Money web

Zamašnjak tehnološkog razvoja se ubrzava. Od pojave Interneta završava industrijska era i štafetu pruzima informacijska revolucija. No dobro, računala su postojala i prije, ali tek je Internet bio katalizator koji je izazvao višestruko ubrzanje i pojačanje. Mreža računala prerasla je u mrežu ljudi i mrežu informacija, ali tu razvoj nije stao. E-commerce je već postao svakodnevna stvar. Novu stepenicu u tehnološkom razvoju predstavlja razvoj kriptovaluta i blockchain tehnologije. Upravo svjedočimo, iako 99,99 % čovječanstva toga nije svjesno, radikalnoj promjeni koja neće zahvatiti samo financijsku industriju, nego cijelo društvo. Internet dobija novu funkciju, postaje Mreža novca, ***Money web***. A time se pred njega stavljaju novi izazovi, jer gdje je novac, tu su i kriminalci.

Kada se Bitcoin projavio 2009. godine, rijetki su to uopće primijetili. Nekolicina tehnoloških zanesenjaka prihvatila se rudarenja, iako ga nisu shvaćali ozbiljno, samo su željeli sudjelovati u nečem novom i uzbudljivom. Tko je tada sanjao da bi to mogao biti kraj novca kakvog poznajemo? Jedan cijenjeni kolega pričao mi je kako je u to pionirsko vrijeme skinuo izvorni kod Bitcoina, prekompajlirao ga i uključio se u rudarenje. S vremenom je zaradio preko 600 bitcoina. Početna cijena BC bila je 0,001 USD. Kad je narasla na 2, pa 3 i zatim 5 $, sve ih je rasprodao i počeo se baviti drugim zanimacijama. Današnja cijena Bitcoina je preko 4000 $, pa sami izračunajte da li se isplatilo prodati ih prerano? Ali tko je mogao predvidjeti sve društvene promjene koje će nova tehnologija izazvati? Drugi kolega "hvalio" se da je imao BC u walletu na svom kućnom računalu. Kad se računalo pokvarilo, izgubio je sve podatke, tako da više ne može do svojih coina. I on je sve to shvaćao kao igru, tek je kasnije shvatio veličinu gubitka.

Oko Bitcoina i ostalih otprilike tisuću njegovih klonova i sljedbenika izgrađena je nova grana financijske industrije. Trgovci oprezno prihvaćaju plaćanje kriptovalutama, ali centralno mjesto u novom svijetu još uvijek drže brojni posrednici, burze koji nude kupovinu i prodaju, zamjenu kriptovaluta. Valutu treba držati u digitalnom "novčaniku". Većini je presložen posao brinuti o walletu na svom računalu ili pametnom telefonu, pa se za njih ljubazno nude on-line walleti, web aplikacije koje omogućuju čuvanje vaših digitalnih valuta. No da li su ta web mjesta jednako pouzdana u čuvanju vašeg novca kao dobre stare banke? SSL enkripcija više nije dovoljna zaštita, primjenjuju se tehnike višestruke autentikacije. 2FA je novi *buzzword*, skraćenica za ***Two factor authentication***. Obično to izgleda ovako: nakon što ste preko sigurne veze upisali par username/password, na broj telefona koji ste prijavili pri otvaranju računa, ili pak na e-mail adresu ako vam je tako draže, doći će vam obavijest da se netko pokušao ulogirati u vaš račun. Priložen je PIN s kojim potvrđujete da ste to vi. PIN iskopirate u web formu i tek će vas tada pustiti do vašeg online ureda. Ako to niste bili vi, bez PIN-a provala neće uspjeti.

