija);
- **Analiza informacija** - identifikovati informacije koje su osjetljive i koje mogu biti meta napada te procijeniti moguću eksponiranost socijalnom inženjeringu;
- **Sigurnosni propisi** - uspostavljanje sigurnosnih politika i procedura za rukovanje osjetljivim informacijama;
- **Testiranje** - izvođenje nenajavljenih, periodičnih testova sigurnosnog okvira (periodično slanje *phishing* e-maila);
- **Pregled** - periodično prolaženje kroz sve navedeno radi unapređenja i praćenje trendova.

Na kraju treba reći i par riječi o informacijskoj sigurnosti. Naime, uobičajeno poimanje je da je informacijska sigurnost oblast zaštite kompjuterskih sistema i mrežne infrastrukture što je samo dijelom tačno. Sigurnost informacijskih tehnologija (IT) i informacijska sigurnost su dvije različite oblasti. U današnje doba digitalizacije informacije se obično obrađuju, pohranjuju ili prenose uz pomoć informacijskih tehnologija (IT), ali informacijska sigurnost je još uvijek većim dijelom „analogna“ puno više nego što stvarno izgleda. Sigurnost povjerljivih informacija nije fokusirana na podatke koji se obrađuju kroz kompjuterske i mrežne sisteme, nego informacijska sigurnost obuhvata svu imovinu kompanije, a što uključuje informacije na digitalnim i štampanim medijima, kao i informacije koje se prenose usmenim putem.

Sistem informacijske sigurnosti čine tri parametra:

- **Ljudi**: zaposlenici su ti koji su svakodnevno u kontaktu s osjetljivim informacijama i mandatorno je za kompanije da ih educiraju vezano za rizike i prijetnje.
- **Procesi**: kompanije bi trebale dokumentovati korake zaposlenih koji utiču na sigurnost, a koji mogu dati neke garancije sigurnosti. Ovo podrazumjeva i definiciju uloga i odgovornosti za aktivnosti vezane uz zaštitu podataka.
- **Tehnologija**: Tehnološki elementi zaštite koje kompanije trebaju primijeniti kako bi se mogli nositi s prijetnjama, kao što su antivirusni softveri, prava pristupa i enkripcija podataka, itd.

Pored naše želje i mogućnosti za zaštitom informacija i cjelokupnog poslovanja, postoje i određeni regulatorni zahtjevi i propisi koji tretiraju ovu oblast. Ovo je posebno izraženo u finansijskom i bankarskom sektoru jer je to grana privrede koja je i od regulatora prepoznata kao meta visokog rizika za sve vrste napada od socijalnog inženjeringa do fizičkih i infrastrukturnih napada. Regulatorni zahtjevi bazirani su na međurodnim standardima, EU direktivama i iskustvima. Sama usklađenost s ovim standardima podiže nivo zaštite na puno viši nivo od postojećeg. Za finansijsko-bankarski sektor tri su osnovna standarda koja utiču na informacijsku sigurnost:

- **ISO 27001** – međunarodni standard informacijske sigurnosti koji pokriva sve oblasti zaštite informacija u bilo kojem obliku ili mjestu pohrane.
- **PCI DSS** – kartičarski standard koji se odnosi na organizacije koje se bave obradom kartičnih transakcija. Uključuje sve što i ISO 27001, a pored toga i puno više i strožije propisuje određene mjere zaštite.
- **GDPR** – Direktiva EU koja propisuje upravljanje ličnim podacima, načine obrade, skladištenja i dijeljenja. Osnovna namjena mu je da kompanije kroz proces usklađivanja imaju dokumentovano gdje i kako upravljaju podacima, s kime ih dijele, te da pri tome ne obrađuju prekomjerno lične podatke.

Pored naše želje i mogućnosti za zaštitom informacija i cjelokupnog poslovanja, postoje i određeni regulatorni zahtjevi i propisi koji tretiraju ovu oblast. Ovo je posebno izraženo u finansijskom i bankarskom sektoru jer je to grana privrede koja je i od regulatora prepoznata kao meta visokog rizika za sve vrste napada od socijalnog inženjeringa do fizičkih i infrastrukturnih napada.

Naravno, pored spomenutih standarda postoji još mnogo drugih, ali osnovna vodilja svih je podizanje nivoa sigurnosti i zaštite informacija na veći nivo. Savremene i agilne kompanije moraju pronaći balans između zahtjeva sigurnosti i zahtjeva poslovne strane te sve to uokviriti u prihvatljiv budžet što je u današnje vrijeme veliki izazov. Pored toga, stalno praćenje dešavanja u ovoj oblasti je neophodno da bi se ostalo na sigurnoj strani. ■

Funkcija praćenja usklađenosti

KOLIKO KOŠTA *COMPLIANCE?*

Koliko zaista košta compliance? Koji su to stvarni troškovi koji trebaju biti alocirani na uspostavu i funcionisanje ove funkcije, koja je podloga tih troškova, šta dobijamo, a šta gubimo?

Autor:
Mujo Vilašević

Kada je 2017. godine po prvi put formalizovana Funkcija praćenja usklađenosti (*compliance*) u bankarskom sektoru, kroz nove entitetske zakone o bankama, *compliance* oficiri su to dočekali kao najbolju vijest nove regulative, edukatori su zadovoljno iščekivali novo polje za edukacije a menadžment se opravdano pitao – Koliko će to sve to nas da košta?

Iluzorno je biti dio finansijskog sektora i ne razmišljati u okvirima *cost – income – ratio*. *Compliance* funkcija, međutim, upravo je u svojoj suštini sve ono izvan krutih finansijskih okvira, a paradoksalno u okvirima pravila - pravila koje uspostavljaju regulator, zakonodavac i internih pravila koje organizacija kreira sama za sebe. Kada na to dodamo još i obavezu poštivanja etičkih principa (što je u poslovnom svijetu dugo prevođeno kao *contradictio in adiecto*), onda je „prodaja" *compliance* koncepta ravna nemogućnoj misiji.

Međutim, koliko zaista košta *compliance*? Koji su to stvarni troškovi koji trebaju biti alocirani na uspostavu i funcionisanje ove funkcije, koja je

podloga tih troškova, šta dobijamo, a šta gubimo?

Rezultati istraživanja

Nažalost, Bosna i Hercegovina siromašna je istraživanjima koji bi dali egzaktne podatke pa nam se u ovom slučaju valja poslužiti međunarodnim istraživanjima koja se već godinama bave ovom temom.

Prema podacima *Forbesa*, *Ponemona* i *Globalscape Reportsa*, organizacijama koje odbijaju da se usklade s regulatornim obavezama ili koje provode usklađivanje neadekvatno, troškovi se povećavaju u prosjeku 2.71 puta na godišnjem nivou. U Sjedinjenim Američkim Državama prosječan trošak *compliancea* je 5,47 mil USD u prosjeku, a trošak neusklađenosti 14,82 mil USD u prosjeku na godišnjem nivou za srednje i velike korporacije.

Ako ove podatke prevedemo i u Evropsku uniju, a naročito nakon stupanja na snagu Uredbe o zaštiti ličnih podataka (GDPR, 2016/379) i činjenice da se državne agencije za zaštitu ličnih podataka ne libe kažnjavati organizaci-

je za kršenje pravila o zaštiti podataka, onda je trošak neusklađenosti u najvećem dijelu zapravo trošak neadekvatnog upravljanja podacima, a u dobu u kome je podatak možda i najvažnija imovina organizacije. Ovdje govorimo o kaznama i u milionima eura, kao što je **Caixa Bank Spain** – kazna od 6 miliona EUR za neusklađenost s GDPR, a izricanje kazne imali smo i u Hrvatskoj, mada sa još uvijek oprečnim podacima o iznosu kazne.

Lokalno, u bankarskom sektoru razvili smo (gotovo identične) metodologije koje identifikuju uticaj neusklađenosti na banke kroz tri parametra:

- regulatorni,
- finansijski i
- reputacijski.

Reputacija banke

Ovisno od stepena eksponiranosti i vjerovatnosti nastupanja neželjenog događaja (neusklađenosti), procjenjujemo rizik usklađenosti. Naravno, prateći regulatorni uticaj, krajnja konsekvenca neusklađenosti je oduzimanje

licence banci. U kontekstu finansijskog uticaja, govorimo o iznosu do 200.000 BAM za banku i pojedinačnim kaznama za odgovorna lica (do 20.000 BAM ili oduzimanja licence članu uprave ili nadzornog odbora). Ovdje govorimo o pojedinačnim kaznama, ne o djelima u sticaju više prekršaja i samo o kaznama predviđenim za kršenje zakona o bankama i podzakonskih akata entitetskih agencija. S druge strane, od navedenih, možda i neprimjetan, a opet najvažniji, je reputacijski uticaj.

Uticaj na reputaciju banke može dovesti (i kako je praksa pokazala, dovodi) do gubitka klijenata. Dovoljan je jedan nepoželjan događaj, medijska eksponiranost ili, možda danas i bitnije, negativan *feedback* na društvenim mrežama da pokrene od 5% klijenata pa na dalje. Ovom

> *Dovoljan je jedan nepoželjan događaj, medijska eksponiranost ili, možda danas i bitnije, negativan feedback na društvenim mrežama da pokrene od 5% klijenata pa na dalje.*

aspektu uticaja neusklađenosti još uvijek se nažalost ne posvećuje dovoljno pažnje, u prvom redu jer reputacijski rizik nije dovoljno regulatorno definisan. No, ovaj rizik može generisati zaista najozbiljniju kosekvencu za organizaciju, a to je odliv klijenata. Jer, pored novčanih kazni koje će opteretiti budžet (a što u većim organizacijama ne bi smio biti nepredviđen problem), odliv klijenata je neželjena posljedica koja alarmira sve instance i postavlja pitanje vlasniku – kako se upravlja poslom koji sam ja kao vlasnik povjerio upravljačkim strukturama.

> *Da li zaista želimo dozvoliti pristup našem životu banci koja trpi kazne jer nije u stanju uskladiti se s propisima, od koje klijenti odlaze zbog pogrešnih i neetičnih odluka, koja puni medijske natpise jer nije bila u stanju organizovati i uspostaviti nešto što se zove compliance?*

Drugo, na reputaciju je važno obratiti pažnju i s još jednog aspekta, a koji se krije u odgovoru na pitanje – Šta je to, zapravo, banka danas?

Banka je postala centralna tačka ljudskog života. Osim što banci povjeravamo naš novac na čuvanje, što od banke posuđujemo novac da rješimo ključna pitanja, banka je postala poveznica u svim našim svakodnevnim aktivnostima. Ne možemo platiti taksi, natočiti gorivo, platiti upis na fakultet, osnovati firmu pa čak ni razvesti se od bračnog partnera a da banka ne zauzima jedno od centralnih mjesta u procesu. Ukratko, svakog dana, svjesno ili nesvjesno, banci povjeravamo najrazličitije segmente svog života. Kome želimo to povjeriti? Ozbiljnoj organizaciji, banci koja je ekonomski pristupačna, efikasna i efektivna, ali i reputacijski „neoštećena".

Da li zaista želimo dozvoliti pristup našem životu banci koja trpi kazne jer nije u stanju uskladiti se s propisima, od koje klijenti odlaze zbog pogrešnih i neetičnih odluka, koja puni medijske natpise jer nije bila u stanju organizovati i uspostaviti nešto što se zove *compliance*?

Pitanje je retoričko.

Dakle, nije teško zaključiti da je reputacija ogledalo upravljanja i to je mjesto rizika kome bi se trebala posvetiti naročita pažnja. Na tom mjestu rizika dolazimo do *compliancea*, usklađenosti i neusklađenosti i posljedicama koje organizacija može „platiti" za neusklađenost.

Usklađenost i trošak usklađenosti

Usklađenost nije samo uspostavljanje odgovarajućeg odjela, tima, odgovorne osobe i zapošljavanja eksperata (iako su ovo ključne osnove *compliancea* bez kojih je dalji razgovor o usklađenosti besmislen). Usklađenost i trošak usklađenosti je onaj trošak koji „platimo" kada odustanemo od poslovnih poduhvata koji nisu u skladu s regulativom ili principima etičkog poslovanja, svjesni izmaklog prihoda takvog posla ili (još važnije) kada takve poslovne poduhvate uskladimo sa smjernicama *compliancea* i regulativama, svjesni da krajnji prihod neće biti prvobitno očekivani ili da će koštati vremena ili resursa – a sve s uvjerenošću da će se takvi potezi dugoročno isplatiti. Konačno, usklađenost je postavljanje principa, vrijednosti, misije i dugoročne održivosti zdrave organizacije ispred kratkoročnih poslovnih ciljeva.

> *Usklađenost je postavljanje principa, vrijednosti, misije i dugoročne održivosti zdrave organizacije ispred kratkoročnih poslovnih ciljeva.*

WHY COMPLIANCE IS THE MOST IMPORTANT PART OF BUSINESS TODAY?

Kako rješiti ova pitanja?

1. Svijest – poslovno okruženje danas apsolutno je različito od okruženja od prije 10 ili 15 godina. Pravila igre su se promijenila. Na „ramenima“ naučenih lekcija, *safe-guard* instrumenti su postali maksimalni prioritet ozbiljnih finansijskih institucija (sjetimo se 2008. i 2009. godine). Dakle, i vlasnici i menadžment moraju biti svjesni da je okruženje takvo da upravljanje rizicima (uključivo rizikom usklađenosti) trenutno ima primat. Ako ćemo i preciznije, poslije prioriteta digitalizacije i banke dostupne svima na klik, vjerovatno je upravljanje rizicima broj 2 na listi prioriteta. Ako nije, vrijeme je da postane. Da li će se ovaj trend nastaviti u perspektivi vremena – vrlo vjerovatno da da jer je *online* poslovanje otvorilo vrata rizicima za koje danas još uvijek nemamo ni naziv.

2. Volja i namjera – vlasnici i menadžment moraju posjedovati istinsku volju i istinsku namjeru za zdravo poslovanje. Dugoročno zdravo poslovanje. Bez toga je uzaludna priča o *compliance* rizicima.

3. Kolaboracija. Zdrava organizacija potiče takvu kulturu. Ma koliko kompleksno bilo *compliance* oficirima da „prodaju“ svoju ulogu upravljačkim strukturama, zdrava organizacija znači interno partnernstvo. Ne postoji „dobar i loš policajac“ u zdravoj organizaciji. Ne postoji

„mi smo upravu, a vi niste“ u zdravoj organizaciji. *Compliance* oficir je tu da ukaže na nepravilnosti i da fascilira put prema pravilnosti.

Compliance oficir nije tu da bude okrivljena strana kada stvari krenu po zlu (vidjeti tužbe *compliance* oficira protiv *Enron* i sl.).

4. Povjerenje – banka koja donosi ključne poslovne odluke imajući na umu usklađenost s regulativama i zdrave etičke principe, reflektovat će povjerenje i unutra i prema vani. Unutra – zaposlenici će biti zadovoljniji, smatrat će svog poslodavca partnerom kojem mogu vjerovati i „na riječ“. Zadovoljstvo povećava motivaciju, motivacija produktivnost, a produktivnost prihode i eto nas na formuli kako *compliance* zapravo povećava konačnu dobit banke. Eksterno – princip je isti. U *generaciji Z*, *millenials*, itd, kada tinejdžeri osnivaju svoje *start-up* kompanije i imaju izuzetno visoku ekološku svijest, za svoje poslove (a koji će neminovno generisati sve veće prihode), žele pouzdanog partnera. Partnera kome mogu vjerovati – ne samo partnera koji im je ekonomski isplativ, jer novi poslovni poduhvati nisu primarno orijentirani na zaradu, oni žele *business with soul*. Da bi banke uspjele doprijeti do ove klijentele, one moraju reflektirati imidž povjerenja, zdrave i osvještene organizacije.

Postoji sigurno još mnogo načina na koji se može sagledati trošak *compliancea*. Posmatrati *compliance* kao *one time job* je slijepa ulica. Kontinuitet integriteta zahtijeva disciplinu.

Banka nema izbor da li će se uskladiti ili ne. Prije ili kasnije, taj trošak se plati. Pitanje je samo u kojem iznosu. ■

Psihologija *phishinga*

ZAŠTO KLIKNEMO NA *PHISHING* LINK

Zašto otvaramo phishing poruke? Ko to upravlja našim ponašanjem, isključuje nam racionalno razmišljanje i kontroliše naše odgovore? Da li znate za termin "Otmica amigdale"? Koju to ranjivost ljudskog faktora iskoriste hakeri pa mi "zaobiđemo" logiku i razmišljanje i kliknemo?

