

ZAŠTITA PODATAKA U INTERNET OKRUŽENJU

Doc. Dr. Stanislav R. Polić, ICTT, Beograd,
srp@ict-tower.com

Apstrakt: U zemlji se zaštiti poslovnih informacijau nije poklanjala posebna i dovoljna pažnja. Možemo konstatovati da poslovne informacije kod nas za sada nemaju pravi tretman i da se ne prepoznaju kao posebna realna vrednost. Takav prilaz poslu i poslovnoj politici je doveo do toga da su formirani IS kompanija uglavnom otvoreni i najčešće u potpunosti nezaštićeni. U većini naših kompanija, nemamo precizno definisano koji su podaci poslovna tajna, koji moraju imati naznaku "**strogo poverljivo**" i shodno tome podvrgnuto sistemu posebnih mera obezbeđivanja. Zahtevi menadžmenta za osmišljenom zaštitom podataka u našem okruženju praktično i ne postoje. Postojeća dosadašnja zaštita je na vrlo niskom nivou, uglavnom vezana za hijerarhijski prilaz pojedinim podacima putem lozinke, tako da u trenutku kada neko sa strane sazna lozinku, praktično ima otvoren sistem i sve podatke na raspolaganju. Internet komunikacija otvara mogućnost za takvu vrstu upada u poslovni IS kompanija. U svetu su razrađene posebne metode zaštite podataka, posebno baza podataka koje su otvorene ka Internetu. Takvom nivou zaštite se sve više podvrgava i redovna poslovna elektronska pošta kao i poslovne poruke koje se razmenjuju između poslovnih partnera u okviru elektronske trgovine.

Ključne reči: Bezbednost, upravljanje rizikom, zakonski propisi, elektronsko poslovanje

DATA SECURITY IN INTERNET ENVIRONMENT

Abstract: There is no special attention for business information security in our country. We may say that business information do not have real value here and that there is no right treatment for them. That kind of business and business politic shows us that company's IS are usually open and totally unsafe. In most of our companies, there is no defined which information is business secret, and which must have "confidential" mark and according to that which must be under specific security. In our business environment there are practically no demands from company management for specific data security. Security is on the very low level, usually connected with hierarchical access to information using a password. That means if someone from the side brakes the password, he'll be able to see and use all informations inside. Internet communication enables such kind of braking through into the business IS of companies. All over the world there are special methods for business security, especially data base security which are open to the Internet. Everyday e-mails, as well as business massages between business partners inside e-trading are under this kind of security.

Key words: Security, Risk control, Law, E-business

1. UVOD

Već duže vreme postoji politička volja da kao zemlja uđemo u Evropu, gde bi po svim realnim elementima trebalo da pripadamo. Sa druge strane moramo se zapitati da li smo tehnološki dovoljno pripremljeni za tu stvar? Da li poslovni i tehnološki standardi i zakonska regulativa, a pre svega naša poslovna praksa prate sve strožije kriterijume koje postavlja Evropska zajednica za ulazak? Da li je blagovremeno naš poslovni menadžment edukovan da primenjuje usvojena i/ili najavljena međunarodna pravila u poslovanju? To su pitanja na koja bi svi želeli da imamo pozitivan odgovor. Da li će odgovor biti pozitivan u mnogome zavisi od nas samih, naše organizacije i shvatanja trenutka u kome se nalazimo, želje i potrebe da se uhvatimo sa tim novim izazovima. Jedna jako široka oblast delovanja i zahtevane edukacije, čija primena predstavlja jedan od uslova ulaska u Evropsku zajednicu, a standardan je deo opšteg poslovanja je **bezbednost poslovnih podataka** u širem smislu tog pojma. Ova kategorija je posebno bitna u elektronskom poslovanju¹. U savremenom svetu, Internet sve više postaje stalan alat u funkciji redovnog poslovanja, on postaje sastavni deo poslovne infrastrukture, tako da poslovni subjekti sve veću pažnju poklanjaju obezbeđivanju kvaliteta i bezbednosti poslovanja u tehnološkom okruženju Interneta. Sageledavajući značaj novih tehnoloških mogućnosti, u svetu se kod prilaza tom problemu poklanja izuzetno velika pažnja. Australija je primer zemlje koja je to pitanje postavila na vrlo visok nivo i poklanja mu punu pažnju. Australiske vladine političke agencije¹ su posebno tretirale problem poslovanja na Internetu, povezujući ostvarena rešenja sa zahtevima bezbednosti i revizije. Trenutno se u svetu mnoge revizorske agencije bave problemom bezbednosti informacija. Jedna od njih je ANAO² koja pomaže opštoj revizorskoj praksi donoseći posebne normativne akte koji regulišu između ostalog i problematiku bezbednosti podataka. Jedan od normativa je publikovan 1997 godine u kome se podvlači značaj obezbeđivanja zahtevanih performansi revizije i finansijskih obračuna. U aktu se zahteva da prikazi budu revidirani od strane posebnih tela javnog sektora vlade da bi se obezbedilo nezavisno izveštavanje za parlament, vladu i zajednicu u celini. Naslov ovog izveštaja je: Bezbednost Interneta unutar vladinih agencija³. Da bi u potpunosti sagledali ovu problematiku, interesantno je razmotriti koji su pripadajući rizici na Internetu. Uočljivo je da rizici po bezbednost podataka i obrada na Internetu stalno rastu, kako u samoj Australiji tako i šire. Ti rizici, odnosno pretnje po bezbednost podataka koje se manifestuju kroz svojevrsne "incidente" nastaju iz različitih razloga⁴. Najčešće kompjuterski "hakeri"⁵ pokušavaju da iskoriste svoja znanja iz oblasti operativnih sistema, aplikacija i komunikacionih protokola da ostvare neautorizovane pristupe i preuzmu kontrolu nad informacionim sistemima kompanija. Neki hakeri pristupaju bez malicioznih namera, isključivo sa ciljem da zadovolje svoju taštinu i testiraju svoje programerske veštine. Međutim, drugi, jasno napadaju informacioni sistem sa malicioznim i kriminalnim namerama i mogu načiniti značajnu štetu u svojoj "pobedi" nad žrtvom. Nastala šteta se može rangirati od nezgoda na

