ASOCIJACIJA ZA KVALITET I STANDARDIZACIJU SRBIJE

FESTIVAL KVALITETA 2007.
34. Nacionalna konferencija o kvalitetu
Kragujevac, 08. - 11. maj 2007.

STANDARDI SERIJE ISO/IEC 27000 NAJBOLJA POSLOVNA PRAKSA ZA SIGURNOST INFORMACIJA

ISO/IEC 27000 SERIES STANDARDS THE BEST BUSINESS PRACTIC FOR INFORMATION SECURITY

Mirko Đapić[1)], Ljubomir Lukić[2)]

Rezime: *Primena savremenih informacionih tehnologija omogućava bolju komunikaciju organizacije sa svojom okolinom. U takvim uslovima informacione vrednosti organizacije se suočavaju sa brojnim sigurnosnim pretnjama. Sledeći to u radu[3)] se predstavlja koncept sigurnosti informacija i serija standarda ISO/IEC 27000 koja daje harmonizovani pristup razvoju, implementaciji i održavanju menadžment sistema za sigurnost informacija (ISMS).*
Ključne reči: *sigurnost informacija, menadžment sistem, ISMS*

Summary: *Using information technology enables better organization communication with its environment. Under that conditions organization information values face serious security threats. Continue to that in this paper are presented information security concept and ISO/IEC 27000 series of standards which provide a harmonize approach to development, implementation and maintains information security management systems (ISMS).*
Ključne reči: *security of information, management systems, ISMS*

1. UVOD

Savremeno poslovanje je danas nezamislivo bez primene informacionih tehnologija. Informacije postaju važan resurs od koga zavisi opstanak i razvoja organizacije. Organizacije postaju sve otvorenije povezujući svoje informacione resurse sa kupcima, dobavljačima i ostalim komintentima. Ovo dovodi do pojave brojnih sigurnosnih prijetnji kao što su računarske prevare, špijunaže, sabotaže, vandalizmi, požari, poplave i sl. Štete nanesene organizacijama u obliku zloćudnog koda, računarskog hakerisanja i uskraćivanja usluge je sve prisutnija pojava.

Bez obzira u kom obliku se čuvaju (pothranjuju) informacije moraju da budu adekvatno zaštićene. Da bi se osigurala adekvatna zaštita informacija svi korisnici moraju da budu familijarni sa konceptom i merama zaštite koje se zahtevaju.

Zaštita informacija, očuvanje njihove poverljivosti, integriteta, odnosno celovitosti i raspoložoivosti postaje od primarne važnosti. Sigurnost informacija je mnogo više od korišćenja odgovarajućih tehničkih rešenja koje nude savremene informacione tehnologije. Jer kao što je navedeno u /1/ "Ako mislite da tehnologijom možete reštit vaš sigurnosni problem onda vi ne razumete ni problem ni tehnologiju".

Oslanjajući se na koncept da je sigurnost informacija mnogo više od primene savremenih tehničkih rešenja koje nude informacione tehnologije, razvijeni svet (pre svih Velika Britanija kroz nacionalno telo za standardizaciju BSI) opredelio se za razvoj odgovarajućih standarda koji pokrivaju ovu oblast. Tako su sredinom devedesetih godina prošlog veka nastali prvi standardi BS 7799-1 i BS 7799-2. Razvoj ovih standarda je od dvehiljadite godine preuzela Međunarodna organizacija za standardizaciju (ISO) zajeno sa Međunarodnom elektrotehničkom komisijom (IEC) kroz zajednički tehnički komitet (JTC1).

Sledeći to u ovom radu se predstavlja koncept sigurnosti informacija i serija standarda ISO/IEC 27000 koja podržava ovaj koncept.

2. ŠTA JE TO SIGURNOST INFORMACIJA?

Informacija: je podatak sa određenim značenjem, odnosno znanje koje se može preneti na bilo koji način (pismom, audio, vizuelno, elektronski ili na neki drugi način).

