UDK: 004.738.5:658

Originalni naučni rad

Gordana Đorđević[1]

Sigurnosni aspekti e-poslovnih modela u mrežnom okruženju

Apstrakt

Visok stepen tehnoloških promena koji karakteriše savremenu ekonomiju, a pre sve intenzivnije korišćenje informacionih i komunikacionih tehnologija dovele su do značajnih promena u poslovnom okruženju. Stvoreni su uslovi za kreiranje elektronskih poslovnih platformi koje bi poslovnim sistemima omogućili bolje pozicioniranje na globalnom tržištu, konkurentsku prednost, veći profit, pružanje usluga korisnicima na efikasniji način. Novi poslovni modeli koji su kreirani u mrežnom okruženju postaju otvoreni i lako dostupni kupcima i korisnicima usluga, ali i potencijalnim napadačima koji različitim tehnologijama i metodama narušavaju integritet sistema na mreži. U takvim uslovima, izgradnja adekvatnih sistema zaštite u obliku sistema informacione sigurnosti postaju značajan deo upravljanja poslovnim modelima u mrežnom okruženju.

Ključne reči: informacione tehnologije, digitalna ekonomija, elektronsko poslovanje, digitalna informacija, poslovni modeli, sistemi zaštite

Uvod

[1] ALFA univerzitet, Beograd,
e-mail: bgordana@yahoo.com

Informaciono-komunikacione tehnologije postale su ključna sila u određivanju tokova i transformaciji ekonomskih i društvenih aktivnosti. Iskorak koji je u poslednje dve decenije načinjen u oblasti IT industrije, uslovljen ekspanzijom povezivanja poslovnih i drugih subjekata elektronskim putem, revolucionarno je izvršio uticaj na poslovni i institucionalni razovj savremenog društva. Uporedo sa rastućim uticajem digitalnih tehnologija rastu i novi izazovi koji se mogu dostići znanjem, kreativnošću, sposobnošću i težnjom za promenama. Informacione tehnologije nisu promenile samo način razmišljanja poslovnih ljudi i vlada državnih zajednica, već su omogućile stvaranje novih oblika poslovanja i pružanja usluga, kao i kreiranje novih poslovnih strategija.

Informacione tehnologije su umrežile celo čovečanstvo i nametnule naophodnost članstva u toj mreži. Tako nastaju e-poslovni modeli koji u mrežnom okruženju realizuju raznovrsne funkcionalne zahteve u skladu sa definisanim poslovnim ciljevima. Osim nekih tehnoloških minitrendova karakterističnih za poslovanje na mreži u novoj ekonomiji kao što su: arhitektura Interneta/intraneta, brzi i jeftini pristup podacima, multimediji, otvoreni standardi i rastuća potreba za distribuiranim aplikacijama, nameće se i potreba za aplikacijama koje su dovoljno prilagodljive i pouzdane da pokrenu i izvode aplikacije presudne za poslovanje. Nova tehnologija postaje neophodna da bi se ubrzale poslovne operacije, bolje reklamirali proizvodi, unapredili odnosi sa kupcima, osigurao rast profita.

Informacione tehnologije nisu samo omogućile brzu i efikasnu realizaciju e-aktivnosti (funkcionalnosti modela na mreži), već su istovremeno izložile ove modele raznovrsnim rizicima, koji su rezultat ranjivosti sistema koji se bazira na ovim tehnologijama, i razvoja brojnih pretnji u e-okruženju.

U ovakvim uslovima nesigurnog e-okruženja, zaštita ličnih podataka i zaštita privatnosti na mreži postaju sve češći sigurnosni zahtevi. Neki sistemi na mreži, iako posluju u svetu promenljivih rizika, više su usmereni ka aktivnostima realizacije profita nego ka aktivnostima zaštite od gubitaka ili narušavanja njihove najvrednije imovine – informacija. Mnogobrojna istraživanja, međutim, pokazuju da još uvek

postoji veliki broj »nepoverljivih korisnika« *online* ponude koji, uz nedovoljnu zainteresovanost vlasnika poslovnih modela na mreži za zaštitu ličnih informacija korisnika, mogu delovati ograničavajuće na dalji razvoj poslovanja na mreži. Zato je neophodno da se savremeni sistemi informacione sigurnosti baziraju na standardima koji daju uputstva i smernice za zaštitu ličnih informacija korisnika, kao i svih ostalih senzitivnih informacija (tim pre, što se ovi standardi baziraju upravo na temeljima zakonskih normi koje nalažu zaštitu privatnosti).

