UDC: 004.738.5:336.719.2 INFO M: str. 15-19

TIPOVI I VRSTE KRAĐA U SISTEMIMA PLAĆANJA PLATNIM KARTICAMA – KRATAK OSVRT NA REALNO STANJE
TYPES AND FRAUD CLASIFICATION IN THE PAYMENT SYSTEMS BASED ON THE PAYMENT CARDS – SHORT OVERVIEW OF THE CURRENT STATE

Marko Ranković

REZIME: U radu je dat pregled najznačajnijih slabosti sistema plaćanja platnim karticama, kao i najčešćih oblika krađa u ovim sistemima. Slabosti sistema mogu iskoristiti faktori koji na organizaciju deluju spolja, ali i oni koji su unutar same organizacije, zato se sigurnosti informacija u organizacijama koje se bave pružanjem ovakve vrste servisa krajnjim korisnicima mora posvetiti posebna pažnja.
Krađe u sistemima plaćanja platnim karticama su veoma opasne, jer pored krađe novca, identiteta ili proizvoda dolaza i do kompromitacije najvažnijeg resursa savremenog sveta – informacije. Krađa informacije omogućuju zlonamernim učesnicima u procesima plaćanja obezbeđuje mogućnost daljeg pristupa sistemu i zbog toga se sve komponente sistema moraju jasno odrediti, definisati ulazne i izlazne informacije, i odrediti odgovarajući mehanizmi zaštite.
KLJUČNE REČI: Slabosti sistema, krađa, identitet, novac, proizvod.
ABSTRACT: This paper describes most important weaknesses of the payment systems based on the payment card, as well as the most often frauds. The System weaknesses can be used by the elements which can influence the organization from the outside world and insider factors. Therefore, special attention must be paid to the information security for this kind of organizations.
Fraud in the payment systems based on the payment cards is very dangerous, because beside the stolen money, identity or product, the most important resource of the modern financial world is compromised – information. Stolen information are enabling to malicious participants in the payment processes to access deeper into the system, and therefore all system components must be clearly defined, to determine input and output from information and to determine appropriate protection mechanisms.
KEY WORDS: The system weaknesses, fraud, identity, money, product.

1. SLABOSTI SISTEMA PLAĆANJA PLATNIM KARTICAMA

Upotreba platnih kartica danas je široko rasprostanjena. Platne kartice se mogu koristiti za:

1. *plaćanje roba i usluga* - korisnik može da koristi karticu za bezgotovinska plaćanja robe i usluga u zemlji i inostranstvu;
2. *podizanje gotovine* - korisnik može da podiže gotovinu na bankomatima i šalterima ovlašćenih banaka u zemlji ili inostranstvu;
3. *plaćanje elektronskim putem* - omogućuje korisniku da vrši plaćanje elektronskim putem (Internet, kataloška ili telefonska prodaja) i korisnik snosi rizik od zloupotrebe koji postoji pri prenošenju broja kartice i ličnih podataka kroz javnu mrežu.

Platne kartice su i u našoj zemlji sve više u upotrebi. Svaka od aktivnosti koja se može obaviti platnom karticom je podložna mogućnosti zloupotrebe i sobom nosi određeni rizik.

Najvažnije slabosti sistema plaćanja platnim karticama su:

– slabost sistema zbog ukradenih informacija
– slabost sistema zbog napada van mreže
– slabost sistema zbog napada unutar mreže-insajder

1.1. *Slabost sistema zbog ukradenih informacija*

Informacija korisnika platnih kartica je široko dostupna na Internetu. Ova informacija može da bude ukradena direktno iz neobezbeđenih baza podataka koje su upravljane od strane kompanija ili provajdera platnih infrastruktura. Najveće objavljeno kompromitovanje informacija o kreditnim karticama do danas bilo je kada je jedan procesor plaćanja otkrio skoro 8 miliona brojeva kreditnih kartica međunarodnoj hakerskoj organizaciji. Platne informacije se takođe razmenjuju na crnim hakerskim tržištima, gde se nude brojevi kreditnih kartica, bankovni računi, brojevi socijalnog osiguranja, itd., na aukcijama za najvišu ponudu. Federalna Trgovinska Komisija (FTC) izveštava da su identiteti oko 27 miliona Amerikanaca bili kompromitovani u poslednjih 5 godina. Najveća promena sistema sigurnosti je da platne informacije klijenata više ne mogu biti čuvane na nivou pojedinca, već kompanije moraju sprovoditi validaciju informacija i pratiti njihovu upotrebu sa ciljem da se zaštite od aktivnosti prevara.