Autorica:
Sanela Vrana

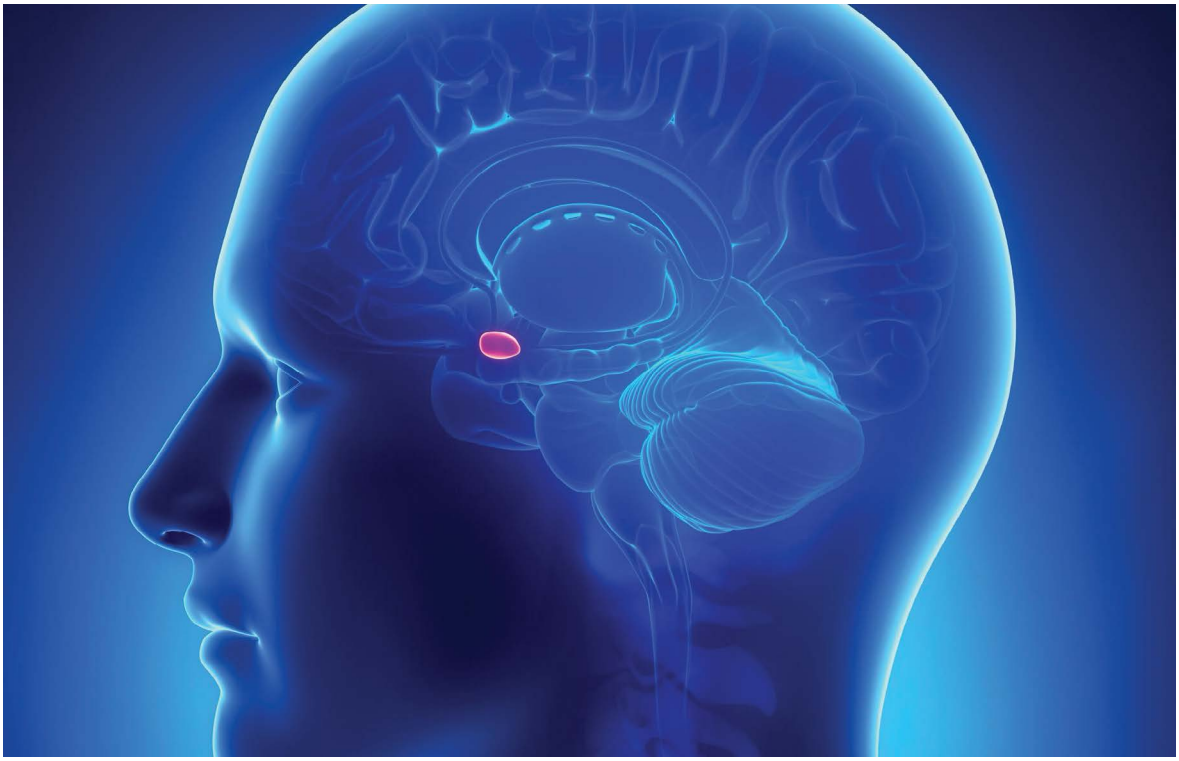
Prije nego otkrijemo kako nas hakeri natjeraju da kliknemo na phishing poruku, zavirit ćemo nakratko u psihologiju. Zašto je phishing metoda godinama jedan od najuspješnijih načina da se dobije pristup nečijim podacima? Zašto takva taktika još uvijek funkcionira?

Studije pokazuju da anksioznost može poremetiti neurone mozga odgovorne za donošenje razumnih, logičkih odluka, te da nas stres može omesti da uočimo negativne informacije ili posljedice. Svi poznajemo osjećaj u stomaku kada shvatimo da smo kliknuli na link na koji nismo trebali. Možda je bila kasna noć ili smo žurili, a možda je i sadržaj e-mail poruke bio alarmantan. Osnovni principi ljudske psihologije sugeriraju da takve situacije mogu lako dovesti do nepromišljenih ili impulsivnih odluka. Bez obzira na razlog, prebrzom

reakcijom i samo jednim klikom smo možda već odali lične podatke i učinili opasnu grešku.

Amigdala – kraljica emocija

Razmotrimo sada ko nas je to "natjerao" da reagiramo na navedeni način. Da bismo to saznali, proučit ćemo poznate činjenice o ljudskom mozgu. Čeoni režnjevi našeg mozga omogućavaju nam obradu informacija, razmišljanje o emocijama, zaključivanje, donošenje odluka, planiranje te racionalan i logički odgovor. Za razliku od ovog "racionalnog mozga", "emocionalni mozak" je brži i jači te u nekim slučajevima preuzme vođstvo. Nije to neuobičajeno ponašanje, već nešto što se obično dešava kod izraženih emocija ili prisutne opasnosti. Kada stres uzrokuje jake emocije: strah, bijes ili agresiju, aktivira se odgovor amigdale - parne žlijezde koja je centar naših emocija u mozgu, tj. naš emocionalni "čip". Amigdala skuplja sve informacije koje pristižu preko čula, obrađuje ih, sortira, i "uključuje alarm" čim prepozna prijetnju koja bi mogla da nas ugrozi. Ona djeluje kao svojevrsna stanica za uzbunu - onaj dio mozga nad kojim nemamo nikakvu kontrolu, on radi šta hoće i kad hoće. Zahvaljujući njoj opstali smo od prahistorije do danas i zahvaljujući njoj i dalje izbjegavamo opasne situacije. S druge strane, ona prikuplja sjećanja i emocije koje su s njima povezane te utiče na emocionalno pamćenje. Kao okidač naše reakcije na rizične situacije, amigdala nas u djeliću sekunde



> *Kada stres uzrokuje jake emocije: strah, bijes ili agresiju, aktivira se odgovor amigdale - parne žlijezde koja je centar naših emocija u mozgu, tj. naš emocionalni "čip".*

savjetuje da bježimo ili da se borimo. Momentalno se odvija odgovarajuća reakcija čitavog organizma. Impuls koji je pokreće ne dozvoljava nam da trezveno razmišljamo. To često rezultira naglom i nelogičnom reakcijom te tada izgovorimo ili učinimo nešto zbog čega ćemo se poslije kajati. Psiholog Daniel Goleman u čuvenom bestseleru Emocionalna inteligencija ovaj trenutak naziva "otmicom amigdale". Otmica amigdale je trenutna i intenzivna emocionalna reakcija koja nije proporcionalna poticaju što ju je pokrenuo. Amigdala "krade" reakciju drugih područja mozga, određujući ponašanje subjekta i isključujući racionalno, logičko razmišljanje. Ukoliko čeoni režnjevi mozga uspiju nadvladati reakciju amigdale, naš odgovor će biti racionalniji i primjereniji.

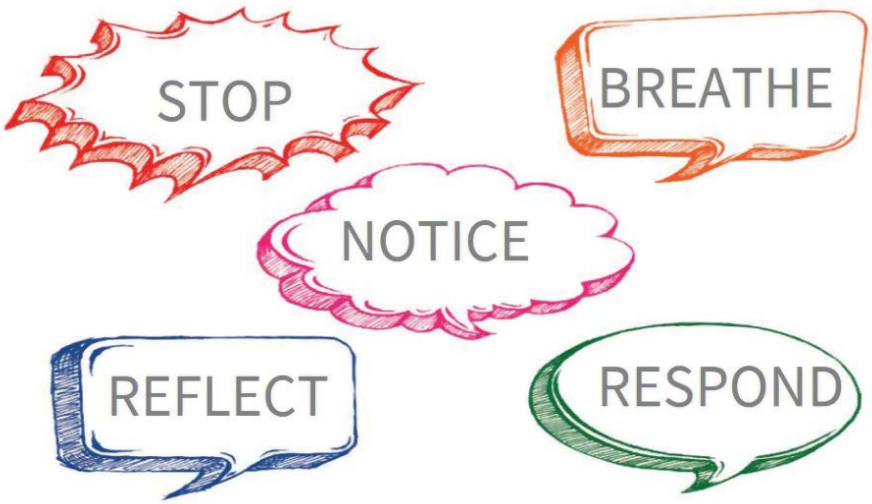
Ako se pitate zašto je ovo relevantno za cyber sigurnost, ubrzo ćete uvidjeti razlog. Prijeteća, uznemirujuća ili zagonetna elektronska pošta, koja stigne u momentu kada svakako žurimo ili nismo u potpunosti fokusirani, dovoljan je faktor stresa da ne razmislimo, ne pregledamo poruku i ne uočimo nepravilnosti ili nelogičnosti. U tom momentu nastaje otmica amigdale, tj. jake emocije "preuzimaju" naš racionalni mozak i mi bez razmišljanja, logičkog rasuđivanja, donošenja odluke, planiranja ... kliknemo.

Kako se zaštititi od sopstvenih brzopletih reakcija

Sačekajte. Prvi je korak priznati da se osjećamo ugroženo ili pod stresom i da je aktiviran naš odgovor borbe ili bijega. Postanimo svjesni situacije i preuzmimo kontrolu. Suočivši se s potencijalnom prevarom, važno je zaustaviti se, sačekati, procijeniti potencijalne rizike, uočiti nelogične pojave: sumnjiv rječnik, pogrešno napisane riječi i sl. Kada čitate elektronsku poruku koja vas primorava, uslovljava, tjera

> *Postanimo svjesni situacije i preuzmimo kontrolu. Suočivši se s potencijalnom prevarom, važno je zaustaviti se, sačekati, procijeniti potencijalne rizike, uočiti nelogične pojave: sumnjiv rječnik, pogrešno napisane riječi i sl.*

na brzu reakciju - zastanite, ne samo da biste se zapitali "na šta me ova poruka nastoji navesti" ili "kako me pokušava natjerati na to", nego da biste dozvolili vašem racionalnom mozgu da sustigne vaš emocionalni mozak, tj. da se hemijska reakcija u mozgu koja bi uzrokovala otmicu amigdale poništi. Hitnost odgovora predstavlja dodatni stres na koji hakeri računaju. Podsjetite se da je ono što osjećate automatski odgovor, a ne nužno najbolji ili najlogičniji. Počnite brojati, dajte sebi vremena između impulsa i akcije, shvatite šta se događa, aktivirajte svoj frontalni logički dio mozga koji je tokom emocionalne reakcije inhibiran. Time ćete dobiti nekoliko trenutaka tokom kojih možete razmotriti



da li postoji bolji ili drugačiji izbor – uključit ćete logiku da proučite da li je elektronska poruka uopće valjana ili nije. Brže nije uvijek i bolje.

Na koje to emocije hakeri najčešće ciljaju?

Prevara je stara koliko i ljudska priroda, a phishing je prevara u cyber prostoru. Kada je u pitanju phishing, moguće je izgubiti sve samo jednim klikom. Zato ćemo se opet vratiti psihologiji. Prevaranti i kriminalci pažljivo osmišljavaju elektronske poruke za krađu identiteta kako bi manipulirali našim emocijama, iskoristili naše nesvjesne predrasude te nas zaveli da zaobiđemo logiku i kliknemo na link. Apelirajući na naše osobnosti i emocije, phishing nas pokušava natjerati da ostanemo u automatskom načinu rada. Hakeri žele da korisnici donose brze i nepromišljene odluke.

Da bi se to postiglo, phishing poruke manipuliraju nama preko takozvanih psiholoških principa uticaja,

> *Prevaranti i kriminalci pažljivo osmišljavaju elektronske poruke za krađu identiteta kako bi manipulirali našim emocijama, iskoristili naše nesvjesne predrasude te nas zaveli da zaobiđemo logiku i kliknemo na link.*

kao što su: autoritet, dosljednost, društveno dokazivanje, reciprocitet, sviđanje ili oskudica. Razumijevanjem naših ranjivosti i razloga zašto ljudi nasjedaju na ovakve prevare možemo početi pronalaziti načine da ih lako prepoznamo i izbjegnemo. Također, uz ova saznanja, obuke za odbranu od phishinga i krađe identiteta mogu biti mnogo učinkovitije. Psihološki faktori koji ljude čine ranjivima, te ih hakeri obično nastoje iskoristiti, su:

- stres (otvaramo elektronsku poštu, a u velikoj smo žurbi),
- strah (prijete nam zaključavanjem bankovnog računa, zadržavanjem novca, gubitkom posla, itd.),
- prekomjerno samopouzdanje (bez obzira na to koliko smo obrazovani ili osviješteni u pogledu cyber sigurnosti, otmicom amigdale naše racionalno razmišljanje više nije u igri),
- pohlepa (ono što nam se čini previše dobro, vjerovatno i nije istinito),
- hijerarhija i autoritet (svjesni smo da ljudi imaju tendenciju da se povinuju zahtjevima autoriteta).

Rad na daljinu

Veća zastupljenost rada na daljinu izazvana pandemijom COVID-19 utiče na psihološka stanja ljudi te ih čini ranjivima na prevare. Rad na daljinu donosi kombinaciju umora od videopoziva, osjećaja "uvijek uključen" i kućnih obaveza. Sve to doprinosi nedovoljnoj fokusiranosti zaposlenika. Ukoliko razmotrimo problem sa stanovišta cyber sigurnosti, bilo kakvo ometanje može narušiti naše sposobnosti donošenja odluka. Također, nemamo signale licem u lice pa je i valjanost elektronske pošte teže provjeriti kada niste u istoj kancelariji s kolegama. Prevare će uvijek biti prisutne, oko toga ne trebamo biti uvijek zabrinuti nego samo oprezni te upoznati se s taktikama koje hakeri mogu iskoristiti i psihološkim faktorima poput stresa, emocija i ometanja na koje trebamo obratiti pažnju. Pokušajmo uspostaviti rutinu - koliko je bitno brzo i efikasno odraditi posao, toliko je bitno i brinuti o sebi kada smo pod stresom ili umorni jer vidimo kako to može doprinijeti negativnom psihološkom uticaju i stvoriti rizike za cyber sigurnost.

> *Prevare će uvijek biti prisutne, oko toga ne trebamo biti uvijek zabrinuti nego samo oprezni te upoznati se s taktikama koje hakeri mogu iskoristiti i psihološkim faktorima poput stresa, emocija i ometanja na koje trebamo obratiti pažnju.*

Ukoliko ste kliknuli na *phishing* link

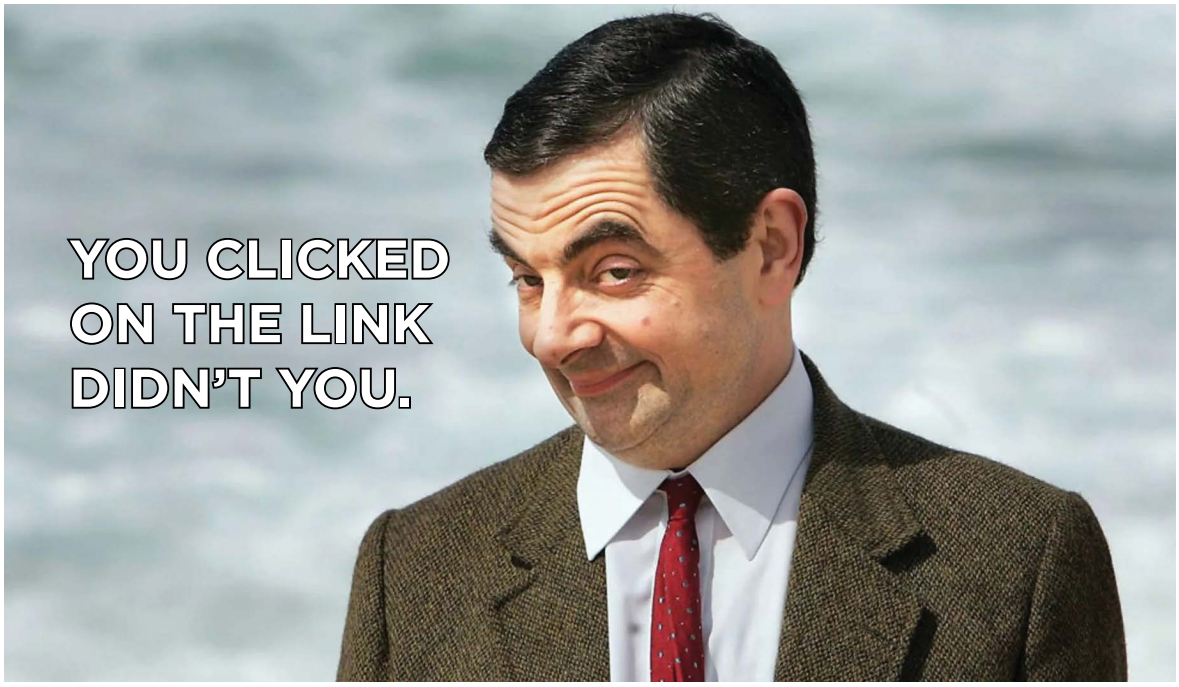
Pored sveg znanja i upozorenja, nekome će se ipak dogoditi da njegova amigdala bude "oteta" te da ipak klikne

na "pogrešan" link. Stoga ćemo dati i par općenitih savjeta šta učiniti ako se to desi:

- Odmah prekinite sesiju, tj. zatvorite stranicu koja vam se otvorila;
- Isključite svoj uređaj s interneta;
- Napravite sigurnosnu kopiju svih vaših fajlova;
- Izvršite potpuno skeniranje sistema koristeći svoj antivirusni softver;
- Promijenite lozinku za pristup svojoj e-mail aplikaciji;
- Prilikom promjene lozinke razmislite o aktiviranju dvofaktorske autentikacije što će obezbijediti dodatni nivo sigurnosti;
- Ukoliko postanete žrtva ovakve vrste napada u svojoj organizaciji, slijedite politiku vašeg poslodavca. Isključite računar kako biste spriječili širenje bilo kakvog malvera na mrežu.