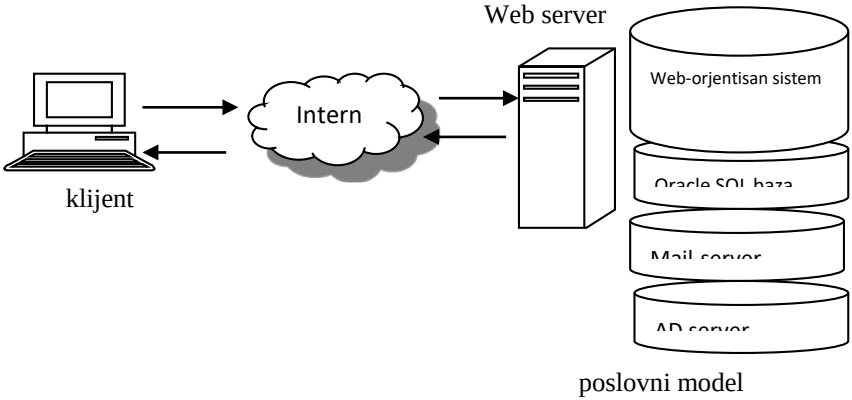
Pretnje i rizici kao i nedostatak vizuelnih (opipljivih) dokumentata u poslovanju na mreži, stvaraju efekat nesigurnosti koji se mora i može prevazići razvijanjem i implementacijom adekvatnih sistema informacione sigurnosti. »Efikasnost i efektivnost sigurnosti je integralni deo poslovnih vrednosti koji odražava sistem koji posluje na mreži; modeli zahtevaju sigurnost za svoje sopstvene operacije i sigurnost za interakciju sa sopstvenim korisnicima odnosno poslovnim partnerima« (IBM, 2005.: 2). S tim ciljem, razvijena su brojna sigurnosna rešenja koja realizuju bezbedne i kvalitetne procedure, čijom se implementacijom može čak i povećati nivo sigurnosti u odnosu na klasičan način realizovanja poslovnih aktivnosti. Pri tome, izbor adekvatnog sigurnosnog rešenja je veoma važan i sa stanovišta funkcionalnosti sistema, jer tehnike zaštite mogu uticati na performanse sistema na mreži.

1. Poslovni modeli u mrežnom okruženju

Savremeni poslovni modeli, kao »sistemi zasnovani na Web-u« čije se aplikacije ili usluge nalaze na serveru, lako su dostupne korisnicima sa bilo kog mesta preko nekog od servisa Interneta (npr. World Wide Web), korišćenjem nekog Web pretraživača. Opšta infrastruktura poslovnih modela koji svoju funkcionalnost realizuju u mrežnom okruženju, bazira se na:

- **platformi zasnovnoj na Web tehnologiji**, koja počiva na *Internetu*, kao globalnoj mreži, *intranet* i/ili *ekstranet infrastrukturi* i obezbeđuje mrežnu povezanost svih učesnika u e-aktivnostima i njihovu efikasnu komunikaciju
- **aplikativnim alatima**, koji čine softverska sredstva poslovnih modela

- **pozadinskim sistemima podrške**; integrisanje sistema poslovnog modela sa tehničkom infrastrukturom kao što su ERP (*Enterprise Resourse Planning*) sistemi, DMS (*Database Management Systems*) i interni tokovi podataka (slika 1).



Slika 1: Fizičke komponente poslovnog modela na mreži
(pojednostavljen model)
Izvor: Laudon, 2001.: 183

Osim jednostavnosti upotrebe, sistemi zasnovani na Web-u imaju još dve veoma važne funkcionalne osobine:

- generisani sadržaji/podaci ažuriraju se u realnom vremenu
- univerzalno su dostupni korisnicima preko Web-a (u zavisnosti od unapred definisanih prava pristupa za svakog korisnika odnosno grupu korisnika)

Poslovni modeli na mreži, nastali su kao rezultat usvajanja prednosti koje su donele informacione tehnologije i nove poslovne aplikacije, a iskorišćeni su za stvaranje novih vrednosti proizvoda i usluga i za kvalitetniju isporuku korisnicima (Whitemore, 2001: 38). Ovi modeli, dodatnu vrednost za klijente, najčešće kvantitativno iskazuju kroz nisku cenu proizvoda i usluga, njihov visok kvalitet ili svoje aktivnosti usmeravaju na postizanje konzistentnosti između obe opcije, poput poznatih i uspešnih kompanija kao što su to Amazon.com, Tesco.com, eBay.com. Ovakve uspešne kompanije nude svojim korisnicima niske cene, ali i širok izbor ponude, visok kvalitet usluga, čitav spektar pogodnosti visokog nivoa, superioran brend i, koristeći

snagu informacija koje već poseduju u kompaniji, kreiraju dodatne koristi za svoje kupce. Proširenim informacijama o proizvodima/uslugama, personalizovanim preporukama, širokim izborom, poslovni modeli su u mogućnosti da transformišu zahteve kupaca.

U nesigurnom i promenljivom okruženju poslovni modeli nikada ne mogu biti konačni i definitivni. Izučavajući poslovne sisteme koji lansiraju nove poslovne modele u pokušaju da započnu sledeću fazu razvoja poslovanja u e-okruženju, neki autori govore o strategiji »lansiranja i učenja«: poslovni sistemi koriste kratko vreme ciklusa da lansiraju nove poslovne modele, a onda usklađuju svoje potrebe, potrebe klijenata i praktična iskustva (sopstvena ili drugih sistema) u jednom stalnom procesu učenja i lansiranja (unapređenje poslovnog modela). Bilo da kreiraju nove poslovne modele ili proširuju postojeću infrastrukturu radi prilagođavanja novim procesima i novim zahtevima, poslovni sistemi, primenom ove strategije, obezbeđuju procese reinženjeringa poslovnih modela na mreži, koji se baziraju na povratnim informacijama od klijenata.