Informacije mogu da budu:

1) dr Mirko Đapić, LOLA Institut, Kneza Višeslava 70a, 11030 Beograd, mdjapic@yahoo.com,
2) dr Ljubomir Lukić, Mašinski fakultet Kraljevo, Dositejeva br 19., 36000 Kraljevo, pbs1@tehnicom.net
3) Rad predstavlja deo istraživanja na projektu TR-6319B koji je delimično finansiran sredstvima Ministrstva nauke i zaštite životne sredine Republike Srbije

- štampane ili napisane na papiru
- odložene (memorisane) elektronski
- prenesene poštom ili elektronskim putem
- prikazane na korporacijskom veb sajtu
- verbalne – izgovorene u konverzaciji
- znanje – veštine zaposlenih

Informacije i njima pripadajući podaci, zatim procesi i sistemi (hardverski, softverski, mrežni itd.) koji se koriste za njihovo generisanje, obradu, prenos, memorisanje kao i pristup predstavljaju važan deo **poslovne imovine** organizacije koju je potrebno prikladno zaštititi ako se želi normalno poslovanje koje će obezbediti opstanak i razvoj. Ovaj zahtev postaje sve važniji zbog distribuirane poslovne okoline organizacije u kojoj su informacije izložene **ranjivostima** usled velikog broja **pretnji** (opasnosti) (slika 2.1).

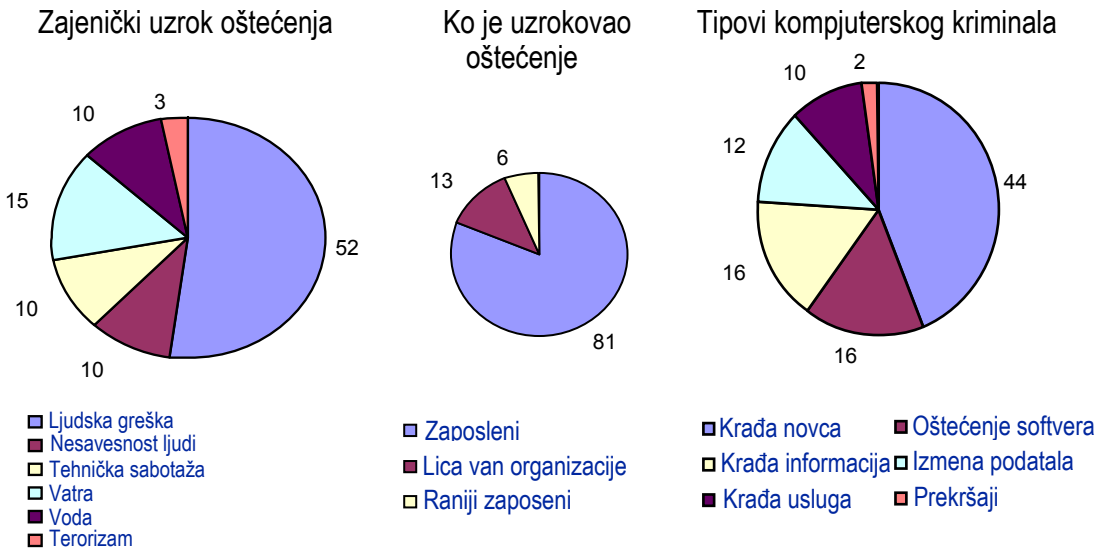
> *"Bez obzira u kom se obliku informacije nalaze ili koje se sredstvo koristi za njihovu prenos, raspodelu i odolaganje (memorisanje) informacije moraju da budu adekvatno zaštićene ... "*
> ISO/IEC 17799:2005

Nezavisno od prirode informacioni resursi (informacione vrednosti) (tabela 2.1) mogu da imaju jednu ili više sledećih karakteristika:

- Prepoznati su na nivou organizacije kao entitet koji ima vrednost
- Ne mogu lako da budu zamenjeni bez utroška resursa kao što su: novac, veštine zaposlenih, vreme itd.
- Čine identitet organizacije bez koga poslovanje organizacije može da bude ugroženo

