IT UPRAVLJANJE U KONTEKSTU KOMPJUTERSKOG KRIMINALA

Prof. Dr Milorad K. Banjanin, e-mail: bozomiko@eunet,yu
Fakultet tehničkih nauka Univerziteta u Novom Sadu
Goran Drakulić, dipl. ing.stipendista MNZŽS Republike Srbije

Apstrakt: *Informacioni sistemi imaju sve veći strategijski značaj, a intenzivnijim korišćenjem Interneta, ekstranetova i intranetova od strane organizacija povećava se i pitanje sigurnosti informacionih sistema. Frekventnost i veličina aktivnosti kompjuterskog kriminala je u rapidnom porastu pa je teško i skupo postavljati zaštitu protiv svih mogućih pretnji za IT sisteme, zbog toga je neophodno obavljati analize ekonomičnosti pre donošenja odluke o tome koliko i koje kontrole treba usvojiti.*

Ključne reči: *Informacioni resursi, Informacione tehnologije, Odeljenje informacionih sistema, Kompjuterski kriminal i Informaciona sigurnost.*

Abstract: *Information systems have growing strategic importance, and with intensive use of Internet, extranets and intranets by organizations there is increase in security of information systems. Frequency and size of computer crime activities are in rapid growth so it is difficult and expensive to protect against all possible threats to IT systems, therefore, it is necessary to use cost-benefit analyses to decide how many and which controls to adopt.*

Key words: *Information Resources, Information Technologies, Information System Department, Computer Crime and Information Security.*

1. Uvod

Većina velikih, mnoge srednje čak i neke male organizacije širom sveta su organizaciono i tehnološki orijentisane na IT-a, a njihovi informacioni sistemi (IS) imaju veliki strategijski značaj. Informacioni sistemi se koriste u cilju povećanja produktivnosti i kao pomoć u postizanju odgovarajućeg kvaliteta i zadovoljstva kako zaposlenih tako i kupaca. Svi informacioni resursi, uključujući kompjutere, mreže, programe i podatke, podložni su nepredvidivim napadima koji dolaze iz njihove okoline. Odbrana od tih napada je i funkcionalna vrlo teška i/ili skupa, iako su danas sagledane i dobro poznate razne varijacije metoda za napad i odbrane od istih. Pored toga, mnoge zemlje nemaju dovoljno dobru zakonsku infrastrukturu koja bi omogućila poželjan uspeh u borbi sa kompjuterskim kriminalcima. Zbog svega ovoga, zaštita umreženih sistema je u suštini veoma kompleksna.

Na godišnjem nivou analize registruje se veliki broj glavnih napada različitim virusima kao i stotine drugih vrsta manjih napada. Svi vidovi napada prouzrokuju velike pričinjene štete kako organizacijama tako i individuama (Ričardson, 2003.). Prema Turban-u (2006), ,»1. Januara 2000. godine svet je shvatio da je šteta na informacionim sistemima usled YK2 problema minimalna. Ipak, samo nakon šest nedelja, u novom milenijumu dolazi do kriminalnih napada na kompjuterske sisteme. Frekventnost i veličina ovih napada kao i drugih sajber kriminalnih aktivnosti je u rapidnom porastu, što direktno ugrožava blagostanje Interneta i e-poslovanja. [10]

Uticaj ljudi ili prirode može da dovede do ponašanja informacionih sistema (IS) drugačijeg od onog koje je planirano. Važno je imati ovo u vidu da bi se mogao obezbediti kontinuiran rad IS-a i da bi se znalo šta treba raditi u slučaju pada sistema. Ovi i slični problemi predstavljaju pitanja za upravljanje informacionim resursima.