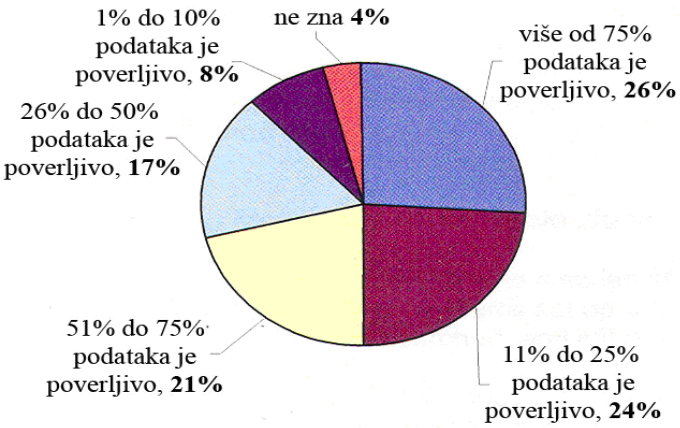
U uslovima globalnog tržišta, povećane konkurencije i izuzetne brzine u realizaciji poslovnih procesa, poslovni sistemi se susreću sa porastom količine informacija koje su od vitalnog značaja za poslovanje. Raznovrsne aplikacije za potrebe realizacije poslovnih aktivnosti, potrebe upravljanja tim aktivnostima na operativnom nivou, a posebno za procese donošenja odluka, koriste informacije koje su prikupljene iz internih (poslovni sistemi) i eksternih (okruženje poslovnih sistema) izvora. U takvim uslovima povećavaju se teškoće u prikupljanju, čuvanju i posebno u upravljanju podacima. Dodatno, koncept zajedničkog korišćenja informacija uslovio je jedan od osnovnih sigurnosnih zahteva: strogo kontrolisanje pristupa i korišćenja podataka.

Koncept sigurnosti poslovnih modela na mreži, ukazuje na usmerenost ka zaštiti aktive, čija je vrednost određena stepenom njihovog značaja za poslovanje. Sa stanovišta poslovanja, aktiva se odnosi na finansijske resurse, poslovne procese, reputaciju, tržišne pozicije, poverenje klijenata, intelektualnu svojinu, poslovne tajne, liste klijenata (kupaca) i druge opipljive i neopipljive vrednosti koje su od

značaja za realizaciju ciljeva poslovnog modela. Sa stanovišta informacionih tehnologija na kojima baziraju poslovni procesi modela u mrežnom okruženju, aktiva se odnosi na informacije, softver, hardver, mrežnu infrastrukturu i njihovu odgovarajuću međusobnu povezanost. Okruženje u kojem su locirane ove vrednosti i u kojem se realizuju aktivnosti primenom odgovarajućih tehnologija, predstavlja operativno okruženje kao opšte radno okruženje koje se bazira na mrežama (Internet, konekcija LAN mreže na WAN mrežu i dr.).

Postupak definisanja značajne aktive i njihove vrednosti je veoma složen. Ipak, najznačajnija aktiva u operativnom okruženju, u kvantitativnom i kvalitativnom smislu, je u obliku informacija koje su memorisane, procesirane ili su u fazi prenosa. Senzitivne (osetljive) informacije[2] su posebno značajne i sa stanovišta poslovnih transakcija i sa stanovišta sigurnosti. Prema istraživanju koje je realizovala *Enterprise Strategy Group* (ESG) na 227 poslovnih sistema u Severnoj Americi, 47% ispitanika klasifikovalo je više od polovine svojih informacija u kategoriju poverljivih (slika 2).

[2] Osobina kakva je senzitivnost (osetljivost) podataka se često pogrešno tumači. Osetljivost je sinonim za važnost ili vrednost. Neki podaci su osetljivi jer moraju ostati poverljivi. Mnogo veća količina podataka međutim, osetljiva je sa stanovišta obezbeđenja njihovog integriteta ili dostupnosti. *The Computer Security Act i OMB Circural A-130* jasno formulišu da su informacije osetljive ukoliko se njihovim neautorizovanim obelodanjivanjem, modifikacijom (gubitak integriteta) ili nedostupnošću može naneti šteta poslovnom sistemu.



Slika 2: Približan procenat sveukupnih podataka koji se smatraju senzitivnim
Izvor: Oltsik J., 2006.:2

Sigurnosni aspekti e-poslovnih modela ukazuju upravo na neophodnost zaštite takvih informacija u operativnom okruženju. Zaštita mora obuhvatiti sve kategorije napada koje se odnose na razotkrivanje aktive od strane neautorizovanih učesnika (gubitak poverljivosti), oštećenje aktive putem neautorizovane modifikacije (gubitak integriteta) ili nemogućnost autorizovanog pristupa aktivi (gubitak dostupnosti), ali nije limitirana samo na navedena sigurnosna narušavanja.

