UDC: 004.738.5:336.7 INFO M: str. 9-14

UPRAVLJANJE RIZIKOM U E-BANKARSTVU
E-BANKING RISK MANAGEMENT

Marko Ranković, Vladimir Simović, Vojkan Vasković

REZIME: U e-bankarstvu postoje brojni rizici. Svi oni predstavljaju opasnost po finansijsku instituciju i nikako se ne smeju zanemarivati, već se svakom od njih treba posvetiti pažnja. Rad identifikuje najvažnije rizike, kako u mikro-okruzenju, tako i u širem okruženju organizacije. U radu su prikazane i mere upravljanja rizikom koje je potrebno preduzeti kako bi se rizik umanjio, na operativnom i strateškom nivou. U radu je posebna pažnja posvećena aktivnostima menadžmenta usmerenim na smanjivanje rizika, kao i značaju standarda ISO 17799. Primena ovog standarda, promenama odgovarajućih procedura i same organizacije, stvara infrastrukturne pretpostavke za sigurno poslovno okruženje. Samim tim, primena standarda predstavlja važno sredstvo za zaštitu informacija i smanjenje rizika u e-bankarstvu.

KLJUČNE REČI: Rizik, e-bankarstvo, standard, ISO 17799

ABSTRACT: There are many risks in the E-Banking. All of them are can jeopardize the financial institution and therefore they can't be disregarded. Each of these risks, in organization's micro-environment, as well as in macro-environment, deserves special attention. This paper identifies the most important risks, on operational and strategic level, as well as identifying the risk management processes and steps which needs to be undertaken in order to mitigate the risk. In the paper the special attention is focused to the activities of the management structures directed to the risk mitigation and to the importance of the standard ISO 17799. Implementation of the requirements given by this standard, through changes of the procedures and the organizational structure, the infrastructure prerequisites will be met to create secure business environment. Therefore, compliance with ISO 17799 is ensuring that information is better protected and therefore the E-Banking risks are mitigated.

KEY WORDS: Risk, e-banking, standard, ISO 17799

UVOD

Postoji više standarda čija primena smanjuje rizik u e-bankarstvu, Najvažniji standardi su: PCI DSS, Basel II standardi i preporuke, ISO 17799. Primena svakog od ovih standarda se odnosi na neki od segmenata poslovanja i stvara pretpostavke za poslovanje sa niskim rizikom u oblasti sigurnosti informacija.

Osnovna namena ovih standarda je da zaštite korisnike od neautorizovanog pristupa podacima. Kako se zloupotrebe u sistemima platnih kartica povećavaju, tako i primena standarda postaje obavezna za sve učesnike u sistemu e-bankarstva. Primena standarda doprinosi ostvarenju visokog nivoa zaštite podataka korisnika kartica.

Čak i ako neke finansijske ustanove ne smatraju aktivnosti e-bankarstva kritičnim kroz obezbeđivanje dostupnosti alternativnih kanala distribucije svojih proizvoda, one moraju pažljivo da razmotre očekivanja korisnika tih servisa i moguće udare na stabilnost sistema, i kako će eventualna nedostupnost tih servisa uticati na (ne)zadovoljstvo i lojalnost korisnika. Kontrola sigurnosti informacija postaje još značajnija zahtevajući, pri tom, dodatne procese, alate, ekspertize i testiranja. Institucije treba da procene koji stepen sigurnosti je potreban u zavisnosti od procene osetljivosti informacija za korisnika i za instituciju i koji je to prag tolerancije rizika.

RIZICI U E-BANKARSTVU

Transakcioni/operacioni rizik

Transakcioni/operacioni rizik se povećava usled opasnosti od prevara, grešaka u procesiranju, sistemskim kvarovima i ostalim nepredviđenim događajima, koji za rezultat imaju nemogućnost bankarske organizacije da isporuči svoje proizvode i usluge. Rizik postoji kod svakog proizvoda ili usluge koji se nude. Na visinu transakcionog rizika utiče struktura procesnog okruženja banke, uključujući tipove proizvoda i usluga koje se nude, zatim, kompleksnost procesa i tehnologija za podršku procesima.