Ovo se isprva činilo kao dovoljna zaštita, ali nije trebalo proći mnogo vremena da se kriminalci s hakerskim vještinama prilagode novoj razini zaštite. Evo primjera: Jered Kenna [1] je radio na svom računalu iza ponoći, kad je dobio obavijest da su na dvije njegove mail adrese promijenjene lozinke. Odmah se pokušao ulogirati i zatražio promjenu lozinke, očekujući da će dobiti kod koji mu to omogućuje, ali mu obavijest nije stigla na njegov pametni telefon. Nazvao je telekom da provjeri o čemu se radi, možda nije platio račun na vrijeme? Dobio je odgovor kako on više nije njihov klijent, već je prenio broj drugom operateru. Što se dogodilo? Haker je uspio prenijeti njegov broj drugom operateru, uzeo novu SIM karticu s istim brojem i sada je mogao redom preuzimati sve Kennine on-line identitete. Momak je bio profesionalan: sedam minuta nakon što je ostao bez prvog email računa, Kenna je ostao i bez narednih trideset, uključujući dvije banke, PayPal, dva Bitcoin servisa, te na kraju i bez svog računa kod Microsofta, pomoću kojeg se prijavljivao na svoj PC. Wow! Očigledno

se haker dobro pripremio, dugo skupljao informacije i onda brzo djelovao.

Da stvar bude gora, Kenna je jedan od ranih bitcoinera, pa je s vremenom skupio lijepu kolekciju Bitcoina. Sreća u nesreći je da samo mali dio držao u on-line walletu, koliko mu je trebalo za kupovine i razne transakcije. Svejedno, šteta je mjerljiva u milionima dolara. Svjestan važnosti sigurnosti, koristio je dugačke i kompliciranе passworde, no haker je naprosto kliknuo na "Zaboravio sam lozinku" i na mobitelu pokupio kod za izmjenu zaporke.

Sreću u nesreći predstavlja činjenica da Kenna veći dio svog blaga drži na kriptiranom tvrdom disku, koji nije on-line, osim u slučaju kad treba prebaciti kovanice nekamo. To je primjer koji treba slijediti. Ali što ako mu provalnik ukrade taj disk? Ima li smisla držati njegovu kopiju on-line? Istrage su pokazale da je dio krađa kriptovaluta počinjen tako što su se hakeri dočepali računa na Dropboxu ili sličnim servisima koji nude kopije podataka.

Jeste li ikada pomislili da telekom može biti slaba karika u vašoj on-line sigurnosti? Želja da se udovolji klijentima može biti veća od obaveze poštovanja propisanih sigurnosnih procedura, pa operateri na help desku ne obave sve provjere kad ih stranka nazove i zatraži pomoć. Kod nas ne možete promijeniti operatera jednim telefonskim pozivom, morate doći u poslovnicu, sklopiti ugovor, skeniraju vam osobnu itd. Ipak smo u nečemu napredni. Ali i kod nas je bilo slučajeva da je zaposlenik zloupotrijebio svoje ovlasti, pa i tu možete očekivati probleme.

Poučeni ovim primjerom, proučite da li vam tvrtka s kojom poslujete na Mreži nudi dodatne zaštite. Na primjer, možete blokirati promjenu passworda, broja telefona, mail adrese i drugih osobnih podataka. Moći ćete to obaviti samo uz dopunske mjere zaštite, poput sekundarnog *passworda* ili *passphrasea*. Moram priznati jedan svoj grijeh: kad sam sklapao ugovor s jednim našim telekomom, pitali su da li želim dodatni *password*. Prodavač mi nije objasnio čemu to zapravo služi. Izdiktirao sam mu password, upisao ga je u računalo, a ja sam ga naivno odlučio zapamtiti. Kad sam nekoliko mjeseci kasnije poželio promijeniti tarifu, nisam se mogao sjetiti dodatne zaporke. "Ljubazni" prodavač odlučio mi je izaći u susret i obavili smo sve što je trebalo i bez dodatnih komplikacija. Kad se sada toga sjetim, prolaze me trnci. Eto koliko smo svi skupa, čak i paranoični među nama, zapravo ranjivi. Nismo ni svjesni koliko su nam važni naš pametni telefon, naš e-mail računi, naši osobni podaci (kad mijenjate zaporku telefonom pitat će vas za adresu, OIB itd). Dodatne sigurnosne provjere samo nas nerviraju i ne daju nam da brzo obavimo posao i odjurimo dalje. Ako sam već prošao autentikaciju, zašto sad još moram čekati da mi dođe obavijest s koje IP adrese se netko pokušao ulogirati u moj račun, uz već toliko puta pročitano i dosadno upozorenje da odmah upozorim tvrtku na pokušaj zloupotrebe. Pa onda ako poruka ne stigne odmah, a u međuvremenu zazvoni telefon, PIN će zastarjeti i morat ću ponoviti autentikaciju - koja gnjavaža!

