немачка сарадња
DEUTSCHE ZUSAMMENARBEIT

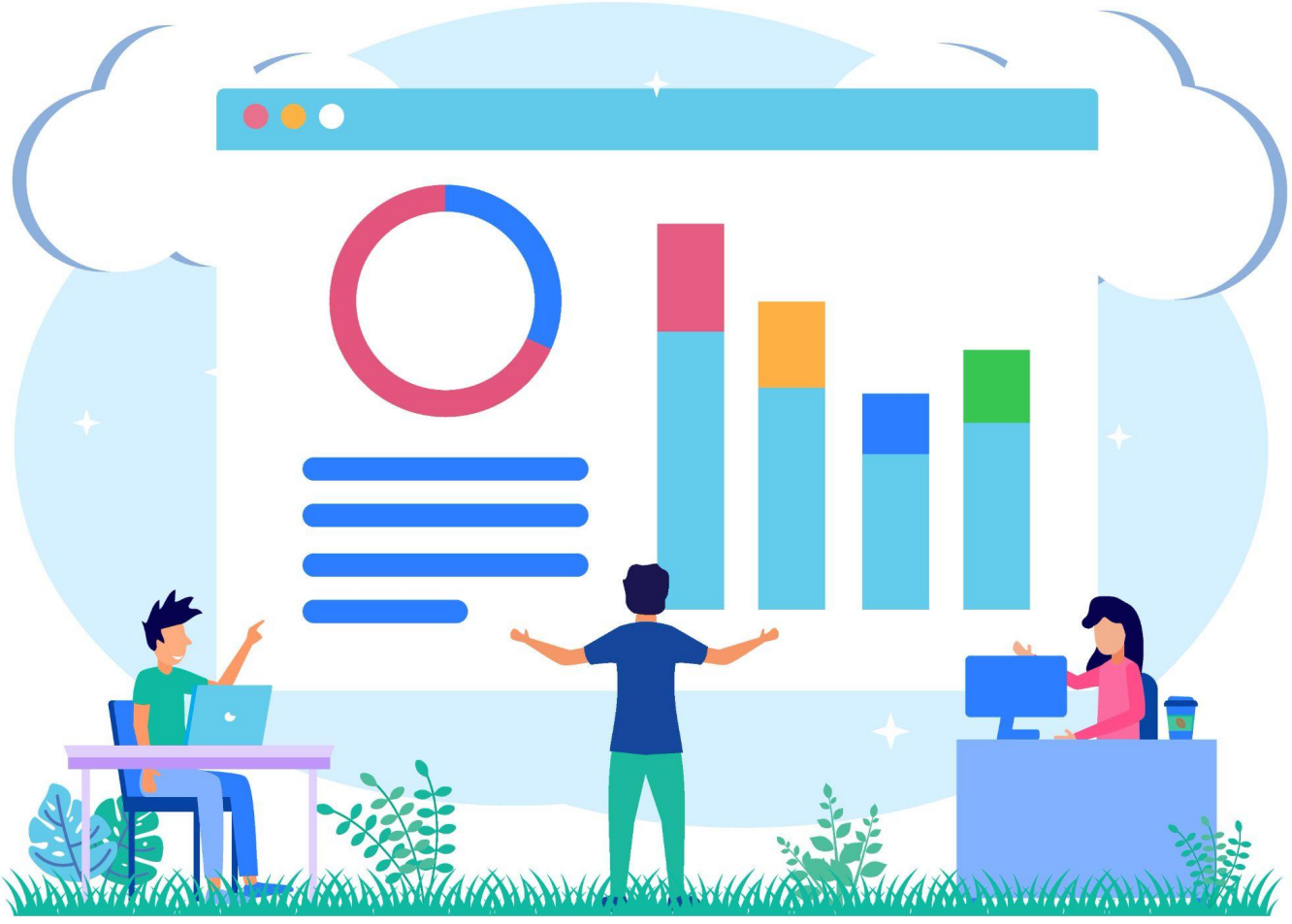
giz

Developing Local
E-commerce Ecosystems
under Covid-19 pandemics

ICT cluster
Central Serbia

Plaćanje i zaštita u online trgovini

Payment and security in e-commerce



Autor: Srđan Radenković

Sadržaj

Uvod u elektronsku trgovinu i i plaćanja

Sa razvojem informaciono-komunikacionih tehnologija, razvila se i elektronska trgovina. Još sedamdesetih godina XX veka se otpočelo sa elektronskim plaćanjem. Tokom devedesetih godina se javlja pojam elektronske trgovine i označava obavljanje raznih vrsta poslovnih transakcija elektronskim putem (prodaja dobara i usluga, komercijalne aukcije). U XXI veku dolazi do masovne proizvodnje i distribucije elektronskih proizvoda i usluga i kupovine i prodaje proizvoda, usluga i informacija putem globalne računarske mreže interneta. Pored elektronske trgovine, javlja se i novi pojam „internet trgovina“ koji predstavlja uži pojam od elektronskog poslovanja.

Sve veći broj potrošača koji robu nabavljaju putem interneta, a plaćanja vrše elektronskim putem, nametnuo je potrebu preciznog definisanja brojnih materijalnih i procesnih pravila koja regulišu materiju sklapanja elektronskih ugovora, ali koja će, pre svega biti usklađena sa pravom Evropske unije. Međutim, napredak u harmonizaciji se meri ne samo donošenjem usaglašenih propisa već dokazivanje da se oni u potpunosti i dosledno primenjuju.

Tokom poslednjih nekoliko godina sve češće se među stručnjacima mogu čuti diskusije o stepenu razvoja elektronske trgovine u Srbiji i da li ona predstavlja sektor u razvoju. Ove diskusije se vode između trgovaca, online trgovaca, finansijskih institucija, banaka, državnih institucija i raznih stručnih udruženja. Opšte mišljenje je da je Srbija još u ranoj fazi razvoja ovog tržišta i da postoje brojne prepreke i izazovi koje treba prevazići.

Glavni pokretač razvoja elektronske trgovine je proces plaćanja. Metode plaćanja su znatno napredovale tokom poslednjih nekoliko godina. Sa razvojem tehnologije, kanali kojima se plaćanje danas obavlja su sve brojniji. Opšte prihvaćeno mišljenje je da

elektronska plaćanja nude brojne pogodnosti svim korisnicima u procesu plaćanja. Istovremeno, elektronsko plaćanje nosi sa sobom i izazove kao što je bezbednost elektronskih transakcija, kontrola rizika u poslovanju, kontrola troškova u poslovanju i slično.

Uvod u industriju elektronskog plaćanja

Elektronska plaćanja su direktno povezana sa e-trgovinom i jedan su od njenih glavnih pokretača. Sa stanovišta potrošača ne postoji ugodniji način plaćanja od elektronskog. Ne morate da ispisujete čekove, provlačite platne kartice kroz automate ili da plaćate gotovinom – dovoljno je da unesete određene podatke u veb pretraživač ili mobilnu aplikaciju i da završite transakciju.

U poređenju sa tržištem Republike Srbije, elektronska plaćanja su mnogo razvijenija i prihvaćenija u svetu. Ovaj način plaćanja ima razne prednosti. Široko rasprostranjeno prihvatanje ovog načina plaćanja nudi brojne mogućnosti kao što su:

- razvoj novih platnih sistema
- bolja zaštita potrošača
- smanjenje sive ekonomije
- niži operativni troškovi

Uz razvoj telekomunikacija, sistemi za elektronsko plaćanje (e-plaćanje) ubrzano zamenjuju tradicionalne metode plaćanja koje podrazumevaju direktan kontakt između kupaca i prodavaca. Sistemi e-plaćanja pružaju brojne prednosti kako fizičkim licima, tako i pravnim licima.

Pregled tržišta e-plaćanja i mobilnog plaćanja

E- plaćanja su plaćanja koja se obavljaju putem interneta, najčešće na jedan od tri načina:

1. Obavljanjem transakcija na daljinu putem platnih kartica uz upotrebu interneta;
2. Upotrebom online bankarstva koje se zasniva na kreditnim transferima ili direktnim zaduženjima računa gde uplatilac koristi portal za online bankarstvo za autentifikaciju
3. Obavljanjem plaćanja preko pružalaca usluga e-plaćanja gde je potrebno da potrošač otvori sopstveni nalog.

Sa druge strane, m-plaćanja su plaćanja kod kojih se podaci i uputstva za plaćanje iniciraju, prenose ili potvrđuju upotrebom mobilnog telefona ili uređaja.