Tabela 2.1 Kategorije informacionih resursa (vrednosti) koje je neophodno zaštiti

Kategorija informacionih resursa (vrednosti)	Primeri:
Informacije	baze podataka i podaci, dokumenta vezana za sistem, korisnički priručnici, materijali za obuku, operativne i sistemske procedure, planovi kontinuiteta, sistem zapisa
Softver	aplikativni i sistemski, alati za razvoj softvera
Fizički resirsi - hardver (kompjuterska oprema)	kompjuterski uređaji (procesori, monitori, laptopovi, modemi), komunkakacioni uređaji (ruteri, svičevi, telefoni), magnetni medijumi (trake, diskovi), ostali tehnički uređajui (sistemi napajanja, hlađenja itd.)
Usluge	Usluge obrade podataka, komunikacione usluge
Osoblje	znanje i veštine osoblja (tehničkog, operatvnog, marketing, finansijskog, itd ...)



Slika 2.1. Uzroci i tipovi kompjuterskog kriminala (Adaptirano iz/5/)

Pretnje informacionim resursima u nekoj organizaciji predstavljaju:

- Zaposleni
- Niska svest o potrebi zaštite informacija (korporativna kultura)
- Porast umreženosti i distribuirane obrade podataka
- Porast složenosti i efektivnosti hakerskih alata i virusa
- E-mail -ovi
- Požar, poplava, zemljotresi itd.

Osnovni ciljevi zaštite informacija u nekoj organizaciji je da se obezbedi:

- kontinuitet poslovanja i
- minimizira rike od potencijalnih šteta (havarija)

Ovo se postiže prevencijom incidentnih događaja i redukovanjem njihovog potencijalnog uticaja.

Definisanje, implementacija, održavanje i unapređenje koncepta sigurnosti informacija može biti od presudne važnosti za ostvarivanje i održavanje konkurentnosti, dotoka novčanih sredstava i obezbeđenja profitabilnosti, kao i zadovoljenja zakonskih odredbi i osiguranja poslovnog ugled organizacije.

Sigurnost informacija je podjednako važna malim i veliki kao i javnim i privatnim organizacijama. Povezanost javnih i privatnih računarskih mreža i deljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uslovima oblici centralizovane kontrole nisu delotvorni. Odnosno, primena tehničkih rešenja, odgovarajuće opreme i proizvoda više nije dovoljna da bi osigurala odgovarajuće upravljanje sigurnošću informacija.

Sigurnost informacija nije isključivi problem informacionih tehnologija (IT) već je to "poslovni" problem. Opšte je mišljenje da primenom odgovarajućih tehnologije se rešava samo jedan deo problema sigurnosti informacija.

Danas se sigurnost informacija postiže primenom odgovarajućih **kontrola** (eng. control), koje se odnose na politiku sigurnosti, poslovne procese, procedure, strukturu organizacije i funkcije hardvera i softvera (sistemskog i aplikativnog).

Kontrole važne za organizaciju sa zakonske tačke gledišta su: a) zaštita informacija i tajnosti ličnih podataka; b) čuvanje organizacionih izvještaja; c) poštivanje prava intelektualnog vlasništva. Kontrole koje u praksi postižu dobre rezulate kod implementacije koncepta sigurnosti informacija su: a) sigurnosna politika; b) raspodela odgovornosti za sigurnosti informacija; c) svest o neophodnosti zaštite informacija, obrazovanje i obuka zaposlenih; d) ispravno procesiranje podataka u aplikacijama; e) upravljanje ranjivostima (slabostima) informacionih resursa; f) upravljanje kontinuitetom poslovanja g) upravljanje sigurnosnim incidentima i unapređenje sistema.

Navedene kontrole je potrebno osmisliti, implementirati, nadzirati, preispitivati i unapređivati kako bi se osiguralo ispunjenje poslovnih i sigurnosnih zahteva organizacije.