¹ Commonwealth Government Agencies.

² Australian National Audit Office.

³ Internet Security within Commonwealth Government Agencies.

⁴ Australijski kompjuterski tim za odgovor na opasnost - Australian Computer Emergency Response Team (AusCERT), kao deo globalne mreže kompjuterske bezbednosti je analizirao statistiku Internet sigurnosti. Jasan je trend povećanja prekida u proteklom godinama. U nastavku se daje broj incidentnih prijavljenih slučajeva u Australiji u periodu od 1996 do 2000 godine. Izvor AusCERT, 2001 godina 1996 1997 1998 1999 2000 incidenti sukcesivno; 309, 572, 1342, 1816, 8197. Do sličnih rezultata tokom svog istraživanja je došao i kordinacioni centar za izveštavanje o bezbednosti i incidentima u USA - CERT Coordination Centre reports u periodu 1996 – 2000 godina, izvor CERT/CC, Incidents reported: 2001 godina 1996, 1997, 1998, 1999, 2000 incidenti sukcesivno; 2573, 2134, 3734, 9859, 21756.

⁵ **Hacker** kao termin postoji u dve namene: **Pozitivan** za programera koji uspešno i brzo rešava sve kompjuterske programe i **pežorativan** – negativan koji označava "kompjuterskog lopova" odnosno programera koji deluje kao maliciozni nametljivac i koji pokušava da otkrije osetljive podatke probijajući se kroz mrežu. Odatle nastaju nazivi "**password hacker**", haker koji otkriva lozinku i "**network hacker**" haker koji deluje u mreži. Originalni engleski naziv za ovaj termin je (eng. cracker). Izvor wikipedia.

samom websajtu kompanije do ugroženosti ili neautorizovanih puštanja u opticaj poslovnih informacija i korišćenja kompjutera u pripremi ugrožavanja web sajtra putem drugih kriminalnih radnji.

2. UPRAVLJANJE RIZIKOM

Mnoge zemlje u svetu su definisale politiku upravljanja rizicima vezano za svoje informacione sisteme. Australija je jedna od njih. Samo priključenje na Internet može da predstavlja novi i nešto različitiji skup rizika u odnosu na dosadašnje situacije. U svetu, kompanije, Vladina odeljenja i agencije imaju tradicionalne zahteve za upravljanjem bezbednošću sredstvima informacionog sistema, bilo da su memorisana elektronski ili na neki drugi način. Proces i postupci upravljanje savremenim rizicima može da bude preduzet kroz različite načine. Neke od elementa dosledne i kvalitetne primene upravljanja rizicima se najbolje uočavaju na praktičnim modelima. To uključuje:

- analizu mogućih pretnji, rizika i procena za agencijske Internet prezentacije,
- razvoj i planiranje Internet "gateway-a"⁶ politike bezbednosti,
- detaljan odgovor na incidente i kontinuirano planiranje poslovanja,
- uključivanje izveštajnih mehanizama u upravljački sistem,
- povećanje svesnosti osoblja i obavljanje pogodnih i detaljnih treninga,
- utvrđivanje odgovornosti osoblja za upravljanje i implementaciju bezbedonosnih mera.