Ovo važi za kupovinu usluga, digitalne ili fizičke robe koja se kupuje putem interneta i tradicionalnim putem.

Mobilna plaćanja mogu se klasifikovati u dve glavne kategorije:

1. M-plaćanja na daljinu se obično obavljaju putem internet servisa ili putem premijum SMS servisa za koje mobilni operater (MO) zadužuje korisnika. Većina mobilnih plaćanja na daljinu koja se obavljaju putem interneta zasnivaju se na šemi platnih kartica. Ostala rešenja, koja se zasnivaju na kreditnim transferima i direktnim zaduženjima računa su tehnički izvodljiva, moguća, bezbedna, efikasna i konkurentna, ali se izgleda slabo probijaju na tržištu
2. M-plaćanja na blizinu se obično obavljaju na mestu prodaje. Upotreba bežične tehnologije kratkog dometa (NFC – Near Field Communication), koja je trenutno vodeća tehnologija za beskontaktna plaćanja, zahteva posebno opremljene telefone koji se mogu aktivirati kada se približe specijalnom čitaču na mestu prodaje (npr. u prodavnici, javnom prevozu, na parkingu)

Ove definicije, posebno one koje se odnose na plaćanja na daljinu, ukazuju na to da je granica između e-plaćanja i m-plaćanja nejasna i da će je biti sve teže definisati u budućnosti.

Elektronska plaćanja su značajno zaživela među potrošačima u pojedinim razvijenim državama. Većina ovih tržišta je dugo radila na izgradnji infrastrukture za elektronska plaćanja. Potrebno je omogućiti pristupačne i široko rasprostranjene finansijske proizvode, „živo" i konkurentno tržište za trgovce, kao i transparentno i produktivno poslovno okruženje.

Kako građani Evropske unije postaju sve aktivniji izvan granica svoje države, prekogranična elektronska plaćanja koja nesmetano funkcionišu značajno olakšavaju njihov svakodnevni život.

Prvi važan korak na ovom putu je uspostavljanje Jedinstvenog područja plaćanja u evrima (engl. Single Euro Payments Area (SEPA)), koja se zasniva na pretpostavci da ne bi trebalo da postoje razlike između prekograničnih i nacionalnih elektronskih plaćanja u evrima u maloprodaji širom Evropske unije. SEPA projekat obuhvata ključne platne instrumente u maloprodaji: kreditne transfere, direktna zaduženja računa i platne kartice. Imajući to u vidu, SEPA je omogućila stvaranje konkurentnog i inovativnog evropskog platnog tržišta na dva načina.

Prvi način se odnosi na sve veći udeo online ili internet plaćanja (e-plaćanja) i mobilnih plaćanja (m-plaćanja). Šta više, masovno prihvatanje pametnih telefona menja izgled tržišta industrije plaćanja i dovodi do razvoja novih aplikacija za plaćanje, npr. elektronski novčanici sve češće zamenjuju obične novčanike i kartice, a virtuelne karte za javni prevoz se nalaze u mobilnom telefonu.

Drugi način podrazumeva primenu postojećih SEPA standarda i pravila na platne instrumente kod ostalih valuta, čime se proširuju granice jedinstvenog tržišta za plaćanja transakcijama u drugim valutama.

Maloprodajno tržište evro zone je jedno od najvećih u svetu - obuhvata milione kompanija i stotine miliona građana.

Šta se dešava sa B2B e-plaćanjem i m-plaćanjem? Zapravo, potrošači su ti koji pokreću internet i mobilnu revoluciju, a ne B2B. B2C zahteva dizajn koji odgovara i koji je prilagođen preferencijama potrošača. Uz maloprodajni sektor koji vrvi od metoda plaćanja – uzmimo u obzir Apple Pay, Bitcoin i Google Wallet – potrošači se susreću sa brojnim načinima za plaćanje robe koju odluče da kupe. Stoga je zaista korisno potrošačima ponuditi čitav niz više-kanalnih opcija za plaćanje (engl. omnichannel), kao i sve popularnije automatizovane i digitalne opcije kao što su govorni automati (engl. Interactive Voice Response – IVR), virtuelno pregovaranje i online ponavljajuća plaćanja.

Iako B2B plaćanja podrazumevaju velike volumene plaćanja, ovaj segment je izuzetno spor kada je reč o usvajanju novih tehnologija u plaćanju. Plaćanja između firmi se obavljaju prvenstveno putem transfera novca (npr. SWIFT), papirnim čekovima, transakcijama putem platnih kartica ili ACH plaćanja. B2B segment nastavlja da se u velikoj meri oslanja na papirne fakture i rok plaćanja od 30 dana. To su ključni razlozi zbog čega se elektronska plaćanja sporo prihvataju u B2B areni.

Sa druge strane, spori proces uvođenja novih metoda plaćanja dovešće do nametanja novih inicijativa na polju elektronskih plaćanja. Jedna od novina u Srbiji je uvođenja i sistema elektronskih faktura.

Uvođenje elektronskih faktura doneće preduzećima u Srbiji milionske uštede na administrativnim i operativnim troškovima, a državi efikasniju kontrolu i naplatu poreza, pokazuju iskustva evropskih zemalja. U Centralnom registru svake godine evidentira se više od četiri miliona faktura, koje prime korisnici budžetskih sredstava iz javnog sektora, a kada Zakon o elektronskom fakturisanju bude u punoj primeni, poreski organi imaće bolji uvid i u milione faktura koje se razmene unutar privatnog sektora. Papirne fakture odlaze u istoriju i njihova dostava, obrada i arhiviranje moraće da se obavlja isključivo elektronski.

Sve ključne novine koje donosi Zakon o elektronskom fakturisanju, kao i demo verzija, rokovi i koraci za uspešnu primenu novog sistema od 2022. godine, mogu se naći na zvaničnoj stranici Ministarstva finansija efaktura.gov.rs.

Izazovi u industriji plaćanja

Danas gotovo da nema neke druge industrije koja se tako brzo razvija i transformiše poput globalne industrije plaćanja. Plaćanja koja su nekada smatrana fundamentalnim elementom poslovanja većine banaka, danas svi učesnici u lancu vrednosti posmatraju iz potpuno drugačije perspektive. Za to imaju dobre razloge. Plaćanja i druge transakcione usluge, kao što su upravljanje gotovinom, izdavanje platnih kartica i finansiranje kredita, za većinu banaka i velikih korporacija su ključni za privredni napredak i odnos sa klijentima. Zapravo, platne transakcije predstavljaju kičmeni stub svetske ekonomije.

Glavni globalni izazovi u industriji plaćanja su direktno povezani sa iskustvima krajnjih korisnika, mobilnim procesima za finiširanje transakcija, biometrijom, rešenjima koja povezuju više platformi koja su dostupna na tržištu i aspektima koji se odnose na

bezbednost. Ovi pokretači će definitivno diktirati način na koji će se plaćanja razvijati u narednim godinama, naročito kada je reč o mobilnim platformama.

Metode i instrumenti plaćanja

Plaćanja se menjaju tako da od industrije koju su definisali zatvoreni standardi i ograničeni pristup postaje industrija u kojoj je otvorenost glavni pokretač uspeha. Plaćanja imaju tri dimenzije koje su uvek prisutne – tehnologiju, poslovni model i poverenje. Bez sve tri dimenzije nema ni brzih, ni bezbednih plaćanja. Tehnologija je osnova za sve vrste plaćanja, ali je naročito važna za elektronsku trgovinu.

Plaćanja su prerasla od onih izuzetno integrisanih sa bankarskim uslugama u materijalno nezavisne usluge. U današnje vreme, mnogi trgovci i potrošači obezbeđuju platne usluge nezavisnim kanalima, a u toku je i debata o tome koliko je važno prihvatanje platnih kartica za bankarstvo. Sve više se prihvata i usvaja mišljenje da banke nisu jedini pružaoci platnih usluga.

Tradicionalni poslovni sistemi plaćanja uglavnom zavise od ograničenog broja poslovnica smeštenih na različitim lokacijama. Time je ograničena pokrivenost svih klijenata. Međutim, uz upotrebu internet usluga, e-platni sistemi su dostupni velikom broju klijenata.

Postoje različite podele metoda plaćanja. Ni jedna od tih podela nije opšte usvojena, a razlog tome je postojanje različitih interesnih grupa od kojih su neke snažnije od drugih. Kao primer možemo navesti snagu brendova kao što su Visa ili MasterCard, koji predstavljaju dva dominantna sistema plaćanja. Stoga se metode plaćanja najčešće dele na plaćanja platnim karticama i alternativne metode plaćanja.