Upravljanje sigurnošću informacija zahteva uključivanje svih zaposenih u organizaciji, a vrlo često je potrebna pomoć spoljnih konsultanata.

Razvojem, implementacijom i sertifikacijom menadžment sistema za sigurnost informacija ISMS (Information Security Management System) pruža određeni nivo poverenja kod komintenata menadžmenta, doeničara i zaposlenih da će njihove informacije adekvatno biti zaštićene.

2.1 Koje su komponente sigurnosti informacija?

Sigurnost informacija obuhvata primenu mera zaštite podataka koji su na **obradi**, ili su **pothranjeni** ili je u toku njihov **prenos** od gubitaka (slika2.2):

- poverljivosti,
  (Odnosi se na zaštitu određenih podataka, odnosno informacija od bilo kakvog namernog ili nenamernog otkrivanja neovlašćenim osobama)
- celovitosti (integriteta)
  (Odnosi se na osiguranje tačnosti i celovitosti informacija i na onemogućavanje neovlašćene promene njihovog sadržaja)
- raspoloživosti
  (Odnosi se na ta da su relevantne informacije u vremenski prihvatljivim terminima raspoložive odgovarajućim subjektima)

kao i sprečavanje gubitka **celovitosti** i **raspoloživosti** samih sistema.

Sigurnosne mere uključuju **mehanizme** i **procedure** koje se implementiraju u cilju:

- odvraćanja,
- prevencije
- detekcije i
- opravke

od uticaja **incidentnih događaja** a koji deluju na **poverljivost**, **celovitost** i **raspoloživost** podataka i odgovarajućih servisa i resursa uključujući izveštavanje o sigurnosnim incidentima.

Sigurnost informacija je ustvari proces upravljanja rizikom. Menadžment sigurnosti bi trebao da bude deo ukupnog menadžmenta rizicima a sigurnost informacija je samo jedan aspekt ukupne sigurnosti organizacije.

Upravljanje rizicima mora da bude stalan, kontinuiran proces pošto su rizici sami po sebi promenjivi, a s druge strane stalno se generišu novi kao odraz promenjivog okruženja u kome organizacija ostvaruje svoju misiju. Ovo znači da je neophodno da se periodično preispituju rizici kao i pretnje i slabosti informacionih resursa. Ovo je upravo ono na čemu bazira menadžment sistem za sigurnost informacija (Information Security Management System - ISMS).

Slika 2.2 Komponente sigurnosti informacija

Jedan harmonizovani proces uspostavljanja ISMS-a dat je u standardu ISO/IEC 27001:2005. Uspostavljanje ISMS sistema koji ispunjava zahteve ISO/IEC 27001 mora da se realizuje kroz projekat koji podrazumeva primenu metoda i tehnika projekt menadžmenta.

3 STANDARDIZACIJA U OBLASTI UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC) su osnovali zajednički tehnički komitet JTC1 u okviru koga radi stalni komitet SC27 (ISO/IEC JTC1/SC27 "IT Security Technique") koji se bavi razvojem standarda u oblasti sigurnosti IT sistema. Ovaj komitet je pokrenuo novu seriju standarda ISO/IEC 27000. Ovo je familija standarda o ISMS (menadžment sistemu za sigurnost informacija) koja je planirana da se razvije u narednih 5-7 godina. Planirano je da ovu seriju (slika 3.1) čine:

- ISO/IEC 27000 ISMS - Osnove i rečnik pojmova
- ISO/IEC 27001 ISMS - Zahtevi
- ISO/IEC 27002 (ISO/IEC 17799 će postati posle 2007 godine) - Kodeks postupaka (dobra praksa) za upravljanje sigurnosti informacija
- ISO/IEC 27003 - ISMS Uputstvo za implementaciju
- ISO/IEC 27004 - Merenja u menadžmentu sigurnosti informacija
- ISO/IEC 27005 - Menadžemt rizika sigurnosti informacija