2. POJAM IT UPRAVLJANJA

Analizom suštine pojma upravljanje, koje obuhvata sve aktivnosti povezane sa planiranjem, organizovanjem, sticanjem, održavanjem, osiguravanjem i kontrolisanjem raznovrsnih IT resursa (uključuju personal, tehnologiju i IT veze) može se zaključiti da su dva dva glavna zadatka IT upravljanja -**procenjivanje rizika** u uvođenju novih tehnologija i **ublažavanje rizika**. Svaki glavni kompjuting resurs: hardver, softver, ljudi, podaci, mreže i procedure utiče i na procenjivanje i na ublažavanje rizika pa je za organizacije neophodno dobro razumevanje rizika da bi bilo uspešno upravljanje rizikom. Jezgro uspešnog IT upravljanja u organizaciji čini sledećih pet odluka:

1.Usklađivanje IT strategije sa poslovnom strategijom.
2. Povezivanje strategije i preduzetničkih-intraorganizacionih ciljeva
3. Merenje IT performansi.
4. Strukturiranje organizacije za olakšanu implementaciju strategije i ciljeva
5. Prilagođavanje i implementiranje IT kontrole

Obrađivanjem ovih odluka za uspešno upravljanje informacionim resursima, koje je podeljeno između *odeljenja* **informacionog servisa** (*Information Sevices Department - **ISD***), koji se najčešće locira u računovodstvenom ili finansijskom odeljenju, i *odeljenja* **krajnjih korisnika,** stvara se i osnova za efektivan razvoj efektivne komunikacije sa krajnjim korisnicima. Radi samih korisnika i njihovih fundamentalnih razlika u kategorijama *karaktera, kognitivnih stilova, edukativne osnove i polne proporcije,* kako međusobno tako i sa ISD osobljem, veze između odeljenja ISD-a i odleljenja krajnjih korisnika su veoma važne. Nažalost te veze nisu uvek optimalne. pa dolazi do razvoja kompjuting-a i *outsourcing*-a i u odeljenju krajnjih korisnika što najčešće predstavlja dodatni izvor rizika u IT upravljanju.

Prema Luftman-u. (2004.):

IT upravljanje predstavlja operativni model organizacionog odlučivanja o upotrebi informacione tehnologije. Predmet IT upravljanja su odluke o alokaciji resursa, proceni poslovnih inicijativa i rizika, prioritetnosti projekata, merenju performansi i mehanizama praćenja, određivanju troškova i njihovom dodeljivanju pojedinim odeljenjima i proceni vrednosti IT investicija. Ukratko, IT upravljanje je koncentrisano na eksternu povezanost organizacije radi dobijanja IT resursa. Ovo povezivanje može obuhvatiti mehanizme kao što su strategijske alijanse, partnerstva, *outsourcing*, udružena preduzeća (radi razvijanja novih IT mogućnosti) i aktivnosti licenciranja.

Prema Američkom **Institutu za IT upravljanje** (*itgi.org*), „IT upravljanje predstavlja integralni deo preduzetničkog upravljanja i u domenu je odgovornosti borda direktora i izvršnog menadžmenta“. U nekim zemljama postoje i posebana stručna tela, napr. „Komitet za upravljanje“ koji se bavi nekim aktivnostima IT upravljanja a pre svega procenama sigurnosti i rizika.

3. ORGANIZACIJA IS odeljenjA

Glavna odluka koja mora biti doneta od strane višeg menadžmenta se odnosi na položaj IS odeljenja (ISD-a) u organizacijskoj hijerarhiji. Istorijski posmatrano, samo ime ISD-a je veoma važno i ono je evoluiralo od Odeljenja za obradu podataka (*Data Processing Department - DPD*), preko Odeljenja za upravljanje informacionim sistemima (*Management Information Systems - MIS*), a potom i Odeljenja infomacionih sistema (*Information System Department - ISD*). [10]

Status ISD-a zavisi od njegove misije i unutrašnje strukture. Agarwal i Sambamurthy (2002.) su zaključili da kompanije obično organizuju svoje IT funkcije na jedan od sledećih načina: postavljaju IT kao aktivnog partnera u poslovnim inovacijama, obezbeđuju IT resurse za inovacije i globalni domašaj ili traže fleksibilnost preko značajne količine *outsourcing*-a. *Outsourcing* predstavlja sporazum u kome jedna kompanija obezbeđuje servise za drugu kompaniju. To je trend koji je sve češći u IT i drugim industrijama i vezan je za servise koji se obično smatraju suštinskim za upravljanje poslovanjem. [4]