Psihološka manipulacija kao fenomen poznata je od davnih vremena, daleko prije interneta i ostalih današnjih sistema i servisa. Zlonamjerne osobe su nagovaranje, pretvaranje ili lažno predstavljanje oduvijek koristile u cilju sticanja nezasluženih dobara. U današnje vrijeme napadi koji se zasnivaju na psihološkom iskorištavanju ljudi najveća su prijetnja u svijetu cyber sigurnosti.

S druge strane, ljudski faktor, za razliku od hardvera i softvera, nije moguće jednostavno usavršiti, unaprijediti - „zakrpiti". Edukacija i podizanje svijesti o potencijalnim prijetnjama i ranjivostima te načinima njihovog iskorištavanja su preventivne mjere, ali predstavljaju jedini način zaštite, obezbjeđuju potrebnu kontrolu te samim tim smanjuju rizik od potencijalnih opasnosti. ■



***Cyber* alerti**

VRSTE ONLINE PREVARA ZBOG KOJIH TREBA BITI NA OPREZU U 2023. GODINI

Phishing, ransomware, scareware, simulirane prevare vanrednih situacija te lažne internetske stranice za kupovinu samo su neke od online prevara za koje se predviđa da će se najčešće dešavati u 2023. godini.

Autor:
Amar Brkan

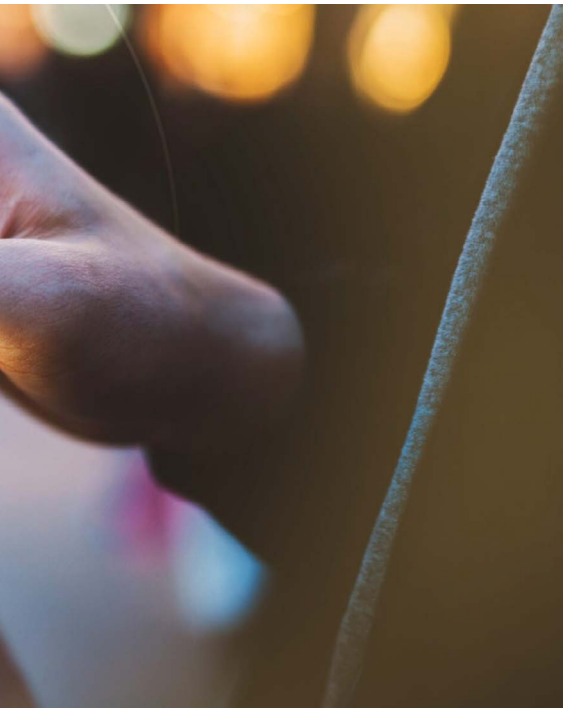
Kako značaj tehnologije raste iz godine u godinu, tako raste i interes *cyber* kriminalaca za pristup što većem broju ličnih i korporativnih informacija i podataka. Zbog toga je sada važnije nego ikada biti svjestan internetskih prijetnji kako ne biste postali sljedeća žrtva. Ovo su najčešće *online* prevare koje treba izbjegavati u 2023. godini.

1. *Phishing* prevara

Phishing ostaje jedna od najčešćih vrsta pokušaja prevare pri čemu *cyber* kriminalci koriste mamac za klikove kako

bi namamili žrtve da kliknu na zlonamjerno preuzimanje.

Ovako se obično odvija *phishing* prevara:



- *Cyber* kriminalac vam šalje e-mail za koji se čini da je iz legitimnog izvora, kao što je banka, stranica za društvene mreže ili *online* prodavnica;
- Na ovaj način ste prevareni da kliknete na zlonamjerno preuzimanje ili lažnu vezu;
- *Cyber* kriminalac instalira zlonamjerni softver i/ili koristi vaše kredencijale da ukrade vaše povjerljive podatke.
- Uobičajeni znakovi upozorenja *phishing* e-maila na koje treba obratiti pažnju su sljedeći:
- pravopisne greške i loša gramatika,
- tekst s fantastičnim porukama ponuda i izuzetnih dobitaka,
- e-mail poruke s prijetnjama s finansijskim ili pravnim posljedicama,
- logotipi entiteta sa sumnjivom slikom,
- adresa e-maila iz sumnjivih izvora.

2. *Ransomware*

Još jedna uobičajena vrsta internetske prevare je *ransomware*. U ovoj vrsti napada *cyber* kriminalci prijete da će objaviti lične podatke žrtve ili trajno blokirati pristup njima osim ako se ne plati otkupnina.

Da biste izbjegli *ransomware*, napravite sigurnosnu kopiju svojih podataka i redovno ažurirajte antivirusni softver kako bi vas upozorio na moguće pokušaje napada.

3. *Scareware*

Scareware je oblik zlonamjernog softvera koji koristi društveni inženjering da izazove šok, anksioznost ili percepciju prijetnje kako bi manipulisao korisnicima da kupuju neželjeni softver. Ovaj softver je lažan i koristi se za instaliranje zlonamjernog softvera koji može ukrasti povjerljive informacije.

Znakovi upozorenja *scarewarea* na koje treba obratiti pažnju su:

- softver vas odmah obavještava da skenira vaš računar na viruse,
- pop-up je teško zatvoriti,
- skočni prozor želi da reagujete brzo,
- nikad niste čuli za softversku kompaniju.
- Da biste izbjegli zastrašujući softver, pazite da ne kliknete na neočekivane obavijesti o zlonamjernom softveru.

4. Simulirane prevare vanrednih situacija

U ovim prevarama *cyber* kriminalac se predstavlja kao član porodice u vanrednoj situaciji kome je hitno potreban novac za neku hitnu situaciju – odlazak iz inostranstva, plaćanje bolničkog računa, kupovina novog mobilnog telefona.

Pandemija COVID-19 dodatno je olakšala prodaju uvjerljivih laži: „U bolnici sam s COVID-om. Molimo pošaljite novac odmah."

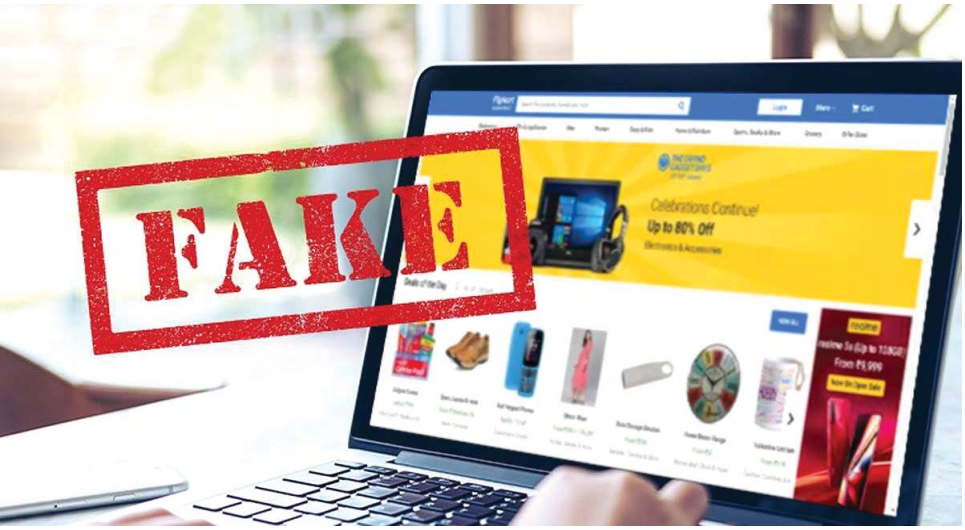
Da biste izbjegli ovu vrstu prevare:

- Oduprite se porivu da odmah djelujete. *Cyber* kriminalci apeluju na raspoloženje i vjeruju da ćete brzo reagovati – prije nego što budete imali priliku da razmislite o stvarima.
- Provjerite identitet kontakta. Postavljajte pitanja na koja stranac ne bi znao odgovor. Potvrdite priču s drugim članovima porodice ili prijateljima, čak i ako (ili posebno ako) sagovornik kaže da je čuvate u tajnosti.
- Nikada nemojte slati gotovinu, poklon vaučere ili transfere novca.

5. Lažne internetske stranice za kupovinu

Cyber kriminalci također mogu kreirati i objavljivati lažne sajtove za kupovinu na mreži koji izgledaju originalno ili repliciraju postojeće brendirane sajtove.

Uobičajeni znak lažnog web-mjesta za kupovinu je ako



Uobičajeni znak lažnog web-mjesta za kupovinu je ako se u radnji pojavi pretjerana ponuda, pronalaženje popularnih brendova i prodaju ih po izuzetno niskim cijenama.

se u radnji pojavi pretjerana ponuda, pronalaženje popularnih brendova i prodaju ih po izuzetno niskim cijenama. Ove stranice obično imaju URL-ove slične brendovima koje pokušavaju imitirati, kao što je **Amaz0n.net**. *Cyber* kriminalci koriste ove strategije kako bi podstakli kupovinu krivotvorenih proizvoda i zabilježili bankovne podatke u trenutku kupovine da bi ih sami koristili.

Formjacking je još jedna tehnika prevare. Ovo se dešava kada je legitimna web stranica za *online* prodaju hakovana i kupci su preusmjereni na lažnu stranicu za plaćanje gdje *cyber* kriminalac krade njihove lične podatke i podatke o kreditnoj kartici. Da biste izbjegli ovu prevaru, provjerite je li URL na stranici za plaćanje isti kao i web lokacija na kojoj kupujete. *Cyber* kriminalci mogu malo promijeniti URL, možda dodajući ili izostavljajući jedno slovo. Provjerite URL prije nego što unesete detalje plaćanja.

Znakovi upozorenja lažnih stranica za kupovinu uključuju:

- preusmjeravanje koje vodi na stranicu s "http://" u URL-u,
- pretjerano niske cijene,
- nema informacija o porijeklu stranice, nema ili su vrlo ograničene kontakt informacije i upitne recenzije.

Zaključak

Može se pretpostaviti da, ako vas neko pita za bankovne ili lične podatke, pokušava da vas prevari. Stoga, nikada ne biste trebali pružati lične podatke nikome na internetu ko vas direktno kontaktira. Ako trebate izvršiti finansijsku transakciju na mreži, pobrinite se da to učinite na sigurnom serveru i putem pouzdane web stranice.

Ako smatrate da ste prevareni, odmah promijenite sve svoje lozinke, izbrišite zlonamjerni softver koji ste možda preuzeli i kontaktirajte svoju banku ako postoji mogućnost prevare korištenjem vaše kreditne kartice. Obratite se lokalnoj policiji kako biste prijavili prijevaru i dobili pomoć oko narednih koraka. ■

Dugoročna strategija koja daje konkretne rezultate

COMPLIANCE NAŠ SVAGDANAŠNJI

Regulatorna usklađenost, integritet, etično postupanje, kodeks ponašanja, zaštita podataka, povjerljivost, zaštita potrošača, prevare, borba protiv korupcije, sukob interesa, procjena primjerenosti, ekološka osviještenost, socijalna osjetljivost, društvena odgovornost, sponzorstva, donacije, nabavke... sve to obuhvata compliance.

Autor:
Nermin Ibradžić

Šta je zajedničko kompanijama HSBC, IKEA, Chicago Hospital, Vauxhall, Pfizer, Quantas? Osnivači? Ne. Sjedište, geografsko odredište? Ne. Nisu čak na istom kontinentu. Djelatnost sigurno nije. Zajedničke su dvije stvari. Profit (stvaranje profita) i *compliance*. Sve navedene institucije imaju isti cilj. Stvaranje dobiti. Ali ne po svaku cijenu. Zato imaju *compliance*.

U igri asocijacija pojam *compliance* bi obuhvatio mnogo toga. Regulatorna usklađenost, integritet, etično postupanje, kodeks ponašanja, zaštita podataka, povjerljivost, zaštita potrošača, prevare, borba protiv korupcije, sukob interesa, procjena primjerenosti, ekološka osviještenost, socijalna osjetljivost, društvena odgovornost, sponzorstva, donacije, nabavke...

U osnovi, ne postoji pojam koji na kraju, na neki način,

ne bi doveo do *compliance* funkcije.

I onda, kada pogledamo šta sve pojam *compliance* danas obuhvata, vaša kolegica ili kolega, koji je službenik za usklađenost ili *compliance* oficir, ne izgleda više kao neko ko sa zelenim ili ružičastim markerom podvlači tekstove propisa i objašnjava zašto je bitno da li je zarez s lijeve ili desne strane pasusa, nego više kao „meštar“ ili žongler.

Žongler prema kojem akrobata u *Cirque du Soleil* izgleda kao pripravnik u trećerazrednoj općini negdje na brdovitom Balkanu. Lično nemam ništa protiv akrobata i općina. Ili Balkana.

Ali u jednom momentu upravljati s toliko različitih stvari zaista je umjetnost. Dakle, *compliance* nije samo znanje, zanat ili zvanje. Compliance je umjetnost. Kako od toliko nijansi propisa, odnosa, procesa, karaktera, želja, planova, strategija i ciljeva sačiniti djelo koje je lijepo, korisno, reputacijski neutralno (u najgorem slučaju), politički korektno i ujedno zrači integritetom, etičkim vrijednostima i usklađenošću. Regulatorni i etički zen.

Pitate se, a gdje je tu profit? Činjenica prva. Compliance u finansijskim institucijama sigurno nije u službi Vojske spasa ili *Greenpeacea*. Vrlo vjerovatno od vas neće tražiti da vraćate nasukane delfine nazad u vodu.

Compliance vam može pomoći da ostvarite profit. Ali na društveno prihvatljiv i etičan način. Zarada zasnovana na integritetu i ispravnom postupanju.

Kako *compliance* doprinosi businessu?

1. Jačanje povjerenja kupaca/klijenata

Niko ne želi trgovati ili stupati u poslovne odnose s prevarantima i smutljivcima. Snažna *compliance* funkcija znači i implementaciju visokih standarda zaštite kupaca, potrošača i klijenata.

Potrošač koji je uvjeren da institucija ili firma s kojom posluje primjenjuje visoke standarde i pruža zaštitu od prevara i štetnog postupanja, sigurno će se prije prikloniti takvoj instituciji nego onoj koja nema sluha za njegova prava kao potrošača i koja posluje po principu *take the money and run.*

> *Potrošač koji je uvjeren da institucija ili firma s kojom posluje primjenjuje visoke standarde i pruža zaštitu od prevara i štetnog postupanja, sigurno će se prije prikloniti takvoj instituciji nego onoj koja nema sluha za njegova prava kao potrošača.*

2. Povećanje prometa

Kroz tačku 1. (jačanje povjerenja klijenata/potrošača) nameće se tačka 2. Povećanje prometa. Formula je prilično jednostavna. Povećanje broja lojalnih klijenata znači povećanje prometa. Povećanje prometa znači povećanje zarade. Povećanje zarade znači neizmjerno zadovoljstvo dioničara. Uz *compliance* funkciju, sve to na društveno prihvatljiv i etičan način.

3. Unapređenje internih i eksternih procesa

Jaka *compliance* funkcija je jedan od osnova unapređenja internih procesa. Kroz edukacije *compliance* funkcije zaposlenici će dobiti jasnu sliku kako raditi ispravne stvari na ispravan način (mada je nemoguće isključiti pojedine, iznimno talentirane pojedince koji će i dalje raditi pogrešne stvari).

Dodatno, usklađenost procesa sa zakonima i standardima određene industrije osigurava da vlasnik i rukovodstvo, u određenom regulatornom okviru, mogu izvući maksimum, pri tome se ne plašeći sankcija i finansijskih gubitaka. Ne treba zanemariti ni eksterne procese u cijeloj priči. Primjena *compliance* standarda na vanjske dobavljače i suradnike može osigurati da isti ispune ciljeve i zahtjeve finansijske institucije na način koji osigurava potpunu usklađenost.