Jedna od najvećih slabosti sistema koji omogućuju zlonamernim pojedincima ili organizacijama jeste reaktivno delovanje sistema, umesto proaktivnog pristupa.

Mnoge kompanije posvećuju glavne napore u sigurnosti na reaktivnom praćenju transakcija koje dolaze na softversku platformu za procesiranje transakcija. Cilj je da se izvrši validacija da li je korisnikova kupovina legitimna ili ne. Ovo sigurno predstavlja najvažniji deo proces sigurnosti, ali on sam po sebi nije dovoljan. Postoje dve glavne slabosti kada ovo predstavlja jedini deo sistema sigurnosti.

Prvo, reaktivni fokus na validaciju korisnikovog zahteva ne prepoznaje proaktivno brute force napade u realnom vremenu. Hakera koji želi da izvrši validaciju platne informacije kroz kartični proces nije briga da li je zahtev ispunjen. Zločin

je često automatizovan i završava se za nekoliko sati ili minuta. Za vreme za koje tim za upravljanje rizikom uoči pokušaj prevare, kompanija je već izložena troškovima autorizacije transakcije. Pored ovoga, kompanija ima i značajne troškove korisničkog servisa da kontaktira legitimnog korisnika kartice i da ih obavesti o narušavanju sistema sigurnosti.

Drugo, front-end pristup praćenja transakcija ne obuhvata slabosti koje se javljaju u back-end delu transakcionog ciklusa, koji je posebno podložan metodu krađe keša. Sistemske slabosti, kao što je interni ili eksterni pristup, mogu omogućiti da se, koristeći privilegije, zaobiđu mnoge sigurnosne procedure unutar samo kompanije. Sposobnost da se prate finansijski događaji kroz čitav sistem sve do sravnjivanja u banci je jedini način da se obezbedi kompletna sigurnosna pokrivenost.

Kod nas se sve više pažnje posvećuje oblasti zaštite osetljivih informacija i stvaranju, pre svega, odgovarajućih organizacionih postavki, ali i aplikativnim rešenjima za zaštitu informacija. Jedna od mera koja se kod nas sprovodi na zaštiti informacija jeste uvođenje standarda ISO 17799.

ISO 17799 je međunarodno priznati standard za menadžment sigurnosti informacija (Information Security Management Standard), prvi put objavljen od strane Međunarodne organizacije za standardizaciju (ISO), u decembru 2000 godine. ISO 17799 je standard visokog nivoa, širokog je domena i opšti je po svojoj prirodi. Ovakav pristup dozvoljava da on bude primenjen u različitim tipovima kompanija, kao i u velikom broju aplikacija. Ovaj standard predstavlja kontroverzu za one koji misle da standardi moraju da budu veoma precizni. Uprkos ovoj kontroverzi standard ISO 17799 je jedini standard koji je posvećen oblasti menadžmenta sigurnosti informacija.

ISO 17799 definiše informaciju kao važan faktor koji postoji u različitim oblicima i ima vrednost za organizaciju. Cilj sigurnosti informacija je da se ona, kao važan faktor za organizaciju, zaštiti na odgovarajući način, kako bi se obezbedio kontinuitet poslovanja, minimizirali gubici u poslovanju i maksimizirao prihod od investicija. Kako je definisano u standardu ISO 17799 sigurnost informacija se karakteriše kao čuvanje:

– poverljivosti – obezbeđuje se da informacija bude dostupna samo onima koji su autorizovani da imaju pristup,
– integriteta – obezbeđivanje tačnosti i kompletnosti informacija i
– dostupnosti – osigurava se da autorizovani korisnici imaju pristup informacijama kada to zahtevaju.