U stvarnosti ova raznolikost metoda plaćanja izgleda mnogo složenija. Postoje brojni kriterijumi prema kojima je moguće izvršiti podelu:

- prema tehnologiji (npr. NFC, e-bankarstvo, Bluetooth, SMS, POS, ATM, ...)
- prema veličini tržišta na kome su odgovarajuće metode plaćanja prisutne (npr. lokalno, regionalno ili globalno tržište).
- prema kanalu (npr. internet, mobilni uređaji ...)
- prema licu kome je metoda plaćanja namenjena (npr. za fizička ili pravna lica)
- prema operativnom sistemu (npr. iPhone, Android ...)
- prema vremenu (npr. u realnom vremenu – online ili offline)

MasterCard, Visa i PayPal su verovatno najprihvaćenije online metode plaćanja u svetu. Druge metode plaćanja su verovatno još popularnije u zemljama u kojima su nastale ili u regionu. Uzevši u obzir složene načine po kojima se metode plaćanja mogu deliti, iskoristićemo one koji se najčešće koriste. Obično se metode plaćanja dele na:

- Platne kartice
- Alternativne metode plaćanja

Danas postoji više od 300 alternativnih šema plaćanja koje funkcionišu širom sveta. Stoga je potrebno da trgovci razumeju koje vrste plaćanja bi trebalo da ponude svojim klijentima. Ta odluka zavisi od toga gde se nalaze njihovi klijenti i kakvu vrstu usluga ti trgovci nude. Obzirom na globalnu prirodu e-trgovine, neophodno je pri meniti strategiju plaćanja koja je usmerena na potrebe klijenata širom sveta.

Platne kartice

Platne kartice se mogu posmatrati kao ključ za bankovne račune klijenata, bez obzira da li je reč o debitnim, kreditnim ili unapred dopunjenim (engl. prepaid) karticama. Kartice se mogu iskoristiti da „otključaju“ račun kupca i prebace novac na račun online trgovca (e-trgovca).

Najčešće korišćeni i prihvaćeni brendovi kreditnih i debitnih kartica su VISA, MasterCard, Maestro, American Express, Diners Club International, Discover, JCB i UnionPay. Pored ovih globalno prepoznatljivih brendova, postoje i oni koji su karakteristični za pojedine države ili regione, kao što su UnionPay u Kini, Hipercard u Brazilu, BC Card u Južnoj Koreji, Dankort u Danskoj, Carte Bleue u Francuskoj ili Dina Card u Srbiji.

Plaćanje karticama može se dalje podeliti na plaćanje kreditnom, debitnom, unapred dopunjenom (pripejd; od engl. prepaid) , poklon karticom i karticom lojalnosti. Ove vrste plaćanja karticama imaju različite karakteristike što predstavlja osnovu za posebnu klasifikaciju. Razlikuju se u pogledu korišćenja, nivoa, prihvaćenosti, regionalnosti, bezbednosti, troškova, obaveza i odgovornosti, itd.

- Kreditne kartice su fizičke ili digitalne (virtuelne) kartice koje predstavljaju takoreći odobren kreditni limit po računu
- Debitne kartice su fizičke ili digitalne (virtuelne) kartice koje predstavljaju debitni račun.
- Unapred dopunjena tj. pripejd (prepaid) kartica je fizička kartica ili jedinstveni broj sa fiksnim maksimalnim iznosom. Mogu se koristiti za kupovinu na internetu ili za tradicionalnu kupovinu.

- Poklon kartice su kartice koje sadrže pohranjeni iznos novca. Dve najrasprostranjenije kategorije poklon kartica su one koje izdaju trgovci i kartice koje izdaju banke. Kartice lojalnosti sadrže informacije koje se koriste za identifikaciju kupca pri svakoj transakciji. Kompanija koja je izdala takvu karticu može da ponudi nagradu za ponovnu kupovinu.

Alternativne metode plaćanja

Platne kartice nisu jedini način za obavljanje online transakcija. Šta više, u svetu e-trgovine postoji više od 300 različitih, alternativnih, metoda plaćanja. Preferencije potrošača zavise od demografskih karakteristika, države, proizvoda i usluga koje potrošači kupuju; stoga je razumevanje lokalnih preferencija ključ za osvajanje međunarodnog tržišta.

Kako je broj alternativnih metoda plaćanja izuzetno veliki, ovde će biti predstavljeni samo oni koji su opšte poznati i globalno prisutni, kao i oni koji su delimično prisutni ili imaju potencijal da se uskoro pojave u određenom regionu. Pored toga, podela alternativnih metoda plaćanja u maloprodaji je raznolika. Stoga je potrebno osvrnuti se i na ostale vrste plaćanja.

Bankovni transferi

Mogu se podeliti na:

- Online bankovne transfere (transfere u realnom vremenu)
- Offline bankovne transfere

Ove metode plaćanja povezane su sa bankom kupca i kupac daje odobrenje da se transfer izvrši (vrši autorizaciju). Transfer priprema trgovac, a samo uz odobrenje kupca banka može da obavi online transfer novca.

Direktna zaduženja računa

Direktna zaduženja računa nisu relevantna za sve trgovce. Ona su ograničena na transakcije manjih vrednosti ili na transakcije koje se ponavljaju. Ona su popularna za redovna, predvidljiva plaćanja, kao što su pretplate, mada kod njih postoji rizik od povećanog broja reklamacija. Direktna zaduženja računa predstavljaju metodu plaćanja gde trgovac inicira transfer novca sa računa kupca na svoj račun. Za njih je obično potrebno imati odobrenje kupca (u papiru ili elektronski, sa različitim stepenom autentifikacije).

E-novčanici ili digitalni novčanici

E-novčanici ili digitalni novčanici predstavljaju vrstu plaćanja koja se u celom svetu najbrže razvija. Oni se, zapravo, definišu kao posebna, treća vrsta ili metoda plaćanja, pored platnih kartica i alternativnih metoda plaćanja. Vrlo lako se koriste i sve više su popularni za kupovinu digitalne robe i video igrica.

U privredama sa razvijenom e-trgovinom, kao što su UK i SAD, tradicionalni pružaoci kartičnih transakcija sve češće prihvataju e-novčanike. Na globalnom nivou, Alipay i PayPal nastavljaju da dominiraju tržištem e-novčanika. Mladi kupci su ti koji pokreću rast. PayPal novčanik je verovatno najpoznatiji.

Digitalni novčanici omogućavaju kupcima da povežu platne kartice ili druge alternativne metode plaćanja sa virtuelnim novčanikom. Potrošači tada mogu da plate koristeći pohranjeni iznos u svom novčaniku ili da odmah plate pomoću svoje registrovane kartice ili alternativnom metodom plaćanja. E-novčanici pružaju bolje korisničko iskustvo pri plaćanju i pojednostavljuju online i mobilni proces kreiranja porudžbine. Potrošači posebno cene to što je plaćanje putem mobilnih uređaja unapređeno i ubrzano.

Mobilna plaćanja

Mobilno plaćanje je jedna od metoda plaćanja koja zahteva upotrebu mobilnog uređaja da bi se potvrdio identitet kupca. Kod nekih od njih naplata se obavlja putem računa za mobilni telefon preko mobilnog operatera, neki od njih funkcionišu kao e-novčanik, a pojedine finansijske ustanove kao što su banke takođe koriste ovu metodu. Mobilna plaćanja spadaju u sledeće kategorije:

- Direktna naplata mobilnih operatera
- Mobilni e-novčanici
- In-app plaćanja
- Premium SMS
- NFC (bežična tehnologija kratkog dometa)

Plaćanje pouzećem

Plaćanje pouzećem je metoda plaćanja gde se koristi gotovina koja se isplaćuje kada se roba isporuči. Kurirske službe preuzimaju novac kada isporuče proizvod. Ova metoda plaćanja postaje sve manje popularna i u razvijenim zemljama i u zemljama u razvoju.

E-bankarstvo

E-bankarstvo je vrsta platne mreže koju je razvila bankarska industrija u saradnji sa pružaocima usluga koji razvijaju tehnologije prilagođene jedinstvenim zahtevima klijenata banke.

Identitet korisnika potvrđuje se u realnom vremenu od strane njegove online bankovne infrastrukture. Raspoloživost sredstava potvrđuje korisnikova finansijska institucija u realnom vremenu. Ona takođe garantuje trgovcu da će plaćanje biti izvršeno.