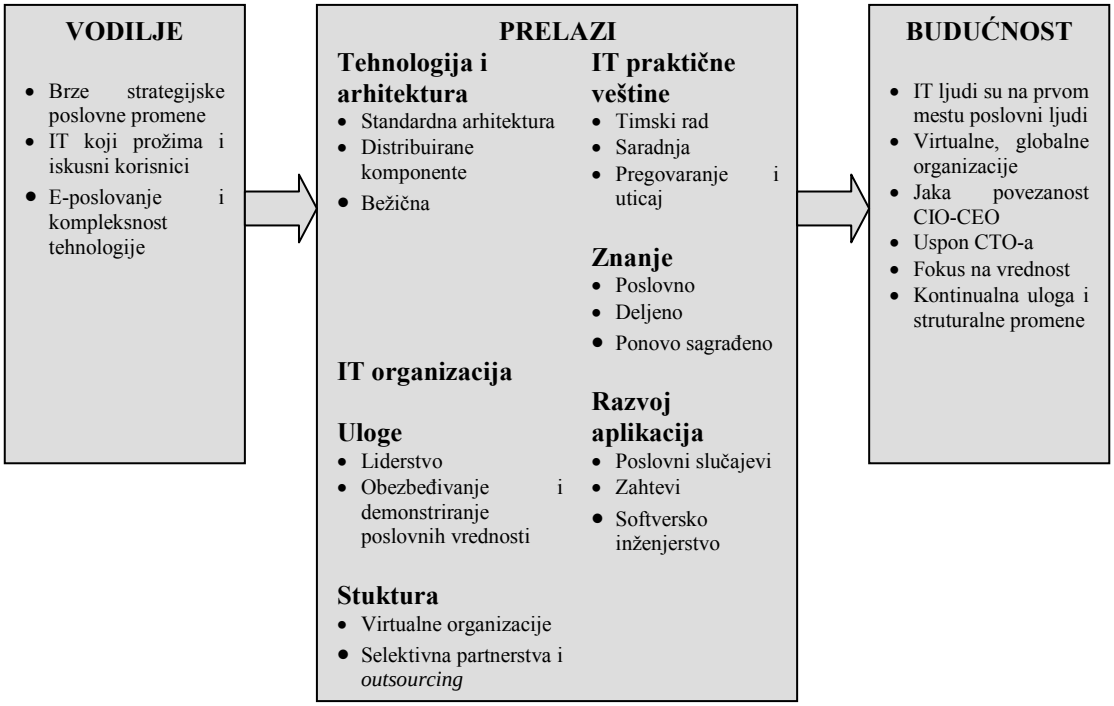
Razvoj **kompjutinga**, gde termin **kompjuting predstavlja funkcionisanje i upotrebu kompjutera i elektronske procese unutar kompjuterskog hardvera**, i ***outsourcing-***a kod krajnjih korisnika je delimično motivisan lošim servisom koji je pružan krajnjim korisnicima od strane ISD-a. Konflikt se javlja iz nekoliko razloga, a pre svega zbog liste prioriteta projekata ISD-a koje se mogu razlikovati od onih koje odgovaraju potrebama krajnjih korisnika. Drugi moćan izvor konflikata je nedostatak komunikacije među odljenjima iz različitih razloga.

Dakle, potrebno je razumevanje o ISD kao organizaciji servisa koja upravlja IT infrastrukturom koja podržava preduzetničke akcije sa IT aplikacijama za krajnje korisnike. U tom smislu jačanje saradnje izumeđu ISD i krajnjih korisnika može biti postignuto sa jednim od tri najčešća tipa dogovora ito: uključivanjem komiteta za upravljanje, ostvarivanjem doslednog sporazumi o nivou servisa ili organizaovanjem informacionog centra

4. . UPRAVLJANJE ISD U WEB OKRUŽENJU

Upravljanje ISD-om je slično upravljanju bilo kojom drugom organizacionom jedinicom. Jedina razlika je što ISD funkcioniše kao odeljenje servisa u veoma promenljivom okruženju, pa je projekcija odeljenja i planiranje teško. IT resursi su raspoređeni širom preduzeća što povećava kompleksnost upravljanja ISD-om.