1.2. *Slabost sistema zbog napada van mreže*

Sve rasprostranjenija kompjuterizacija i umrežavanje poslovnih procesa učinili su platne sisteme osetljivijim na specifičnu formu hakovanja poznatu kao Brute Force napad. Koristeći ovaj metod hakeri mogu preko mreže, na kojoj je računar, da prodru u sigurnosni sistem i da direktno pristupe osetljivim informacijama ili, čak, i da izvrše finansijsku transakciju.

Softverski paketi koji se mogu naći u hakerskim chat sobama automatizuju proces provaljivanja lozinke i mogu identifikovati gde greške u mrežnoj konfiguraciji mogu obezbediti ulazak na „zadnja vrata“ u poslovni sistem.

Druga prevara je poznata kao „carding“. Ova prevara se obavlja slanjem ogromnog broja pokušaja kupovine, kako bi se slučajno pogodio neki validan broj kreditne kartice. Ako odgovarajući sistem sigurnosti ne funkcioniše kako treba, jednom će doći do pogotka validnog broja kreditne kartice i sistem će biti uvučen u validaciju stvarnih informacija o korisniku. Brute force ranjivost zahteva od kompanija da postave efikasna real-time rešenja monitoringa kako bi ovi automatizovani napadi bili brzo identifikovani i blokirani pre nego što naprave štetu.

Neki od najpoznatijih napada van mreže su i:

– skimming, kao način upada u sistem korišćenjem ukradenih informacija sa platne kartice
– phishing, kao način upada u sistem putem „pecanja“ korisnika na Internetu, korišćenjem lažnih obaveštenja
– pharming, kao način upada u sistem putem „presretanja“ korisnika na Internetu i preusmeravanjem na pogrešan.

Sve dosadašnje faze praćenja i proučavanja tokova zloupotreba u svetu savremenog bankarstva ukazivale su na potrebu nastajanja integralnih i sistematskih rešenja. Usložnjavanje uslova poslovanja nosi sa sobom ne samo pozitivne, već i izvesne neželjene efekte i rizike kojih su svi učesnici tržišta svesni.

Savremena rešenje, koja se sve više koriste, su najčešće WEB aplikacije namenjene praćenju zloupotreba u bankarskim sistemima. Takva rešenja pružaju visok nivo detekcije i odgovara zahtevima svih međunarodnih finansijskih institucija, uključujući Visa-u i MasterCard.

Ovakve vrste aplikacija su u osnovi podeljene na dva dela: strana izdavaoca platne kartice i strana primaoca platne kartice. Osnovni način funkcionisanja je iskakanje upozorenja tj. uzbune (alert-a) koji ukazuje na moguće sumnjivo ponašanje određene transakcije, koje može kao takvo prouzrokovati niz neželjenih posledica na računu te kartice.

Savremena rešenja omogućavaju potpunu card fraud detekciju u Real - time, Near - time ili Batch načinu slanja i obradi transakcija.

– Real-time sa sobom nosi mogućnost odbijanja sumnjivih transakcija. Neophodnost rada u real time režimu je postojanje čvrste veze između fraud scoring sistema i autorizacionog sistema banke kako bi u trenutku transakcije bio izmeren nivo fraud-a, na osnovu pondera određenog u scoring sistemum i na osnovu ove informacije bila odobrena ili odbijena transakcija.
– Near-time rešenjem se sama zloupotreba ne može sprečiti direktno. Međutim, ovako se fraud može uočiti mnogo brže nego pre, samo par trenutaka pošto je transakcija učinjena i, ukoliko je ta transakcija fraud, blokadom zloupotrebljene kartice od strane banke može se sprečiti dalja šteta.
– U Batch režimu sumnjive transakcije dospevaju sa danom zakašnjenja.

Sve kompanije imaju pristup ogromnoj količini internih informacija koje im omogućuju da sprovode real-time sigurnosno praćenje. Međutim, ovo obično nije dovoljan nivo ili obim informacija koji može da pruži pravu sliku o platnim

prevarama. Pravo, pouzdano praćenje sigurnosnih informacija se jedino može obaviti preko tri horizonta:

1. u okviru kompanijske mreže,
2. preko udruženih mreža više kompanija i
3. preko Interneta.