Takvi upravljački "alati" mogu biti zastupljeni i primenjeni unutar različitih organizacionih struktura i situacija da bi se efikasno upravljalo pripadajućim rizicima unutar Interneta. ANAO prepoznaje da značajan broj Vladinih departmenta i agencija u Australiji već sada imaju mere koje su poverene specijalizovanim kompanijama na izvršavanje, takozvani outsourcing⁷ rad, vezano za svoje IT infrastruktura. Priručnik Vlade Australije za zaštitu bezbednosti⁸ podržava stav da jedna agencija ili odeljenje mora zastupati stav za primenu čvrstih upravljačkih odluka za ultimativnu odgovornost za bezbednost vladinih informacija. Pri tom odgovornost ostaje na odgovarajućim relevantnim sekretarima ili šefovima i izvršnim rukovodiocima zaposlenih u Agencijama. Sama funkcija bezbednosti može biti delegirana na "outsorce" rad **ali odgovornost ne može**. Važno je napomenuti da agencije ili odeljenja koja imaju primenjena "outsorsing" rešenja na deo ili ukupnu Internet prezentaciju su sposobna da koristi iste menadžment alate i da ostvare iste efekte zaštite kao da funkcionišu u kući (eng. in house). U "outsorsing" situacijama, menadžment pripadajućeg rizika u jednoj Internet prezentaciji postaje sastavni deo u ugovornom menadžmentu. Sama politika bezbednosti mora biti kreirana od strane ugovarača ili Vladine agencije, međutim, ultimativna odgovornost za zaštitu informacija leži na agencijskom vrhu, Agencije bi trebalo da efikasno upravljaju posredstvom ugovarača zaduženim za "outsorsing" rad koji je dužan da isporuči izlaze i rezultat koji će predložiti kroz definisanu politiku i projektovane procedure. Određena iskustva, mada nedovoljna, postoje na planu zaštite i kod nas i obavljaju se kroz rad sa VPN⁹-om, odnosno tehnološkim rešenjima u kojim se stvara poseban "kriptografski tunel" kod razmene podataka između dve mreže putem Interneta. Taj metod, je moguće primeniti u kompanijama u kojim postoji više dislociranih mreža. Međutim, dosadašnji transfer podataka između mreža unutar jedne

⁶ **Gateway** –prioritetan termin za ovaj pojam je "eng. protokol converter", pretvarač protokola odnosno priključenje mreža koje koriste različite protokole. Izvor rečnik foldoc.

⁷ **Outsourcing**; plaćanje nekoj drugoj kompaniji da obezbedi servis ili uslugu koju kompanija može inače da obavi sama, zapošljavajući svoje sopstveno osoblje, na primer, razvoj softverskih rešenja. Izvor rečnik foldoc.

⁸ Commonwealth Protective Security Manual – Priručnik komonvelta, veza za zaštitu i bezbednost.

⁹ **VPN** – Virtual Private Network – Privatna virtuelna mreža – formirana posebno, pod Linux operativnim sistemom uslovno rečeno "**privatni tunel**" kroz Internet mrežu koji obezbeđuje sigurnu jeftinu razmenu podataka koja je kriptografski zaštićena od napada spolja (prema elektronskom rečniku **foldoc**).

kompanije se najčešće vrši klasičnim komutacionim linijama, odnosno fajl transferom, bez ikakve zaštite. Procenjujemo da će na našim prostorima vrednost poslovnih podataka sve više da dobija na značaju sa povećanom konkurencijom i da će poslovni podaci dobijati određenu tržišnu vrednost. Samim tim će učestati napadi na postojeće informacione sisteme kompanija. U praksi se već sada prodaju "ilegalno" prikupljene liste poslovnih e-mail adresa. Posebnu cenu u kriminalnim radnjama imaju brojevi elektronskih kartica za plaćanje. Sve ovo upućuje da se određene baze podataka u poslovnim sistemima moraju posebno zaštititi. Bez malo u svim definisanim poslovnim linijama, posebno u poslovnim linijama koje su namenjene ASP¹⁰ poslovanju, moraju se sprovesti rigorozne mere zaštite. Procenjujemo da će samo softverska rešenja koja korisnicima garantuju apsolutnu zaštitu poslovnog integriteta i sigurnost u radu, dugoročno imati prođu na našem tržištu. Smatramo da se ovom problemu mora prići krajnje ozbiljno i profesionalno i da kompanije moraju detaljno razraditi sopstvene modele kriptografske zaštite kao svoj standard, kako u zaštiti sopstvenih baza podataka tako i u zaštiti pojedinih softverskih rešenja koja imaju plasman kroz ponuđene informatičke usluge na tržištu. Bezbednost podataka predstavlja jednu od investicija koja je u ovom trenutku nužna i koja u prvom trenutku ne može doneti direktni finansijski efekat. Međutim, može se očekivati da će stečeno znanje iz ove oblasti naći svoje potencijalne kupce pre svega u velikim poslovnim sistemima koji ovom poslu nisu blagovremeno prišli, a imaće potrebu da se u relativno kratkom vremenu adekvatno zaštite. U tom trenutku može doći do pune komercijalizacije tako formiranog znanja, ali, nažalost, to ne treba očekivati u skorom vremenskom periodu.