Plaćanje se obavlja putem transfera koji inicira korisnik od strane njegove finansijske institucije ka trgovcu, što je suprotan smer od debitnog transfera gde transfer inicira trgovac. Plaćanje se obavlja direktno sa računa korisnika, a ne preko računa neke treće strane.

Pre-pay vaučeri

Korisnici treba da kupe vaučer pre nego što započnu transakciju. Ovi vaučeri se obično odmah odobravaju. Većina pre-pay proizvoda ima ograničena sredstva, pojedine šeme ne omogućavaju da više kartica/vaučera bude iskorišćeno za plaćanje jedne transakcije. To znači da pre-pay metode nisu pogodne za kupovinu robe veće vrednosti.

Digitalne valute

Digitalne valute ili kriptovalute postaju sve popularnije uprkos velikim barijerama za njihov ulazak na tržište. Državne uprave i centralne banke ih ne podržavaju pa njihova vrednost oscilira u velikoj meri.

Ljudi širom sveta sve više prihvataju bitkoin kao digitalni novac. Bitkoin je digitalna valuta zasnovana na P2P (engl. peer-to-peer) tehnologiji koja funkcioniše bez centralnog nadzornog organa. Bitkoin koristi kriptografiju da bi se kontrolisale i evidentirale transakcije. Kada transakcija prođe potrebne provere, ona se evidentira u javnoj glavnoj knjizi koja je poznata pod nazivom Block Chain. Zatim se ove transakcije šalju svim ostalim članovima na mreži, čime se sprečava dupla naplata i vodi računa da svi drugi članovi „pošteno“ posluju.

Transferi novca

U svetu sveprisutnih bankomata, uređaja za plaćanje jednim dodirom ili klikom i automatizovanih bankarskih depozita, još uvek se dešava da je neophodno poslati ili

preuzeti gotovinu. Zbog toga i servisi za transfer novca kao što su Western Union i MoneyGram imaju desetine hiljada agenata u gradovima širom sveta.

Stanje na srpskom tržištu e-plaćanja i m-plaćanja

Popularnost internet kupovine (e-trgovine) u Srbiji pokazuje trend stabilnog rasta tokom prethodnog perioda. Republika Srbija ima istoriju e-trgovine i e-plaćanja. Astra banka je nudila e-commerce uslugu još 1999. godine. To je bio prvi sistem za autorizaciju i naplatu platnih kartica koji je trgovcima davao mogućnost da obavljaju online naplatu. Takođe, potrošači su mogli da koriste platne kartice i da obave elektronsko plaćanje.

Danas gotovo sve banke koje posluju u Srbiji omogućavaju svojim klijentima korišćenje svih servisa elektronskog plaćanja. Takođe, svi operateri podržavaju usluge m-plaćanja razvnih servisa i usluga.

U Srbiji trenutno posluje i više posredničkih firmi, takozvanih procesora plaćanja, koji omogućavaju prodaju preko interneta, bez otvaranja posebnog računa u banci, bez investicije u infrstrukturu, te prihvatanje platnih kartica na internet prodavnicama u Srbiji.

Zaštita na internetu

Moderni računari upravljaju našim novcem, zdravstvom, železnicom, aviosaobraćajem i sl. Od nas se očekuje da verujemo u informacione tehnologije. Mnoge koristi našeg partnerstva sa mašinama su jasne. Međutim, potpuno poverenje u modernu računarsku tehnologiju može da bude apsurdno i, u dosta slučajeva, opasno. U svakom ozbiljnom sistemu danas se razmatraju bezbednosni izazovi primene savremenih informacionih tehnologija: pravne dileme, etička pitanja i rizici pouzdanosti.

Da li znali da svakim klikom na internetu, od web sajtova do društvenih mreža, ostavljate ličnepodatke? Znate li možete li ih i kako obrisati?

Iako je internet medij bez kojega je danas gotovo nemoguće raditi, na kome pronalazimo važne informacije, zabavljamo se i putem koga komuniciramo s drugima, često zaboravljamo na različite opasnosti od kojih se moramo zaštititi. No, krenimo redom.

Ljudi koriste računare kao podršku svom poslu, ali vrlo često i za kršenje zakona. Računari su moćni alati u rukama kriminalaca, a računarski kriminal je rapidno rastući problem. Danas je računar u mnogim situacijama kod kriminalaca zamenio klasično oružje. Računarski kriminal se često definiše kao bilo koji zločin učinjen zahvaljujući znanju ili korišćenjem računarske tehnologije.

Niko ne zna pravi obim računarskog kriminala. Mnogi računarski zločini prođu neopaženi. Oni koji se otkriju, često prođu neprijavljeni zato što se kompanije plaše da mogu izgubiti više zbog negativnog publiciteta nego od stvarnog zločina.

Većinu računarskih zločina počine insajderi kompanije (zaposleni unutar kompanije), a njih ne prijavljuju vlastima, čak i kada su uhvaćeni na delu. Da bi se izbegle nezgode, mnoge kompanije prikrivaju računarske zločine koje su počinili njihovi zaposleni i

rukovodioci. Organizovani kriminal je odavno prešao na računarsku tehnologiju. Eksplozivni razvoj Interneta i servisa za trgovanje i plaćanje putem Interneta postali su meta računarskog kriminala, kako Internet veze, tako i računarski sistemi koji su povezani na Internet.

Još jedan vid računarskog kriminala je sabotaža hardvera ili softvera. Reč sabotaža dolazi iz početaka industrijske revolucije, kada su buntovni radnici isključili nove mašine udarajući drvenim cipelama, zvanim "saboti ", u zupčanike. Moderni računarski saboteri za izvršenje destruktivnog dela obično koriste zlonameran softver (malver (engl.Malware)). Zlonamerni softver je skup instrukcija koji se pokreću na korisnikovom računaru i čine da korisnički računar radi ono što napadač želi. Nazivi koji su dati sabotirajućim destruktivnim programima – virusi, crvi i trojanski konju – zvuče više nalik biologiji nego tehnologiji, a većina programa čak i imitira ponašanje živih organizama.

- Virus - Inficira host fajl, samo-kopira se, u većini slučajeva mu je potreban ljudski faktor da bi se samo-kopirao (otvaranje fajla, čitanje mejla, butovanje sistema, ili izvršavanje inficiranog programa)
- Crv - Širi se putem mreže, samo-kopira se, u većini slučajeva nije mu potrebna ljudska interakcija da bi se širio
- Trojanski konj - Izgleda kao koristan program, ima prikrivenu malicioznu svrhu
- Adver (engl.Adware), Špijun (engl.Spyware) - Špijun -špijunski softver, Adver-reklamni špijunski softver, često se sadrže u drugim softverima
- Maliciozni mobilni kod - Čine ga mali programi skinuti sa nekog udaljenog sistema i pokrenuti lokalno sa minimalnim, ili bez učešća korisnika
- Bekdor (engl.Backdoor) - Zaobilazi sigurnost sistema da bi omogućio pristup napadaču

- Rutkit (engl.Rootkit) - Manipuliše sa srcem operativnog sistema, kernelom, skriva se i stvara bekdor
- Kombinovan Malver - Kombinacija više različitih tehnika prethodno prikazanih da bi se stvorio bolji malver

Šta je internet zaista i kako funkcioniše?

Internet je sistem koji omogućava različitim uređajima da međusobno komuniciraju ili razmenjuju podatke. Postoje dve vrste uređaja: server (računari na kojima se nalaze podaci, koji pružaju usluge drugim uređajima kao što su Internet serveri, serveri e-pošte itd.) i klijent (oni uređaji koji se povezuju na tu mrežu računara i preko kojih se čitamo podatke). Da bi se svi ovi uređaji međusobno razumeli, postoje i različiti protokoli kojima putuju određeni podaci i zajednički programski „jezik" preko kojeg uređaji prepoznaju podatke.

Povezujemo se na Internet preko ISP-a, prvo na njegovu mrežu, a zatim na globalnu Internet mrežu. Svaki uređaj koji se povezuje na Internet ima svoje jedinstveno ime, ili IP adresu, neku vrstu lične karte. IP adresa se menja u zavisnosti od mreže preko koje pristupate Internetu (mreža na poslu, kod kuće, u biblioteci itd.). Međutim, putem IP adrese mogu se saznati određeni lični podaci, kao grad iz kojeg se povezujete na Internet, poštanskog broja i Internet servera preko kojeg ste povezani.

ISP u svakom trenutku vidi ko je, sa kog uređaja i kada je pristupio Internetu, čak i sa koje web lokacije. On je dužan da ove podatke dostavi policiji ili drugim pravnim organima na zahtev. Vlasnici web lokacija / raznih usluga / igara i sličnih medija kojima pristupamo takođe imaju pristup našim IP adresama. Međutim, najčešće ih koriste samo kao statistiku o opštem prometu na svojim stranicama.