U većini slučajeva, aktivnosti e-bankarstva će povećati kompleksnost aktivnosti date finansijske institucije i količinu transakcionog/operacionog rizika, pogotovo ako banke nude neke inovativne servise, koji još uvek nisu standardizovani. Pošto korisnik očekuje da servisi e-bankarstva budu aktivni 24 časa, 7 dana u nedelji, banke moraju obezbediti dovoljan kapacitet i redudansu kako bi postigle dostupnost traženih servisa.

Ključ u kontroli transakcionog rizika leži u tome da se vrši stalno prilagođavanje politike, procedura i metoda kontrole, kako bi se što pre upoznali sa nadolazećim rizicima koje nosi e-bankarstvo, i samim tim, kako bi se verovatnoća dešavanja nepredviđenih događaja što više smanjila. Osnovna interna kontrola uključuje sagregaciju dužnosti i obaveza i dualnu kontrolu.

Kreditni rizik

Generalno, kreditni rizik finansijske institucije se ne povećava zbog činjenice da se kredit dodeljuje putem kanala e-bankarstva. Međutim, menadžment mora da razmotri oprez kada razmatra zahteve i odobrava kredit elektronski, obezbeđujući da menadžment informacioni sistem efikasno prati performanse portfolija koji su pokrenuti preko elektronskih kanala.

On-line pokretanje procesa i odobravanja kredita predstavlja za menadžment izazovan proces koji u mnogome zavisi od sledećih aspekata:

– verifikacija identiteta korisnika za on-line kreditnu aplikaciju i kontakt bez viđenja,
– praćenje i kontrola rasta, cena, postavljenih standarda i kredita koji se daju, a u okviru toga poštovanje dinamike vraćanja, itd., a čiji je postupak pokrenut preko elektronskih kanala,
– monitoring i nadzor nad trećim licima koji obavljaju poslove kao agenti ili u ime finansijske institucije i
– vrednovanje mogućnosti za uzimanje u zalog, koa garanciju, na širim geografskim područjima.

LIKVIDNOST, KAMATNA STOPA TRŽIŠNI RIZIK I RIZIK CENA

Rizici vezani za fondove i investiranje mogu da narastu sa inicijativama finansijske institucije da uvede i razvija aktivnosti e-bankarstva, pri čemu će značajno zavisiti i od stabilnosti i cena prikupljenih depozita. Internet omogućuje bankama da svoje proizvode i usluge plasiraju na globalno tržište. Advertajzing programi koji se baziraju na Internet tehnologijama mogu efikasno da upare proizvodno orijentisane investitore sa potencijalno visokim depozitima za proizvodnju. Međutim, depoziti prikupljeni preko Interneta moraju da privuku potencijalne korisnike koji su usmereni samo na kamatnu stopu i mogu da obezbede izvor finansiranja sa karakteristikama rizika sličnim kako kod brokerskih depozita. Bankarska organizacija može da kontroliše ovu potencijalnu nestabilnost i prošireni geografski domet preko svojih ugovora o depozitu, praksi otvaranja računa, koji mogu prerasti u sastanke lice u lice ili razmeni papirne korespondencije. Bankarske organizacije treba da modifikuju svoju politiku ukoliko dođe do sledećih slučajeva:

– potencijalno povećanje zavisnosti od brokerskih fondova ili drugih visoko osetljivih depozita,
– potencijalna akvizicija fondova sa tržišta na kojima institucije nisu licencirane da obavljaju bankarske poslove,
– potencijlani udaru preko rasta zajmova ili depozita sa rastućeg Internet tržišta, uključujući udare kao čto su povećanja racia kapitala i
– potencijalno povećanje nestabilnosti fondova, što može negativno uticati na poverenje korisnika.