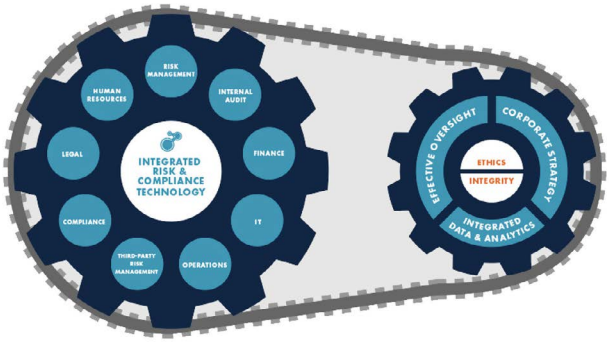
4. Zaštita institucije od pravnih postupaka

Usklađenost s regulatornim i etičkim standardima, ili

> *Usklađenost s regulatornim i etičkim standardima, ili posebnim standardima neke industrije, značajno smanjuje rizik od pravnih postupaka ili bar onih koje bi kompanija mogla da izgubi.*

posebnim standardima neke industrije, značajno smanjuje rizik od pravnih postupaka ili bar onih koje bi kompanija mogla da izgubi.

To, s druge strane, smanjuje i iznose rezervisanja koje kompanija mora da odvoji, kao i reputacijski rizik u kontekstu da će detalji nekog sudskog postupka dospjeti u javnost i izazvati negativne konotacije kod javnosti, a time i finansijsku štetu (uključivo i značajne iznose koje moramo izdvojiti da reputacijsku štetu saniramo).



5. Izbjegavanje kazni i odšteta

Jedan od osnovnih ciljeva *compliance* funkcije je smanjenje rizika od regulatornih kazni, prekršaja i odšteta. S druge strane, visoki standardi usklađenosti mogu značiti i dodatno smanjenje troškova i uštede ili čak dodatni profit. Tako usklađenost s nekim ekološkim ili socijalnim standardima može sa sobom nositi neke porezne ili druge olakšice, poticaje, povoljniji novac na tržištu kapitala i sl.

Da bi se postigli navedeni ciljevi, koji su istovremeno u službi usklađenosti i održivog profita, potrebno je ispunjenje određenih preduslova. Konkretno, svako unapređenje procesa, standarda i usklađenosti zahtijeva određeno ulaganje u alate, u ljude, u sisteme, kontrole i sl.

Efikasan *compliance*, utopija ili stvarna mogućnost?

Svi za sebe volimo misliti da smo najbolji u svom poslu. I to je sasvim OK. Jača samopouzdanje, motiviše nas, omogućava da se izborimo sa svakodnevnim izazovima.

Ipak, na kraju, to je naš subjektivni osjećaj, onako kako sami sebe vidimo. Prava istina koliko smo zapravo dobri vidi se kroz mjerenje efikasnosti posla koji radimo.

Mislite da efikasnost *compliance* funkcije nije moguće mjeriti? Imate osjećaj da radite dane i dane na jednom te istom, bez pomaka, bez rezultata? Niko ne priznaje vaš rad i kada vas pitaju šta konkretno radite, ne znate to objasniti?

Da, to može biti prilično demotivirajuće odvesti vas u vrtlog malodušnosti i frustracije iz kojeg je teško izaći.

A možda samo nemate jasnu *compliance* strategiju i plan? Vjerovali ili ne, koliko god se čini da je u srži *compliance* funkcije *ad hoc* i *case by case* postupanje, *compliance* dugoročna strategija je, ustvari, ono što daje konkretne rezultate.

Da bi bila uspješna, treba ispoštovati neke osnove.

1. Planirajte unaprijed

Predviđanje i pogled unaprijed umjesto žaljenja za onim što je bilo?

Da, u *complianceu* uvijek i svugdje.

Planirajte unaprijed i riješite se nepotrebnog stresa. Planovi rada ne trebaju biti samo ispunjenje forme. Oni moraju donijeti suštinska unapređenja.

Da li provjeravate sjednice zakonodavnih organa i kada bi koji nacrt zakona mogao biti na kojoj sjednici? Prezentirate li nacrte zakona nadležnim službama?

Planirate li edukacije prema događajima koji se sezonski redovno ponavljaju? Npr. edukacija o darovanju prije novogodišnjih praznika, edukacija o sponzorstvima po usvajanju budžeta za donacije i spozorstva, edukacija o značaju antikorupcije i sprečavanja sukoba interesa prije važnih izbora ili nakon nekih većih policijskih akcija protiv privrednog kriminala. Ankete, kada su ljudi najodmorniji?

> *Planiranje unaprijed će vam dati i jednu dodatnu vrijednost. Odnos između onog što ste već uradili prema onom što vas tek čeka. I već tada ćete znati koliko ste bili, a koliko želite biti efikasni.*

Opširne edukacije nikad krajem izvještajnog kvartala, ali kratke edukacije vezane za etično poslovanje i interne i eksterne prevare da. Planiranje unaprijed će vam dati i jednu dodatnu vrijednost. Odnos između onog što ste već uradili prema onom što vas tek čeka. I već tada ćete znati koliko ste bili, a koliko želite biti efikasni.

2. Sakupljanje i analiza podataka

Prikupljajte podatke. Oni vam mogu puno toga reći. Prigovori klijenata, izlazni intervjui zaposlenika koji odlaze iz banke, rast ili pad broja disciplinskih postupaka, nalazi interne revizije i regulatora, prijave operativnih rizika, rast ili pad broja i iznosa donacija i sponzorstava, broj postupaka nabavke i vrijednost nabavke, broj vendora koji su ponovno izabrani za pružanje neke usluge, prisustvo na raznim komisijama i odborima unutar banke (za praćenje rezultata, rješavanje prigovora i sl.). Niti jedan podatak nije nevažan.

Jednom kad uspostavite svoju ličnu evidenciju informacija koje želite imati i pravilno je struktuirate, imat ćete i statistički uporedive podatke koji vam mogu dati podlogu za odluku gdje su potrebne dodatne edukacije i zašto, gdje je potrebno djelovati malo oštrije i zašto. Podaci koje prikupite su vaš saveznik i iz njih je jasno vidljivo da li se u banci unapređuje ili unazađuje ono što *compliance* radi i kontroliše.

3. Pratite kretanja u jednom vremenskom okviru

Rast broja prigovora klijenata za 30% na godišnjem nivou, veći broj prijava mobinga, veći broj preporuka interne revizije, viša rezervisanja za kreditne gubitke, lošija ocjena na SREP-u... Mislite da vas se ovo mnogo ne tiče jer nije u vašoj liniji direktne odgovornosti? Varate se.

Praćenje opipljivih podataka iz domena ključnih rizika je izuzetno bitno.

Ono vam može pružiti i jasnu sliku o tome koliko su vaš *compliance* program i vaša strategija efikasni.

Broj prijavljenih poklona raste nakon vaše edukacije? Broj prijavljenih potencijalnih sukoba interesa raste nakon što ste svima pojasnili da to (još uvijek) nije krivično djelo?

Imate puno pravo da tvrdite da je to vaša zasluga. Podaci to pokazuju. Ali ako ih ne pratite, nećete nikad biti sigurni koliko ste uspješni ili efikasni.

4. Kreirajte sistem eskalacija /podizanja problema na viši nivo

Ništa ne može riješiti problem brže od efikasnog sistema eskalacije tog istog problema. Jasno je da rukovodioci ne mogu biti odgovorni za operativno izvršenje preporuka *compliance* funkcije. Međutim, oni su i dalje odgovorni da stvore uslove da vaše preporuke budu realizirane.

Žao vam je kolege ili kolegice koji već tri mjeseca kasni sa izvršenjem preporuke jer znate da ima mnogo drugih obaveza? Zapitajte se da li ćete i dalje biti tako bliski u momentu kada vas, zbog neizvršenja te iste preporuke, pred bankom dočeka sasvim

> *Jasno je da rukovodioci ne mogu biti odgovorni za operativno izvršenje preporuka compliance funkcije. Međutim, oni su i dalje odgovorni da stvore uslove da vaše preporuke budu realizirane.*

opravdano razjarena grupa deponenata naoružanih vilama i drugim priručnim alatkama i koji ne mogu do svog novca jer je vama bilo žao.

Sistem eskalacije nije „tužakanje" nego insistiranje na izvršenju onog što je najbolje za banku u dijelu usklađenosti. Na banalnom primjeru iz stvarnog života to izgleda ovako. Rezervisali ste i platili kartu za neku super predstavu u prvom redu. Dolazite u pozorište i kažu vam da su vaša mjesta već zauzeta i data nekom drugom. Da li se okrećete i odlazite s napomenom da ćete doći ponovo za 15 dana ili tražite da razgovarate s nekim od šefova koji vam može pomoći? Dobar *compliance* ne bi trebao imati problem s eskalacijom problema iz dva razloga: a) zato što propis tako nalaže i b) zato što čuva interes banke, a ne svoj lični interes.

5. Edukacije

Kako očekivati od bilo koga da zna kako postupiti ako ga nismo tome poučili? Da, jasno, određene norme, zdrava logika i ponašanja se očekuju u radu u finansijskim institucijama, ali ne treba zaboraviti da ih kod pojedinca prije svega kreiraju porodica, škola i društvo.

A nisu sve porodice iste, zar ne? Prema tome, osim standardizacije procesa, postupaka i prihvatljivog ponašanja, jako je bitno sve zaposlenike poučiti zašto je to važno. I ako im nije važno, koje su posljedice. Edukacije trebaju pratiti aktuelne trendove događanja na tržištu, u branši ili u banci. Edukacija o prevari čekovima iz 1998. godine izgleda zanimljivo. Da. Ali zar nismo sad u eri kriptovaluta i digitalnih transfera novca u 2 minuta s kraja na kraj svijeta?

Za efikasan *compliance* edukacija je jako moćna „poluga".

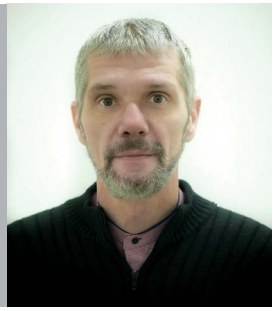
Naprijed navedeni prijedlozi su samo dio „asortimana" koji može pomoći da se efikasnost compliance funkcije mjeri i procijeni te da se na osnovu toga donese ocjena temeljena na objektivnim, a ne subjektivim kriterijima. Kao nužno u tom procesu potrebno je cijeniti saradnju između compliance oficira u cijelom bankarskom sektoru. Dobre compliance prakse drugih kolegica/kolega su i više nego dobrodošle jer će nekom drugom smanjiti potrebno vrijeme za realizaciju i procjenu.

Zato je jako bitno da compliance funkcije međusobno komuniciraju i zato su bitne zajedničke edukacije i okrugli stolovi s regulatorom i svim drugim nosiocima funkcija koje su vezane ili jesu compliance. ■

Prepoznavanje i prevencija

ŠTA JE INSAJDERSKA PRIJETNJA I KAKO SE ZAŠTITITI?

Ukoliko je zaposlenik nezadovoljan svojim radnim uslovima, platom, kolegama ili smatra da je organizacija prema njemu nepravedna, može iskoristiti svoju poziciju za nezakonite radnje te time nanijeti neprocjenjivu štetu svojoj organizaciji.



Autor:
Eldin Mulić

Insajderska prijetnja je prijetnja koja dolazi iz unutrašnjosti organizacije, odnosno od ljudi koji su već zaposleni u organizaciji ili imaju neki drugi legitimni pristup unutar nje. Ova vrsta prijetnje može biti posebno opasna jer ljudi koji su u vezi s organizacijom mogu imati pristup osjetljivim podacima ili sistemima te ih mogu iskoristiti za nezakonite radnje.

Pored navedenog, insajderske prijetnje mogu se definisati i kao vrsta sigurnosnog rizika koji proizlazi iz unutarnjih izvora. Ove prijetnje mogu dolaziti od zaposlenika, bivših zaposlenika, saradnika ili čak od članova porodice zaposlenika. Oni imaju pristup povjerljivim podacima i sistemu unutar organizacije, a što ih čini posebno opasnim.

Jedna od glavnih insajderskih prijetnji je krađa povjerljivih podataka. Ovo može uključivati sve od ličnih podataka klijenata ili drugih zaposlenika pa do komercijalnih i poslovnih tajni. Zaposlenici, koji su izloženi ličnim, društvenim ili finansijskim pritiscima, mogu biti skloni da kradu podatke kako bi ih prodali u svrhu obezbjeđivanja materijalne koristi ili ih koristili za vlastite svrhe.

> *„Zaposlenici, koji su izloženi ličnim, društvenim ili finansijskim pritiscima, mogu biti skloni da kradu podatke kako bi ih prodali u svrhu obezbjeđivanja materijalne koristi ili ih koristili za vlastite svrhe."*

Druga vrsta insajderske prijetnje je sabotiranje sistema. Ovo se može dogoditi kada je zaposlenik nezadovoljan svojim radnim uslovima, platom, kolegama ili smatra da je organizacija prema njemu nepravedna. Oni mogu naškoditi sistemu unutar organizacije što bi moglo dovesti do prekida rada, gubitka podataka i na kraju do finansijske štete za organizaciju. Insajderske prijetnje mogu uključivati i neovlašteno korištenje resursa. Zaposlenici mogu neovlašteno koristiti poslovne kompjutere, telefone ili druge resurse za vlastite svrhe što može dovesti do gubitka učinkovitosti i produktivnosti i opet do finansijske štete za organizaciju.

Kako prepoznati i prevenirati?

Da bi se spriječile insajderske prijetnje, organizacije trebaju imati dobro definisane sigurnosne politike i procedure. Zaposlenici trebaju biti edukovani o sigurnosnim rizicima i odgovornostima vezanim uz njihov rad. Također, važno je redovno provoditi sigurnosne provjere zaposlenika kako bi se identificirali potencijalni rizici.

Osiguravanjem odgovarajuće sigurnosti i edukacijom zaposlenika, organizacije mogu smanjiti rizik od insajderskih prijetnji i zaštititi svoje povjerljive podatke i sisteme.

Plan zaštite od insajderskih prijetnji je dokument koji detaljno opisuje kako organizacija planira spriječiti i suzbijati insajderske prijetnje. Sam plan ne može zaštiti ništa, ali postupanje po njemu može. Ovaj plan obično uključuje detaljne postupke za identificiranje i praćenje unutarnjih sigurnosnih rizika, kao i mjere za sprečavanje i otkrivanje insajderskih prijetnji.

Plan zaštite od insajderskih prijetnji obično uključuje sljedeće elemente:

1. **definiciju** insajderskih prijetnji i načina na koje one mogu utjecati na organizaciju,
2. **analizu** postojećih sigurnosnih procedura i pravila vezanih uz radne uvjete, rad s povjerljivim podacima i korištenje resursa,
3. **plan za identificiranje potencijalnih insajderskih prijetnji** kroz redovne sigurnosne provjere zaposlenika i monitoring rada,
4. **plan za reagiranje na insajderske prijetnje** uključujući postupke za ispitivanje i sankcioniranje zaposlenika i
5. **edukaciju zaposlenika** o insajderskim prijetnjama i njihovim odgovornostima vezanim uz sigurnost podataka i sistema.

Plan zaštite od insajderskih prijetnji važan je dio cjelokupnog sigurnosnog programa organizacije. On omogućava organizaciji da prepozna i suzbije insajderske prijetnje prije nego što one nanesu štetu. Postoji nekoliko načina na koje organizacije mogu prepoznati insajderske prijetnje. Važno je redovno provoditi sigurnosne provjere zaposlenika i nadzor njihovog rada kako bi se identificirali potencijalni rizici. Također je važno pratiti promjene u ponašanju zaposlenika i obratiti pažnju na bilo kakve sumnjive aktivnosti, a pri tome definisati nivoe rizika za pojedina radna mjesta.

Sljedeći su neki znakovi koji bi organizaciji trebali dati do znanja da se može događati insajderska prijetnja:

- zaposlenik ima pristup povjerljivim podacima i sistemu, ali ima finansijske ili lične probleme;
- zaposlenik ima loše odnose s kolegama ili poslodavcem;
- zaposlenik ima neovlašteni pristup resursima organizacije ili ih koristi za vlastite svrhe;
- zaposlenik pokazuje nestabilnost u svom ponašanju ili promjenu u navikama;
- zaposlenik ima povećan interes za povjerljive podatke ili sistem organizacije.

Ako se prepoznaju ovakvi znakovi, organizacija bi trebala odmah poduzeti odgovarajuće mjere kako bi spriječila insajdersku prijetnju. To bi moglo uključivati razgovor sa zaposlenikom, ograničavanje pristupa povjerljivim podacima ili čak otpuštanje zaposlenika ako se utvrdi da je izvršio neovlaštene radnje.

Insajderske prijetnje mogu nanijeti različite vrste šteta organizaciji. Zavisno o tome koji su podaci ili sistem unutar organizacije, moguće su sljedeće vrste potencijalnih šteta:

- Gubitak povjerljivih podataka kao što su lični podaci klijenata ili poslovne tajne. Ovo može dovesti do gubitka povjerenja klijenata i šteti ugledu organizacije.