3. ISTORIJAT PROBLEMA BEZBEDNOSTI NA INTERNETU

Tokom 1988 godine pojavljuju se prvi put stvarni bezbedonosni problemi u mreži Interneta, poznati pod nazivom "Crv Interneta", odnosno "eng. Internet worm". Tada se u svetskoj štampi pojavljuju mnogi novinski napisi kao što su "crv na Internetu", "crv je pušten sa uzice" i slično. Šta je zapravo "crv" ili sada odomaćeni popularni naziv "kompjuterski virus". To je destruktivni program čije izvršavanje izaziva negativne posledice po rad računara. Njegova namena je da onespособi rad računara, odnosno izvrši brisanje memorisanog softvera i korisničkih podataka. Karakteristika virusa je da se ilegalno, kao svojevrsan "Trojanski konj"¹¹ prenosi putem Interneta. Bez obzira na pojavu uočenih problema izazvanih "virusima" i "crvima" masovno korišćenje Interneta uzima sve više maha. Sa druge strane, uz pojavu sporadičnih bezazlenih problema, istovremeno nastaju i prvi ozbiljniji problemi. Dolazi do prve pojave "hakera" koji svesno ugrožavaju privatnost učesnika u mreži Interneta. Suočeni sa tim problemima, počinje borba za zaštitu i privatnost u digitalnom svetu. Kao interesantan primer navodimo da je 01.11.1998 jedan "Internet worm" privremeno onespособio za rad preko 6.000 računara od 60.000 hostova koji su tada bili prikačeni na mrežu Interneta.

¹⁰ **ASP** - **A**pplication **S**ervice **P**rovider – servis, odnosno usluga koja se obezbeđuje pristupom sa udaljene lokacije u jedan aplikacioni program kroz mrežni protokol. Izvor rečnik foldoc.

¹¹ **Trojan horse: Neologizam**, pojam razvijen od strane Massachusetts Institute of Technology MIT. Hakersko postavljanje **National Security Agency** (NSA) aveti Dan Edvards. Maliciozni bezbednosni prekid programa koji je prerušen kao nešto dobroćudno, benigno, nešto kao izlistač direktorija, arhiva ili igara, ili (u jednom poznatom ozlogašenom primeru iz 1990 godine na kompjuterima MAC) programa koji nalazi i razrušava – uništava viruse) Trojanski konj je sličan kao **backdoor**.

Izvor: www.worldwideschool.org/library/books/tech/computers/TheHackersDictionaryofComputerJargon

3.1 Problem bezbednosti

Obezbeđena celovita zaštita u elektronskom poslovanju je zapravo preduslov rada elektronskog poslovanja. Bezbedan rad može da bude ugrožen sa više strana, a menadžment kompanija mora da bude upoznat sa mogućim problemima na koje može delovati određenim organizacionim merama.

- **Zlonamerni udari unutar korporacije:** Svetska praksa pokazuje da menadžment mora da preduzme mere da se zaštiti od nesavesnih radnji svojih službenika. Na to ukazuju i revizorski standardi koji predviđaju i zahtevaju čitav niz mera koje su potrebne da se sprovedu kako bi obrada u okviru informacionog sistema korporacije, pa i u okviru elektronskog poslovanja bila maksimalno zaštićena. Bilo bi idealno, da se naročito u velikim korporacijama uspostavi **posebno koordinaciono telo** na vrlo visokom hijerarhijskom nivou, koje bi povremeno (najmanje jednom mesečno) analiziralo ugroženost informacionog sistema i elektronskog poslovanja i preduzimao potrebne preventivne mere zaštite u skladu sa svetskim trendovima.
- **Kompjuterski »virus« koji napada PC:** Sadašnji informacioni sistemi su sada najčešće postavljeni na personalnim računarima. Ovakva tehnološka postavka ih izlaže napadima od strane "hackera" koji fabrikuju kompjuterske "vire", koji uništavaju programe i podatke na kompanijskim diskovima. Savetuje se menadžmentu kompanija da preduzmu mere korišćenja antivirus programa poznatih svetskih kompanija i da ih ažuriraju na dnevnoj osnovi.
- **Zlonamerni udari spolja u IS:** Informacije koje su memorisane u računarima kompanije postaju meta napada konkurencije u cilju dolaženja do podataka o kretanju poslovanja i dugoročnim strateškim planovima. Popularan savremeni naziv za takav vid napada konkurencija je najčešće "industrijska špijunaža". Menadžment određenim merama preventivne zaštite, pre svega lozinkama, kriptografijom, kao i fizičkim obezbeđenjem, uz analizu pristupa pojedinim strateškim podacima (ko je pristupio, sa kog telefona, sa kog računara, u koje vreme) može da obezbedi potrebnu zaštitu.