2. Sigurnosno okruženje modela na mreži

Brzi razvoj i eksponencijalni porast novog načina poslovanja, prihvatanje novih poslovnih modela kao neophodnih formi za realizaciju tog novog, efikasnijeg načina poslovanja, naterao je mnoge poslovne sisteme da ubrzano uvedu nove tehnologije bez potpunog razumevanja sigurnosnih postupaka. Inovativno uvođenje i korišćenje informacionih tehnologija je često sagledavano samo kroz značaj za unapređenje produktivnosti i efikasnosti. Međutim, praksa je pokazala da nije

dovoljno posmatrati nove tehnologije samo kroz »snagu i mogućnosti«, već je neophodno sagledati i »izazove i pretnje« koji predstavljaju kritična ograničenja za realizaciju prednosti koje ove tehnologije nose. Pretnje kojima su izloženi sistemi u mrežnom okruženju moraju biti obuhvaćene aktivnim procesima upravljanja rizicima (UNCTAD, 2005.: 22).

Poslovno okruženje u digitalnoj ekonomiji je izuzetno turbulentno, a izazovi i pretnje ostvaruju rastuće procente u odnosu na prethodne godine. Čak je i Symantec korporacija koja svake godine objavljuje izveštaje o istraživanjima proboja u sisteme na mreži i krađi podataka, 2013. godinu nazvala godinom »mega proboja«. Prema podacima do kojih je istraživanjem došla, ova korporacija je rangirala informacije koje su bile najugroženije u 2013. godini (tabela 1).

Tabela 1: Najugroženiji podaci u realizovanim probojima u 2013. godini

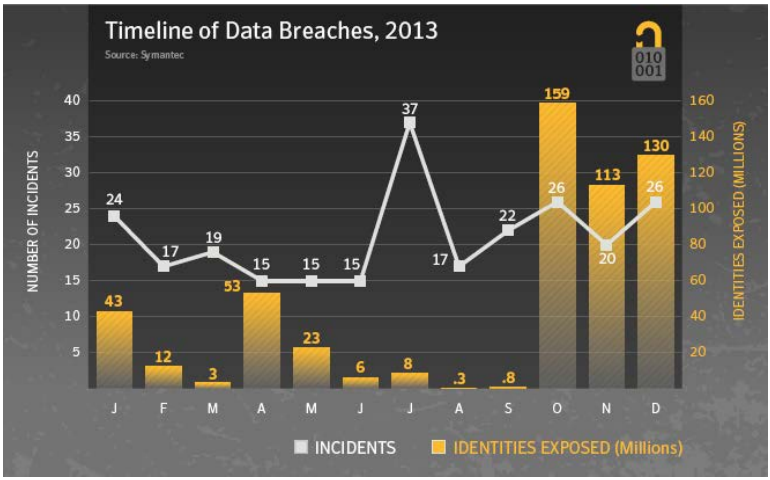
rang	tip informacije
1	lično ime
2	datum rođenja
3	identifikacioni brojevi zaposlenih u državnim institucijama
4	adresa stanovanja
5	medicinski zapisi
6	telefonski brojevi
7	finansijske informacije
8	e-mail adrese
9	korisničko ime i lozinka
10	podaci o osiguranju

Izvor: Symantec, 2014.: 12

Hakerski napadi su i dalje primarni uzroci izloženosti senzitivnih podataka sistema u mrežnom okruženju. Izuzetno visok procenat sigurnosnih proboja i gubitka ličnih podataka uticao je na podrivanje poverenja u poslovne sisteme i narušavanje njihove reputacije. Prema poslednjem izveštaju Symantec korporacije[3], u 2013. godini je bilo čak

[3] *Internet Security Threat Report* 2014 predstavlja rezultate istraživanja koje je *Symantec* korporacija obavila u 157 zemalja.

62% proboja (ukupno 253) više nego u 2012. godini (ukupno 156). Pri ovim probojima, u čak 8 slučajeva, više od 10 miliona senzitivnih podataka je bilo izloženo napadima spolja (i to po svakom proboju). U 2012. godini samo jedan slučaj proboja izložio je opasnosti 10 miliona senzitivnih podataka, dok je u 2011. godini takva izloženost realizovana u 5 proboja. Ukupna izloženost podataka u 2011. godini iznosila je 232 miliona, što je oko polovine izloženosti u 2013. godini (552 miliona) (slika 3). Međutim, u odnosu na 2012. godinu kada je ukupno 93 miliona senzitivnih podataka bilo izloženo hakerskim napadima, u 2013. godini ova izloženost se povećala čak 493%.