Praktično, sama kompanija nema resurse da prati sigurnost informacija izvan sopstvenog platnog sistema. Da bi ovo moglo da se ostvari i da bi mogao da se pokrije taj deo transakcionog životnog ciklusa, potrebno je naći pouzdanog partnera za oblast sigurnosti.

1.3. *Slabost sistema zbog napada unutar mreže-insajder*

Dok napadi na mrežu u kojoj se računar nalazi predstavljaju klasičan pokušaj hakera da prodru spolja, pretnja od insajdera je mnogo direktnija. Isti postupak koji kompaniju vodi u povećanje poslovne efikasnosti, integracijom i povezivanjem njenih poslovnih aktivnosti, on vodi i ka tome da osetljive informacije o klijentu postaju široko dostupne zaposlenima. Mnoga odeljenja korisničkih servisa mogu pristupiti podacima preko CRM (Customer Realtionship Management) platformi. Insajder koji ima pristup ili zaposleni koji zloupotrebljava privilegije pristupa može lako doći do velikog broja osetljivih informacija.

U nedavnoj studiji Harris Interactive-a skoro 50% zaposlenih, koji imaju pristup podacima o korisnicima, kaže da bi moglo da uzme te podatke, a da ne bude primećeno. Napad insajdera je veoma opasan i zato što velika većina kompanija dizajnira svoje sisteme zaštite tako da štite od napada spolja. Bez odgovarajuće interne kontrole insajder sa pristupom može lako da dođe do informacija o korisnicima, kao i da zloupotrebi finansijsku transakciju na njenom toku kroz kompaniju. Ovo predstavlja jedan razlog više zašto mora da postoji jasna zakonska regulativa o visokotehnološkom kriminalu i o poverljivosti informacija.

Nedostatak koji se javlja pri samoj arhitekturi sistema jeste nedovoljna transparentnost životnog ciklusa transakcije. Kontrola životnog ciklusa i jasan uvid u tok transakcije od početne do krajnje tačke može omogućiti lako uočavanje prevare od strane insajdera. Transparentnost i informacije obezbeđuju glavnu vrednost kompaniji koja joj omogućuje da osigura svoju platnu mrežu od napada i pokušaja prevare – potpuna kontrola nad svakom fazom transakcionog životnog ciklusa.

Glavne koristi od platne sigurnosne platforme koja obezbeđuje informacije i kontrolu su višestruke. Kompanije sa većim uvidom u rizik koji nosi transakcija su slobodnije da prošire svoje prodajne kanale i na taj način da poveća svoje tržišno učešće i ukupan prihod. Sa odgovarajućom kontrolom na odgovarajućem mestu kompanija ne samo da smanjuje izloženost riziku i potencijalne ekonomske gubitke, već povećava ukupnu efikasnost u svome radu. Efikasna alokacija resursa redukuje troškove zaštite i obezbeđuje trenutno najbolje rešenje.

Praćenje i analiza mogućnosti napada od strane osobe kja u kompaniji radi posebno je značajna, jer je u poslednjih nekoliko godina ovaj vid krađa zauzimao značajno mesto.

2. KRAĐE U SISTEMIMA PLAĆANJA PLATNIM KARTICAMA

Postoje mnoge slabosti platnih mreža i platnih sistema, uopšte. Kriminalci ovo mogu da iskoriste i ostvare veliku finansijsku korist. Zato je neophodno da kompanije razviju sveobuhvatne i efikasne sisteme da poboljšaju end-to-end sigurnost. Hakeri napadaju nekonzistentnosti u sigurnosti platnih sistema do kojih dolazi kada kompanije ne usvoje holistički pristup. Holistički pristup zahteva da čitav transakcioni životni ciklus bude proziran (od prikupljanja sredstava do sravljivanja), pristup najširem spektru informacija, koje treba proslediti za analizu rizika, kao i potpuna kontrola nad tokom sredstava kroz svaku fazu transakcionog ciklusa.