Kao rekapitulativni pregled osnovnih bitnih elementa koji moraju biti ugrađeni u bezbedonosnu politiku kompanije, sa ciljem da se maksimalno obezbede poslovne transakcije spada rešavanje pitanja:

1. Poverenja,
2. Privatnosti,
3. Autentičnosti,
4. Neporicanja.
5. Integriteta,
6. Enkripcije.

Da bi ubrzala svoje elektronsko poslovanje i obezbedila bezbednost u radu kroz razvoj opšte identifikacije i poverenja, plaćanje i trgovačke standarde koji su interoperabilni, Australija je pristupila korišćenju Identrusa¹² i u sklopu toga je primenila sve potrebne propozicije kod primene "Business to Business – B2B"¹³ tehnologije. Samim tim ona omogućava svojim članovima da isporuče totalno integrisano

¹² **Identurs** - konzorcijum opštih finansijskih institucija formiran da olakša povećanje bezbednosti B2B i B2C elektronskog poslovanja. "Identrus" rešenja počinju sa prihvatanjem standarda PKI tehnologije za proveru autentičnosti i bezbednosti transakcija. Međutim to je mnogo više nego kolekcija tehničkih rešenja. Identurs je kompletna infrastruktura za pomoć kompanijama da efikasno i bezbedno funkcionišu na Internetu, kroz međunarodne ekonomske i političke granice, sa prisnim poslovnim partnerima i novim individualcima. Tehnologija koju uključuje Identrus rešenja obuhvata: PKI zasnovanu krypto-bezbednost digitalne identifikacije i u realnom vremenu proveru potrebnih identiteta.

¹³ **B2B - Busness to Busness** – Poslovanje ka poslovanju. Pod ovim pojmom se podrazumeva potpuno drugi filozofski pristup u poslovanju, odnosno radu. Primena B2B tehnologije napušta interfejs "čovek – računar" i prihvata kao standard interfejs "računar – računar". Naime, formirana otpremnica u jednom računaru predstavlja validan autorizovani dokumenat za automatsko formiranje prijemnice u drugom računaru (prema elektronskom rečniku **foldoc**).

neposredno rešenje za oba aktera i za kupca i za prodavca. Pri tom su definisani osnovni kriterijumi koji moraju da se ispune i to:

- Autentičnost,
- Neopozivo plaćanje,
- Uslovno plaćanje (po izvršenoj isporuci),
- Garancija plaćanja,
- Neposredno neopozivo trenutno plaćanje,
- Datum budućeg plaćanja (pri čemu se podrazumevaju normalni trgovački termini),
- Usaglašenje.

Sistemi informacionih tehnologija su u praksi najčešće vrlo pouzdani, ali slično svemu drugom i oni mogu biti subjekt nepredviđenih događaja. Kada se dogodi nepredviđeni događaj, korisnik se nalazi pred situacijom da ono, u šta su svi verovali da je dostojno poverenja, odnosno Informacioni sistem kompanije, postane neupotrebljiv. U takvim situacijama korisnici moraju da budu sposobni da nastave redovno poslovanje za vreme perioda neupotrebljivosti računara, odnosno informacionog sistema, što može biti od nekoliko sati, dana, a prema primerima iz prakse i do nekoliko meseci. Treba imati u vidu da uzrok duže neupotrebljivosti sistema informacionih tehnologija može biti vrlo redak, ali kada se to desi, on može biti katastrofalan po organizaciju, ako nisu načinjene planske, unapred potrebne mere predostrožnosti. Potreba za pouzdanošću informacionih tehnologija se svakim danom povećava. U modernom poslovanju postoji malo oblasti koje su bez uslovljenosti od strane informacionih tehnologija i koje neće trpeti posledice ako su njegove performanse pogoršaju. U kompanijama se potencijalni rizik primene Informacionih tehnologija stalno povećava i postaje sve više raznolik po svom uzroku, na primer; korisnici informacionih tehnologija sada imaju situaciju da se suočavaju sa rizikom od dejstva hakera, infekcije "kompjuterskih virusa", destruktivnim industrijskim akcijama uperenim neposredno od strane sopstvenog nezadovoljnog kompjuterskog osoblja ili drugih insajdera. Kako se važnost kompjuterske obrade unutar poslovne organizacije kontinuirano povećava, tada su efekti mogućeg prekida kompjuterskog sistema, potencijalno višestruko štetni. Pored toga, korišćenjem globalne svetske mreže, kompjuterski sistemi se povećano izlažu potencijalnim pretnjama od napada hakera i ulaska kompjuterskih "virusa". Za vreme trajanja smanjenja vremena rada Informacionog sistema u Kompaniji, može se očekivati da eskalira gubitak u Kompaniji. Zato je neophodno da se vreme kada je kompjuter, odnosno Informacioni sistem neupotrebljiv, svede na minimum. Planiranje nepredviđenih situacija je proces u okviru kojeg menadžment kompanije priprema da radi sa jednim neplaniranim događajem koji je izazvao katastrofu i prekid u radu. U terminu informacionih tehnologija to najčešće znači gubitak ili trajnu dužu neupotrebljivost kompjuterskog sistema. Kako se stepen kompjuterizacije unutar jedne organizacije stalno nastavlja i povećava, tako su efekti mogućeg "ispadanja" (eng. breakdown) kompjuterskog sistema potencijalno mnogo opasniji događaji. Pored toga, izlaskom Kompanija na Internet, povećana je izloženost kompjuterskog sistema od drugih potencijalnih pretnji.