Slika 3: Izloženost podataka različitim napadima u 2013. godini prikazana po mesecima
Izvor: Symantec, 2014.: 40

Istraživanje Symantec korporacije pokazalo je da je najveći broj upada u sistem izvršen kod velikih kompanija koje imaju više od 2.500 zaposlenih (39%), kao i kod malih poslovnih sistema, do 250 zaposlenih (30%). Najšešće mete napada bili su sistemi državnih institucija (16%), sistemi koji nude usluge putem Interneta (oko 15%), proizvodni sistemi (13%) i finansijski sistemi (13%). Sistemi koji prodaju putem Interneta (e-trgovina) i koji su uvek bili najizloženiji raznovrsnim oblicima

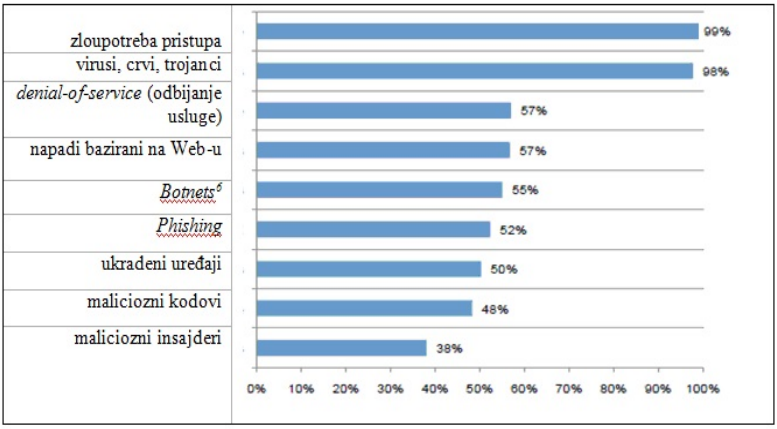
napada, u ovom istraživanju su se pokazali kao sistemi koji nisu bili tako često napadani u 2013. godini (2%) (Symantec, 2014: 29).

Ponemon Institut je svojim istraživanjima u 2013. godini obuhvatio šest zemalja sveta (SAD, Velika Britanija, Australija, Nemačka, Francuska, Japan) i 234 različitih kompanija. Izveštaj pokazuje da su sve ove kompanije bile meta čak 343 napada nedeljno (1.4 napada nedeljno po kompaniji) (*The Ponemon Institute*, 2013.: 10). Iskustva mnogih poslovnih sistema pokazuju da se napadi od strane insajdera mnogo češće realizuju u odnosu na napade spolja i da su velika opasnost za poslovne, senzitivne podatke upravo zaposleni u poslovnim sistemima koji imaju prava pristupa ovim podacima i mogu ih zloupotrebiti. Ovo istraživanje Ponemon instituta je to potvrdilo i pokazalo da su ispitani poslovni sistemi, u proseku, imali oko 55 zaposlenih koji su na neki način bili povezani sa incidentima ili probojima u sisteme u poslednjih 12 meseci, a čak 38% od svih napada je realizovano od strane zaposlenih (The Ponemon Institute, 2013.: 12). U 99% kompanija zloupotrebljeno je pravo pristupa, a više od 50% kompanija bilo je izloženo napadima koji se baziraju na Web tehnologijama, a koji su omogućili onesposobljavanje sistema da realizuje implementirane funkcije u Web okruženju ili da presreću poslovne informacije i kopiraju ih (kradu) ili modifikuju (botnets[4], phishing[5]) (slika 4).

[4] Napadi na računarske mreže ili računarske sisteme koji će omogućiti vlasniku kreiranog softvera da kontroliše i/ili upravlja radom napadnutog sistema.

[5] Predstavljajući se kao pouzdani učesnik u elektronskoj komunikaciji, korisnik ovog štetnog programa može da »ukrade« senzitivnu informaciju poput korisničkog imena, lozinke, podatke sa kreditnih kartica, novac.

Slika 4: Tipovi sajber napada na organizacije u 2013. godini



Izvor: The Ponemon Institute, 2013.: 10

3. Informaciona sigurnost mrežnih poslovnih modela

Prvobiti napori učinjeni u cilju zaštite poslovanja na mreži bili su usmereni na sigurnost implementiranih informacionih tehnologija, a ne prevashodno na informacionu sigurnost. Međutim, savremeni trendovi, a pre svega mnogobrojna istraživanja u ovoj oblasti, ukazali su na neophodnost zaštite senzitivnih informacija od rizika. Ova kretanja rezultat su:

- promene prirode informacionih rizika – Tokom mnogo godina, prvi i najjasniji cilj sigurnosti informacionih tehnologija bio je da zaštiti poslovne aktivnosti od malicioznih aktivnosti. Ovakav pristup je i dalje temelj zaštite informacionih resursa, ali su uočeni i neki novi trendovi koji zahtevaju promenu pristupa. Ti novi trendovi definisani su sledećim faktorima: porast internih pretnji, evaulacija zloupotreba i izmenjena prirode eksternih napada, kao i promena značenja termina »unutar poslovnog sistema«.
- rastućeg broj napada na senzitivne podatke – Poslovni sistemi dugo nisu bili svesni izloženosti sopstvenih poverljivih podataka. Tek kada se količina izloženih podataka merila stotinama miliona i kada je ovaj broj nastavio da raste, sistemi postaju svesni važnosti pitanja informacione sigurnosti.