- Sabotiranje sistema. Ovo može dovesti do prekida rada i gubitka podataka, a što bi moglo nanijeti velike finansijske gubitke organizaciji.
- Neovlašteno korištenje resursa. Ovo može dovesti do smanjenja produktivnosti i učinkovitosti zaposlenika, a što bi moglo utjecati na finansijske rezultate organizacije.

Zato je od velike važnosti da organizacije prepoznaju insajderske prijetnje i poduzmu odgovarajuće mjere kako bi ih spriječile ili suzbile. To može uključivati edukaciju zaposlenika o sigurnosti, redovne sigurnosne provjere i dobro definisane sigurnosne politike i procedure.

> *Od velike je važnosti da organizacije prepoznaju insajderske prijetnje i poduzmu odgovarajuće mjere kako bi ih spriječile ili suzbile. To može uključivati edukaciju zaposlenika o sigurnosti, redovne sigurnosne provjere i dobro definisane sigurnosne politike i procedure.*

Postoji više razloga zbog kojih se insajderske prijetnje pojavljuju. Među glavnim razlozima su sljedeći:

- zaposlenik ima finansijske ili lične probleme i vidi krađu podataka ili sabotiranje sistema kao način da riješi svoje probleme;
- zaposlenik ima loše odnose s poslodavcem ili kolegama i vidi sabotiranje sistema kao način da se osveti racionalizirajući pri tome svoje postupke tražeći opravdanje;
- zaposlenik ima nezadovoljstvo radnim uslovima ili smatra da je organizacija prema njemu nepravedna i vidi sabotiranje sistema kao način da se osveti;
- zaposlenik ima nedostatak edukacije o sigurnosti i nije svjestan posljedica svojih radnji;
- zaposlenik je pod utjecajem vanjskih faktora, kao što su pritisak od strane konkurentne organizacije ili kriminalne skupine (ucjena), i vidi insajdersku prijetnju kao način da zaradi novac ili zadovolji zahtjeve vanjskih faktora.

Sprečavanje insajderskih prijetnji zahtijeva da se organizacije fokusiraju na razumijevanje ovih razloga i da poduzmu odgovarajuće mjere kako bi spriječile da se insajderske prijetnje dogode. To može uključivati edukaciju zaposlenika o sigurnosti, pružanje podrške zaposlenicima u teškim situacijama i redovne sigurnosne provjere.

Postoji nekoliko načina na koje organizacije mogu ublažiti insajderske prijetnje. Uobičajeni načini su sljedeći:

1. **Dobro definisane sigurnosne politike i procedure.** Organizacije trebaju imati jasno definisane sigurnosne politike i procedure koje se odnose na rad

s povjerljivim podacima i korištenje resursa. Ove politike i procedure trebaju biti jasno objavljene i redovno se trebaju provjeravati i ažurirati.

2. **Edukacija zaposlenika o sigurnosti.** Organizacije trebaju edukovati svoje zaposlenike o sigurnosnim rizicima i odgovornostima vezanim uz njihov rad. Ovo uključuje obuku o pravilima i procedure vezanim uz rad s povjerljivim podacima i korištenje resursa.
3. **Redovne sigurnosne provjere zaposlenika.** Organizacije trebaju redovno provoditi sigurnosne provjere zaposlenika kako bi identifikovale potencijalne rizike. Ove provjere mogu uključivati pregled finansijskih ili ličnih podataka zaposlenika, a što uključuje i eventualne probleme te provjeru radnih odnosa i praćenje rada zaposlenika.
4. **Plan za reagovanje na insajderske prijetnje.** Organizacije trebaju imati jasan plan za reagovanje na insajderske prijetnje koji uključuje postupke za ispitivanje i sankcionisanje zaposlenika. Ovaj plan treba biti jasno definisan i treba se redovno provjeravati i ažurirati.

Ako se sumnja da je došlo do curenja podataka, organizacija bi trebala poduzeti odgovarajuće mjere za istraživanje ovog događaja. Sljedeći su neki koraci koji bi se mogli poduzeti u takvoj situaciji:

1. Odmah blokirati pristup povjerljivim podacima i sistemu. To će spriječiti da se podaci i dalje koriste za neovlaštene svrhe i omogućit će da se provjere njihove sigurnosti.
2. Obavijestiti odgovorne osobe o curenju podataka. To uključuje IT, sigurnosni tim i druge relevantne pozicije koje bi mogle pomoći u istraživanju događaja.
3. Izvršiti detaljnu analizu sigurnosnih zapisa i drugih relevantnih podataka. Ovo će vam pomoći da identificirate tačno kada se curenje podataka dogodilo i ko bi mogao biti odgovoran za to.
4. Provjeriti zapise rada zaposlenika i pratiti njihove aktivnosti. Ovo će pomoći da se identifikuju bilo kakve sumnjive aktivnosti ili promjene u ponašanju zaposlenika.
5. Razgovarati sa zaposlenicima koji su imali pristup povjerljivim podacima. Ovo će pomoći da se sazna da li je bilo koji od tih zaposlenika imao motiv ili mogućnost da izvrši krađu podataka.
6. Analizirati posljedice curenja podataka i poduzeti odgovarajuće mjere za njihovo otklanjanje. Ovo uključuje obavještavanje relevantnih strana, poput klijenata ili regulatornih tijela, te poduzimanje mjera za zaštitu podataka i sistema od budućih curenja.

Istraživanje curenja podataka je važan dio zaštite organizacije od insajderskih prijetnji. To puno pomaže da se utvrdi uzrok curenja podataka te da se poduzmu odgovarajuće mjere za njegovo sprečavanje u budućnosti. Ono što je bitno naglasiti, na kraju, je da sprečavanje insajderskih prijetnji zahtijeva stalnu brigu i pažnju. Organizacije trebaju redovno provjeravati svoje sigurnosne procedure i educirati zaposlenike kako bi se smanjio rizik od insajderskih prijetnji. ■

PROFIL FRAUD MENADŽERA

Prevara se može dogoditi bilo kada i ne postoji garancija da smo u potpunosti zaštićeni od iste. U nastavku donosimo vam niz vještina i znanja koje svaki fraud menadžer treba posjedovati kako bi svoju organizaciju zaštitio od neovlaštenih aktivnosti.

Autor:
Vedran Vinšalek

Finansijske institucije su izložene mnogim vrstama rizika od prevara, od interne prevare, kao što je zloupotreba imovine banke, do eksterne prevare kada klijenti (ili treća lica) zloupotrebljavaju slabosti u sistemima, procesima i proizvodima institucije u svoju vlastitu korist. Općepoznato je da se prevara može dogoditi bilo kada i da ne postoji garancija da smo u potpunosti zaštićeni od iste.

Implementacija adekvatnih mjera mitigacije rizika od nastanka neovlaštenih aktivnosti može spriječiti nastanak prevarne aktivnosti, pomoći u bržem otkrivanju iste i smanjiti finansijske gubitke.

Rizik od nastanka prevare može se mitigirati:

- kroz efikasno definisanje uloga i odgovornosti u procesu upravljanja prevarama;
- kroz implementaciju efikasnog sistema internih kontrola;
- kroz blagovremeno i adekvatno postupanje prilikom prijave svake sumnje na prevaru;

- kroz definisanje adekvatnih preventivnih i korektivnih mjera te
- kroz aktivnosti podizanja svijesti o upravljanju rizikom od prevara.

Kako bi uspješno upravljali aktivnostima vezanim za upravljanje prevarama, u nastavku se nalaze neke od najvažnijih vještina ***fraud menadžera*** koje je poželjno posjedovati u svakodnevnom radu.

Analitičke vještine

Aktivnosti upravljanja prevarama su analitički procesi u kojima se identificiraju scenariji koji bi se mogli dogoditi, uzroci i pokazatelji, štete koje bi te prevare mogle generirati te načine na koje ispitati i pratiti pokazatelje koji su otkriveni. Navedene aktivnosti zahtijevaju značajnu količinu dijagnostičkog i istraživačkog rada da bi se otkrilo šta se zaista događa.

Vještina otkrivanja prevara

Menadžeri trebaju biti u mogućnosti otkriti prevarne aktivnosti kako bi spriječili da do njih dođe. To od njih zahtijeva da imaju temeljno razumijevanje poslovanja i finansijske evidencije kompanije, kao i sposobnost da identifikuju nepravilnosti koje mogu ukazivati na prevaru. Oni, također, moraju biti u mogućnosti da brzo i precizno analiziraju velike količine podataka kako bi pronašli dokaze o prevari.

Vještine rješavanja problema

Vještine rješavanja problema neophodne su fraud menadžerima da bi identificirali i riješili probleme. Oni koriste ove vještine kada pregledavaju podatke, analiziraju trendove i istražuju slučajeve prevare. Uz snažne sposobnosti rješavanja problema, fraud menadžer može brzo i efikasno pronaći izvor problema. To im omogućava da minimiziraju svaku štetu uzrokovanu prevarom i zaštite imovinu svoje kompanije.

Istražne vještine

Potrebna je detaljna istraga da bi se otkrila prevara. Fraud menadžeri koriste svoje istražne vještine kako bi ispitali podatke i utvrdili postoje li nepravilnosti u informacijama. Također istražuju sumnjive aktivnosti intervjuisanjem zaposlenih, pregledom dokumenata i analizom transakcija. To im pomaže da identifikuju potencijalne rizike i spriječe buduće prevarne aktivnosti.

Upravljanje vremenom

Upravljanje vremenom je sposobnost planiranja i izvršavanja zadataka na način koji osigurava da ispoštujete rokove. Kao fraud menadžeru, vještine upravljanja vremenom su važne jer vam omogućavaju da završite svoj posao prema rasporedu i osiguravate da sve preporuke koje date imaju dovoljno dokaza.

Upravljanje rizikom

Fraud menadžeri koriste svoje vještine upravljanja rizicima kako bi procijenili potencijal za prevaru u kompaniji. Oni analiziraju podatke i daju preporuke o tome kako kompanije mogu smanjiti svoju izloženost prevarama. Naprimjer, ako analitičar primijeti da nekoliko zaposlenih ima pristup velikim količinama gotovine, može preporučiti primjenu novih mjera sigurnosti ili promjenu uloga zaposlenika kako bi se ograničila potencijalna mogućnost štete.

Komunikacijske vještine

Fraud menadžeri provode mnogo vremena intervjuirajući svjedoke i osumnjičene te komunicirajući s relevantnim tijelima (sudovi, tužilaštva). Dobar komunikator će znati kako tražiti dokaze i priznanja, kako strukturirati pitanja i intervjue i kako pisati izvještaje koje su razumljivi. Fraud

> *Fraud menadžeri moraju biti osobe od povjerenja i ulijevati sigurnost svim zaposlenicima kako bi se isti mogli „otvoriti“ prema njima i ukazati na štetne događaje i aktivnosti.*

menadžeri moraju biti osobe od povjerenja i ulijevati sigurnost svim zaposlenicima kako bi se isti mogli „otvoriti“ prema njima i ukazati na štetne događaje i aktivnosti.

IT vještine

Razvojem tehnologije moguće je vrlo efikasno analizirati ogromne baze podataka. Dostupni alati i baze pružaju neke od najboljih dokaza da li je počinjena prevara ili ne. Otkrivanje i istraga prevara u realnom vremenu sve više uključuje korištenje tehnologije.

Finansijska analiza

Finansijska analiza je sposobnost tumačenja finansijskih podataka i predviđanja na osnovu njih. Fraud menadžeri koriste vještine finansijske analize kada pregledaju aplikacije, analiziraju transakcije i procjenjuju tokove prihoda.

Organizacijske vještine

Snažna organizacijska vještina važna je za fraud menadžere jer im omogućava da prate mnoge datoteke i dokumente koje mogu da efikasnije analiziraju podatke i identifikuju potencijalne rizike. Također im pomaže da komuniciraju s drugim članovima organizacije kao što su rukovodioci ili menadžeri.

biti tokom istrage, kao i da efikasno organizuju tim eksperata koji učestvuje u istrazi. Efikasna organizacija prikupljanja informacija će omogućiti da završe istragu na vrijeme.

Poslovno znanje

Jako je bitno vladati poznavanjem poslovanja i procesa srodnih sektora u instituciji, posebno procesom prodaje. Ovo znanje je važno za fraud menadžere jer im omogućava

Fleksibilnost

Fleksibilnost je sposobnost prilagođavanja promjenjivim okolnostima. Kao fraud menadžer možda ćete morati prebaciti fokus s jednog zadatka na drugi ili promijeniti radno vrijeme ako je potrebno. Fleksibilnost vam može pomoći da ostanete fokusirani na završetak posla i ispunjavanje rokova, a istovremeno se prilagođavate nepredviđenim promjenama u rasporedu.

Ostale vještine koje su izuzetno korisne fraud menadžerima su sljedeće:

- poznavanje građanskih i krivičnih zakona, kriminologije, pitanja privatnosti, prava zaposlenih, drugih pravnih pitanja vezanih za prevaru;
- istraga i rješavanje prevara uvijek uključuje pravna pitanja kao što su: da li slučaj treba voditi u krivičnim ili građanskim sudovima, da li su određene tehnike prikupljanja dokaza zakonite, kada treba uključiti provođenje zakona i slično;
- poznavanje ljudskog ponašanja, uključujući zašto i kako ljudi racionalizuju nepoštenje, kako reaguju kada su uhvaćeni i koji je najefikasniji način da se pojedinci odvrate od prevare. ■

Edukativni prilog

CASE STUDY KAO EFIKASNA EDUKATIVNA METODA ZA SPREČAVANJE KREDITNIH PREVARA

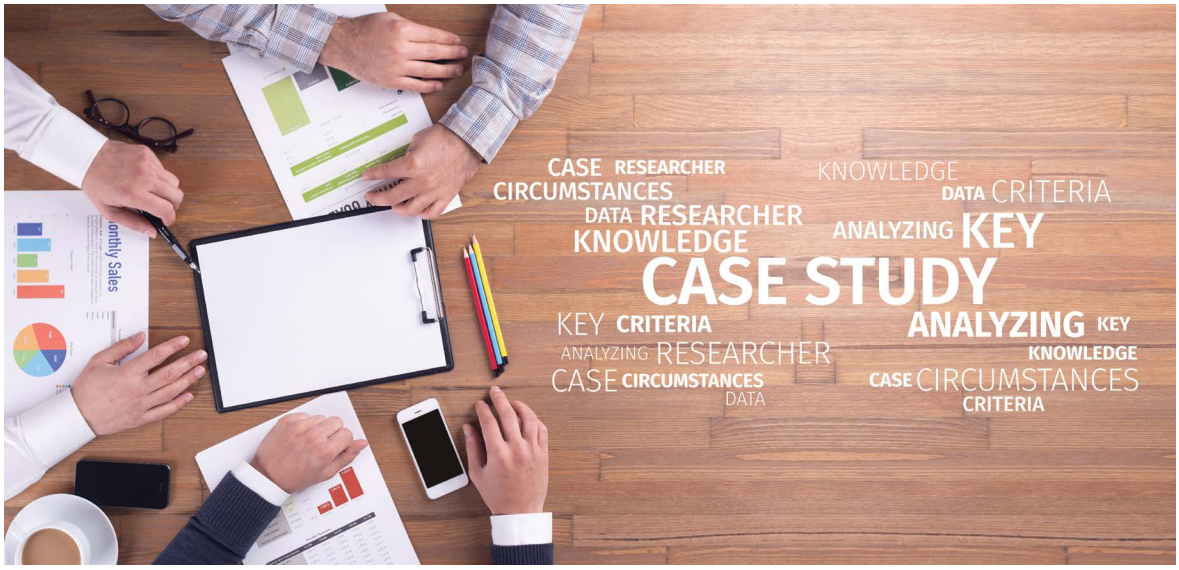
Kreditni službenici su prvi koji mogu posumnjati na elemente prevare ili prevarno ponašanje. Pored znanja o pravilima i procedurama, neophodni su i kontinuiran trening i edukacija o posljednjim aktuelnostima na temu prevarnih obrazaca.

Autor:
Uredničkitim Fraud Info

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

Kreditni službenici su prvi koji mogu posumnjati na elemente prevare ili prevarno ponašanje. Pored znanja o pravilima i procedurama, neophodni su i kontinuiran trening i edukacija o posljednjim aktuelnostima na temu prevarnih obrazaca. Organizacije koje imaju programe obuke za borbu protiv prevara doživljavaju manje skupe gubitke, brže rješavaju slučajeve prevare i imaju poboljšanu reputaciju u zaštiti korisnika usluga. Stoga, uposlenici trebaju biti kontinuirano educirani o tome koje radnje predstavljaju prevaru, kako prevara šteti svima u organizaciji i kako prijaviti sumnjivu aktivnost.