Značaj analize krađa koje se obave platnim karticama je veći ukoliko se ima u vidu finansijski efekat tih krađa. Pregled statističkih podataka o rastu krađa u SAD, u poslednjih 5 godina, prikazan je u tabeli ispod.

Tabela 1. – *Statistike zloupotreba kreditnih kartica u SAD, 2003- 2007*

Godina	Ukupna šteta naneta zloupotrebom (USD milijardi)	Stopa rasta Online zloupotreba	Iznos Online zloupotreba (USD milijardi)
2003	2,3732	2,5%	1,22788
2004	2,6649	2,4%	1,45692
2005	2,7454	2,2%	1,61139
2006	3,0288	2,0%	1,72900
2007	3,2127	2,0%	1,98835

Sa rastom kompanije (banke ili procesora) više transakcija dolazi na njenu softversku platformu za procesiranje i kompanija postaje sve ranjivija. Hakeri uočavaju ovu činjenicu i imaju dizajnirane sisteme prevara da to zloupotrebe. Sistemi platnih prevara evoluiraju neverovatnom brzinom sa razvojem novih tehnoloških inovacija i grubo mogu biti svrstani u tri glavne kategorije:

1. Krađa identiteta
2. Krađa proizvoda i
3. Krađa keša

3.1. *Krađa identiteta*

WEB servisi omogućuju da se poslovne transakcije obavljaju 24x7, bilo gde u svetu. Ova pogodnost omogućuje kompanijama da povećaju prodaju i da pospeše rast. Ovo, takođe, zahteva da kompanija prikaže resurse (softver, hardver) o procesingu transakcija globalnoj publici. Potencijalni klijenti moraju da budu upoznati sa resursima kojima procesor raspolaže. Krađa identiteta predstavlja glavni cilj brute force napada na podatke o transakcijama. Takvi napadi uključuju pokušaje provaljivanja lozinke, kako bi se stiglo do jezgra kompanijskog platnog sistema (kompanijska krađa identiteta) ili kartične napade, kako bi se izvršila uspešna validacija podataka sa kreditne kartice (korisnička krađa identiteta). Značajan broj kompanija nema planove za odbranu od sistematskih napada na njihove platforme. Prevara sa platnim karticama može da napravi značajnu štetu za samo nekoliko sati. One kompanije koje predstavljaju

priznatu marku na tržištu i koje imaju visok nivo transakcija koje se procesiraju pre će postati mete ovakvih napada nego neke manje kompanije sa malim obimom poslovanja. Sistemi velikih kompanija su dizajnirani da upravljaju velikim obimom transakcija. Međutim, svaki pokušaj da se ograniči pristup ima direktan uticaj na obim prodaje koji kompanija može da ostvari. Ova vrsta napada se efikasno može sprečiti inteligentnim praćenjem obima transakcija- monitoringom u realnom vremenu količine transakcija na mreži. Inteligentno praćenje obima ne samo da proverava kvantitet procesiranja, već analizira izbor i sadržaj transakcija. Ovaj metod omogućuje maksimalnu fleksibilnost da se odgovori na napad, obezbeđujući, pri tom, da se legitimna prodaja normalno odvija. Obzirom da su ovi napadi usmereni direktno na platnu mrežu, od suštinske je važnosti da se ovaj inteligentni sistem praćenja i obaveštavanja što pre integriše u softversku platformu.

Transakcioni podaci zastupljeni koji se moraju posebno pratiti kako bi se na vreme uočila krađa identiteta i sva odstupanja od uobičajene rutina korisnika platne kartice su sledeći:

– podaci o karticama (card),
– trgovcima (merchant) i
– uređajima za prihvat transakcije (ATM, POS, Internet sajt).