- uticaja zakonske regulative - Zaštita senzitivnih informacija postaje primarna regulatorna oblast širom sveta, sa inicijativama koje su rangirane od regulacija svake pojedine države, do industrijskih standarda poput PCI (*Payment Card Industry*), DSS (*Data Security Standard*) i HIPAA (*US Health Insurance Portability and Accountability*) i mandata koji imaju međunarodni uticaj uključujući Direktivu zaštite privatnosti Evropske unije (*European Union Data Privacy Directive*).
- očiglednih i opipljivih gubitaka nastalih narušavanjem informacione sigurnosti

Nacionalni institut za standardizaciju i tehnologiju, SAD, u svojoj publikaciji 800-12 ukazuje na sledeće osnovne elemenate na kojima bazira opšti pristup definisanja i izgradnje sistema informacione sigurnosti:

- informaciona sigurnost treba da podržava realizaciju ciljeva poslovnog modela
- informaciona sigurnost je integralni element zdravog menadžmenta
- implementirani sistem informacione sigurnosti treba da bude isplativ
- izgradnja adekvatnog sistema informacione sigurnosti podrazumeva jasno definisan sistem odgovornosti
- izgradnja informacione sigurnosti zahteva sveobuhvatan i integrativni pristup
- sistem informacione sigurnosti trebalo bi periodično preispitati (redizajnirati)
- informaciona sigurnost je u izvesnoj meri limitirana društvenim faktorima

Definisani ciljevi poslovnog modela u velikoj meri određuju tehnološku stranu sistema informacione sigurnosti, odnosno izbor odgovarajućih sigurnosnih rešenja i mera. Nakon definisanja ciljeva i izbora odgovarajućeg sistema koji će na mreži podržavati realizaciju tih ciljeva, mogu se precizno utvrditi sigurnosni zahtevi koji proizilaze iz takve uloge. Ovakvim pristupom sistem informacione sigurnosti direktno podržava ciljeve poslovnog modela, mada često može biti i limitirajući faktor nametanjem lošeg izbora sigurnosnih rešenja ili dosadnih i pre svega nepotrebnih sigurnosnih pravila i procedura za korisnike, menadžere i sistem u celini. Adekvatna izgradnja i implementacija

sistema sigurnosti nije sama sebi cilj, već ima ulogu zaštite važnih vrednosti (pre svega podataka) čime će obezbediti podršku sveukupnim aktivnostima, a tako i ciljevima poslovnog modela. Uloge i funkcije sistema informacione sigurnosti ne moraju biti ograničene samo na pojedinačne elemente poslovnog modela, već koristi mogu osetiti svi učesnici u aktivnostima tog modela[6].

Računarski i informacioni sistemi, kao kritični resursi za realzaciju ciljeva poslovnog modela, zajedno sa ostalim resursima (novac, fizička aktiva ili korisnici) izloženi su rizicima i kao takvi moraju biti predmet zaštite. Najveći broj poslovnih sistema, polazeći od činjenice da je »upravljanje rizicima proces procene rizika, preuzimanje koraka za njihovo redukovanje na prihvatljiv nivo i realizacija postupaka za održavanje tog nivoa rizika« (UNCTAD, 2005: 22) rutinski upravlja mnoštvom rizika. S obzirom da sistemi u mrežnom okruženju nikada ne mogu biti apsolutno sigurni, dizajniraju se i implementiraju se sistemi koji će podržati funkcionalnost, finansijsku stabilnost i efikasnost poslovnog sistema u slučaju nepovoljnih događaja koji izazivaju gubitke, uz prihvatanje određenog nivoa rizika odnosno određenog nivoa gubitaka. Osim toga, mora se utvrditi i prihvatljiv nivo neophodnih troškova implementacije sigurnosnih rešenja.

Sagledavanjem očekivane koristi i procenom vrednosti aktive koju treba zaštititi, može se utvrditi isplativost sistema informacione sigurnosti. Implementirana sigurnost treba da bude odgovarajuća, ali i proporcionalna vrednostima aktive, zahtevanom nivou pouzdanosti sistema poslovnog modela, kao i jačini, verovatnoći i obimu potencijalnih narušavanja. Sistemi informacione sigurnosti obuhvataju raznovrsna sigurnosna rešenja usled raznovrsnosti sigurnosnih zahteva u

[6] Da bi, na primer, poslovni model e-trgovine bio uspešan, posebno kada je reč o poslovnom modelu iz kategorije B2B trgovine, svaki od učesnika zahteva sigurnosne kontrole za zaštitu svojih resursa. Ako implementirani sistem sigurnosti obezbedi adekvatnu sigurnost svih aktivnosti na strani svakog od učesnika, onda će on doneti korist za prodavca. Kupac obavlja sigurnu trgovinu koja će prodavcu omogućiti povećan profit.

zavisnosti od kategorije poslovnog modela koji treba zaštititi. Prednosti koje donosi implementirani sistem sigurnosti treba posmatrati ne samo kroz podršku realizacije ciljeva, već i kroz direktne[7] i indirektne[8] troškove.