Osim neizbežne IP adrese, na Internetu ostaje sve što objavite na društvenim mrežama, fotografije koje ste postavili kao profilne fotografije na raznim internet nalozima ili bilo koji sadržaj (slika, video, tekst) koji ste ikada igde postavili. Ovaj sadržaj ostaje snimljen na Internet serverima čak i ako ste ga u međuvremenu izbrisali.

Ovo je veoma važna činjenica koja se često zaboravlja: sve što objavite na internetu ostaje na internetu! Čak i ako slučajno nešto objavite i odmah izbrišete, to ostaje zapamćeno na nekom serveru i tu ostaje zauvek. Zato morate paziti šta objavljujete.

Kako zaštititi lične podatke kada ste na mreži?

1. Koristite složene lozinke
   Ne dozvolite drugom da vide vaše pristupne podatke. Da biste se prijavili na bilo koji od svojih uređaja i online medijskih naloga - koristite što složenije lozinke da biste zaštitili svoje podatke. Ovo je posebno važno za e-poštu i društvene mreže. Nemojte koristiti datum rođenja ili jednostavnu i čestu lozinku kao što je 1234. Umesto toga, koristite dugu kombinaciju velikih i malih slova, brojeva i znakova. Takođe, nemojte koristiti istu lozinku za sve postojeće naloge. Obavezno zapamtite da lozinke ne ostavljamo na komadima papira na vidljivom mestu, kao što je računar ili na stolu u kancelariji.
2. Vodite računa o svojim uređajima
   Ne ostavljajte svoje uređaje bez nadzora! Da li se vaš mobilni telefon automatski povezuje na društvene mreže, e-mail servise i slično? Врло често имамо укључену такву опцију јер нам олакшава свакодневну рутину. Međutim, pazite da ne ostavite svoj uređaj bez nadzora. Stoga, kada ste u kancelariji i idete na ručak ili sastanak, zaključite radnu stanicu, dok ste u kaficu, vodite računa o svom mobilnom telefonu i obavezno na njemu koristite složenu lozinku.
3. Pazite šta objavljujete

Kao što smo već spomenuli, sve što ne biste želeli da svi vide, čak i kada to izbrišete, nemojte to objavljivati na mreži. Ne objavljujte svoje ili tuđe lične podatke, izbegavajte pisanje tačnog datuma i mesta rođenja, ne objavljujte fotografije ličnih dokumenata itd. Izbegavajte postavljanje slika ili video snimaka dece i maloletnika i adresa na kojima živite ili boravite.

4. Ne postavljajte fotografije / video zapise unutrašnjosti soba u kojima živite Izbegavajte razmenu informacija o svom odmoru ili vremenu kada nećete biti kod kuće. Kada ste na društvenim mrežama, pazite sa kim se povezujete u „prijateljstvima“ i koristite opciju da ograničite prikaz sadržaja koji gledate ili objavljujete. Sad tako postaje vidljiv samo vašim prijateljima, a ne svim korisnicima te društvene mreže ili interneta.
5. Pazite šta otvarate
   Pre nego što kliknete na internet vezu, bez obzira ko vam je poslao, razmislite dva puta! Različiti računarski virusi su programirani tako da je potreban samo jedan klik da biste ih preuzeli na uređaj koji koristite da biste ga zarazili.
6. Izbegavajte javne računare
   Koristite javne računare samo za traženje informacija i ne za povezivanje sa bilo kojim od postojećih Internet naloga (e-mail, društvene mreže, bankarski servisi itd.). Javni računari su dostupni svima, pa su svi podaci na njima dostupni svima: od istorije pretraživanja do informacija potrebnih za prijavu na internet naloge.

Osnovne sigurnosne pretnje u elektronskom poslovanju

1. Zlonamerni kod
   Ovu grupu štetnih uticaja čine virusi, crvi, trojanski konji i bad applets koji su pretnja integritetu sistema i njegovoj kontinuiranoj operativnosti. Njihovo

delovanje, donekle rizično, uglavnom se ispoljava u promeni načina rada sistema ili promeni dokumenata kreiranih u okviru sistema.

2. Hakeri i sajbervandalizam
   Haker se definiše kao pojedinac koji želi da ostvari neovlašćeni pristup računarskom sistemu. Nekada im je dovoljno to što prodru u fajlove e-trgovinskog sajta, ali ima slučajeva kada im je namera vezana za tzv. Sajbervandalizam što podrazumeva prekidanje, promenu ili uništavanje sajta. U okviru hakerske zajednice, krekerima se nazivaju hakeri koje preduzimaju kriminalne aktivnost. Tokom vremena, aktivnosti hakera se menjaju i šire pa se, osim na upad u sistem, orijentišu i na krađu informacija i robe, kao i na uništavanje sistema.
3. Zloupotreba kreditnih kartica
   To je najčešća pojava i jedan od glavnih razloga zbog kojeg više potrošača ne učestvuje u e-trgovini. Najčešći slučaj je izgubljena kartica ili ukradena koju koristi neko drugi kao i krađa brojeva kreditnih kartica radi dalje zloupotrebe i lažnog predstavljanja identiteta vlasnika kartice.

U e-trgovini najveća pretnja kupcima je da će prodavac server izgubiti podatke o kreditnim karticama koji su na njemu deponovani ili će dozvoliti da se koriste u kriminalne svrhe. Osim toga, e-trgovinski sajtovi su odličan izvor personalnih podataka kupaca (ime, adresa, broj telefona) koji mogu da se zloupotrebe.

1. Lažno predstavljanje
   Hakeri nekad pokušavaju da prikriju svoj pravi identitet ili se lažno predstavljaju na osnovu lažne e-mail adrese. Spoofing narušava i princip autentičnosti i inegriteta jer otežava utvrđivanje identiteta prave ličnosti koja šalje poruku.
2. Napadi usmereni na odbijanje sajta
   Hakeri nekad opterete web sajt beskorisnim porukama da bi opteretili mrežu,

što često izaziva zatvaranje mreže i nanosi reputaciji sajta i odnosima sa potrošačima. Za online prodaje takvi napadi su skupi jer dok je sajt zatvoren kupci ne mogu da poručuju robu.

3. Njuškanje
   Tip programa za prisluškivanje koji prate informacije koje se kreću po mreži i omogućavaju hakerima da ukradu poverljive informacije sa bilo koje lokacije na mreži uključujući e-mail poruke, fajlove kompanije i poverljive izveštaje. Njuškanje je zaparvo pretnja da će poverljive informacije biti javno prezentovane.
4. Napadi iznutra
   Iako je najveća pretnja od spoljašnjih napada, postoji i značajna opasnost da zaposleni ,iznutra, neovlašćeno koriste podatke i informacije koje su im dostupne.

SSL sertifikati: zašto su bitni i kako dodati HTTPS na vaš sajt?

Ako mislite da vaš sajt neće izgubiti svoje posetioce zbog manjka sigurnosti, grešite. Momenat kada nam svima bezbednost sajta postane od izuzetne važnosti jeste kada treba da unesete podatke svoje kartice i kupite nešto online. Jedno od istraživanja kaže da čak 85% internet kupaca odustane od kupovine na sajtu koji im se ne čini bezbednim. Većina ljudi prepoznaje simbol katanca u URL-u kao znak bezbednosti, ali šta ovo zapravo znači i zbog čega je bitno?

Ako ste ikad pogledali URL na vrhu ekrana web pretraživača, sigurno ste videli da neki sajtovi počinju sa “HTTP”, a neki sa “HTTPS”. Upravo ovo S znači “secure”, iliti bezbedno – i postiže se obezbeđivanjem vašeg sajta SSL sertifikatom. Ono što zapravo HTTPS sajtovi imaju jeste dodatni sloj zaštite za sve osetljive podatke koji se razmenjuju.

Kao što smo već pomenuli, sajtovi koji su zaštićeni SSL-om obično imaju zeleni katanac koji se prikazuje u prozoru URL-a. Ovo je ikonica koju internet korisnici prepoznaju kao znak poverenja za online prodavce.

SSL je oblik šifrovanja podataka gde web pretraživač koji koristite uspostavlja sigurnu vezu sa web stranicom koju posećujete. To radi tako što podatke deli napred i nazad između ta dva i šifruje ih. Podatke može videti samo sajt koji ima SSL sertifikat, jer poseduje ključ za dešifrovanje.