3.2 Bezbednost i zakonski zahtevi u svetu

Informacioni sistem u okviru organizacije bi trebalo da bude permanentno nadgledan da bi se obzbedilo da on može maksimalno efikasno da nastavi svoj kontinuirani rad i da se osigura da se on povinuje sa prisutnom relevantnom zakonskom regulativom. Pored toga, monitoring informacionog sistema bi trebalo da proveriti da li je on bezbedan na pretnje kao što su virusi i hakeri. Svi potencijalni modaliteti ovih problema su razmatrani imajući u vidu zakonodavstvo koje postoji u

Velikoj Britaniji, koja je vrlo daleko otišla definišući zakonske okvire zaštite. Pri tom ćemo ukazati na dva osnovna zakona – Akta iz te oblasti:

- *Akt - zakon o kompjuterskim zloupotrebama iz 1990 godine*¹⁴
- *Akt - zakon o zaštiti podataka iz 1998 godine*

Zakon o zaštiti podataka u Velikoj Britaniji je inicijalno uveden 1984 godine zbog dva osnovna razloga:

1. da djeluje nasuprot pretnjama na privatnost podataka. Pretnje su uzrokovane zbog povećane sposobnosti kompjutera da zadrži, transferiše i obrađuju personalne podatke pojedinaca. U okviru ovoga, možemo usvojiti kao definiciju da: ***personalni podaci pojedinaca predstavljaju informacije o individualnim licima***,
2. da omoguće Velikoj Britaniji da zadovolji svoje obaveze na ovom planu i da ratifikuje konvenciju o zaštiti podataka, koja je doneta od strane Evropske Unije¹⁵. Kada primena zakona postane potpuno operativna, ova konvencija će omogućiti zemljama koje su je potpisale da **odbiju transfer podataka drugim zemljama** koje nemaju ekvivalentne zaštitne zakone vezano za zaštitu podataka.

Pomenuti zakon, odnosno akt Velike Britanije je dopunjen posebnim amandmanima 1998 godine. Novi dopunjeni zakon je počeo da se primenjuje od marta 2000 godine. Dopuna pomenutog zakona se odnosi na posebne zahteve kojim se države Evropske Unije moraju povinovati, u skladu sa direktivom Evropske Unije o zaštiti podataka¹⁶, a vezane su za proširenje obima zakonske regulative koja se više ne odnosi samo na kompjuterski memorisane slogove personalnih podataka, već isto tako i na ručno formirane evidencije.

3.3 Ostvrt na svetska iskustva mera bezbednosti u elektronskom području

U situaciji kada kao zemlja nemamo dovoljno iskustva vezano za mere bezbednosti u elektronskom poslovanju i Internet okruženju, a u cilju sagledavanja složenosti problematike i potrebnih mera koje treba preduzeti u ovoj oblasti, korisno je pogledati prilaz problematici bezbednosti podataka u razvijenim zemljama. U tom smislu interesantan je izveštaj koji je publikovan u Velikoj Britaniji početkom ove godine, pod nazivom "Bezbedonosni izveštaj, februara 2006 godine o potencijalnim krađama online identiteta"¹⁷.

3.3.1 Kratak pregled situacije

U Velikoj Britaniji postoji preko pet miliona broadband¹⁷ korisnika. Potrošači su povećali korišćenje Interneta da bi svoj život učinili lakšim kroz priključenje na svakodnevne zadatke, takve kao što su bankarske operacije i nabavka u online režimu rada. Otprilike jedna petina ljudi u Velikoj Britaniji većinom rade svoje bankarske transakcije preko Interneta, naročito počev od 2005[ⁱⁱⁱ]. godine. Međutim, potrošači su još uvek nesvesni pravog rizika u tom radu koji dolazi kako od novih tako i od postojećih pretnji pa često drže "glavu u pesku" ili komentarišu "to se nikad nije desilo

¹⁴ **UK Data Protection Act** – Zakon o zaštiti podataka Velike Britanije

¹⁵ **Council of Europe Data Protection Convention**, Kongres saveta Evrope o zaštiti podataka

¹⁶ **EU's Data Protection Directive** – Direktiva odnosno zakon Evropske Unije o zaštiti podataka