Promenljiva uloga ISD-a ističe činjenicu da CIO postaje važan član organizacionog top menadžment tima (Ross i Freeny, 2000.), tako da davanje titule bez autoriteta može da ošteti ISD i njegovo funkcionisanje. Svaka organizacija koja je veoma zavisna od IT-a treba da ima CIO i da on bude postavljen na važnije organizacione pozicije ukoliko organizacija shvata potrebu za planiranjem nesreća koja je zasnovana na IT-u, kao i važnost IT-a u svakodnevnim organizacionim aktivnostima (Luftman et al., 2004.).



Slika 1. Prelazno okruženje (Izvor: Horner-Reich i Nelson, 2003.)

Glavna uloga CIO-a jeste usklađivanje IT-a sa poslovnom strategijom. Sporedne uloge su implementacija savremenih rešenja i obezbeđivanje i poboljšanje pristupa informacijama. Koordiniranje IT-om zahteva jako IT rukovođenje i saradnju ISD-a i krajnjih korisnika unutar organizacije. CIO-CEO povezanost je presudna za efikasno i uspešno korišćenje IT-a, posebno u organizacijama koje veoma zavise od IT-a, u kojima se CIO pridružuje grupi šefova u top menadžmentu.

Prema Ross-u i Freeny-u (2000.), Luftman-u et al. (2004.) i Earl-u (1999.-2000.) na ulogu CIO-a u eri zasnovanoj na Web-u utiču sledeća tri faktora: promene tehnologija i upravljanja, promene, stavova izvršne vlasti i povećavanje interakcija sa prodavcima .

Kako informaciona tehnologija postaje centralna u poslovanju, CIO postaje ključni pokretač u rangu vrhovnog menadžmenta. Sa rastom sveobuhvatnog kompjutinga i *outsourcing*-a dovodi se u pitanje budućnost ISD-a kao dela organizacije. Horner-Reich i Nelson (2003.) su vizualizovali glavne promene u stvaranju i radu ISD-a, gde se vidi da se u sadažnjem trenutku nalazimo u sredini tranzicije, (što je prikazano na Slici 1).

Prema Duffy-u (1999.) najbolja investicija kompanije je u CEO koji poznaje tehnologiju. Kada CIO i CEO poseduju neophodne veštine za informaciono doba njihova kompanija poseduje veliki potencijal pa je unapređenje CIO-e u CEO-e u trendu kod mnogih kompanija. [10]

5. KARAKTERISTIKE IS-a SA ASPEKTA NJEGOVE Ranjivost

Informacioni sistemi su složena matrica mnogo interaktivnih komponenti koje mogu biti smeštene na nekoliko lokacija, što povećava njihovu neotpornost ili ranjivost od mnogih potencijalnih opasnosti ili pretnji. [1]

Tabela 1. Ključna terminologija u polju IT sigurnosti

Termin	Definicija
Backup	Dodatna kopija podataka i/ili programa, koja se čuva na sigurnoj lokaciji/lokacijama.
Deskripcija	Transformacija skremblovanog koda u čitljive podatke posle transmisije.
Enkripcija	Transformacija podataka u skremblovani kod pre transmisije.
Izloženost	Povreda, gubitak ili šteta koja nastaje ukoliko nešto pođe naopako u informacionim sistemima.
Kontrolisanje informacionog sistema	Procedure, uređaji ili softver koji pokušava da obezbedi da se sistem ponaša kao što je i planirano.
Integritet (podataka)	Garancija za tačnost, kompletnost i pouzdanost podataka.
Rizik	Verovatnoća da će se pretnja materijalizovati.
Pretnje (ili povrede)	Različite opasnosti kojima sistem može biti izložen.
Ranjivost	Osetljivost sistema na povrede prouzrokovane pretnjama koje postoje.
Malware	Opšti termin za softver koji omogućuje zlonamerne radnje protiv kompjuterskog sistema.