> *„Organizacije koje imaju programe obuke za borbu protiv prevara doživljavaju manje skupe gubitke, brže rješavaju slučajeve prevare i imaju poboljšanu reputaciju u zaštiti korisnika usluga."*



Case study ili *Studija* slučaja kao edukativna metoda

Studije slučaja se već dugo koriste u poslovnim školama, pravnim školama, medicinskim školama i društvenim naukama, ali se mogu koristiti u bilo kojoj disciplini ili djelatnosti kada treneri žele da **sudionici istraže kako se ono što su naučili primjenjuje na situacije u praksi**. Naime, većina zadataka kod Studija slučaja zahtijeva od učesnika da odgovore na otvoreno pitanje ili razviju rješenje otvorenog problema s više mogućih rješenja.

> *Primjeri i slučajevi iz prakse imaju najveći uticaj na uposlenike, prema mnogim stručnim istraživanjima, upravo iz razloga što šalju najsnažniju poruku.*

Primjeri i slučajevi iz prakse imaju najveći uticaj na uposlenike, prema mnogim stručnim istraživanjima, upravo iz razloga što šalju najsnažniju poruku. Dakle, pored izlaganja o teoretskom dijelu iz oblasti politika i procedura sprečavanja kreditnih prevara, **kroz interaktivne vježbe koje omogućava Studija slučaja, uposlenici su u prilici iskazati svoje vještine i usvojena znanja kako uočiti potencijalno sumnjivo ponašanje** klijenta, nedosljednosti i potencijalni falsifikat dokumenta ili nekog elementa sa Zahtjeva za kredit i sl. Ovakva vrsta treninga doprinosi i jačanju samopouzdanja kod uposlenika jer **s treninga nose potrebnu vrstu znanja i iskustva koju će primjenjivati u svakodnevnom radu**.

Prednosti upotrebe Studije slučaja u praksi

Glavni ciljevi edukacije putem Studije slučaja su sljedeći:

- **Praktična obuka**: Kroz realistične problemske situacije iz svakodnevnog rada, studije slučaja mogu

pomoći u pripremi uposlenika za djelovanje u profesionalnom i radnom životu;

- **Motivacija**: Realan slučaj potiče uposlenike da se aktivno uključe u Studiju slučaja;
- **Sticanje i primjena znanja**: Znanje se stiče kroz praktične situacije, a teorijski koncepti se primjenjuju u uslovima prakse;
- **Komunikacijske i konfliktne vještine**: Ako se Studija slučaja rješava u obliku grupnog rada, mogu se poboljšati i komunikacijske vještine uposlenika. Također, uče kako da se nose s mišljenjima i kritikama svojih kolegica i kolega i kako da rješavaju sve sukobe koji se pojave. Tokom prezentacije rezultata uposlenici mogu uvježbati svoje prezentacijske i argumentacijske vještine;
- **Nezavisnost**: U Studijama slučaja uposlenici mogu planirati vlastiti proces učenja i naučiti preuzeti odgovornost za njega;
- **Vještine rješavanja problema i donošenja odluka**: Srž Studije slučaja sastoji se od složene, realne problemske situacije iz profesionalnog i radnog života na osnovu koje uposlenici razvijaju, diskutuju i odabiru alternativna rješenja:
  - uposlenici uče da prepoznaju i analiziraju navedene probleme,
  - na osnovu dobijenih informacija uposlenici razvijaju različita alternativna rješenja i ocjenjuju ih te
  - uz pomoć evaluiranih opcija rješenja uposlenici donose utemeljenu odluku u korist rješenja.

U najjednostavnijoj primjeni, prezentacija Studije slučaja uspostavlja okvir za analizu. Studija slučaja bi trebala pružiti dovoljno informacija sudionicima da pronađu rješenja, a zatim da identifikuju kako primijeniti ta rješenja u drugim sličnim situacijama. Treneri mogu izabrati da koriste i nekoliko slučajeva kako bi sudionici mogli identifikovati i sličnosti i razlike među slučajevima.

Studije slučaja pokušaja kreditne prevare

U Studiji slučaja namijenjenoj konkretno za kreditne službenike, najbolje je unaprijed pripremiti nekoliko primjera Studija slučaja u kojima su pravovremeno spriječeni pokušaji kreditne prevare ili su se neki čak i dogodili nekada u prošosti.

Detalji u vezi sumnjivog ponašanja i postupaka osoba koje su pokušale ili počinile prevaru dosta pomažu u razvijanju svijesti uposlenika o prepoznavanju tih indikatora ubuduće u praksi.

Također, u našoj zemlji još uvijek koristimo papirnu dokumentaciju gdje se pojedini dokumenti mogu zloupotrijebiti u dijelu elemenata osnovnih kreditnih dokumenata, ali isto tako i prateće dokumentacije, potrebne kod apliciranja za kredit, te su generalni detalji u vezi takvih primjera jako korisni da se ukaže uposlenicima na što obratiti pažnju.

Preporuka je da trener, koji će voditi Studiju slučaja na temu kreditnih prevara, pripremi strukturiran(e) slučaj(eve) koji će sadržavati:

- detalje slučaja prevara (koja je spriječena ili se desila),
- ključne smjernice za otkrivanje i sprečavanja prevara (teoretski dio iz internih akata) te
- proces prijava bilo kakve sumnje u prevaru kroz interne alate i komunikacijske kanale.

Trener iz oblasti sprečavanja prevara tokom treninga opisuje slučaj(eve) s detaljima ponašanja počinioca, vrste dokumenta ili elemente dokumenta koji je označen kao sumnjiv, kao i kako je završen slučaj. Sve vrijeme trener potiče interaktivnu diskusiju s uposlenicima kako bi i sami analizirali korak po korak i iznijeli svoje mišljenje i stav kako bi postupili u samom slučaju.

Također, trener ujedno u slučaj inkorporira proces sprečavanja kreditnih prevara u skladu s važećim politikama, procedurama i uputama kako bi slučaj(eve) iz prakse vezali i uz teoretski dio. To je ujedno prilika da se sudionicima pojasne određena pravila u procesu sprečavanja prevara koja su im možda do tada bila nejasna ili nepoznata budući da se slučajevi kreditnih prevara ne dešavaju stalno i u istim poslovnim jedinicama.

Edukacija je prilika da se sudionicima pojasne određena pravila u procesu sprečavanja prevara koja su im možda do tada bila nejasna ili nepoznata budući da se slučajevi kreditnih prevara ne dešavaju stalno i u istim poslovnim jedinicama.

Fokus treba biti na detekciji što više elemenata prevare u predmetnim slučajevima koji se realno mogu detektovati na vrijeme, ali isto tako i na procesu prijave potencijalne prevare budući da je rano oktrivanje iste ključno da bi se izbjegao bilo kakav gubitak te da bi se izvršila pravovremena prijava slučaja i poduzele daljnje potrebne aktivnosti.

Tokom diskusije poželjno je da uposlenici razmijene i sva potencijalna iskustva s pokušajima prevara, ukoliko su se susretali s istima u praksi, jer je ovakva vrsta edukacije prilika i za razmjenu iskustva koja je izuzetno korisna za sve prisutne sudionike. Naravno, treneri za sprečavanje kreditnih prevara unaprijed trebaju pripremiti izlaganje i o dodatnim ili sličnim slučajevima pokušaja prevara gdje opet mogu iskoristiti priliku za interaktivni dijalog ili diskusiju uz podsticanje sudionika da iskažu svoje mišljenje o postupanju u određenim situacijama koje trener iznese.

Očekivani benefiti Studije slučaja pokušaja kreditne prevare

Osnaživanje uposlenih sa znanjem i sviješću o potencijalnim prevarama ključno je za detekciju i sprečavanje prevara u praksi. Kada uposlenik prepozna prevarnu aktivnost, organizacija može biti sigurna u predanost uposlenika kodeksu i želji da spriječi prijevaru. Učinivši vaš trening interaktivnim i smislenim, podići ćete svijest i razviti borce protiv prevara u cijeloj vašoj organizaciji.

Ove vrsta treninga veoma efikasno utiču na podizanje svijesti uposlenika o potrebi za kontinuiranim oprezom u svakodnevnom radu. Kao rezultat, uposlenici će imati više samopouzdanja u otkrivanju potencijalnih kreditnih prevara i obrazaca ponašanja te će sigurno biti više motivirani u traženju savjeta od kolega saradnika za proces sprečavanja prevara ukoliko imaju nekih nedoumica u praksi. ■

Prevencija

PROCJENA PRIMJERENOSTI (FIT&PROPER) ČLANOVA ORGANA BANKE I KLJUČNIH FUNKCIJA

Izbor pogrešnog kandidata na vodeće pozicije u banci može prouzrokovati ne samo reputacijski rizik nego i direktan finansijski gubitak. Kako provesti procjenu primjerenosti, koje alate koristiti i na šta treba obratiti posebnu pažnju prilikom izbora kandidata, saznajte u nastavku.

Autor:
Nermin Ibradžić

Procjena primjerenosti, popularno nazvana *fit& proper* procjena, jedna je od relativno novijih aktivnosti koje su banke dužne provoditi u odnosu na članove organa banke (uprava, nadzorni odbor...) te u odnosu na ključne funkcije.

Nažalost, u određenom broju slučajeva provjera primjerenosti svodi se na administriranje dokumentacije kandidata, popunjavanje upitnika

te eventualno brze provjere informacija o kandidatu na internet pretraživačima. U takvim okolnostima izjave kandidata se uzimaju „zdravo za gotovo“ i bez dodatne provjere. U ekstremnim slučajevima se kod provođenja procjena isključuju neke bitne funkcije kao što je to funkcija praćenja usklađenosti (popularno *compliance*).

Ovakvo postupanje otvara mogućnost nastupanja više rizika.

Prije svega, sasvim realnu mogućnost da za određenu poziciju banka ne dobije pravog kandidata, odnosno kandidata sa dostatnim znanjem, raspoloživosti vremena ili vještinama. Izbor takvog kandidata može prouzrokovati ne samo reputacijski rizik nego i direktan finansijski gubitak.

Dakle, jako je bitno za odgovorne, naprijed navedene funkcije, provesti detaljnu i adekvatnu analizu primjerenosti, što podrazumijeva detaljno upoznavanje s kandidatom, njegovim vještinama pa čak i njegovom prošlošću i ličnim životom.

Procjena primjerenosti ne bi trebala biti svedena na nivo upitnika po principu *thick the box*.

Svakom slučaju treba prići posebno, sa dužnom pažnjom i analitičnosti. Nijedan kandidat, u pogledu traženih znanja, iskustva, vještina i integriteta nije isti profil i svaki od njih kao stručnjak i čovjek ima različite sposobnosti i osobine.

Obim procjene

Obim procjene primjerenosti u BiH je određen u oba entiteta identičnim propisima Agencija za bankarstvo (dalje: supervizora) pod nazivima *Odluka o sistemu internog upravljanja u banci* (FBiH), odnosno *Odluka o sistemu upravljanja u banci* (RS).

> *Kao koristan alat, osim akata supervizora, svakako može i treba poslužiti Vodič o procjenama sposobnosti i primjerenosti u aranžmanu ECB-a, revidirano izdanje iz decembra 2021. godine.*

Tako je jasno propisano koja funkcija se procijenjuje i u kojim segmentima te šta je to potrebno posebno cijeniti. Ipak, ono što stvara dilemu u praksi je: kojom metodologijom, kako, koliko duboko i s kakvim efektima.

Kao koristan alat, osim akata supervizora, svakako može i treba poslužiti *Vodič o procjenama sposobnosti i primjerenosti* (dalje: Vodič) u aranžmanu ECB-a, revidirano izdanje iz decembra 2021. godine.

Razlog leži u činjenici da su navedene odluke oba supervizora snažno oslonjenje na ECB standarde i smjernice, a pomenuti Vodič pruža i više nego dostatnu podršku u izradi adekvatnih procjena primjerenosti.

Valja naglasiti da revidiranje Vodiča nije došlo samo po sebi.

Jedan od osnovnih razloga je činjenica da je ECB u 2021. godini izvela 17 reprocjena za nekoliko članova organa upravljanja bankom u osam zemalja. Od ukupnog broja samo 5 ih je bilo pokrenuto

od strane samih banaka zbog promjena i novih činjenica koje su nastale na strani organa upravljanja.

U čak 12 slučajeva ECB je provela superviziju na osnovu informacija iz drugih izvora uključujući i izvještavanja u medijima.

Navedeno je ukazalo na činjenicu da okvir za procjene primjerenosti treba ojačati u dijelu adekvatnosti provedenih procjena s naglaskom na praćenje promjena koje mogu uticati na primjerenost članova organa banke u toku trajanja obavljanja funkcije, ali i na procjenu i odgovornost organa upravljanja kao cjeline, a ne samo i isključivo u odnosu na pojedine imenovane članove. Drugačije rečeno, niti jednu informaciju kod procjene primjerenosti ne treba odbaciti i korištenje više izvora za informacije je više nego poželjno.

Uporedba svih elemenata Vodiča s odlukama supervizora bi zahtijevala puno više vremena i prostora nego je to jedan novinski članak.

Puno praktičnije je fokusirati se na dio procjena koji u praksi može izazvati i najviše dilema u postupanju, a to su:

- ugled,
- neovisnost mišljenja i
- primjerenost cjelokupnog sastava organa banke i raznolikost.

Procjena ugleda

Procjena ugleda kandidata za člana organa banke ili ključnu funkciju nije zadatak kojem se svako raduje.

Ipak, u mnogim slučajevima upravo ova procjena se pokazala ključnom. Posebno ukoliko nije provedena adekvatno. Ono što je otežavajuća okolnost i u nekim slučajevima „kočnica“ adekvatne procjene ugleda jeste što se procjenom ugleda ulazi u lični prostor kandidata, a ne samo u njegov profesionalni put. No međutim, to ne bi trebalo posebno da brine. Jer odluke supervizora izričito nalažu i provjeru i procjenu ličnog statusa kandidata.

Kod procjene ugleda kandidata nije dovoljno samo izvršiti pregled dokumentacije i informacija koje govore o tome da li je ili nije protiv kandidata u toku ili ranije vođen upravni, parnični, prekršajni ili krivični postupak i kakva je njegova težina.
Prilikom procjene ugleda kandidata, osim raznovrsnih potvrda upravnih ili sudskih organa, u obzir treba uzeti i tzv. *soft facts*.

Tačno je da presumpcija nevinosti postoji u pravu u BiH. Ipak, ukoliko prilikom procjene primjerenosti zanemarimo ili nedovoljno ispitamo negativne medijske natpise

o kandidatu ili druge informacije (npr. fotografije ili tekstove objavljene na društvenim mrežama koji ukazuju na druženje sa licima koja su dio kriminalnog miljea), vrlo lako je moguće da time činimo grešku koja će svoje negativne rezultate pokazati u bliskoj budućnosti. Lice ili lica koja rade procjenu ugleda kandidata moraju ispitati svaku dostupnu informaciju i istu dokumentovati, ma koliko god se ona činila u tom momentu nevjerovatnom. Pouzdanost izvora informacije i njena relevantnost se cijeni u daljem postupku procjene, ali se svakako treba uzeti u obzir.

U odnosu na navedeno, kod procjene ugleda Vodič ide i korak dalje.

Tako se, naprimjer, u obzir uzimaju i informacije o kreditnoj zaduženosti kandidata, načinu i rokovima u kojima ispunjava svoje finansijske obaveze. Dodatno, ukoliko je kandidat osnivač drugog privrednog društva, u obzir se uzima i finansijsko stanje i rezultati tog društva. Ukoliko kandidat nema potrebne vještine da vodi vlastito društvo ili je vlastito društvo namjerno oštetio, šta je garancija da se neće jednako ponašati i prilikom imenovanja u organe upravljanja banke?

Informacije bi trebalo provjeriti i u slučaju da je kandidat trenutno ili je bio na značajnoj

> *Ukoliko kandidat nema potrebne vještine da vodi vlastito društvo ili je vlastito društvo namjerno oštetio, šta je garancija da se neće jednako ponašati i prilikom imenovanja u organe upravljanja banke?*

poziciji u društvu koje je krivično gonjeno ili je finansijski nestabilno (npr. prijeteći stečaj). U svakom slučaju potrebno je ispitati ulogu i ovlaštenja kandidata u tom društvu te isto dokumentovati.

Neovisnost mišljenja

Neovisnost mišljenja je također jedan od kriterija koji u različitim slučajevima može biti prilično volatilan u pojedinim segmentima.

U dijelu koji se odnosi na sukob interesa i njegov uticaj na neovisnost mišljenja, stvari su prilično jasne. Postoje različiti segmenti sukoba interesa i različite mjere koje se mogu odrediti za upravljanje sukobom interesa. I sve su manje-više poznate.