Izgradnja odgovarajućeg sistema informacione sigurnosti podrazumeva i izgradnju odgovarajućeg sistema odgovornost svih učesnika u poslovnim aktivnostima koje mora biti eksplicitno definisano. Ovakav sistem, definisanjem obaveza i očekivanog ponašanja svih učesnika, određuje odgovornost u najširem smislu, ali i predstavlja osnovu na bazi koje se ostvaruje mogućnost izgradnje svesti učesnika da odgovorno obavljaju svoje aktivnosti. S obzirom da su učesnici u aktivnostima poslovnih modela na mreži zapravo »spoljni korisnici«, odgovornost vlasnika poslovnog modela podrazumeva, između ostalog, deljenje odgovarajućih saznanja o postojanju, obimu i veličini implementiranih sigurnosnih mera. Ovakvim informisanjem svojih korisnika i klijenata o prirodi sigurnosti poslovnog modela, korisnici stiču poverenje da učestvuju u interakciji sa sistemom koji je adekvatno osiguran. Osim toga, sistem odgovornosti podrazumeva obavezu pojedinaca čiji je zadatak održavanje sigurnosti »da treba da deluju pravovremeno i da na koordinisan način spreče i/ili odgovore na proboje sigurnosti« (*Organisation for Economic Co-operation and Development*, 1992.: 28).

Da bi se obezbedila efektivna informaciona sigurnosti neophodan je sveobuhvatan pristup koji treba da razmotri mnogobrojne i raznovrsne sigurnosne aspekte unutar i van granica informacione sigurnosti. Ovaj pristup mora se primenjivati tokom čitavog »životnog ciklusa« sistema informacione sigurnosti.

Sistem informacione sigurnosti bazira se na sigurnosnim kotrolama čija efektivnost zavisi od odgovarajućeg funkcionisanja drugih kontrola (upravljačke, operacione i tehničke) koje, ukoliko su adekvatno

---

[7] Direktni troškovi nastaju usled nabavke, instalacije i administriranja sigurnostnih mera kao što je to npr. softver za kontrolu pristupa.

[8] Implementiranje sigurnosnih mera i implementacija bilo kog sigurnosnog rešenja uvek zahteva dodatnu obuku, što u krajnjem slučaju dodatno uvećava inicijalne troškove (indirektni troškovi).

izabrane, mogu imati sinergijski efekat. Sveobuhvatan i integrativni pristup u izgradnji sistema informacione sigurnosti podrazumeva, ne samo obuvatanje svih sigurnosnih aspekata poslovnog modela, već i pravilnog razumevanja međuzavisnosti sigurnosnih kontrola, jer one zapravo mogu »potkopavati« jedna drugu[9]. Osim toga, efektivnost sigurnosnih kontrola zavisi i od upravljanja sistemom, pravne regulative, nivoa pouzdanosti sistema i internih i upravljačkih kontrola. Na kraju, informaciona sigurnost, koja je podsistem računarske sigurnosti, »mora delovati zajedno sa tradicionalnim sigurnosnim disciplinama uključujući i fizičku i personalnu sigurnost« (NIST, SP 800-12: 13).

Efektivni i efikasni sistemi informacione sigurnosti deluju u okruženju koje je izuzetno dinamično; tehnologije i korisnici, podaci i informacije u sistemu, rizici i sigurnosni zahtevi su stalno promenljivi. Mnoge od tih promena deluju i na sisteme sigurnosti; razvoj tehnologija i mogućnost njihove primene radi uspešnije odbrane poslovnog modela, povezivanje na javne mreže, promene vezane za vrednosti koje se štite i uprotrebu informacija, pojavljivanje novih vrsta napada. S druge strane, razvoj novih tehnologija omogućio je da maliciozni korisnici i operatori sistema otkrivaju nove načine za namerno ili nenamerno premošćavanje ili probijanje sigurnosti. Osim toga, stroga primena procedura je retka, a same procedure mogu biti zastarele tokom vremena. S obzirom da promene u sistemu ili okruženju mogu kreirati nove ranjivosti, sigurnost nikada nije perfektna. Zato se implementirani sistem informacione sigurnosti mora održavati i povremeno preispitivati da bi se utvrdio stepen sigurnosnih efekata sistema na promene u okruženju.

Zaključna razmatranja

[9] Utvrđivanje međuzavisnosti sigurnosnih kontrola, u stvarnosti, je izuzetno komplikovan i težak proces. Često se može desiti da, usled nedostatka odgovarajućih treninga gde bi se zaposleni podučili kako i kada treba koristiti softvere za detekciju virusa, korisnici mogu primenjivati softver na neadekvatan način i prema tome neefikasno. Kao rezultat loše primene ovog softvera, korisnici mogu verovati da je njihov sistem bez virusa, a da ipak pri tome nenamerno dalje šire virus.