Prema CVE (Common Vulnerabilities and Exposure) postoji razlika između ranjivosti i izloženosti napadima.

Opšta ranjivost je stanje u kompjuterskom sistemu (ili skupu sistema) koje dozvoljava napadaču da:

- izvrši komande kao drugi korisnik;
- pristupi podacima, što je u suprotnosti sa specifikovanim restrikcijama pristupa podacima;
- predstavi se kao drugi entitet; ili
- sprovede odbijanje servisa.

Izloženost napadima je stanje u kompjuterskom sistemu (ili skupu sistema) koje nema karakteristike opšte ranjivosti, ali potencijalnom napadaču ipak dozvoljava da :

- sprovede aktivnosti prikupljanja podataka;
- sakrije određene aktivnosti;
- demonstrira neko očekivano ponašanje, ali koje lako može biti kompromitovano; Teorijski posmatrano, postoje stotine tačaka u korporativnom informacionom sistemu koje mogu biti predmet neke pretnje i uzrok ranjivosti informacionih sistema. U praksi, postoje hiljade različitih načina na koje informacioni sistemi mogu biti napadnuti ili oštećeni. Ove pretnje mogu biti klasifikovane kao *nenamerne* (ljudske greške, opasnosti iz okruženja i otkazi kompjuterskog sistema) ili *namerne* (krađu podataka; neadekvatno korišćenje podataka; krađa vremena mejnfrejm kompjutera; krađa opreme i/ili programa; namerna manipulacija u rukovanju, unošenju, obrađivanju, prenošenju ili programiranju podataka; štrajkovi, pobune ili sabotaže; zlonamerna šteta na kompjuterskim resursima; uništavanje virusima i sličnim napadima; i različite zloupotrebe kompjutera i Internet prevare).

6. Ukratko o kompjuterskom kriminalu

Prema Američkom Institutu za kompjutersku sigurnost (Computer Security Institute) broj, veličina i raznovrsnost kompjuterskog kriminala je u stalnom porastu, a skorašnje povećanje prevara povezanih sa Internetom i e-trgovinom to nedvosmisleno pokazuje. Kompjuterski kriminal se može pojaviti u mnogo oblika. Prvo, kompjuteri mogu da budu *mete* kriminala. Kompjuter može biti *sredstvo* ili *alat* u napadima, tako što kreiraju okruženje u kome se kriminal ili prevara mogu ne samo pojaviti već i održavati. Na kraju, kompjuter se može koristiti za *zastrašivanje* ili *prevare*. Kriminal koji se dešava na Internetu, nazvan sajber kriminal, može da se svrsta u svaku od ovih kategorija.

Kriminal može biti počinjen od strane ***autsajdera*** koji prodiru u kompjuterski sistem (najčešće preko komunikacionih linija) ili od strane ***insajdera*** koji su autorizovani za korišćenje kompjuterskog sistema ali svoju autorizaciju koriste na pogrešan način. **Haker** je termin koji se često koristi za opisivanje osobe autsajdera koja prodire u kompjuterski sistem. Međutim, svi hakeri nisu kriminalci. *White-hat* hakeri izvode etičko hakovanje, tj. izvode testove prodiranja u sisteme njihovih klijenata u cilju otkrivanja slabih tačaka, s ciljem njihovog ispravljanja. *Black-hat* hakeri, koji se često nazivaju i cracker-i, jesu kriminalci. **Cracker** je zlonameran haker, koji može da izazove ozbiljne probleme korporaciji. [2]

U strategiji nazvanoj **socijalni inženjering,** kompjuterski kriminalci ili korporativni špijuni izgrađuju vezu sa poverenjem sa insajderima u cilju dobijanja osetljivih informacija ili privilegija neautorizovanog pristupa.