ZAKONSKI RIZIK

Pravna pitanja se nameću zbog rastuće upotrebe e-bankarstva i razlika između elektronskih i procesa baziranih na papirnim dokumentima. E-bankarstvo je novi kanal za isporuku gde pravo i pravila upravljanja elektronskom isporukom određene finansijske institucije mogu biti nejasni, dvosmisleni ili još u razvoju. Posebni regulatorni i pravni izazovi uključuju:

– nesigurnost oko pravne jurisdikcije i zakoni koje zemlje pokrivaju određenu elektronsku transakciju,
– davanje kredita po određenim pravnim regulativama,
– čuvanje tražene odgovarajuće dokumentacije za on-line advertajzing, aplikacija i izjava i
– ustanovljavanje legalno pravnih elektronskih ugovora.

Principi kojih se treba pridržavati kada se govori o upravljanju zakonskim rizikom su:

– odgovarajuće otkrivanje strukture servisa e-bankarstva,
– privatnost korisničkih informacija,
– kapacitet, poslovni kontinuitet i kontigencijsko planiranje da bi se obezbedila dostupnost sistema i servisa e-bankarstva i
– planiranje reakcija na iznenadne neželjene događaje.

STRATEŠKI RIZIK

Upravljačke strukture u finansijskim institucijama moraju da razumeju rizik koji je povezan sa servisima e-bankarstva i da procene cenu upravljanja tim rizikom u odnosu na vraćanje investicije za date usluge e-bankarstva. Loše planiranje u e-bankarstvu i loše odluke po pitanju investicija mogu povećati strateški rizik finansijske institucije. Oni koji se prvi prilagode na nove servise e-bankarstva mogu sebe da ustanove kao inovatore koji izlaze u susret željama svojih korisnika, ali zato mogu i da povećaju cene svojih usluga i kompleksnost njihovih operacija može biti veća, upravo zbog novih rešenja određenih usluga. Nasuprot njima, oni koji se kasnije prilagode mogu da izbegnu visoke cene i povećanu kompleksnost, ali time stvaraju veći rizik da njihovi korisnici žele nove proizvode ili usluge. U upravljanju strateškim rizikom vezanim za servise e-bankarstva finansijske institucije moraju da postave jasno definisane ciljeve e-bankarstva, na osnovu kojih će institucija moći procenjuje uspešnost sprovođenja svoje strategije e-bankarstva.

Finansijske institucije moraju da obrate pažnju na sledeće:

– adekvatan menadžment informacioni sistem, kako bi se pratila upotreba i profitabilnost,
– praćenje troškova sa praćenjem aktivnosti e-bankarstva ili praćenje troškova kroz nadzor prodavaca i dobavljača tehnologije,
– dizajn, isporuka i određivanje adekvatnih cena kako bi se zadovoljili zahtevi korisnika,
– čuvanje elektronskih ugovora o zajmovima i ostalih elektronskih ugovora u formatu koji će biti prihvatljiv u procesima parničenja,
– troškovi i dostupnost kadrova koji će obezbediti tehničku podršku za promene, koja će uključivati nove operativne sisteme, web browsere i komunikacione uređaje,
– takmičenje sa drugima provajderima e-bankarstva i
– odgovarajuća tehnička, operativna ili marketing podrška za proizvode ili usluge e-bankarstva.

RIZIK ZA REPUTACIJU

Odluka institucije da ponude usluge e-bankarstva, pogotovo za veoma kompleksne transakcione servisa, značajno povećava nivo rizika za reputaciju.

Postoji nekoliko faktora koji mogu uticati na institucijinu reputaciju, a neki od njih su:

– gubitak poverenja usled neovlašćenog pristupa korisničkim računima (npr. hakeri),
– gubitak ili krađa poverljivih informacija od strane neovlašćenih strana,
– neuspeh u ispunjavanju marketinških zahteva,
– nemogućnost da se obezbedi pouzdanost servisa, bilo usled preopterećenosti ili zbog kvara sistema,
– žalbe korisnika zbog komplikovanosti servisa e-bankarstva i nemogućnost institucijinog help deska da reši probleme i
– konfuzija između servisa koje nudi finansijska institucija i servisa koje nude druge kompanije, a koji su linkovani preko web sajta.