Jedno od najstarijih pravila trgovine, fizičke ili online, jeste da ljudi uvek kupuju od brendova kojima veruju. Kada kupujete uživo, ovaj momenat je mnogo lakši, ali, kako možete najlakše da utvrdite to online?

Odgovor je jednostavan – autentifikacijom SSL bezbednosti, jer se tada poverenje između kupca i online prodavca može postići najefikasnije.

Kao protokol, SSL bezbednost je postala popularna alatka za zaštitu podataka. SSL sertifikat omogućava ljudima da koriste kreditnu karticu, svoje privatne podatke poput adrese, JMBG-a i slično, između email servera, pretraživača i sajta. Na ovaj način SSL sertifikati svakodnevno štite milione transakcija na internetu.

Dakle, ukoliko sajt ima “HTTPS://”, to znači da poseduje SSL sertifikat, dok ukoliko samo vidite “HTTP”, nije bezbedan. Svakako, u julu 2018. godine, Google Chrome je počeo da označava sajtove kao nebezbedne (not secure), pa će vam detekcija biti mnogo lakša.

Online korisnici svakog dana postaju sve obrazovaniji kada je reč o internetu, bezbednosti i slično. Činjenica da imate SSL sertifikat pokazuje vašim klijentima i posetiocima da imate najviši nivo bezbednosti i da mogu da vam veruju. Kao dodatni bonus, u miru ste, jer znate da postoji mala verovatnoća da dođe do kršenja podataka na vašem sajtu. Bez SSL-a, podaci koji putuju između kupca i sajta prilikom online

trgovine, u opasnosti su i podložni hakerskim napadima koji kradu podatke onda kada su najosetljiviji.

Pored ovih, postoji još jedan veliki razlog za dodavanja SSL sigurnosti – Google. Google uzima u obzir SSL kao faktor za svoje SEO algoritme, tako da se sajtovi sa SSL-om više rangiraju od onih koji ga nemaju. A, iskreno, u ovim današnjim teškim ratovima za što bolji rang na Google-u, sve ide u prilog da dobijete koji bod više.

Šta je i na koji način štiti dvostepena autentikacija?

Lozinke su već godinama na lošem glasu kao nešto što je teško pravilno izabrati i kasnije zapamtiti. Korisnici često biraju trivijalne password-e, koriste iste ili slične nizove znakova na raznim sistemima, teško pamte složene kombinacije slova i brojeva koje neki sistemi nameću, a posebno su neradi da povremeno menjaju teško zapamćenu šifru. Mnoge „provale“ na sisteme desile su se zbog loše izabranih ili loše čuvanih lozinki, čak i od strane navodno iskusnih administratora. Zato IT svet već dvadesetak godina traga za alternativom password-ima, za sada bez pravog uspeha. Sve više sajtova i servisa forsira dvostepenu autorizaciju kao način da se osigurate od zlonamernog pristupa vašim podacima. Uprkos tome, lozinke su i dalje važne. Oni jednostavno nisu ni približno tako efikasni kao što su bili. Ljudi koriste slabe lozinke i ponovo ih koriste od lokacije do lokacije. Osim toga, hakeri su prikupili milijarde korisničkih imena i lozinki. Iz ovih razloga, lozinke na veb lokacijama nisu ni približno sigurne kao što su bile.

Zato je prirodna ideja da se lozinka, dakle nešto što znate, dopuni još nečim, što neće biti tako lako zloupotrebiti. Recimo, nečim što imate i što stalno nosite sa sobom. Dvofaktorska autentikacija (2FA) je dodatni sloj sigurnosti povrh lozinki. Deluje kao neka vrsta druge lozinke prilikom prijavljivanja na sajtove. Na ovaj način, ako neko uspe

da prenese vaše korisničko ime i lozinku na veb lokaciju, i dalje neće moći da pristupi vašem nalogu osim ako nema pristup vašem „drugom faktoru“.

Šanse su da ste već koristili 2FA, a da toga niste svesni. Neke banke osiguravaju pristup računu malim uređajem („token“) koji generiše jednokratne lozinke, ali je teško očekivati da nosite sa sobom deset takvih uređaja pa da jedan koristite za banku, drugi za Gmail, treći za Facebook... Ostaje da se koristi neki univerzalni uređaj koji svako već ima, a to je pametni telefon. Čest primer je kada vaša banka pošalje tekstualnu poruku sa kodom koji morate da unesete pre nego što pristupite svom računu.

U opštem slučaju, dvostepena autentikacija funkcioniše tako što, kada se ulogujete na neki sistem unoseći korisničko ime i lozinku, sistem zamrzava proces prijavljivanja i šalje jedinstveni kod koji primate na mobilnom telefonu. Tek kada unesete taj kod u masku koja se ispisuje na ekranu računara, proces prijavljivanja se uspešno završava i dobijate pristup sistemu. Dakle, ako neko zna vašu lozinku, ne može da se prijavi bez vašeg mobilnog telefona. Ako na neki način dođe do telefona (nađe ga ili ukrade), ne može se prijaviti bez lozinke. Zvuči jednostavno i efektno, ali krije mnoge finese i potencijalne probleme.

Tekstualne poruke su najosnovniji oblik 2FA koji se danas koristi i takođe najslabiji oblik 2FA. Trenutno su u upotrebi tri primarna oblika 2FA.

- Tekstualne poruke – nakon što unesete lozinku, preduzeće vam šalje tekstualnu poruku sa jednokratnim kodom. Ovo morate da unesete na veb lokaciju u određenom vremenskom periodu da biste završili proces prijavljivanja. Iako je zgodan, ovo je najmanje siguran metod jer ljudi mogu presresti ove poruke. Međutim, i dalje je vredno koristiti 2FA zasnovanu na SMS-u ako je to jedina opcija koju veb lokacija nudi. I dalje je znatno bolje nego samo korišćenje lozinke.

- Kodovi zasnovani na aplikacijama – korak dalje je korišćenje aplikacije za autentifikaciju kao što je Google Authenticator, koja je dostupna i na Android-u i na iOS-u. Aplikacije za autentifikaciju rade sa više veb lokacija, tako da morate da preuzmete samo jednu aplikaciju da biste se prijavili na više lokacija. Aplikacije generišu pokretne kodove koji se menjaju otprilike dva puta svakog minuta. Nakon što unesete lozinku na veb lokaciju, sajt će od vas zatražiti da otvorite aplikaciju da biste pronašli trenutni kod. Još uvek postoje određeni rizici za ovaj oblik 2FA. Neki lopovi će pokušati da vas navedu da unesete lozinku na lažnom sajtu, a zatim će od vas zatražiti vaš 2FA kod. Ako date kod, lopov se može odmah prijaviti na vaš nalog.
- Fizički ključevi – fizički ključevi su trenutni zlatni standard za 2FA. Takođe su lakši za upotrebu od drugih oblika. Fizički ključ je mali uređaj koji se uključuje u USB port računara ili se bežično povezuje sa računarom. Kada unesete lozinku, sajt će od vas tražiti da dodirnete svoj ključ ili pritisnete dugme na njemu, u zavisnosti od tipa. Ključevi se mogu koristiti na više veb lokacija.

Dvostepena autentikacija svakako nije savršen metod, ni sa aspekta lakoće upotrebe, niti sa aspekta bezbednosti. Ipak, njeno korišćenje bitno povećava sigurnost vašeg korisničkog naloga, odnosno umanjuje mogućnost da se vašim podacima neovlašćeno pristupa ili da oni budu obrisani. Primena te tehnike zahteva da uvek nosite smartfon (zar to svi ne radimo?) a u najvećem broju slučajeva i da taj telefon ima pristup Internetu. Primena pomalo usporava rad, ali je to usporenje prihvatljivo kada se uzme u obzir povećanje bezbednosti.

Stručnjacima za bezbednost ostaje da dalje tragaju za nekim jednako sigurnim, ali komfornijim metodom. Nažalost, uz sve priče o biometriji i prepoznavanju lica, takav metod još nije ni blizu realizacije. Zato preporučujemo Two Step Authentication (ili Verification kako mnogi kažu), ali uz pun oprez da ne biste s jedne strane realno

umanjili bezbednost želeći da je povećate, a s druge izgubili mogućnost da se ulogujete na sopstveni nalog jer ste nešto pogrešno podesili. Korak po korak do sigurnijeg Interneta!

Zlonamerna upotreba e-pošte

Hipotetički govoreći, recimo da primite e-poštu koja izgleda kao da je od vašeg šefa, vašeg provajdera usluga e-pošte, možda čak i od vašeg najboljeg prijatelja. Vi biste prirodno bili skloni da ga otvorite, zar ne? Razmislite ponovo.