Za sada su objavljena samo dva standarda iz ove serije. To si ISO/IEC 27001:2005 i ISO/IEC 17799:2005 (slika 3.1)

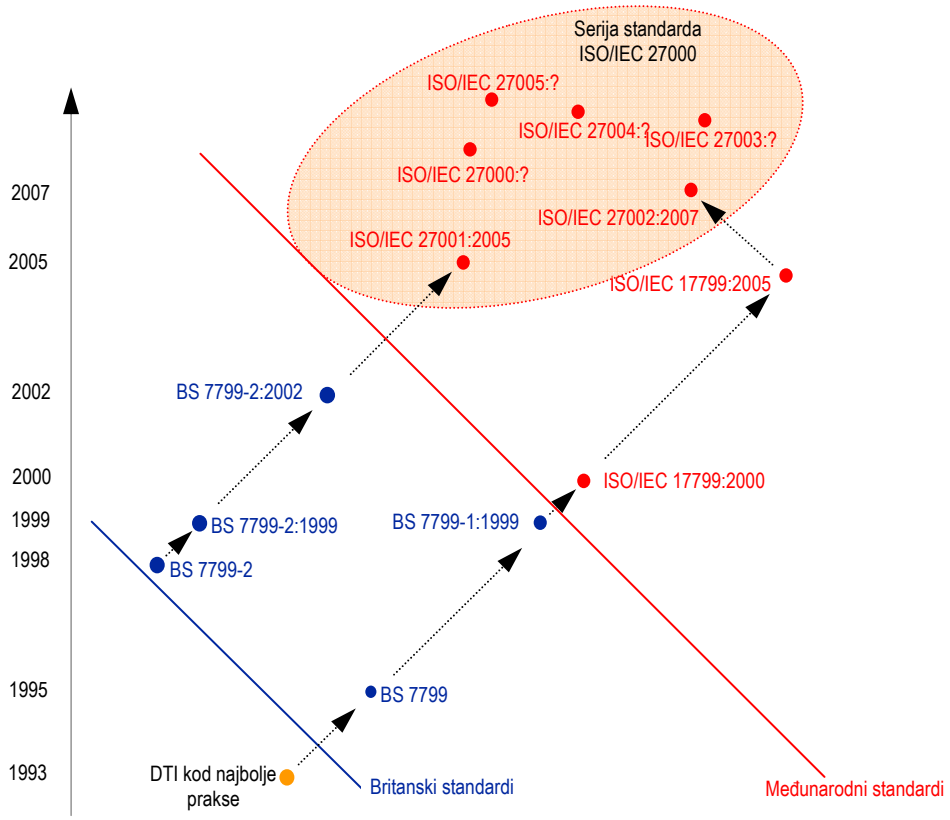
Standard ISO/IEC 17799:2005 definiše kodeks dobre poslovne praksa u oblasti sigurnosti informacija. Čitav standard bazira na jedanest sigurnosnih kategorija (poglavlja) koje pokrivaju sve aspekte sigurnosti informacija. Te kategorije su:

- Sigurnosna politika
- Organizacija za sigurnost informacija
- Upravljanje resursima
- Sigurnost ljudskih resursa
- Fizička sigurnost
- Upravljanje komunikacijama i operacijama
- Kontrola pristupa
- Nabavka, razvoj i održavanje informacionih sistema
- Upravljanje sigurnosnim incidentima
- Upravljanje kontinuitetom poslovnih procesa
- Usklađivanje sa zakonskim i drugim propisima

Svaka od navedenih sigurnosnih kategorija definiše sigurnosne ciljeve kao i kontrole koje je potrebno sprovesti da bi se ispunili ti ciljevi. Važno je napomenuti da se kontrole definišu kao: način upravljanja rizicima, što podrazumeva politike, procedure, uputstva, organizacione strukture koje mogu da budu administrativne, tehničke, upravljačke ili pravne.