UPRAVLJANJE RIZIKOM U E-BANKARSTVU

Osnovne karakteristike e-bankarstva su prožete određenim izazovima u upravljanju rizikom koji ih prati.

Neki od tih izazova su i:

– brzina promena koje se dešava na polju tehnologije i inovacije korisničkih servisa u e-bankarstvu je izuzetno velika. Istorijski, nove bankarske aplikacije su se implementirale u relativno dugom periodu vremena i posle detaljnih testiranja. Danas, međutim, banke su pristisnute konkurentskim pritiskom i primorane da brzo reaguju, tako da od pojave do implementacije neke aplikacije prođe samo nekoliko meseci. Ova povećana konkurancija intenzivira izazov menadžmenta da da obezbedi odgovarajuću stratešku procenu, analizu rizika i sigurnosne procene, kao prioritetne u implementiranju novih aplikacija e-bankarstva.
– Transakcioni web sajtovi e-bankrstva i odgovarajuće maloprodajne i veleprodajne poslovne aplikacije su obično integrisane koliko god je to moguće sa sovtferom koji omogućuje kontrolu zakonitosti transakcija, kako bi se obezbedile valjane transkacije, sa pravnog aspekta. Ovakva automatizacija procesiranja transakcija smanjuje mogućnosti prevare i ljudske greške, kao važnih faktora rizika, ali sa druge strane povećava zavisnost od primene IT tehnologija.
– E-bankarstvo povećava zavisnost banke od IT tehnologija, te stoga se povećava kompleksnost mnogih operativnih i bezbedonosnih pitanja, što se prenosi dalje i povećava potrebu za novim partnerstvima, alijansama i outsource aranžmanima, od kojih mnogi nisu pravno regulisani. Ovaj razvoj vodi ka stvaranju novih poslovnih modela, u koje su uključene banke i nebankarski entiteti, kao što su Internet servis provajderi, telekomunikacione kompanije i ostale slične firme.
– Internet je globalan po svojoj prirodi. To je otvorena mreža kojoj se može pristupiti sa bilo koje tačke na svetu, od strane nepoznatih lica, rutirajući, pri tom, poruke preko nepoznatih lokacija pomoću, sve više zastupljenih, bežičnih uređaja. Ovo utiče na značajno povećanje kontrole sigurnosti, tehnika korisničke autentifikacije, zaštitu podataka i standarde koji se tiču privatnosti korisnika.

PRINCIPI UPRAVLJANJA RIZIKOM U E-BANKARSTVU

Principi upravljanja rizikom u e-bankarstvu svrstani su u tri grupe, čija se odgovornost ne retko preklapa.

I Nadzor od strane menadžmenta (principi od 1 do 3):

1. Efektivan nadzor menadžmenta nad aktivnostima e-bankarstva.
2. Ustanovljavanje sveobuhvatnog procesa za kontrolu sigurnosti.
3. Sveobuhvatan nadzor menadžmenta nad procesima stvaranja outsourcing odnosa sa trećim stranama.

II Kontrola sigurnosti (principi od 4 do 10):

4. Autentikacija za korisnike e-bankarstva.
5. Ogovornost za transakcije u e-bankarstvu.
6. Ogovarajuće mere da se obezbedi sagregacija dužnosti.
7. Odgovarajuća kontrola autorizacije za sistem e-bankarstva, baze podataka o aplikacije.
8. Integritet podataka u transakcijama e-bankarstva, podacima koji se čuvaju o informacijama.
9. Ustanovljavanje jasnog sistema praćenja za transakcije u e-bankarstvu.
10. Pouzdanost ključnih informacija za banku.

III Upravljanje rizikom sa pravnog aspekta i sa aspekta reputacije (principi od 11 do 14):

11. Odgovarajuća prozirnost transakcija e-bankarstva.
12. Privatnost korisničkih informacija.
13. Kapacitet, poslovni kontinuitet o kontigencijsko planiranje da se obezbedi dostupnost sistema o servisa e-bankarstva.
14. Planiranje za odgovor na nepredviđene događaje.