Internet okruženje predstavlja okruženje u kome je veoma lako sprovoditi ilegalne aktivnosti, koje su poznate kao **sajber kriminal**. Stotine različitih metoda i „trikova“ se koristi od strane *inovativnih kriminalaca* za uzimanje novca od nevinih ljudi, da se obavi kupovina bez plaćanja, da se proda bez isporuke, za uznemiravanje ljudi, krađu identiteta, ili njihovo povređivanje i još mnogo toga. Internet sa svojim globalnim pokrivanjem takođe ima uticaj i na rast prevara izvan granica zemlje. Postoji rastuće interesovanje za pretnju **sajber rata**, takođe poznatog kao *warefare*, u kojoj informacioni sistemi zemlje mogu biti paralizovani masivnim napadom destruktivnim softverom. Ciljani sistemi mogu biti poslovni, industrijski i vladini IS-ovi, kao i mediji i vojni komandni sistemi.

7. Metode napada na kompjuterska postrojenja

Postoji mnogo metoda za napad, a svakodnevno se pojavljuju sve noviji i noviji.

Tabela 2. Neke od metoda programerskih napada na kompjuterske sisteme

Metod	Definicija
Virus	Tajne instrukcije umetnute u programe (ili podatke) koje se naivno pokreću tokom uobičajenih zadataka. Tajne instrukcije mogu da unište ili promene podatke, kao i da se prošire unutar ili između kompjuterskih sistema.
Crv	Program koji se umnožava i probija u ispravni kompjuterski sistem. Može se proširiti unutar mreže, probijajući se u sve povezane kompjutere.
Trojanski konj	Ilegalni program, koji se nalazi unutar drugog programa, koji „spava“ sve dok se ne desi neki određen događaj, koji aktivira ilegalni program koji izaziva štetu.
Mala vrata	Tehnika koja omogućava provaljivanje u kod programa, a samim tim omogućava i dodavanje dodatnih instrukcija.
Logička bomba	Instrukcija koja aktivira odloženi zlonamerni akt.
Odbijanje servisa	Previše zahteva za servisom, koji dovode do pada Web sajta.
Sniffer	Program koji prikuplja šifre ili sadržaj iz paketa podataka koji prolaze

	Internetom.
Cracker šifri	Program koji pokušava da pogodi šifru (može biti veoma uspešan).
Dajler	Programi koji automatski biraju hiljade telefonskih brojeva u pokušaju da pogode jedan koji omogućava konkciju modemom.

Prema CSI/FBI izveštaju ističu se kao najfrekventnije metode napada na kompjuterska postrojenja: virusi, insajder zloupotrebe Internet pristupa, neautorizovani pristup od strane insajdera, krađa laptopova, napadi sa odbijanjem servisa (DoS), proboj u sistem, sabotaže i krađa ličnih informacija. Dva osnovna pristupa za namerne napade na kompjuterske sisteme su: *kvarenje podataka* i *programerski napadi*. [5]**Kvarenje podataka** je najčešći oblik napada koji koriste insajderi i realizuje se kroz unošenje lažnih, falcifikovanih ili obmanjivih podataka u kompjuter ili zamenu ili brisanje postojećih podataka. **Programerski napad** je popularan kod kompjuterskih kriminalaca koji imaju programerske veštine i znanje o ciljnim sistemima a koriste programerske tehnike za modifikovanje kompjuterskih programa, da li direktno ili indirektno. [7]

8. Sprovođenje sigurnosti: Proveravanje i upravljanje IT-om

Sprovođenje sigurnosti u organizaciji može biti veoma komplikovan zadatak, posebno u velikim, decenralizovanim kompanijama. Od mnogo pitanja uključenih u sprovođenje sigurnosti, tri najvažnija su: proveravanje informacionih sistema, analiza rizika i IT sigurnosni trendovi, uključujući upotrebu naprednih inteligentnih sistema. [8]

8.1. Proveravanje Informacionih sistema

Proveravanje se, u organizacionoj strukturi, obično odnosi na periodična ispitivanja i kontrole finansijskih i računovodstvenih podataka i procedura. U okruženju informacionog sistema, proveravanje se može posmatrati kao dodatni sloj kontrola ili bezbednosnih mera i smatra se zastrašivanjem za kriminalne aktivnosti (Well, 2002.), posebno kod insajdera.