Kada otvorite imejl koji je napravljen tako da izgleda kao da je došao od nekoga kome verujete, smatrajte da ste „prevareni imejl". Prevara e-pošte se odnosi na slanje e-poruka sa falsifikovanom adresom „od". Ovo je uobičajena taktika koju ciber prevaranti koriste da steknu poverenje svojih žrtava - aka, vi.

Iako nedavne studije ukazuju na skoro 30.000 napada lažiranja e-pošte svakog dana, njegova sveprisutna priroda ne znači da ga ne treba shvatati ozbiljno. Pošto sajber kriminalci znaju da je veća verovatnoća da ćete se baviti pouzdanim sadržajem e-pošte, bilo da se radi o klikanju na vezu ili otvaranju priložene datoteke, to im olakšava da izvedu uspešnu prevaru. Pretvarajući se da ste neko koga poznajete ili poznajete, ovi prevaranti vas na kraju mogu prevariti da predate vitalne podatke, poput podataka o kreditnoj kartici, podataka o socijalnom osiguranju, lista se nastavlja.

Dakle, šta lažnjaci žele i kako štitite svoju adresu e -pošte od lažiranja u budućnosti? Zato smo ovde: da vam prenesemo neke jednostavne i praktične načine da ostanete bezbedni.

Šta lažnjaci žele?

Iako se prave namere mogu razlikovati od slučaja do slučaja, počinilac na kraju želi da napravi neku vrstu štete, kao što je:

- Ubeđujući vas da šaljete novac na mreži
- Ubeđuje vas da navedete svoje podatke za prijavu/lozinku
- Davanje osetljivih poslovnih i ličnih podataka
- U nekim slučajevima, međutim, namera je veoma lična. Dobro lažirane e-poruke mogu da dobiju pristup kompjuterskim podacima svog cilja, poslovnim kontaktima, čak i njihovim nalozima na društvenim mrežama

Na kraju krajeva, lažiranje e-pošte je po prirodi ometajuće i zlonamerno. A kada je loš glumac prevario svog primaoca, oni mogu da divljaju i usput prave razne štete.

Kako se boriti protiv lažiranja e-pošte?

- Koristite softver za zaštitu od malvera.
- Koristite filtere za neželjenu poštu e -pošte.
- Koristite obrnuto traženje IP adrese (reverse IP).
- Zaštitite svoju lozinku.

Zaštita podataka

U e-poslovanju i razmeni elektronskih dokumenata učestvuju brojni partneri i svi moraju da imaju odgovarajući nivo zaštite.

Pod zaštitom podataka podrazumeva se namera da podaci ostanu poznati samo pošiljaocu i primaocu (enkripcija podataka) i tako da jedino oni mogu da ih koriste. Mogućnost uvida trećih lica može da dovede do zloupotrebe određenih podataka, a to može da izazove negativne posledice po učesnike u razmeni. Podaci mogu da se podele na sledeće četiri grupe:

- Javni podaci - podaci u koje svi mogu da imaju uvid
- Autorizovani podaci - podaci u koje svi imaju uvid, ali su od neautorizovanog korišćenja zaštićeni autorskim pravom
- Poverljivi podaci - podaci koji su tajni (ciji sadržaj ne sme da bude čitljiv neovlašćenim licima)

Za zaštitu informacionih sistema od negativnih uticaja sa Interneta obično se koriste firewall i antivirusni softveri i slično.

Motiv svih sajber-kriminalnih radnji nisu vezani za novac, neki napadi su sračunati samo na to da unište ili onesposobe web stranicu. Gubici u takvim slučajevima ne čine samo sredstva koja su potrebna za obnavljanje svoje web strane već i gubitak reputacije, kao i prihoda koji bi se ostvario u periodu dok sajt nije radio.

Još jedan jako zastupljen vid prevare je phishing ili pecanje. Uobičajeni naziv za sajtove koji na prevaru dolaze do poverljivih podataka kao što su brojevi kreditnih kartica, korisnički podaci, šifre itd. Banke i druge kompanije koje čuvaju ovakve podatke, posebno su izložene phishingu.

Najčešći phishing scenario je da se napravi identična kopija sajta neke kompanije. Kopija se međutim nalazi na phishing serveru i svi podaci koje posetioci ostave čuvaju se na phishing serveru. Retko se dešava da se kopija nekog sajta nađe na serveru klijenta, što može biti još veći problem jer je zaista reč o validnom domenu, samo što je sad na nekom poddomenu ili u folderu tog sajta. Često je teško razlikovati lažni sajt od pravog, naročto kada se koriste web adrese slične pravom sajtu.

Nakon toga, obično se šalje mail u kome se od primaoca traži da sledi link naveden u mailu i da promeni ili ažurira svoje kontakt podatke. Ovakav mail bi trebalo korisnicima

da bude veoma sumnjiv, iako vrlo malo kompanija upozorava svoje korisnike da ne koriste svoje podatke na ovakav način.

Danas su sve češće u upotrebi takozvani IDN-domeni (domeni sa internacionalnim karakterima u nazivu) koji se koriste sa phishing. Registruju se nazivi domena koji imaju veoma slične karaktere onima u nazivu domena kojui nisu IDN. Ovako kreirane adrese se veoma teško razlikuju od originalnih, naročito na prvi pogled.

Kako da se zaštitite?

Nikad ne bi trebalo da sledite linkove u mailovima opisanim ranije u tekstu. Bezbednije je da potražite pošiljaoca peko pretraživača ili da u browser ukucate ispravnu adresu.

Banke i druge firme obično ne traže od svojih korisnika da menjaju svoje podatke na ovakav način. E-mail koji sadrži ovakav zahtev bi trebalo proveriti direktnim kontaktom sa bankom ili firmom koja stoji kao pošiljalac ovakvog maila.

Kada se u legitimnom mailu traži ovakva akcija od korisnika, onda takav mail obično sadrži i neke korisničke podatke za verifikaciju. To može biti ime naloga, prvih nekoliko cifara kreditne kartice i slično. Odsustvo ovakvih informacija u mailu treba da bude upozorenje da mail nije legitiman.

Uvek koristite najnovije verzije browsera, oni vrše proveru da li se sajt koji posećujete nalazi u bazi phishing sajtova. Takođe, browser će Vas upozoriti ukoliko sajt ima sumnjiv sadržaj.

Kako obezbediti dobar nivo sigurnosti u e-poslovanju?

Potpuna sigurnost ne postoji. Svaki sigurnosni sistem može da bude “provaljen”, ukoliko se u ostvarenje takve namere ulože dovoljna sredstva. Ali trajna sigurnost u

informatičkoj eri nije ni potrebna. Podaci obično imaju vrednost u određenom vremenskom periodu tako da se prema potrebi zaštite jedan dan, mesec ili godinu.

Nivo sigurnosti povezan je sa sagledavanjem dva odnosa:

- Odnos nivoa sigurnosti i lakoće upotrebe sajta je divergentan. Brojne mere sigurnosti koje se događaju e-trgovinskom sajtu čine da sajt postaje sporiji i teži za korišćenje. Tako prevelika sigurnost može da naškodi profitabilnosti dok nedovoljan nivo sigurnosti, s druge strane, može vlasnika da izbaci iz posla.
- Takođe postoji divergentan odnos između nastojanja pojedinaca da obezbede svoju sigurnost i sakriju svoj identitet i potrebe da se obezbedi odgovarajući nivo javne sigurnosti koju mogu da ugoze kriminalci i teroristi.

Sistemi zaštite

Najosetljivije tačke na kojima treba postaviti zaštitne mehanizme, sa tehnološkog gledišta, jesu sledeći nivoi zaštite:

- Zaštita na nivou telekomunikacione mreže
- Zaštita na aplikativnom nivou
- Zaštita na nivou poruke

Verovatno ste čuli izraz „kupac je uvek u pravu“. To je mantra za vlasnike tradicionalnih preduzeća da pokažu da idu dalje od puke dužnosti za svoju klijentelu. Međutim, novi načini poslovanja zahtevaju još jedan skup veština koje će vam pomoći da sprečite otvaranje vrata za prevarante, prevarante i kriminalce.

Preduzeća na mreži postaju pametna u vezi sa taktikama koje koriste sajber kriminalci. U ovoj evolutivnoj trci u naoružanju, kriminalci se neprestano pomeraju i okreću se ka još sofisticiranijim načinima phishinga, hakovanja i potpune krađe.