AKTIVNOSTI UPRAVLJAČKIH STRUKTURA (MENADŽMENTA)

Menadžment finansijskih institucija je odgovoran za razvoj poslovne strategije e-bankarstva, koja treba da uključuje:

– racionalnost i strategiju za nuđenje servisa e-bankarstva, uključujući i informativnu, transakcionu ili podršku za elektronsko poslovanje,
– cost-benefit analizu, procenu rizika i ocenu alternativa aktivnostima e-bankarstva, kao što je angažovanje trećih lica kao provajdera,
– ciljeve i očekivanja koje menadžment može da koristi da meri efektivnost strategije e-bankarstva i
– odgovornost za razvoj i održavanje politike upravljanja rizikom i kontrolu upravljanja rizicima e-bankarstva i proveru aktivnosti.

STRATEGIJA E-BANKARSTVA

Menadžment bankarske organizacije treba da izabere nivo usluga e-bankarstva koji se obezbeđuje za različite segmente korisnika, baziran na njihovim potrebama, uzimajući u obzir i procenu rizika. Ove odluke donosi najviše rukovodstvo bankarske organizacije. Neke finansijske institucije mogu da ne

pružaju usluge e-bankarstva ili da se ograniče na usluge kakve su informativni web sajtovi. Bankarske organizacije bi trebale da periodično preispituju ove odluke da se uvere da su one još uvek ispravne, odnosno da su odgovarajuće za trenutnu poslovnu strategiju. Uspeh se može definisati na više načina, kao što su povećanje tržišnog udela, poboljšanje odnosa sa korisnicima, smanjenje troškova, itd. Ako bankarska organizacija utvrdi da treba da uvede transakcioni sajt, sledeća odluka je da proizvodi i usluge postanu dostupni korisnicima elektronskim putem. Da bi ove proizvodi ili usluge mogli da budu isporučeni moraju da postoje određeni mehanizmi na web sajtu (više strana, linkovi, itd.).

COST-BENEFIT ANALIZA I PROCENA RIZIKA

Finansijske institucije moraju da svaku svoju odluku, o implementaciji proizvoda ili usluga e-bankarstva, baziraju na iscrpnoj analizi troškova i koristi koje donosi takva akcija.

Neki od razloga zbog kojih se institucije odlučuju da korisnicima nude servise e-bankarstva su:

– niski operativni troškovi,
– veća geografska diverzifikacija,
– poboljšana ili stabilna konkurentska pozicija,
– povećanje zahteva korisnika za uslugama i
– nove mogućnosti za prihod.

Oni koji rade cost-benefit analizu treba da razumeju da rizici vezani za e-bankarstvo treba da se posmatraju i kroz troškove koji se stvaraju da bi se ti rizici umanjili. Bez takve ekspertize, cost-benefit analiza će najverovatnije potceniti i vreme i resurse potrebne za odgovarajuće nadgledanje aktivnosti e-bankarstva, obično nivo tehničke ekspertize potreban da se obezbedi kompetentan nadzor nad aktivnostima u organizaciji ili aktivnostima koje su izdvojene. Pored očiglednih troškova zaposlenih, hardvera, softvera i komunikacija, analiza treba da obuhvati i:

– promene u politici, procedurama i praksi,
– odgovarajuću arhitekturu mreže, sigurnosnu ekspertizu i softverske alate da održe dostupnost sistema i da zaštite i odgovore na neovlašćene pokušaje pristupa,
– obučeno osoblje neophodno za podršku servisima e-bankarstva, spremno da radi prekovremeno i bez geografskih ograničenja,
– razvijen menadžment informacioni sistem (MIS),
– veći nivo pravne kontrole i kontrole odgovornosti,
– prošireni MIS za praćenje sigurnosti e-bankarstva, upotrebe i profitabilnosti, i da meri uspeh strategije e-bankarstva,
– cenu osiguranja aktivnosti e-bankarstva,
– potencijalni prihod za različite cene,
– potencijalne gubitke usled prevara i
– oportunitetne troškove vezane za alokaciju kapitala naporima e-bankarstva.