¹⁷ **Broadband** - Klasa komunikacionih kanala sposobna da podrži širok rang frekvencija, tipično za audio i video frekvencije. **Broadband** kanal može preneti višestruke signale kroz deobu ukupnog kapaciteta u višestruke, nezavisne bandwidth kanale, u kojem svaki kanal funkcioniše sam na specifičnom rangu frekvencije. Termin je počeo da se koristi za bilo koju vrstu Internet konekcije sa download brzinom većom od 56 kilo boda. Izvor rečnik foldoc.

meni" uprkos tome što cyber¹⁸ kriminal postaje glavni predmet stručnih debata vezanih za rad kompjuterskih mreža, znatno više nego što je poslednjih godina bilo rasprava o problemu droge^{iv}].

Studija pokazuje da preko 62 procenta potrošača u Velikoj Britaniji misli da online pretnje ne mogu da se dogode njima, a preko 40 procenata kaže da oni nisu svesni da li su već postali žrtve online pretnji ili ne. Od ukupnog broja anketiranih, jedan u deset slučajeva takođe ukazuje da on ne treba da ima sumnju oko davanja svojih detalja kreditnih kartica jednoj ne identifikovanoj trećoj strani^v]. Sigurno da kriminal na Internetu nije vezan samo za kreditne kartice. Glavne nove i brzo šireće pretnje su online krađe identifikacionih podataka, što znači da mnogi Internet korisnici koriste ukraden identitet, ilegalno, bez znanja individue kao žrtve. To je jedan od najbržih oblika povećanja pretnji u Velikoj Britaniji. Procenjuje se da osam procenata korisnika PC-ja u Velikoj Britaniji zapadaju kao žrtve ovih online pretnji a 15 procenata znaju nekoga koji je bio meta od strane Internet kruiminala^{vi}]. Ovakav trend porasta krimanalnih aktivnosti posredstvom Interneta predstavlja ozbiljan problem za Internet korisnike, sem ako se oni nisu edukovali i postali sposobni da se sami zaštite od uzroka pretnji i njihovih mogućih posledica. Krađa online identifikacije takođe postavlja rizik daljeg nastavka usvajanja Interneta kao kanala za kompanijsku i potrošačku interakciju. U borbi protiv krađe identiteta treba da se postavi jasan cilj delovanja, a to je potreba da se osposobe neposredni potrošači i da se oni udruže u borbi protiv krađa identiteta. Potrebno je ozbiljno oceniti sadašnji trend povećanja ovog problema tako da vlada Velike Britanije, sve proizvodne delatnosti i neposredni potrošači moraju da rade zajedno da bi pronašli pravo rešenje ovog problema. Izveštaj o bezbednosti, prvi u ovoj seriji, svodi primenjivanje raznih profesionalnih veštine, iskustva, istraživanja vlade, primenjivanje zakona u industriji i agencijama, uključujući u to BT, CPP, Get Safe Online, Lloyds TSB, Metropolitan Police i Yahoo!. Svi ovi učesnici bi trebalo da ocene koje su sve vrste krađa online identiteta moguće, tekuću situaciju i gde mi kao društvo u celini idemo u ovoj oblasti, pre svega kao krajnji korisnici kao i pokušaj industrija da smanji taj rizik.

3.4 Krađa identiteta

Krađa identiteta (ili nepersonalizovanih prevara) bilo da se radi o online ili offline režimu rada, je zloupotreba identiteta "žrtve", takvih kao što je (ime, podatak o rođenju, tekuća adresa ili prethodna adresa) od strane druge osobe, bez znanja ili saglasnosti "žrtve". Dobiti neke personalne detalje nije kriminalni prekršaj, ni kreiranje falsifikovanog računa usluge ili bankarskog obračuna koji može da se koristi kao dokaz da ste vi ta osoba. Jedan prekršaj je samo izvršavanje kada neko pokuša da koristi ukradeni identitet da bi obezbedio robu ili uslugu – utvrđeno kao krađu. Utvrđena prevara je mnogo više opšta nego što mnogi ljudi misle, kod dela društva u Velikoj Britaniji odrasle osobe su bile žrtve takvih prevara ili su znale nekog ko je bio takva žrtva^{vii}] u saglasnosti sa CIFAS^{viii}, postoji 137.000 slučajeva tokom 2005 godine što predstavlja povećanje od 14 procenata u odnosu na 2004 godinu. Ministarstvo unutrašnjih poslova Velike Britanije procenjuje identitet prevara sa troškom od 1,7 milijardi funti ili 35 funti po prevarenoj odrasloj osobi^{ix}] godišnje, upoređujući to sa 1,3 milijardi funti u 2002 godini. Postoje brojni načini u kojem identitet može da bude ukraden a najopštiji primeri su:

- **Bin raiding - kanta za đubre i iznenadni napad;** neobučen prevarant pretražuje dokumenta kao što su bankarski obračuni, on koristi račune ili čak staru poštu koju

¹⁸ **Cyber** - computers and information systems, **Cyber** je prefiks koji potiče od pojma cybernetics (kibernetiski) i slobodnije znač direktno korišćenje kompjutera.

je korisnik bacio u đubre van kuće. Dobijene informacije mogu da budu korišćene da bi se primenile lažne kreditne obaveze na korisničko ime.