Aplikacija koje se bave obradom ovih podataka koriste veliki broj ugrađenih funkcija za izračunavanje složenih proračuna i vođenje statistika za određeni period. Neki od ulaznih parametri su u većini slučajeva i izlazni parametri. Karakteristična računanja (npr. proseka, ukupnih i pojedinačnih iznosa kao i ukupnog broja transakcija) vrše se uglavnom po kartici (PAN), identifikacionom broju određene banke (BIN), trgovcu (Merchant), MCC-u (Merchant Category Code), zemlji trgovca (Merchant Country) i po drugim parametrima, podjednako važnim za detektovanje zloupotreba. Na ovaj način, dodatnom kontrolom trgovaca štiti se i strana prihvatioca transakcije.

3.2. *Krađa proizvoda*

Ovaj vid krađe je najšire rasprostranjen vid platnih krađa. Hakeri koriste ukradene informacije da sprovedu lažnu kupovinu pod okriljem legitimnog identiteta korisnika. Kada je platna kartica zloupotrebljena za kupovinu bankarska industrija kompaniju smatra odgovornom za tu transakciju i za istu će izdati chargeback kojim se od kompanije zahteva da vrati sredstva. Obzirom da se prosečni chargeback izdaje oko mesec dana posle kupovine, hakeri imaju dosta vremena da počine zločin pre nego što je otkriven.

Kompanije se od ove vrste krađe brane reaktivno. One prave listu krađa koje su se već desile i blokiraju poslove sa identitetima korisnika koji su na tim listama. Iako je ovo veoma važan korak u obezbeđivanju platnih mreža, on, nažalost, ne štiti posao od trenutne štete, već jednostavno obezbeđuje da se, sa tim korisnikom, prevara ne dogodi ponovo. Kompanije treba da primenjuju proaktivni pristup i koriste bazu prošlih krađa kao model za predviđanje budućih pokušaja prevare. Ovaj način može da smanji aktivnosti krađa, međutim, on takođe može netačno neku aktivnost kategorizovati kao krađu i, na taj način, automatski smanji prodaju. Gartner procenjuje da se odbaci, skoro, do 3% ispravnih transakcija u procesu procene rizika. Za kompaniju sa 100 miliona dolara prodaje ovo predstavlja gubitak od 3 miliona dolara. Da bi indikatori rizika bili što tačniji potrebno je značajno posmatranje aktivnosti transakcija. Bez ovih podataka kompanija će pre da ograniči rast nego da ga podrži.

Zloupotreba kartica (fraud) predstavlja rastući globalni problem u sektoru bankarskih usluga. Mnoge banke pokušavaju da se suprotstave ovom problemu kako bi smanjile realnu štetu i gubitak reputacije, ili preduzimaju odgovarajuće aktivnosti kako bi se prilagodile zahtevima međunarodnih finansijskih organizacija. Nažalost, fraud je opšte prisutan problem koji se prilagođava novim tehnologijama.

Kako su uslovi savremenog poslovanja danas nepredvidivi, neophodno je reagovati na vreme na svaku vrstu zloupotreba. Zloupotreba platnih kartica poprima dimenzije globalne industrije koja nema granica. Po predviđanjima Visa-e International falsifikovanje i skimovanje kartica (counterfeit, skimming) će iznositi 65% godišnje. Visa procenjuje da šteta naneta na ovaj način strani izdavalaca platnih kartica iznosi 513 miliona EUR-a godišnje, dok na strani primalaca iznosi 471 miliona EUR-a godišnje. Procenjuje se da će u Britaniji industrijski gubici porasti na 11 U.S dolara po kartici do kraja 2008.godine. Ipak, značajno je napomenuti da u ovoj zemlji zloupoteba pokazuje postepeno opadanje. Talas zloupotreba pokazuje tendenciju sve većeg pomeranja iz oblasti zapadne ka zemljama centralne i istočne Evrope.

Direktni troškovi zloupotrebe su samo deo ukupnog problema nastalog na ovaj način. Troškovi procesiranja chargeback-ova, vreme i napor uloženi u istraživanje i praćenje transakcija kao i šteta naneta reputaciji veći su od bilo kakvih direktnih troškova.

Kako bi se zloupotreba stavila pod kontrolu potrebna je rana detekcija, održavanje zahtevanog nivoa tačnosti, snabdevanje pravovremenim i pouzdanim informacijama kao i sistem praćenja zloupotreba adaptibilan na promene neminovne u uslovima savremenog poslovanja.