PRAĆENJE I ODGOVORNOST

Kada se strategija e-bankarstva implementira, menadžmet treba da periodično ocenjuje efektivnost strategije. Ključni aspekt ove evaluacije je poređenje trenutne pozicije sa ciljevima i očekivanjima koji su postavljeni. Neki elementi koji se mogu pratiti da bi se merio uspeh i troškovna efektivnost strategije e-bankarstva su:

– ostvareni prihod,
– procenat dostupnosti web sajta,
– broj korisnika koji aktivno koriste servis,
– procenat računa koji su prijavljeni za servise e-bankarstva,
– broj i cena transkacija.

Bez jasno definisanih i merljivih ciljeva menadžment neće moći da utvrdi da li servis izlazi u susret zahtevima korisnika, sa rastom same institucije i njenim očekivanjima po pitanju profita.

Prilikom evaluacije efektivnosti strategije e-bankarstva menadžment treba da utvrdi da li se sprovodi usvojena politika i da li se poštuju postavljene procedure i da li postoji odgovarajuća kontrola. Ukoliko se strategijom ne ustanovi jasna odgovornost za razvoj politike i kontrole, menadžment neće moći da utvrdi gde je i zašto došlo do loših rezultata.

ISPITIVANJE/PROVERAVANJE

Važna komponenta nadzora je odgovarajuća nezavisna funkcija proveravanja/ispitivanja. Bankarske organizacije koje nude proizvode i usluge e-bankarstva treba da prošire svoje polje ispitivanja u skladu sa povećanjem kompleksnosti i rizika koji nose aktivnosti e-bankarstva. Ta funkcija ispitivanja treba da uključuje i:

– celokupan obim svih aktivnosti e-bankarstva,
– osoblje sa dovoljno tehničkog znanja da proceni sigurnosne pretnje kontrolu na otvorenoj mreži i
– nezavisne pojedince ili kompanije koji će obavljati funkciju proveravanja i ispitivanja bez konflikata.

STANDARD ISO 17799 KAO SREDSTVO UPRAVLJANJA RIZIKOM

Međunarodna organizacija za standardizaciju izdala je standard ISO 17799 kako bi pobojšala upravljanje sigurnošću informacija i uvela neke standardizovane kontrole i procese koje će se koristiti. Efikasno upravljanje sigurnošću informacija obezbediće i smkanjivanje rizika u sektoru e-bankarstva, jer je u u e-bankarstvu glavni resurs upravo informacija.

U standardu ISO 17799 se kaže da je "Informacija imovina koja kao i ostala važna imovina u poslovanju ima vrednost za organizaciju i mora biti stalno odgovarajuće zaštićena."

Upravo taj standard ISO17799 definiše šta bi sve organizacija trebala da preduzme da bi se osigurala zaštita informacija. U samom standardu ISO17799 ima 11 poglavlja, 132 kontrole čime se sveobuhvatno, na današnjem stepenu tehnološkog razvoja predlaže šta bi se sve trebalo preduzimati u cilju zaštite informacija.

ŠTA JE 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.

ISO 17799 standard je nastao na osnovu BS 7799-1 standarda. ISO 17799 je zvaničan standard, ali bolje ga je protumačiti kao skup smernica koje je moguće upotrebiti. Trenutno ovaj standard je pod revizijom, kako bi se u budućnosti mogao uskladiti sa izmenjenim standardom ISO 27001. Standard

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.

Kako je kao standard načelan, **ISO 17799 nije**:

– tehnički standard,
– proizvodno ili tehnološki usmeren,
– metodologija za evaluaciju opreme, kakav je standard za Uobičajene kriterijume, ISO 15408, koji se bavi sa funkcionalnim i sigurnosnim zahtevima određene opreme,
– zasnovan na "Opšte prihvaćenim principima bezbednosti za sisteme" ("Generally Accepted System Security Principles" ili GASSP), koji predstavlja zbirku najboljih praksi iz oblasti sigurnosti,
– zasnovan na "Vodiči za menadžment IT sigurnosti" ("Guidelines for the Management of IT Security" ili GMITS) koji se sastoji iz pet nastavaka i odnose se na standard ISO 13335, koji obezbeđuje načelan okvir za menadžmet IT sigurnosti.