- **Phishing¹⁹ – vrbovanje;** publikovanje "varljivog" e-mail koji se pravi kao da je napravljen od korisničke banke u kojem se pita za korisničke detalje bankarskog računa. Čim se dobiju ti detalji oni se koriste kao operativni podaci za prevaru na korisničkom računu.
- **Skimming - brzi pregled;** estrahovanje kartice za plaćane korišćenjem jedinica spojenih na mašine za gotovinu ili kopirane od strane beskrupoloznih individua sa pristupom na kredit/debit karticama, na primer, to radi ili dozvoljava da se uradi osoblje u restoranu ili benzinskim pumpama.
- **Moving house - pokretna kuća;** klasična pošta se još isporučuje na vašu staru adresu i ona se može koristiti da se podese lažni finansijski ugovor na vaše ime.
- **Social engineering - Socijalni inženjering;** nepažljivo obelodanjena personalnih informacija kroz prevaru. (ovde markirani tekst treba izbaciti)

Međutim, sa javnom svesnošću o opasnosti **krađe identiteta**, broj krađa se povećao tokom 2005 godine, publicitet se usmerio uglavnom na rizike postavljene od strane offline prevara, takvih kao što su prebacivanje identifikovanih dokumenata kao na primer korišćenih računa u kantama za smeće. Skoro 90 procenata povećanja prodaje mašina za uništavanje poverljivih dokumentu tokom 2005 godine pokazuje koliko dobro "ste iseckali dokumente" izveštava ministarstvo unutrašnjih poslova Velike Britanije, policija i industrija koja je postala promoter tih uređaja. Međutim, ukradena dokumenta iz ljudskog smeća je samo jedan od načina na koji kriminal može ukrasti vaš identitet. Personalni detalji mnogih individua mogu mnogo lakše da budu ukradeni korišćenjem Interneta nego offline rada.

ZAKLJUČAK

Razvoj informacionih tehnologija, posebno Interneta, zahteva blagovremeno prilagođavanje poslovnog okruženja, pa i revizije novim uslovima rada. Elektronsko poslovanje je to koje pred menadžment postavlja čitav niz novih zahteva, kako bi odgovorili izazovima novih tehnologija. Primer mera koje preduzima vlada Australije je indikativan i ukazuje kako organizovano treba prići tom problemu. Obzirom da je elektronsko poslovanje definisano kao strateški cilj naše zemlje i naši menadžeri bi trebali blagovremeno da pristupe pripremi kako bi kvalitetno i kvalifikovano odgovorili novim izazovima.

LITERATURA

1. ACCA (Association of Chartered Certified Accountants) – Information Systems – December 2004 – January 2005.
2. Dr. Stanislav R. Polić, Revizija i bezbednost u internet okruženju. Revizor, 19-20, 2002 Beograd
3. Jaap Akkerhuis, NlnetLabs, Daniel Karrenberg, RIPE NCC, Internet Security An "Edgy" Business
4. Bruce Schneier, Managed Security Monitoring: Closing the Window of Exposure, Counterpane Internet Security, 2000.

¹⁹ **Phishing:** vrbovanje, Etymology: promena (uticaj od strane osobe koja dobija ilegalan pristup u telefonski sistem) u pecanju, prevara u kojoj je jedan e-mail korisnik prevaren u obelodanjivanju personalnih ili poverljivih informacija koje prevarant može da koristi nezakonito. (izvor merriam webster online)

Endnotes:

ⁱ Izvor: DR. Stanislav R. Polić, Primena zaštite podataka u Internet okruženju, časopis Računovodstvo 9-10 SRRS, Beograd.

ⁱⁱ Korišćen članak sa Interneta, Security Report Online Identity Theft February 2006, www.btplc.com/onlineidtheft/onlineidtheft.

ⁱⁱⁱ Izvor: Lloyds TSB, January 2006, from a Tickbox.net survey of 1,000 people during December 2005.

^{iv} Izvor: Valerie McNiven, US Treasury advisor, November 2005.

^v Izvor: MasterCard Europe, December 2005.

^{vi} Yahoo! Security Report, June 2005.

^{vii} Izvor: Which? Magazine, March 2005.

^{viii} Izvor: CIFAS, December 2005, CIFAS Credit Industry Fraud Avoidance Scheme (UK), UK's Fraud Prevention Service.

^{ix} Izvor: Home Office, February, 2, 2006.