Postoje dva tipa kontrolora (i provera): interni i eksterni. Interni kontrolor je obično zaposlenik korporacije, koji nije član ISD-a. Eksterni kontrolor je korporativni autsajder, koji pregleda odluke internih provera i inpute, obradu i autpute informacionih sistema.

IT proveravanje se odnosi na sve potencijalne opasnosti i kontrole u informacionim sistemima. Fokusirano je na teme kao što su razvoj novih sistema, rukovanje i održavanje, integritet podataka, softverske aplikacije, sigurnost i tajnost, planiranje nesreća i oporavak od njih, kupovanje, budžet i troškovi, naplate, upravljanje prodavcima, dokumentacija, osiguranje i garantovanje, trening, kontrola troškova i produktivnost. politika i planovi za sigurnost podataka, plan poslovnog kontinuiteta (Von-Roessing, 2002.), dostupnost strategijsko-informacionog plana, odgovornosti IT sigurnosti, merenje uspešnosti organizacione IT sigurnosne šeme, postojanje programa za sigurnosnu svesnost i sistema za prijavljivanje sigurnosnih incidenata.

Koriste se dva tipa provera kako bi se odgovorilo na ova pitanja. *Operativna provera* utvrđuje da li ISD radi ispravno. *Provera pridržavanja* utvrđuje da li su kontrole implementirane ispravno i da li su adekvatne. Proveravanje je posebno usmereno ka opštim kontrolama i ka aplikativnim kontrolama (Sayana, 2002.).

8.2. Upravljanje rizikom i analize ekonomičnosti

Nije ekonomično pripremati zaštitu za sve moguće pretnje. Zbog toga IT sigurnosni program mora da obezbedi proces za procenjivanje pretnji i odlučivanje o

tome za koje pretnje će se pripremati, a koje će ignorisati ili za koje će pripremiti umanjenu zaštitu. Prema CSI/FBI 2006 pregledu *većina organizacija sprovodi neke oblike ekonomskih procena njihovog sigurnosnog troška (najčešće RIO).* Postavljanje kontrolnih mera je bazirano na ravnoteži između cene kontrola i potrebe da se smanje ili eliminišu pretnje. Takva analiza, gde se očekivani gubitak upoređuje sa cenom njegovog sprečavanja, je osnovni pristup upravljanja rizikom, koji pomaže u identifikovanju pretnji i odabiru sigurnosnih mera prema ceni i efikasnosti (Hiles, 2002., Volonino i Robinson, 2004.). [5]

8.3. IT sigurnosni trendovi

Pouzdanost sistema se povećava upotrebom kriterijuma koji se zove „**tolerancija nedostataka**“. **To podrazumeva funkcionisanje** informacionog sistema i u slučaju pojave otkaza nekih njegovih delova. Nekoliko PC proizvođača obezbeđuje karakteristiku koja skladišti podatke na više od jednog diska u isto vreme; pa se u sliučaju otkaza jednog diska ili naapada na njega postiže dostupnost podataka.

Kompjuterski sistemi postaju sve kompleksniji, zahtevaju veće količine ljudskih intervencija za pnjihovo podobno funkcionisanje. Pošto se nivo kompleksnosti povećava, postoji sve veća potreba za **samo-izlečivim kompjuterima**. Idealno, oporavak može da se obavi trenutno ukoliko kompjuteri pronađu i isprave problem samostalno, pre pada sistema.

Za detektovanje napada na poverljive informacije i finansijske podatke se koriste ekspertski sistemi i neuralne mreže kao **sistemi za ranu detekciju napada**. Ovaj pristup upoređuje korisničke aktivnosti na mreži radne stanice sa istorijskim profilom i analizira značajnost bilo kakvih promena. Cilj je detektovanje narušavanja sigurnosti.

Inteligentni sistemi se koriste za povećanje zadatka IS proveravanja. Na primer, ekspertski sistemi procenjuju kontrole i analiziraju osnovne kompjuterske sisteme, dok se neuralne mreže i pronalaženje podataka koriste za detekciju prevara (Sheridan, 2002.).