Poslovni modeli u mrežnom okruženju realizovali su prednosti koje su donele informacione tehnologije jer su ih stavili u funkciju stvaranja novih vrednosti usluga i proizovda usmerenih na realizaciju poslovnih ciljeva. Međutim, nije dovoljno samo implementirati ove tehnologije zbog prednosti koje one donose i zahteva digitalne ekonomije za njihovom primenom, već je neophodno kreirati sigurno e-okruženje u kojem su svi učesnici u poslovanju i komunikaciji potpuno zaštićeni. To je međutim, izuzetno kompleksan proces pun kompromisa i pažljivih analiza koje se baziraju na proceni vrednosti koja se želi zaštititi, na proceni ukupne ranjivosti sistema (koliki su ukupni rizici) i na kvantitativnom izražavanju maksimalnog nivoa rizika koji se mora prihvatiti. Apsolutna zaštita se ne može ostvariti (niti se ona očekuje od sistema sigurnosti), ali se doslednom primenom metoda i postupaka zaštite može znatno otežati njeno narušavanje, što i jeste glavni cilj svakog sistema primenjene zaštite. Kreiranje sigurnog e-okruženja jeste proces koji će omogućiti dalji razvoj modela na mreži odnosno dalji razvoj digitalne ekonomije.

Za modele u mrežnom okruženju, zaštita informacija na kojima se bazira celokupna poslovna aktivnost je krucijalno važna. Osim toga, stalna aktivnost i dostupnost sistema na mreži, kao i pouzdanost i sigurnost realizacije njegovih e-aktivnosti jesu osnovni sigurnosni zahtevi na čijim temeljima se grade sistemi informacione sigurnosti. E-poslovni modeli raspolažu određenom količinom tajnih i poverljivih informacija koje se moraju zaštititi ne samo dok su u procesu prenosa mrežom, već i u procesu čuvanja ovih podataka u bazama podataka. Zaštita ličnih podataka e-korisnika usluga ili e-kupaca obuhvaćena je strogim zakonskim regulativama, tako da su sigurnosni zahtevi modela, ne samo poslovna, već i zakonska obaveza.

Problem informacione sigurnosti u oblasti poslovanja u mrežnoj ekonomiji jeste jedan od najvažnijih problema s kojim se suočavaju svi poslovni sistemi koji izlaskom na mrežu postaju podložni skupu novih rizika i ranjivosti sistema. Poslovni modeli na mreži, kompleksni i po strukturi i po funkcionalnosti, zahtevaju sisteme informacione sigurnosti koji ne mogu biti jednostavani, već njihova koncepcija i struktura mora zavisiti od poslovnih funkcija i važnosti podataka koji su povereni

sistemu zaštite. Primena informacionih tehnologija za realizaciju tih specifičnih zahteva uslovila je neophodnost rešavanja sigurnosnih problema na »specifičnim tačkama« modela i izbor odgovarajućeg seta sigurnosnih kontrola koji je u skladu sa specifičnim, a ponekad i jedinstvenim sigurnosnim zahtevima modela. Analize već implementiranih sistema informacione sigurnosti modela koji realizuju značajne aktivnosti i imaju već dugogodišnja iskustva, pokazale su da sistemi informacione sigurnosti jesu adekvatni, pouzdani i efikasni samo ukoliko obuhvataju sve specifičnosti nekog modela.

Literatura

1. Đorđević G. (2007) Informaciona sigurnost – strategija zaštite senzitivnih podataka u svetu promenljivih rizika«, VII Međunarodna konferencija o elektronskoj trgovini i elektronskom poslovanju, E-trgovina, 18. – 20. april 2007, Palić, u zborniku radova - elektronsko izdanje
2. Đorđević G. (2007) *Sistemi informacione sigurnosti u poslovnim modelima mrežne ekonomije*, neobjavljena doktorska disertacija, Fakultet za trgovinu i bankarstvo, Beograd..
3. IBM (2005) »Introduction to Business Security Patterns«, *White Paper*.
4. Laudon C.K., Traver G.C. (2001) *E-Commerce: business, technology, society*, Addison-Wesley.
5. NIST (2012) »An Introduction to Computer Security: The NIST Handbook«, *Special Publication 800-12, jul 2002.*
6. Oltsik J. (2006) »The Time Has Come for Information-Centric Security« *Enterprise Strategy Group, White Paper, april 2006.*

7. Organisation for Economic Co-operation and Development (1992) »Guidelines for the Security of Information Systems«, Paris
8. Symantec (2014) »Internet Security Threat Report»
9. The Ponemon Institute (2013) »Cost of Cyber Crime Study: Global Report«, O*ctober 2013.*
10. UNCTAD (2005) »Information Economy Report«, *New York and Geneva*.
11. Whitmore J.J. (2001) »A Metod for Designing Secure Solutions«, *IBM*.

Gordana Đorđević

Security aspects of e-business models in a network environment

Abstrakt

The high degree of technological change which characterizes the modern economy and the intensive use of information and communication technologies have led to significant changes in the business environment. They have provided the conditions for the creation of an electronic business platform that enables better positioning of business systems in the global market, competitive advantage, higher profits and providing customer service in a more efficient manner. New business models that are created in the network environment become open and easily accessible to customers and service users but also to potential attackers that violate the integrity of the systems on the network. In such conditions, the construction of adequate protection systems in the form of information systems security are becoming an important part of managing business models in a network environment.

Keywords: information technology, digital economy, e-business, digital information, business models, systems of protection