Da bi se smanjila količina krađa i prevara u Srbiji pri privrednoj komori Srbije, odnosno njenom Odboru za bankarstvo i osiguranje 2004. godine formiran je Forum za prevenciju zloupotreba platnih kartica, koji okuplja skoro sve banke i autorizacione centre u Srbiji sa zajedničkim ciljem da se efektivno i efikasno smanjuju nivo zloupotreba platnih kartica. U radu foruma učestvuju i predstavnici Ministarstva unutrašnjih poslova Srbije i Specijalno odeljenje za visokotehnološki kriminal pri Tužilaštvu Republike Srbije. Nivo zloupotreba platnih kartica kod nas se institucionalno prati, ali još uvek nedovoljno precizno.

Ovaj projekat je nastao kao rezultat faktora navedenih ispod:

- Projekat je nastao kao izraz potrebe pravovremene pripreme za period ubrzanog razvoja kartičarstva koji će doneti i probleme zloupotreba i prevara.
- Tržišta u razvoju kao i izdavaoci kartica u fazi širenja posla sa karticama predstavljaju “laku metu” za lica i grupe koje su iskustvo u zloupotrebama sticali na razvijenim tržištima, koja već imaju razvijene metode prevencije.
- Izraz potrebe da se, umesto priče o saradnji, učini korak dalje i ponudi forma za institucionalizaciju saradnje.

3.3. *Krađa novca*

Svako sa privilegovanim pravom pristupa softveru za procesiranje transakcija ima ključeve za pristup bankovnom računu kompanije. Iz ove pozicije moći, pojedinac može kontrolisati tok sredstava kroz i izvan kompanije. Krađa keša predstavlja daleko najteži oblik krađa koji ima najveće posledice po posao danas. Ovaj metod krađe je najčešće sproveden od strane grupacija organizovanog kriminala. Haker koji uspe da obezbedi pristup softveru za procesiranje transakcija kompanije može da obavlja transakcije u ime kompanije. Najčešći princip krađe je da se provali u sistem gde je obim transakcija veliki, zatim da se sredstva preusmere na račun hakera. Ta sredstva se brzo premeštaju na neke račune prekookeanskih banaka ili se prebacuju sa računa na račun dok im se trag ne izgubi i veoma ih je teško povratiti.

Metod krađe keša pogađa poslednji deo transakcionog ciklusa mnoge kompanije i ne planiraju sigurnosne procedure da ih blokiraju. Krađa keša je, takođe, metod koji je često korišćen od strane insajdera, koji, zbog svoje pozicije u kompaniji, mogu ne samo da izvrše transakciju, već i da obrišu tragove praćenja u sistemu. Upravo kontrola tog poslednjeg dela transakcionog cilkusa predstavlja ključ sprečavanja ovog izuzetno opasnog metoda krađe.

Izloženost podataka, koja najčešće dovodi do krađe novca u poslednjem delu transakcionog ciklusa, pokušava se sprečiti uvođenjem određenih standarda zaštite podataka. Najvažniji standarad koji se bavi, između ostalog, i ovom problematikom je PCI DS standard (Payment Card Industry Data Security). PCI standard obuhvata sve delove transakcionog ciklusa i na taj način smanjuje mogućnost direktne krađe novca od strane napadača spolja ili insajdera. PCI standard pored obaveznih elemenata zaštite sa aplikativnog nivoa, propisuje i nivoe pristupa pojedincima u kompaniji u zavisnosti od njihove pozicije. Primena ovog standarda i usklađenost je obavezna za sve učesnike sistema plaćanja platnim karticama. Na ovaj način su obuhvaćene čak i one aktivnosti koje sprovode kompanije koje predstavljaju „podizvođače“ banke, kao nosioca finansijskih servisa prema krajnjim korisnicima, ali i prema kartičnim organizacijama. Rigorozne mere koje ovaj standard propisuje pomoći će da se najosetljiviji delovi životnog ciklusa transakcije osiguraju od mogućnosti zloupotrebe informacija.