Upravljanje digitalnim izlogom ili drugim online poduhvatom bez razumevanja moderne prevare može biti kao hodanje kroz minsko polje bez zaštite. Morate imati jake alate i taktike za borbu protiv rizika. Ključno je sprečiti prevare i krađe, posebno kada se vaše preduzeće može smatrati finansijski odgovornim za nastale gubitke.

Kada shvatite vrste prevare i šta treba da uradite u slučaju da je vaš posao meta, moći ćete da reagujete na brz i profesionalan način kako biste sprečili lopove da napreduju sa svojim planom!

Metode za sprečavanje prevare u e-trgovini

Sa toliko metoda prevare za krađu, može izgledati nemoguće zaustaviti plimu krađe na mreži. Uz to, postoje solidne strategije za primenu koje mogu sprečiti većinu, ako ne i sve, online prevare.

Prvi korak, ako birate platformu treće strane na kojoj ćete hostovati svoje poslovanje, jeste da odaberete onu sa solidnom reputacijom za najbolje prakse u oblasti bezbednosti.

Popularni sajtovi trećih strana implementiraju bezbednosne protokole neophodne za verifikaciju klijenata i zaštitu baza podataka. Praktična lista za proveru koja će vam pomoći da odlučite koju platformu ili hosting kompaniju treba da izaberete treba da sadrži:

Implementacija CAPTCHA će zaustaviti skoro sve napade botova. CAPTCHA je skraćenica za „potpuno automatizovani javni Tjuringov test za razlikovanje računara i ljudi“ i jedan je od načina da se osigura da je vaš klijent ljudsko biće na drugom kraju te veze. Ova metoda zahteva od korisnika da u polje unese slova koja vidi na ekranu. Obično se ova slova i/ ili brojevi vizuelno mešaju i primoraju kupca da se fokusira i

proceni ono što vidi na ekranu. Ponekad je kontroverzna pošto CAPTCHA može biti teška sa stanovišta upotrebljivosti, ona i dalje ostaje kao dobar alat za sprečavanje automatizovanih prevara i curenja podataka.

Pomozite svojim klijentima da zaštite svoje račune sa dodatnim nivoom bezbednosti. Podstaknite složenije lozinke. Iako se čini brzo i lako kreirati nezaboravnu lozinku od nekoliko slova, koristite sistem koji prihvata samo duže znakove sa uključenim brojevima i velikim slovima.

Vrlo je uobičajeno da pojedinci ponovo koriste stare lozinke ili uzimaju uobičajene ideje iz rečnika, datuma rođenja, imena dece itd. Podstičite upotrebu generatora lozinki, kao što su Last Pass i Passwords Generator, kako biste pomogli u ovom procesu.

Provera adresa i vrednosti kreditne kartice su drugi standardi usklađenosti koji će držati prevarante na odstojanju. AVS (address verification system), sistem za verifikaciju adresa, upućuje na adresu za naplatu kupca sa podacima uskladištenim u samom sistemu kreditne kartice. I CCV i AVS koriste banke i mreže kartica, ali trgovac takođe može koristiti AVS na svom kraju kao dodatnu opciju verifikacije.

CCV (credit card value), vrednost kreditne kartice, je poznati trocifreni kod na poleđini svih kreditnih kartica. Možda ste takođe čuli za alternativna imena kao što su CVV, CVC ili CVV2. U skladu sa PCI, CCV podaci se nikada ne čuvaju sa brojevima kreditnih kartica u bazi podataka online prodavaca. Sa ovom sigurnošću na mestu, hakeri ne mogu da pribave ove informacije, a da ne ukradu karticu u stvarnom životu.

PCI (Payment Card Industry) usklađenost

Savet za standarde za bezbednost industrije platnih kartica, skraćeno PCI, je grupa glavnih globalnih brendova kreditnih kartica koji su razvili protokol za zaštitu podataka potrošača specifičan za industriju. Ono što se sada naziva PCI usaglašenost, osigurava

da prodavci poštuju PCI standarde širom sveta kada kupci plaćaju svojim kreditnim karticama.

Prednost PCI usaglašenosti striktno je da se prodavac na mreži može osloniti na svoj procesor plaćanja da obradi sve ove detalje. PayPal i drugi su ovu usklađenost ugradili direktno u svoje poslovanje kako bi skinuli pritisak sa prodavca.

Web lokacija Saveta za bezbednosne standarde PCI pruža sve detalje koji će vam pomoći da bolje razumete ovaj globalno korišćen protokol plaćanja.

Otkrivanje prevara

Kao vlasnik preduzeća, vaša je odgovornost da nadgledate sve transakcije kako do njih dođe. Možete ili da razvijete sopstvene sisteme za otkrivanje prevara od nule ili da koristite rešenja spremna za upotrebu koje nude renomirani provajderi. Ako nešto izgleda sumnjivo, pametno je da tu kupovinu odložite dok ne budete mogli pravilno da potvrdite poreklo plaćanja.

Pored toga, preporučuje se da se omogući dvofaktorska autentikacija (2FA) i SCA (Strong Customer Authentication ili 2FA za kartice) što pomaže da se izbegne preuzimanje naloga i sprečava neovlašćeno korišćenje informacija o kartici.

Ažuriranje operativnih sistema i svih poslovnih softvera neophodno je za sprečavanje hakera da iskoriste sve slabosti. Pokretanje antivirusnog softvera i instaliranje novih zakrpa će vam omogućiti nesmetan rad.

Kada je Magentov softver za e-trgovinu otkrio više nedostataka u njihovom sistemu do kojih je došlo nakon popravljanja i zakrpa prethodnih problema, vlasnici prodavnica su bili podložni napadima. Ako vlasnici prodavnica koji koriste Magento nisu ažurirali svoj softver, ostali bi ranjivi na napade preko skimera platnih kartica. Kompanija je javno

pozvala sve klijente da odmah redovno ažuriraju svoj softver kako bi izbegli ovakve probleme.

Svaki vlasnik prodavnice e-trgovine naići će na pokušaj prevare u nekom trenutku svog poslovanja. Vodite evidenciju o svim prethodnim pokušajima prevare. Praćenjem njih možete videti obrazac ako postoje ponovljeni pokušaji iz jednog izvora ili jasne metode napada.

Koristite ovo znanje da ih sprečite da probiju vašu odbranu. Uspostavite bezbednosne protokole i obučite svoje zaposlene o tome šta da traže, posebno tokom praznika. Određeno doba godine, kao što su Crni petak, Sajber ponedeljak, Božić, i kad god se obično vrše velike kupovine, dan su na terenu za onlajn kriminal. Ako vaša e -trgovina u ovom trenutku ima veliki obim, možda ćete lako propustiti nekoliko prevara.

Mudro je imati plan upravljanja kriznim situacijama u slučaju da vaše preduzeće postane plen šeme onlajn prevare. Posedovanje niza akcija koje treba da sledite u pogledu odnosa sa javnošću i izjava kupcima i dilerima omogućiće vam da brzo reagujete na frontu sa kojim se suočava javnost dok interno rešavate probleme.

U situaciji kontrole štete, od vitalnog je značaja da se suprotstavite situaciji koja smanjuje vrednost i poverenje vaše kompanije. Zaustavite tok značajnih gubitaka i žalbi kupaca tako što ćete biti spremni i razumeti uslove u kojima se prevara dogodila.

Trendovi u novim načinima kupovine će na kraju dovesti do obrazaca koji se pojavljuju u lažnom ponašanju. Plaćanje kreditnim karticama i dalje je glavni izvor kupovine na mreži, međutim, sa porastom PayPal -a, poslednjih godina pojavili su se novi konkurenti. Od vitalnog je značaja da preduzeće e-trgovine analizira informacije koje dolaze prilikom uvođenja nove opcije plaćanja. Kriminalci će uvek testirati novu metodu za ranjivosti i rupe u sistemu.

Zaključak

Zaštita vašeg preduzeća i kupaca od mrežnih prevara stalni je posao koji bi trebao biti na vrhu liste prioriteta svakog trgovca. Sajber kriminal neće nestati. Postaće sofisticiraniji i pametniji, tako da je na prodavcu da nastavi da prilagođava strategije u toku.

Od poštovanja bezbednosnih protokola do angažovanja spoljnih agencija za nadgledanje i savetovanje, zaštita vaših poduhvata od prevare ne mora da bude ogromna. Zdrav razum i razumevanje alata koje treba koristiti će zaštititi vaše poslovanje od većine napada.

Da su korisnici praktikovali često ažuriranje svog softvera, ne bi postali osetljivi na ovu vrstu napada.