Međutim, kad se dođe do ličnih karakteristika kandidata i njegove mogućnosti da „iznese“ funkciju na adekvatan način, moguć je uticaj subjektivnog osjećaja onog ko vrši procjenu u odnosu na samog kandidata.

> *Da li kandidat ima hrabrosti da se uhvati ukoštac s izazovima? Da li ima problem s tim da challenguje ostale članove tima, odnosno organa upravljanja? Da li se priklanja većini u odlučivanju ili jasno artikuliše svoje argumente i stavove? Da li se povlači pod pritiskom?*

Da li kandidat ima hrabrosti da se uhvati ukoštac s izazovima? Da li ima problem s tim da *challenguje* ostale članove tima, odnosno organa upravljanja? Da li se priklanja većini u odlučivanju ili jasno artikuliše svoje argumente i stavove? Da li se povlači pod pritiskom?

Da subjektivni osjećaj u odnosu na kandidata ne bi bio jedini alat za procjenu mogućnosti izražavanja neovisnog mišljenja, svakako bi procjenu trebalo argumentovati: koje značajne odluke je kandidat donosio u prošlosti i zašto, u kojim kolektivnim odlukama je učestvovao i zašto se priklonio jednom ili drugom mišljenju, natpisi u medijima o ranijoj karijeri.

Ipak, kako Vodič dopušta, a odluke supervizora ne zabranjuju, u dijelu mogućnosti donošenja i artikulisanja neovisnih mišljenja svakako je korisno potražiti i savjet eksternih saradnika koji su kvalifikovani za donošenje takvih zaključaka.

Primjerenost cjelokupnog sastava organa banke i raznolikost

Vodič ECB-a primjerenost cjelokupnog sastava organa banke cijeni ujedno i kroz raznolikost organa banke.

Prema Vodiču, jedan od elemenata procjene primjerenosti cjelokupnog sastava organa banke prema ECB-u je i znanje o klimatskim i okolišnim rizicima koje je, prema mišljenju ECB-a, bitno iz razloga što nepoznavanje navedene materije može uzrokovati i direktne finansijske gubitke. Segment znanja o klimatskim i ekološkim rizicima međutim nije obuhvaćen odlukama supervizora.

Organi banke u pravilu djeluju kao kolektivni organ i kao kolektivni organ donose odluke. Upravo iz navedenog razloga je potrebno napraviti

> *Organi banke u pravilu djeluju kao kolektivni organ i kao kolektivni organ donose odluke. Upravo iz navedenog razloga je potrebno napraviti adekvatan balans između znanja, iskustva i vještina svih članova organa banke, a kako bi „dobitna" kombinacija donijela i očekivane rezultate.*

adekvatan balans između znanja, iskustva i vještina svih članova organa banke, a kako bi „dobitna" kombinacija donijela i očekivane rezultate.

U odnosu na odluke supervizora, ECB Vodič za procjenu primjerenosti cjelokupnog sastava organa banke propisuje u jednoj mjeri drugačije uslove gdje se kod kolektivne primjerenosti utvrđuju sljedeća znanja, iskustva i vještine, odnosno poznavanje:

- svih pojedinih značajnih aktivnosti institucije,
- poslovanja kreditne institucije i glavnih rizika povezanih s njime,
- upravljanja institucijom,
- važnih područja sektorske i finansijske nadležnosti, uključujući finansijska tržišta i tržišta kapitala, solventnost i modele,
- rukovodećih vještina i iskustva,
- finansijskog računovodstva i izvještavanja,
- strateškog planiranja,
- upravljanja rizicima, usklađenosti s propisima i interne revizije,
- informacijske tehnologije i sigurnosti,
- klimatskih i okolišnih rizika,
- lokalnih, regionalnih i globalnih tržišta, ako je primjenjivo,
- pravnog i regulatornog okružja te
- upravljanja međunarodnim i nacionalnim grupama i rizicima povezanim sa strukturama grupe, ako je primjenjivo.

Vodič ECB-a nudi i matricu pomoću koje je objektivno moguće procijeniti navedene segmente. Slična matrica je u primjeni i uz Odluku Agencije za bankarstvo Republike Srpske.

Jedan od elemenata primjerenog sastava organa banke je i raznolikost njegovih članova, i to ne samo po nivou znanja i iskustva, nego i ostalim karakteristikama.

U svakom slučaju, jedan od elemenata primjerenosti organa banke kao cjeline je i zastupljenost žena i muškaraca u organima upravljanja. Kao imperativ supervizori su propisali, a podržano je i standardima ECB-a, obavezu banaka da definišu:

- opis načina za poboljšanje moguće nedovoljne zastupljenosti određenog spola u organu banke u skladu s ciljem banke, raspoloživih mogućnosti i karijernih perspektiva u organu banke.

Ovaj cilj zastupljenosti nije samo formalan jer je banka u obavezi i da se odredi prema roku u kojem će postići planiranu raznolikost.

U ovom dijelu ostaje otvoreno pitanje za supervizora o postupanju u slučaju da je banka navedene kriterije usvojila, ali ne i implementirala ili ukoliko su navedeni kriteriji ispunjeni djelimično. Da li će u takvim slučajevima supervizor izdavati bankama zahtjeve za korektivnim

mjerama i rokom njihovog ispunjenja tek ostaje da se vidi u budućnosti.

Zaključak

Procjena primjerenosti (*fit &proper*) članova organa banke i ključnih funkcija nije puko prikupljanje dokumentacije i upitnika.

Procjena zahtijeva multidisciplinaran pristup i učešće više stručnih službi ili pojedinaca u vršenju procjene, u zavisnosti od nivoa ekspertize kojom raspolažu (HR, *compliance*, pravna funkcija, eksterni saradnici).

Cilj sveobuhvatne i adekvatne procjene nije samo odabir odgovarajućih kadrova na najodgovornije pozicije nego i omogućavanje djelovanja organa banke kao kolektiva u interesu banke te preventivna uloga da se eventualne devijacije ili nelogičnosti otkriju na vrijeme i na taj način se spriječe reputacijski i drugi gubici koji mogu nastati uslijed neadekvatnog upravljanja bankom ili neadekvatno izabranih ključnih funkcija banke. Čarobna formula za izbor i najbolju kombinaciju ne postoji. Međutim, određene sugestije mogu pomoći da procjena na kraju bude adekvatna:

- ostaviti dovoljno vremena za procjenu primjerenosti;
- razmišljati izvan okvira;
- uobziriti sve dostupne informacije, uključivo i *soft facts*;
- od kandidata zahtijevati transparentnost i iskrenost te
- nelogične informacije i podatke provjeriti iz više izvora.

Ukratko, kod procjene primjerenosti članova organa banke i ključnih funkcija bi važilo:

pristup *thick the box* – NE,
pristup *case by case* – DA. ■

Edukativni prilog

VODIČ ZA KRIPTOVALUTE

Iako ih ne izdaju centralne banke niti se vežu uz račune u poslovnim bankama, nisu vezane ni za koju zemlju ili podložne regulativi, kriptovalute su postale globalno prihvaćene za međunarodna plaćanja i ulaganja.

Autor:
Amar Brkan

Kriptovalute, zvane i virtuelne valute, globalno su prihvaćene za međunarodna plaćanja putem interneta, ali i za ulaganja. Ne izdaju ih centralne banke niti se vežu uz račune u poslovnim bankama, za transakcije nema naknade, pa su međunarodna plaćanja jednostavnija i jeftinija jer kriptovalute nisu vezane ni za koju zemlju ili podložne regulativi. Na taj način svako s internetskom vezom može postati dijelom tog finansijskog sistema, a da se ne služi standardnom bankarskom mrežom.

Takvi sistemi gotovo da su otporni na inflaciju i manje su ovisni o monetarnim politikama zemalja. S druge strane, postoje i mnoge opasnosti i neizvjesnosti koje proizlaze iz prirode kriptovaluta.

Kriptovalute su dobile svoje ime po kriptografskim tehnikama koje omogućavaju

ljudima da ih kupuju, prodaju ili trguju na siguran način bez potrebe za trećom stranom, poput vlade ili finansijskih institucija, da potvrdi transakciju.

Bitcoin, kao i ostale kriptovalute, nastaje na računalima širom svijeta rješavanjem složenih računarskih jednačina (takozvanim rudarenjem), a mogu se kupiti i putem bankomata, odnosno na internetskim berzama. Drže se u elektronskom novčaniku na nekoj od brojnih web-stranica koje pružaju tu uslugu.

Naprimjer, *bitcoin* je prvenstveno razvijen da bude oblik plaćanja koji nije kontroliran ili distribuiran od strane centralne vlade; ***ethereum*** omogućava programerima da grade automatizovane aplikacije u onome što je postalo poznato kao decentralizovane finansije; a ***tether*** je stabilna valuta čija je vrijednost vezana za američki dolar.

> *Bitcoin, kao i ostale kriptovalute, nastaje na računalima širom svijeta rješavanjem složenih računarskih jednačina (takozvanim rudarenjem), a mogu se kupiti i putem bankomata, odnosno na internetskim berzama.*

Zašto ljudi ulažu u kriptovalute?

Ljudi ulažu u kriptovalute jer vjeruju da, ako potražnja za određenom kriptovalutom poraste, porast će i njezina vrijednost. Uzmimo pojednostavljeni primjer s *bitcoinom*. Teoretski, ako i kompanije i potrošači smatraju da je *bitcoin* bolje iskustvo pri kupovini nego korištenje američkog dolara, potrošač bi mogao konvertirati više svog novca iz dolara u *bitcoin*, dok bi poslovanju odgovaralo više *bitcoin* plaćanja. Ako bi se to dogodilo u ogromnim razmjerama, potražnja za *bitcoinom* bi porasla, a zauzvrat bi se povećala i njegova cijena u dolarima. Dakle, ako ste kupili jedan *bitcoin* prije tog povećanja potražnje, teoretski biste mogli prodati taj jedan *bitcoin* za više američkih dolara nego što ste ga kupili, ostvarivši profit.

Isti principi važe i za *ethereum*. *Ether* je kriptovaluta *ethereum blockchaina* gdje programeri mogu graditi finansijske aplikacije bez potrebe za finansijskom institucijom treće strane. Programeri moraju koristiti *ether* za izgradnju i pokretanje aplikacija na *ethereumu* tako da, teoretski, što je više izgrađeno na *ethereum blockchainu*, veća je potražnja za *etherom*.

Međutim, važno je napomenuti da neke kriptovalute uopće nisu ulaganja. *Bitcoin* entuzijasti, naprimjer, pozdravljaju ga kao znatno poboljšani monetarni sistem u odnosu na naš trenutni i radije bi ga potrošili i prihvatili kao svakodnevno plaćanje.

Kako funkcionira kriptovaluta?

Kriptovalute su podržane tehnologijom poznatom kao ***blockchain*** koja održava evidenciju transakcija otpornu na neovlašteno mijenjanje i prati ko šta posjeduje. Upotreba *blockchaina* rješavala je problem s kojim su se suočavali prethodni napori da se stvore čisto digitalne valute: sprečavanje ljudi da prave kopije svojih fondova i pokušaj da ih potroše dva puta.

> *Za razliku od tradicionalnih procesora plaćanja, poput PayPala i kreditnih kartica, većina kriptovaluta nema ugrađenu funkciju povrata ili povrata sredstava, iako neke novije kriptovalute imaju rudimentarne osobine povrata.*

Izvorni kodovi i tehničke kontrole koje podržavaju i osiguravaju kriptovalute vrlo su složene. U funkcionalnom smislu, većina kriptovaluta predstavlja varijacije *bitcoina*, prvoj široko korištenoj kriptovaluti. Kao i tradicionalne valute, vrijednost kriptovaluta izražena je u jedinicama. Naprimjer, može se reći: „Imam 2,5 bitkoina", baš kao što bi rekli, „imam 2,50 dolara". Nekoliko koncepata reguliše vrijednosti, sigurnost i integritet kriptovaluta.

Blockchain kriptovalute je glavni zapis koji bilježi i čuva sve prethodne transakcije i aktivnosti ovjeravajući vlasništvo nad svim jedinicama valute u bilo kojem trenutku. Kao do sada zabilježena čitava historija transakcija kriptovalute, *blockchain* ima ograničenu dužinu - koja sadrži ograničen broj transakcija - koja se vremenom povećava. Identične kopije *blockchaina* čuvaju se u svakom čvorištu mreže kriptovalute, mreže decentralizovanih farmi servera, kojom upravljaju pojedinci ili grupe pojedinaca poznatih kao rudari, a koji kontinuirano bilježe i potvrđuju transakcije s kriptovalutama. Transakcija kriptovaluta tehnički se ne dovršava sve dok se ne doda u *blockchain*, a što se obično događa u roku od nekoliko minuta. Jednom kada je transakcija finalizovana, obično je nepovratna. Za razliku od tradicionalnih procesora plaćanja, poput *PayPala* i kreditnih kartica, većina kriptovaluta nema ugrađenu funkciju povrata ili povrata sredstava, iako neke novije kriptovalute imaju rudimentarne osobine povrata. Za vrijeme između pokretanja i finalizacije transakcije, jedinice nisu dostupne za upotrebu nijednoj strani. Umjesto toga oni se drže u svojevrsnom *escrow-limbo* stanju za sve namjere i svrhe. Blok lanac na taj način sprečava dvostruko trošenje ili manipulaciju kriptovaluta kodom kako bi se omogućilo dupliciranje i slanje istih jedinica valute višestrukim primaocima.

Svaki vlasnik kriptovalute ima **privatni ključ** koji potvrđuje njegov identitet i omogućava mu razmjenu jedinica. Korisnici mogu kreirati svoje privatne ključeve, koji su formirani kao cijeli brojevi dužine od 1 do 78 cifara, ili ih mogu dobiti pomoću generatora slučajnih brojeva. Jednom kada dobiju ključ, mogu nabaviti i trošiti kriptovalute. Bez ključa vlasnik ne može potrošiti ili pretvoriti svoju kriptovalutu - čineći svoje udjele bezvrijednim osim ako i dok ključ ne povrati. Iako ova sigurnosna osobina smanjuje krađu i neovlaštenu upotrebu, ona je također drakonska. Gubitak privatnog ključa digitalni je ekvivalent bacanju gomile novca u smeće. Iako se može kreirati još jedan privatni ključ i ponovo početi akumulacija kriptovaluta, ne mogu se povratiti udjeli zaštićeni starim izgubljenim ključem. Korisnici kriptovalute pažljivo štite svoje privatne ključeve, obično ih čuvaju na više

digitalnih (zbog sigurnosnih razloga uglavnom nisu povezani s internetom) i analognih (tj. papirnih) lokacija.

Korisnici kriptovalute imaju "**novčanike**" s jedinstvenim informacijama koje ih potvrđuju kao privremene vlasnike svojih jedinica. Dok privatni ključevi potvrđuju autentičnost transakcije kriptovaluta, novčanici smanjuju rizik krađe za jedinice koje se ne koriste. Novčanici su osjetljivi na hakovanje. Naprimjer, japanska berza ***Bitcoin Mt. Gox*** proglasila je bankrot prije nekoliko godina nakon što su je hakeri sistematski "oslobodili" za više od 450 miliona dolara u *bitcoinima* razmijenjenim preko njenih servera. Novčanici se mogu čuvati na *cloudima*, internim hard diskovima ili eksternim uređajima za čuvanje. Bez obzira na način čuvanja novčanika, preporučuje se barem jedna sigurnosna kopija.

Rudari služe kao čuvari zapisa u zajednicama kriptovaluta i indirektni su arbitri vrijednosti valuta. Koristeći ogromne količine računarske moći, koja se često manifestuje na privatnim farmama u vlasništvu rudničkih kolektiva koji broje desetine pojedinaca, rudari koriste visokotehničke metode da provjere kompletnost, tačnost i sigurnost blokovskih lanaca valuta. Opseg operacije nije različit od potrage za novim primarnim brojevima, što također zahtijeva ogromne količine računarske moći. Rudarski rad periodično stvara nove kopije *blockchaina* dodajući nedavne, prethodno neprovjerene transakcije koje nisu uključene ni u jednu prethodnu *blockchain* kopiju – efektivno dovršavajući te transakcije. Svaki dodatak poznat je kao blok. Blokovi se sastoje od svih transakcija izvršenih od trenutka kada je stvorena posljednja nova kopija *blockchaina*. Izraz "rudari" odnosi se na činjenicu da rad rudara bukvalno stvara bogatstvo u obliku potpuno novih kriptovalutnih jedinica. Ustvari, svaka novostvorena *blockchain* kopija dolazi s dvodijelnom novčanom nagradom: fiksnim brojem „novopronađenih" kriptovalutnih jedinica i varijabilnim brojem postojećih jedinica prikupljenih od neobaveznih naknada za transakcije (obično manje od 1% od vrijednost transakcije) koju plaćaju kupci.