4. ZAKLJUČAK

Poslednjih godina ubrzani razvoj tehnologije doveo je do sve šire i značajnije upotrebe plastičnih kartica, kreditnih, debitnih, charge kartica, pre-paid kartica, itd. i elektronskih bankarskih sistema. Značajnim uplivom elektronski baziranih sistema u sisteme banaka i u same sisteme plaćanja dovodi do logične, sve šire, upotrebe plastičnih kartica.

Smanjivanje rizika od potencijalnih pokušaja prevare jedino se može postići zajedničkim naporima svih učesnika u sistemu plaćanja platnom karticom, a to su:

– finansijska institucija,
– korisnik,
– ATM/POS proizvođač- service provajder.

Finansijska institucija treba da istakne da je izuzetno važna saradnja korisnika. On mora da obrati pažnju kada koristi uređaj i da prijavi svaku sumnjivu radnju ili moguću neregularnost. Mnogi klijenti koriste isti ATM dnevno ili nedeljno u svojim „bankarskim“ rutinama. Uobičajeno je da ako se isti ATM koristi često, bolje se zapažaju njegove karakteristike i okruženje. Pažljiv korisnik ATM ili POS uređaja treba odmah da prijavi svaku neregularnost koju primeti, bilo da se radi o napravi koja je prikačena na ATM ili o sumnjivom okruženju, na broj koji se nalazi na ATM uređaju ili na kartici ili da se obrati policiji.

Finansijska institucija treba da obezbedi da njihovi zaposleni (ATM ili POS servis provajder, kao i oni koji su vezani za novac (CIT (Cash In Transit) kompanija)) mogu da prepoznaju najnovije tehnike prevara. Tehničari zaduženi za servis moraju biti veoma dobro obučeni da mogu da obave evaluaciju svake komponente uređaja, kako bi se uverili da niko nije vršio promene koje će uticati na funkcionalnost ATM-a, bilo da se radi o promenama u softveru ili hardveru (postavljanje dodatnih uređaja, npr. kamera, dodatnih čitača kartica, uređaja za unos PINa, itd.).

Klijentima treba preporučiti da bar jednom mesečno kontrolišu svoj račun, bilo preko papirnog izvoda ili putem Interneta, kako bi se uverili da nije bilo neovlašćenog korišćenja njihovog računa.

Sa ubrzanim razvojem sistema elektronskih plaćanja ubrzano se razvijaju i nove mogućnosti za krađe i prevare, pa zato sistemi za On-line Fraud Monitoring sve više dobijaju na značaju. Ovi sistemi su izuzetno važni u oblasti preventivnog delovanja, kao i otkrivanja novih slučajeva krađa i prevara, kroz praćenje određenih pravila i paterna koji se definišu kroz aplikativni softver sistema za Fraud Monitoring.

Identifikacija i sistematizacija najznačajnijih slabosti sistema, kao i najčešćih oblika krađa u sistemima plaćanja platnim karticama će pomoći da se neke od slabosti i potencijalni rizici uoče i da se na njih preventivno deluje, kako implementacijom odgovarajućih softverskih aplikacija, tako i uspostavljanjem odgovarajućih organizaionih preduslova.

LITERATURA

[1] VeriSign® Fraud Protection Services, Securing the Enterprise Payments Network, VeriSign, 2004
[2] Diebold – ATM Fraud and Security – White Paper, September 2002, http://buy.cuna.org/download/diebold_fraudpaper.pdf
[3] Vasković V., Sistemi plaćanja u elektronskom poslovanju, FON, Beograd, 2007.
[4] Ranković, M.: Modeli i tehnike zaštite sistema plaćanja platnim karticama, magistarska teza, FON, Beograd, 2008

Mr Marko Ranković, Project Manager, EuroPlanet, Beograd
mrankovic@eeft.com
Oblasti interesovanja: upravljanje projektima u oblasti finansijskih servisa i usluga, procesiranje elektronskih finansijskih transakcija, modeli i tehnike zaštite sistema plaćanja platnim karticama.