Ekspertski sistemi, neuralni kompjuting, prepoznavanje glasa i fazi logika mogu se koristi za povećanje sposobnosti nekoliko **biometrijskih sistema**. [3]

Tabela 3. Druge informacione tehnologije koje su važne za antiterorističke aktivnosti

IT	Opis
Obrada videa	Analizira, detektuje, ekstrahuje i digitalno obrađuje (smanjuje šum, unapređuje boju i kontrast slike i uvećava rezoluciju u selektovanoj oblasti) ponašanja korisnika ili aktivnosti u videu (sumnjive aktivnosti povezane sa teroristima).
Vizualizacija	Obezbeđuje grafički displej, uređene informacije, grafikone zasnovane na vremenu i ugrađene alate kao pomoć analitičarima i istraživačima u otkrivanju, raspoznavanju i vizualizaciji mreža međusobno povezanih informacija (veze između reči, koncepata, ljudi, mesta ili događaja) ili u vizualnom izlaganju neočiglednih šablona, veza i anomalija u velikim skupovima podataka.
Upravljanje tokom posla	Kreira optimizovane tokove posla i mape poslovnih procesa zasnovane na aktivnostima koristeći tehnike kao inteligentni VI endžini, tako što posmatraju, uče i snimaju aktivnosti više korisnika koji koriste više aplikacija u više sesija.

Izvor: Popp et al. (2004.).

9. UMESTO ZAKLJUČKA

Uspešno ostvarivanje misije u digitalnoj ekonomiji IS odeljenje postižu sa visokom prilagodljivošću promenama. Trend sve većeg korišćenja IT-a, pozicionira IT na najvažniju tehnološku i stratešku poziciju uloga mnogih organizacija, malih i velikih, privatnih i javnih, širom sveta. Efikasna IS odeljenja pomažu svojim firmama da primene IT u toku transformacije istih u e-poslovanje, u redizajniranju procesa i u pristupu potrebnim informacijama koristeći mali budžet.

Sa intenzivnijim korišćenjem Interneta, ekstranetova i intranetova u organizacijama se zaoštrava i pitanje njihove sigurnosti. Zato je bitan princip u poslovanju da svi zaposleni znaju ko je odgovoran za koju informaciju i da oni razumeju potrebu za sigurnosnom kontrolom. U mnogim organizacijama većina informacionih resursa je u rukama krajnjih korisnika. Zbog toga, funkcionalni menadžeri moraju da razumeju i uvežbaju upravljanje IT sigurnošću i upravljanje drugom IT aktivom. Programi sigurnosne svesnosti su važni za organizaciju, Oni treba da ohrabre poslovna odeljenja za preuzimanje odgovornosti za identifikovanje, procenjivanje i upravljanje sigurnosnošću i rizicima.

LITERATURA

1. Andrew M. Colarik, *"Cyber Terorism: Political and Economic Implications,"* Idea Group Publishing, 2006.
2. Bruce Middleton, "Cyber crime investigator's field guide," CRC Press LLC, 2002.
3. Ilkka Tuomi, *"Networks of Innovation,"* Oxford University Press Inc., New York, 2002.
4. John Baschab, Jon Piot, *"The Executive's Guide to Information Technology,"* John Wiley & Sons, Inc., 2003.
5. Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, *"2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY,"* Computer Security Institute, 2006.
6. Banjanin M. K, *"Metodologija inženjeringa - inženjerske analize i mreže znanja,"* drugo prerađeno izdanje, DISPUBLIK, Beograd, 2006.
7. Rick Lehtinen, *"Computer Security Basics,"* 2nd Edition, O'Reilly, 2006.
8. Robert J. Benson, Thomas L. Bugnitz, William B. Walton, *"From Business Strategy to IT Action,"* John Wiley & Sons, Inc., 2004.
9. Sean B. Eom, *"Inter-Organizational Information Systems in the Internet Age,"* Idea Group Publishing, 2005.
10. Turban, Leidner, McLean and Wetherbe, *"Information technology for management,"* www.wiley.com/college/turban, 2006.