Pošto ISO 17799 pokriva samo izbor i upravljanje kontrolom bezbednosti informacija, ove kontrole mogu:

– zahtevati korišćenje Uobičajenih kriterijuma za nivo sigurnosti opreme,
– inkorporisanje GASSP vodiča i
– implementaciju GMITS koncepata.

Suštinski, standard sadrži polazno poglavlje „Procena i upravljanje ICT rizikom" sa 11 delova u kojima su grupisane bezbjedonosne odredbe:

1. ***Bezbedonosna politika***

Donošenje bezbedonosnog dokumenta sa smernicama o informacionoj bezbednosti, podržanog standardima i procedurama kao i jasno iskazanim stavom menadžmenta o informacionoj bezbednosti.

2. ***Organizacija informacione bezbednosti***

Definisanje i implementacija upravne strukture za informacionu bezbednost.

3. ***Upravljanje imovinom***

Definisanje – prepoznavanje informacione imovine koju organizacija poseduje. Klasifikacija informacija.

4. ***Bezbednost kod zaposlenih***

Podela odgovornosti i definisanje prava pristupa među zaposlenima. Edukacija i obuka zaposlenih u pogledu informacione bezbednosti.

5. ***Fizička zaštita i zaštita okoline***

Zaštita IT opreme od zlonamernih ili nenamernih oštećenja, gubitaka, kao i oštećenja usled neadekvatnih radnih uslova.

6. ***Upravljanje komunikacijama i operacijama***

Uspostavljanje bezbedonosnih kontrola za upravljanje IT sistemom i komunikacijama.

7. ***Kontrola pristupa***

Nadzor i kontrola pristupa ICT sistemu i podacima u cilju sprečavanja neovlašćene upotrebe.

8. ***Nabavka, razvoj i održavanje informacionih sistema***

Vođenje informacione bezbednosti u svim fazama životnog ciklusa ICT sistema (razvoj/nabavka, testiranje, implementacija, održavanje)

9. ***Upravljanje bezbedonosnim incidentima***

Promptno izveštavanje o bezbedonosnim incidentima i sprovođenje odgovarajuće kontrole incidenata.

10. ***Upravljanje poslovnim kontinuitetom***

Analiza, dokumentovanje i testiranje plana postupanja u slučaju nepredviđenih okolnosti, prirodnih ili ljudski uzrokovanih havarija.

11. ***Usklađivanje***

Usklađivanje informacionih sistema sa zakonskom regulativom, standardima i tehničkim uputstvima kao i način korišćenja audit alata i zaštita od njihove zloupotrebe.

ZAKLJUČAK

E-bankarstvo ima jedinstvenu karakteristiku da poveća ukupan rizik za instituciju i nivo rizika vezan za tradicionalne finansijske usluge, operacioni, zakonski i rizik za reputaciju. Ove jedinstvene karakteristike e-bankarstva uključuju i:

– brzinu tehnoloških promena,
– promena očekivanja korisnika,
– povećanje vidljivosti mreža koje su široko dostupne (npr. Internet),
– manje interakcije lice u lice sa korisnicima usluga finansijskih institucija,
– potreba za integracijom e-bankarstva sa postojećim računarskim sistemom,
– zavisnost od trećih strana zbog neophodne tehničke ekspertize i
– povećavanje pretnji i ranjivosti zbog mreža koje su široko dostupne.

Menadžment mora da prati svaki od ovih procesa i da proširi svoje aktivnosti upravljanja rizikom, ako je to neophodno.

Sa povećanjem učešća informacionih tehnologija u bankarskom sektoru značajno se smajuju troškovi, raste, ne samo kvalitet usluga, već i konkurencija i rizik. Da bi finansijska institucija mogla da opstane ona mora stalno da identifikuje, procenjuje i donosi odluke za izbegavanje ili smanjivanje rizika, upravo ove aktivnosti predstavljaju upravljanje rizikom i one su ključ uspeha. Jedno od veoma efikasnih sredstava za kontrolu i smanjenje rizika je, svakako, standard ISO 17799, koji obezbeđuje sigurnost informacija, odnosno obezbeđuje sigurnost najvažnijeg resursa elektronskog sveta.