Paralelno sa ovim standardom razvijan je standard (ISO/IEC 27001) koji definiše zahteva koje menadžment sistem za sigurnost informacija mora da zadovolji i po kome se sprovodi sertifikacija ISMS ako se to zahteva. Ovi zahtevi baziraju na ciljevima i kontrolama (dobroj poslovnoj praksi) koje su definisane u standardu ISO/IEC 17799.

Ceo koncept sigurnosti informacija koji je definisan u standardima ISO/IEC 27001 i ISO/IEC 17799 bazira na konceptu upravljanja (menadžmentu) rizicima. Ocena rizika je definisana kao ocena pretnji informacijam (pretnje koje dovode do povrede poverljivosti, integriteta i raspoloživosti informacija) njihovog uticaja na informacije i na ranjivost (slabost) informacija i informacionih sistema kao i verovatnoće njihove pojave.



Slika 3.1 Razvoj standarda ISO/IEC 27001 i ISO/IEC 17799

Upravljanje (menaddžment) rizikom je definisan kao proces identifikacije, kontrole i umanjivanja ili eliminacije sigurnosnih rizika koji mogu da utiču na informacije i informacione sisteme a koji mora da bude finansijski opravdan.

4 ZAKLJUČAK

Informacione tehnologije igraju značajnu ulogu u razvoju i održavanju konkurentnosti savremenih organizacija. Uvođenje interneta, intraneta, elektronskog poslovanja itd. značajno je unapredilo sposobnost organizacija da brzo reaguju na stalne promene koje se dešavaju u okolini u kojoj organizacije ostvaruje svoje poslovne aktivnosti. Bez primene ovih tehnologija one teško mogu da prežive na tržištu koje se sve više globalizuje.

Otvaranje informacionih resursa organizacije prema spoljnjem svetu ima i svoje negativne strane. Informacije i informacioni resursi (hardverski i softverski) izloženi su brojnim sigurnosnim pretnjama kao što su računarske prevare, industrijske špijunaže, hakerske sabotaže, virusi itd. Opstanak organizacija je u direktnoj vezi sa njenom sposobnosti da zaštiti svoje informacione vrednosti. Tako koncept zaštite, odnosno sigurnosti informacija izbija u prvi plan.

Savremena poslovna praksa pokazuje da problem sigurnosti informacija nije isključivi problem informacionih tehnologija nego je to više "poslovni" problem kojim mora da se pozabavi najviši nivo menadžmenta organizacije. U njenoj srži je problem upravljanja (menadžment) rizicima.

Serija standarda ISO/IEC 27000, odnosno njeni standardi ISO/IEC 27001:2005 i ISO/IEC 17799:2005 daju jedan harmonizovani pristup upravljanju rizicima kojim su izložene informacione vrednostu u organizaciji kroz razvoj, implementaciju i održavanje menadžment sistema za sigurnost informacija (Information Security Management System - ISMS).

LITERATURA

[1] Kenning, M., *Security management standard - ISO 17799/BS 7799*, BT Technology Journal, Vol 19, No 3, July 2001, (pp 132-136).

[2] Humphreys, T., Plate, A., *An International Common Language for Information Security*, ISMS Journal, Issue 6, Jan 2006, (pp. 2-3).

[3] Vermeulen, C., Van Solms, R., *The infomation security management toolbox - taking the pain out of security management*, Information Management & Computer Security, Vol 10, No 3, 2002, (pp 119-125).

[4] Broderick, S., *ISMS, security standards and security regulations*, Information Security Technical Report IT, 2006, (pp 26-31).
[5] Solms, R., *Information security management: why standards are important*, Information Management & Computer Security, Vol 7, No 1, 1999, (pp 50-57).
[6] Fawaz, M., *Information security management systems* (power-point prezentacija), QMI seminar, Malezija, 2004.
[7] ISO/IEC 27001:2005, *Information technology - security techniques - information security management systems - Requirements*.
[8] ISO/IEC 17799:2005, *Information technology - security techniques - code of practice for information security management.*.