Trenutne cijene kriptovaluta

Da biste stekli osjećaj svijeta kriptovalute, može vam pomoći da se upoznate sa sredstvima kojima se najčešće trguje. Ispod je lista glavnih kriptovaluta prema tržišnoj kapitalizaciji[1].

Zašto postoji toliko mnogo vrsta kriptovaluta?

Važno je zapamtiti da se *bitcoin* razlikuje od kriptovalute općenito. Iako je *bitcoin* prva i najvrednija kriptovaluta, tržište je veliko.

Više od 22.000 različitih kriptovaluta se javno trguje, prema **CoinMarketCap.com**, web stranici za istraživanje tržišta. I dok neke kriptovalute imaju ukupne tržišne vrijednosti u stotinama milijardi dolara, druge su nejasne i u suštini bezvrijedne.

[1] https://www.nerdwallet.com/article/investing/cryptocurrency

The top 10 cryptocurrencies by market cap

24H | 7D | 30D | YTD | 1Y | All

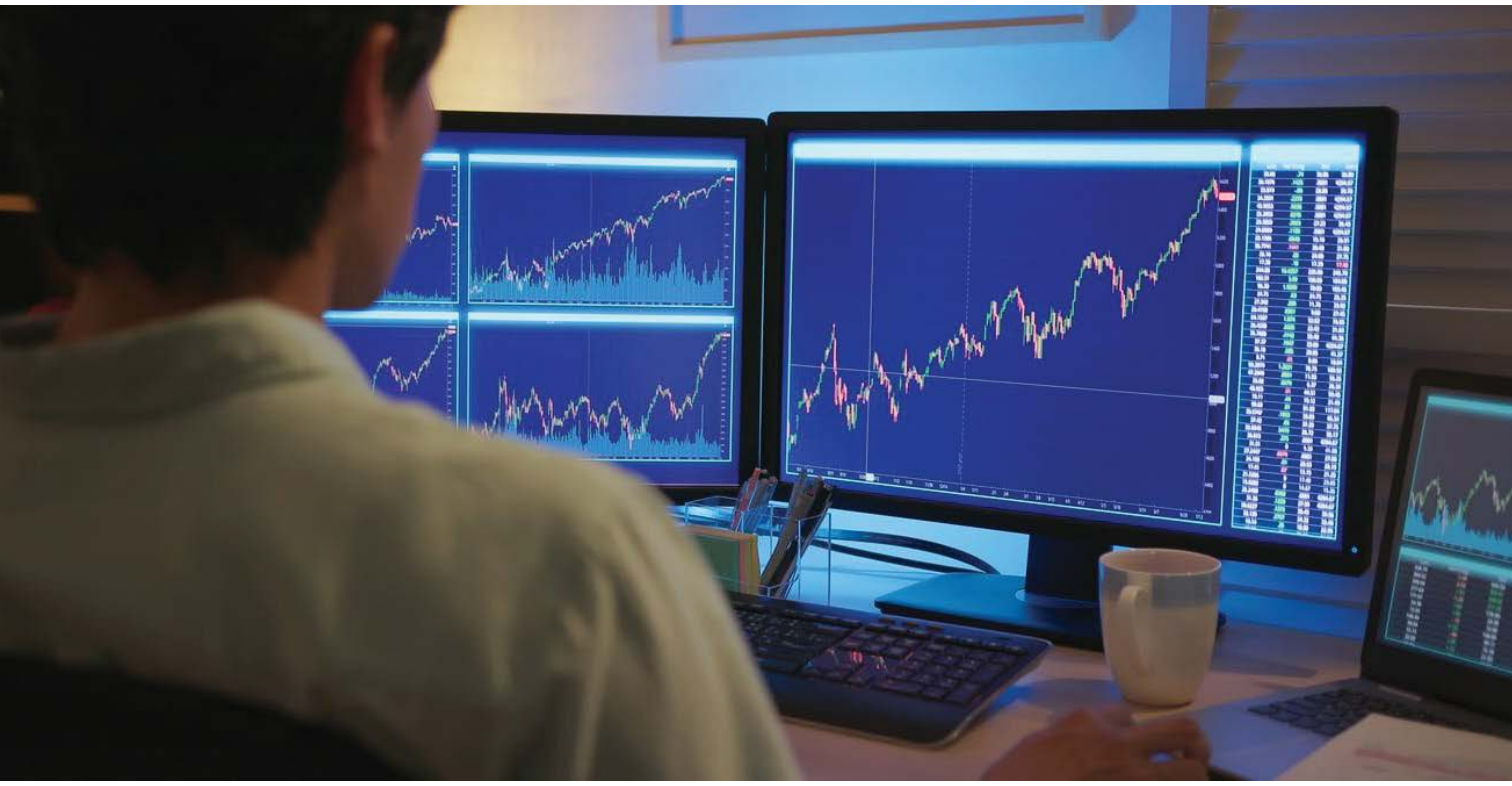
Asset	One Week Return	Market Capitalization ↑
Bitcoin BTC	0.81%	$471.2B
Ethereum ETH	-0.65%	$204B
Tether USDT	-0.004%	$70.6B
BNB BNB	0.54%	$49.6B
USD Coin USDC	0.003%	$42.1B
XRP XRP	-0.11%	$20.2B
Cardano ADA	-3.61%	$13.6B
Binance USD BUSD	0.01%	$12.4B
Polygon MATIC	-5.05%	$12.3B
Dogecoin DOGE	-1.99%	$11.4B

Updated at: 7:07 AM, 02-24-2023

Ako razmišljate o ulasku u kriptovalutu, može biti od pomoći da počnete s onom kojom se obično trguje i koja je relativno dobro uspostavljena na tržištu.

NerdWallet je kreirao vodiče za neke široko rasprostranjene kriptovalute, uključujući *bitcoin* i neke *altcoine*, ili *bitcoin* alternative:

- ***Bitcoin*** je prva i najvrednija kriptovaluta.
- ***Ethereum*** se obično koristi za obavljanje finansijskih transakcija složenijih od onih koje podržava *bitcoin*.
- ***Cardano*** je konkurent *ethereumu* na čelu s jednim od njegovih suosnivača.



- ***Litecoin*** je adaptacija *bitcoina* namijenjena da olakša plaćanje.
- ***Solana*** je još jedan konkurent *ethereumu* koji naglašava brzinu i isplativost.
- ***Dogecoin*** je počeo kao šala, ali je izrastao u jednu od najvrednijih kriptovaluta.
- ***Shiba Inu*** je još jedan žeton sa složenijom mehanikom.
- ***Stablecoins*** uključujući *tether* i USDC su klasa kriptovaluta čije su vrijednosti dizajnirane da ostanu stabilne u odnosu na stvarnu imovinu kao što je dolar.

Međutim, promišljen odabir vaše kriptovalute nije garancija uspjeha u tako nestabilnom okruženju. Ponekad se problem u duboko povezanoj kriptoindustriji može raširiti i imati široke implikacije na vrijednosti imovine.

Naprimjer, u novembru 2022. tržište je pretrpjelo veliki udar jer se berza kriptovaluta FTX borila da se nosi s problemima likvidnosti usred naglog povlačenja. Kako se pad širio, i velike i male kriptovalute zabilježile su pad vrijednosti.

Da li su kriptovalute vrijednosni papiri poput dionica?

Da li je kriptovaluta vrijednosni papir ili ne, trenutno je to sve u sivoj zoni. Generalno, vrijednosni papir u finansijama je sve što predstavlja vrijednost i čime se može trgovati. Dionice su vrijednosni

papir jer predstavljaju vlasništvo u javnom preduzeću. Obveznice su vrijednosni papir jer predstavljaju dug prema vlasniku obveznice. S obje vrste može se trgovati na javnim tržištima.

Regulatori sve više počinju da signaliziraju da kriptovalute trebaju biti regulirane slično kao i drugi vrijednosni papiri poput dionica i obveznica. Ali ovaj pokušaj se odbija; naučnici, pravne firme i neki od najvećih igrača u kriptoindustriji se protive tvrdeći da se pravila koja se primjenjuju na dionice i obveznice, naprimjer, ne primjenjuju tako široko na kriptovalute.

> *Regulatori sve više počinju da signaliziraju da kriptovalute trebaju biti regulirane slično kao i drugi vrijednosni papiri poput dionica i obveznica.*

Nedavno je Komisija za vrijednosnice i berzu Sjedinjenih Američkih Država (*The Securities and Exchange Commission* - SEC) stavila u fokus kriptoulaganje tvrdeći da bi dobit od ulaganja trebala biti registrirana kao vrijednosni papir. U februaru 2023. godine SEC je primorao kriptoberzu Kraken da zatvori svoj program investicija navodeći da Kraken nije uspio registovati svoju ponudu za ulaganje kao obezbjeđenje.

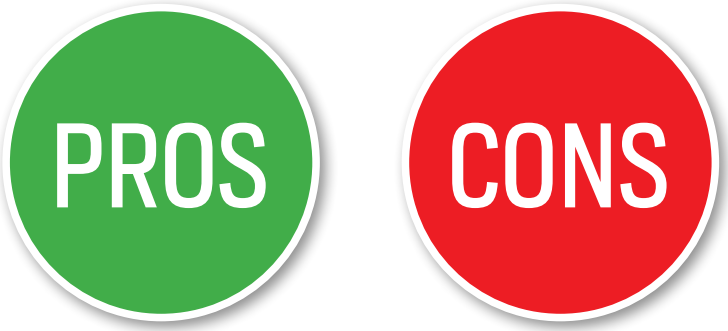
Da li su NFT kriptovalute?

NFT-ovi, tokeni koji se ne mogu zamijeniti, su digitalna sredstva koja prenose vlasništvo nad onim što bi se moglo smatrati originalnom kopijom digitalne datoteke. Oni dijele mnoge sličnosti s kriptovalutama, a mogu se kupiti i prodati na mnogim istim tržištima. Međutim, NFT-ovi se razlikuju od kriptovaluta zbog one nezgrapne riječi u njihovom nazivu: nezamjenjivost.

Kriptovalute su zamjenjive tako da je svaka jedinica određene kriptovalute u osnovi ista kao i svaka druga.

Prednosti kriptovaluta

- Nekim pristašama se sviđa činjenica da kriptovalute uklanjaju centralne banke iz upravljanja novčanom opskrbom jer s vremenom te banke imaju tendenciju da smanje vrijednost novca putem inflacije.
- Drugi zagovornici vole *blockchain* tehnologiju koja stoji iza kriptovaluta jer je to decentralizirani sistem za obradu i snimanje



i može biti sigurniji od tradicionalnih sistema plaćanja.
- Neke kriptovalute nude svojim vlasnicima priliku da zarade pasivni prihod kroz proces koji se zove ulaganje. Kriptoulaganje uključuje korištenje vaših kriptovaluta za potvrđivanje transakcija na *blockchain* protokolu. Iako ulaganje ima svoje rizike, može vam omogućiti da povećate svoje kriptovalute bez kupovine dodatnih.

Nedostaci kriptovalute

- Mnogi projekti kriptovaluta nisu testirani, a *blockchain* tehnologija općenito tek treba da dobije široku primjenu. Ako osnovna ideja koja stoji iza kriptovalute ne dosegne svoj potencijal, dugoročni investitori možda nikada neće vidjeti povrate kojima su se nadali.
- Za kratkoročne kriptoinvestitore postoje i drugi rizici. Njegove cijene imaju tendenciju da se brzo mijenjaju. I dok to znači da su mnogi ljudi brzo zaradili novac kupovinom u pravo vrijeme, mnogi drugi su izgubili novac čineći to neposredno prije pada kriptovaluta.

> *Rudarenje bitcoina širom svijeta troši dvostruko više energije od cjelokupne stambene rasvjete u SAD-u. Procjene govore da svaka bitcoin transakcija utroši oko 1.173 kilovat sata (kWH) električne energije.*

- Te divlje promjene u vrijednosti također mogu umanjiti osnovne ideje iza projekata koje su kriptovalute stvorene da podrže. Naprimjer, manje je vjerovatno da će ljudi koristiti *bitcoin* kao sistem plaćanja ako nisu sigurni koliko će vrijediti sljedećeg dana.
- Uticaj *bitcoina* i drugih projekata koji koriste slične rudarske protokole je značajan. Poređenje Univerziteta u Cambridgeu, naprimjer, kaže da rudarenje *bitcoina* širom svijeta troši dvostruko više energije od cjelokupne stambene rasvjete u SAD-u. Procjene govore da svaka *bitcoin* transakcija utroši oko 1.173 kilovat sata (kWH) električne energije.
- Neke kriptovalute koriste drugačiju tehnologiju koja zahtijeva manje energije.
- Vlade širom svijeta još uvijek se nisu u potpunosti obračunale s načinom na koji se ponašaju s kriptovalutama tako da regulatorne promjene i suzbijanja imaju potencijal da utiču na tržište na nepredvidive načine.

Pravna i porezna pitanja kriptovaluta

Nema sumnje da su kriptovalute legalne u SAD-u, iako je Kina u suštini zabranila njihovu upotrebu, a na kraju da li su legalne zavisi od svake pojedinačne zemlje.

Međutim, pitanje da li su kriptovalute zakonski dozvoljene samo je jedan dio pravnog pitanja. Ostale stvari koje treba razmotriti uključuju kako se kriptovalute oporezuju i šta možete kupiti kriptovalutom.

- **Zakonsko sredstvo plaćanja**: Možete ih nazvati kriptovalutama, ali one se razlikuju od tradicionalnih valuta na jedan važan način: na većini mjesta ne postoji zahtjev da budu prihvaćene kao "zakonito sredstvo plaćanja". Zemlje širom svijeta koriste različite pristupe kriptovaluti. El Salvador je 2021. godine postao prva zemlja koja je usvojila *bitcoin* kao zakonsko sredstvo plaćanja. U međuvremenu, Kina razvija sopstvenu digitalnu valutu.
- **Porezi na kriptovalute**: Kriptovalute se npr. u SAD-u oporezuju kao imovina, a ne kao valuta. To znači da ćete, kada ih prodate, platiti porez na kapitalnu dobit, odnosno razliku između cijene kupovine i prodaje. A ako dobijete kriptovalute kao plaćanje ili kao nagradu za aktivnost kao što je rudarenje, bit ćete oporezovani na vrijednost u trenutku kada ste ih primili.

Da li je kriptovaluta dobra investicija?

Kriptovaluta je relativno rizična investicija. Uopšteno govoreći, visokorizične investicije trebale bi činiti mali dio vašeg ukupnog portfolija – jedna uobičajena smjernica je ne više od 10%. Možda ćete htjeti prvo istražiti kako biste ojačali svoju mirovinsku štednju, otplatili dug ili investirali u manje promjenjive fondove sastavljene od dionica i obveznica. Postoje i drugi načini upravljanja rizikom unutar vašeg kriptoportfelja, kao što je diverzifikacija raspona kriptovaluta koje kupujete. Kriptoimovina može rasti

i pasti različitim stopama i u različitim vremenskim periodima, tako da ulaganjem u nekoliko različitih proizvoda možete se izolirati - do određenog stepena - od gubitaka u jednom od svojih posjeda.
Možda je najvažnija stvar da, kada ulažete u bilo šta, uradite sopstveni domaći zadatak. Ovo je posebno važno kada su u pitanju kriptovalute koje su često povezane s određenim tehnološkim proizvodom koji se razvija ili uvodi. Kada kupite dionicu, ona je povezana s kompanijom koja podliježe dobro definiranim zahtjevima finansijskog izvještavanja što vam može dati uvid u njene izglede.

Ako imate finansijskog savjetnika koji je upoznat s

kriptovalutama, možda bi bilo vrijedno pitati za unos. Za investitore početnike također može biti vrijedno da ispitaju koliko se kriptovaluta široko koristi. Većina renomiranih kriptoprojekata ima javno dostupne metrike koje pokazuju podatke kao naprimjer koliko se transakcija obavlja na njihovim platformama. Ako upotreba kriptovalute raste, to može biti znak da se etablirala na tržištu. Kriptovalute, također, općenito stavljaju na raspolaganje "bijele knjige" koje objašnjavaju kako će raditi i kako namjeravaju distribuirati tokene.

Obavezno razmislite o tome kako se zaštititi od prevarana koji vide kriptovalute kao priliku da privlače investitore. ■

UPRMBiH

Udruženje profesionalnih rizik menadžera

UREDNIČKI TIM

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

Nermin Ibradžić
Direktor Sektora za
usklađenost poslovanja,
sprečavanje pranja
novca i sigurnost
NLB Banka d.d. Sarajevo

Eldin Mulić
Information Security
Specialist
Raiffeisen Bank dd BiH

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

Vedran Vinšalek
Voditelj odjela
za upravljanje
nekreditnim rizicima
NLB Banka d.d. Sarajevo

Sanela Vrana
Voditelj sigurnosti
informacionog sistema
**Razvojna banka
Federacije BiH**