U godinama koje slede videćemo da će osnovni zadatak biti obezbeđivanje efikasnog elektronskog plaćanja kroz povećanje učešća informacionih tehnologija u poslovanju. U budućnosti ova kombinacija biće početna tačka u eri elektronskog poslovanja, koje predstavlja fundamentalnu promenu u trgovini, još od kako je papirni novac uveden u trgovinu. Ovo čekanje za jasan signal početka ovog novog doba će biti konačno određeno kada trenutno stanje posmatramo iz druge perspektive. Osnovna politika koju nudi Internet je direktni pristup dobavljača potrošačima, bez pratećih troškova izazvanih održavanjem fizičkih kanala distribucije – ljudi, materijala itd. Pomoću elektronskih medija konkurenti se mogu pojaviti bilo gde u svetu. Oni nisu prostorno ograničeni. Strateške implikacije za sve poslove su naročito značajne za trgovce na malo i finansijske organizacije.

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.

LITERATURA

[1] Marko Ranković, Vojkan Vasković, The Economic Models for the ATM Network Implementation, The IPSI - Transactions Advanced Research, Volume 5, Number 2, 16-21, 2009.
[2] Dejan Simić, Proces primene PCI standarda, InfoM, br. 31 – časopis za informacione tehnologije i multimedijalne sisteme, broj rada: 2, 2009.
[3] Marko Ranković Marko, Vojkan Vasković Vojkan, Quantitive Website Analysis: Case Study of the Serbian Banks, Industrija, No. 2, 2011.
[4] Marko Ranković, Vojkan Vasković, Uloga procesora plaćanja u servisiranju online transakcija, Istraživanje i projektovanje za privredu, broj: 3, 139-146, 2010.
[5] Marko Ranković, Tipovi i vrste krađa u sistemima plaćanja platnim karticama, InfoM, br. 28 – časopis za informacione tehnologije i multimedijalne sisteme, broj rada: 3, 2008.
[6] Marko Vulić, Marko Ranković, Vojkan Vasković, Metodološki pristup procesu zaštite sistema e-plaćanja, InfoM, br. 35 - časopis za informacione tehnologije i multimedijalne sisteme, broj rada: 2, 2010.
[7] Marko Ranković, "Istraživanje uloge procesora plaćanja u servisiranju online finansijskih transakcija", doktorska disertacija, Fakultet organizacionih nauka, Beograd, 2010.
[8] Marko Ranković, "Modeli i tehnike zaštite sistema plaćanja platnim karticama" – magistarska teza, Fakultet organizacionih nauka, Beograd, 2008.
[9] Vladimir Simović, Osnovni teorijski modeli P2P sistema plaćanja, InfoM, br. 32 – časopis za informacione tehnologije i multimedijalne sisteme, broj rada: 6, 2009.
[10] Federal Financial Institutions Examination Council, Authentication in an Internet Banking Environment, 2004, http://www.ffiec.gov
[11] Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, http://www.bis.org/publ/bcbs82.pdf
[12] Jonathan G. Gossels, ISO 17799:Pay Attention to this One-Executive Insight Series, http://systemexperts.com
[13] Tom Carlson, Information Security Management: Understanding ISO 17799, http://www.lucent.com

Dr Marko Ranković, EuroPlanet, d.o.o
Mail: 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.

Mr Vladimir Simović, Visoka škola za informacione tehnologije
Mail: vladimir.simovic@its.edu.rs

Oblasti profesionalnog interesovanja: elektronsko poslovanje, sistemi plaćanja, modeli primene kreditnog biroa i zaštita finansijskih informacija.

Dr Vojkan Vasković, Beogradska Poslovna Škola
Mail: vaskovic@bvcom.net

Oblasti profesionalnog interesovanja: elektronsko poslovanje, internet tehnologije, mobilne tehnologije, e-goverment