Kad plaćate kreditnom karticom, ako na vrijeme prijavite krađu ili prijevaru, transakcije mogu biti poništene. Kartičari/bankari vratit će vam novac, jer su osigurani za takve slučajeve. No u svijetu kriptovaluta ne može se poništiti transakciju, nakon što je ona već sjela u blok i distribuirala se širom svijeta. To se zapravo reklamira kao jedna od prednosti kritptovalute i blockchaina! Nema naknadnih knjigovodstvenih preknjižavanja i kreativnog knjigovodstva!

Mediji su puni vijesti o krađama kriptovaluta, tako da to gotovo više i nije vijest. Cijela ta grana financijske industrije još nije regulirana kao što su poslovanje banaka i kartičara, a nema ni zaštitnih mehanizama koje propisuje država. Na primjer, ako banka propadne, država garantira za vašu štednju do određenog iznosa. Servisi koji čuvaju vaše *wallete* ne nude takve pogodnosti.

Pogledali smo koje sve metode zaštite klijenata i poslovanja koriste neki najveći i najuspješniji exchangeri kriptovaluta

- Kraken koristi 2FA autentikaciju, uz dodatnu zaštitu: za slanje poruka klijentu koriste PGP/GPG ključeve za enkripciju poruka. Osim toga nude "zaključavanje" osobnih podataka i master key za oporavak korisničkog računa. Koriste "*cold wallete*", što znači da nisu on-line, a k tome su zaključani kriptografijom. *Hot wallet* kreira se samo za vrijeme trajanja

transakcije.

- Coinbase također drži wallete i osobne podatke klijenata *offline*, kriptirane. Višestruki backup distribuiran je na brojnim mjestima širom svijeta. Također koriste dvostruku autentikaciju, te obavljaju stroge sigurnosne provjere svih svojih zaposlenika. Na poslu svi koriste kriptirane diskove, komplicirane zaporke i ostale tehnike poput zaključavanja ekrana.

Preporučujemo da se malo raspitate prije nego što odlučite otvoriti račun kod nekoga od *exchangera*. Zdravo je provjeriti da li su imali provala i drugih problema u poslovanju. Na primjer, Bitfinexu su hakeri ukrali 120.000 Bitcoina, da bi nakon toga bili prisiljeni ograničiti isplate u USD jer se očigledno ostatak financijske industrije počeo ograđivati od poslovanja s njima. Sve je to dovelo do gubitka klijenata. Nemojte vi naivno uletjeti samo zato što ste na brzinu odlučili otvoriti wallet za Bitcoine, jer vam neki on-line biznis nudi isplatu zarade u kriptovaluti. Ljudi obično pitaju prijatelja gdje si je otvorio account, pa onda slijede njegov primjer. Zato se iskusni igrači ograđuju i ne vole dijeliti savjete, jer ne žele da ih poslije okrivljuju ako nešto ne ispadne dobro.

Svakodnevno na tržištu, čitaj Internetu, niču novi igrači koji žele uzeti svoj dio kolača od trgovanja kriptovalutama. Nedavno se pojavila jedna Cryptocoin banka registrirana u Hong Kongu. Nastoje privući klijentelu nudeći svakakve slatkiše, na primjer obećavaju da će udvostručiti broj Bitcoina koji se kupe preko njih u promotivnom periodu. Ali kad krenete otvarati korisnički račun shvatite da za logiranje čak ne koriste ni HTTPS protokol, nego username/password putuje Mrežom nekriptiran! Ajme meni, pa recite vi meni tko će preko njih poslovati? Ako mislite da ljudi nisu toliko naivni, prevarili ste se. U mjesec dana skupili su desetke tisuća ljudi koji su spremni olako povjerovati u brzu zaradu.

ned, 2017-08-13 19:17 - Aco Dmitrović**Kategorije:** Kolumna [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: kolumna informacijska sigurnost kriptovalute [3]

Source URL: https://sysportal.carnet.hr/node/1751

Links
[1] https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#71b23d4938ba
[2] https://sysportal.carnet.hr/taxonomy/term/71
[3] https://sysportal.carnet.hr/taxonomy/term/112