NORME INFORMACIJSKE SIGURNOSTI ISO/IEC 27K

UDK 006.3/8
Stručni rad

Javor Bogati, univ.spec.oec.
Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica
Virovitica, Matije Gupca 5
E-mail: javor.bogati@morh.hr

SAŽETAK *- Svaka moderna organizacija ima razvijen informacijski sustav, a jedan od najvažnijih ciljeva organizacije je osiguranje kontinuiteta poslovanja. Za održavanje neometanosti poslovnog kontinuiteta bitno je da resursi informacijskog sustava u svako vrijeme budu dostupni i cjeloviti, a da povjerljivost podataka i informacija ne bude dovedena u pitanje. Kako bi se to postiglo, potrebno je uvesti sustav upravljanja sigurnošću informacijskih sustava. Taj sustav uz nesmetanost obavljanja djelatnosti organizacije pomaže da se organizacija u svakom trenutku može suočiti s najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na eventualne sigurnosne incidente, te kao takva postaje prepoznata kao pouzdan i moderan poslovni partner.*
Na osnovu praktičnih iskustava u Velikoj Britaniji 1993. godine počelo se s razvojem normi informacijske sigurnosti. Razvijem IT poslovanja, tijekom vremena broj povećavao se i broj normi kao i područja koje one pokrivaju. Dvije međunarodne norme informacijske sigurnosti usvojene su od strane Hrvatskog zavoda za norme, a to su: HRN ISO/IEC 27001 i HRN ISO/IEC 17799.

Ključne riječi*: sigurnost informacijskih sustava, upravljanje sigurnošću, ISO/IEC 27001.*

SUMMARY *- Every modern organization has a developed information system. In order to achieve one of its most important goals, that is the continuity of business, the organization (firm, company) must make sure that the resources of its information system are constantly at hand and complete without compromising data confidentiality. In order to achieve that an information security system has to be installed. That system provides that the business is conducted without interruption and that the organization (firm, company) is ready to face and react to the latest security threats. That in turn makes that firm a reliable and modern business partner.*
Following a practical experience in the UK the development of information security standards has begun in 1993. With the spread of IT businesses, the number of security standards and the fields they cover has gradually expanded. Two international standards of information security have been adopted by the Croatian standards institute: HRN ISO/IEC 27001 i HRN ISO/IEC 17799.

Key words*: information system security, security management, ISO/IEC 27001.*

1. UVOD

Često se informacijska sigurnost isključivo povezuje s klasificiranim podacima i dokumentima. Takvo povezivanje je netočno u današnje vrijeme kada se informacijska sigurnost bavi informacijskim prostorom u cjelini te uvijek postavlja u kontekst sva tri ključna sigurnosna svojstva podataka i dokumenata: povjerljivost, cjelovitost i raspoloživost. Tajnost je pri tome samo jedna potkategorija svojstva povjerljivosti. Svojstvo povjerljivosti danas se promatra u širokom opsegu pojavnosti, od raznih vrsta i stupnjeva tajnosti do privatnosti u smislu fizičkih osoba ili pravnih osoba što uključuje službene ili interne podatke i neklasificirane podatke. Cjelovitost podataka i njihova raspoloživost predviđenim korisnicima vrijedi za sve podatke pa i za one javno objavljene jer i takvi podaci moraju imati vlasnika ili onoga tko vodi brigu o tim podacima u ime vlasnika.

Zakon o informacijskoj sigurnosti (NN 79/07) propisuje obvezu provođenja informacijske sigurnosti za sva tijela državne uprave, jedinice lokalne i područne samouprave, pravne osobe s javnim ovlastima ali i za pravne i fizičke osobe koje ostvaruju pristup klasificiranim i neklasificiranim podacima. Zakon o zaštiti osobnih podataka (NN 103/03) propisuje tu obvezu za sve organizacije u Republici Hrvatskoj koje prikupljaju osobne podatke. Nadalje, Uredba o mjerama informacijske sigurnosti (NN 46/08) propisuje da se za zaštitu neklasificiranih podataka i podataka stupnja tajnosti "ograničeno" među ostalima, za tijela državne uprave koja u svom djelokrugu koriste klasificirane i

neklasificirane podatke, utvrđuje i primjenjuje odgovarajući skup mjera informacijske sigurnosti sukladno normama za upravljanje informacijskom sigurnošću, HRN ISO/IEC 27001 i HRN ISO/IEC 17799.

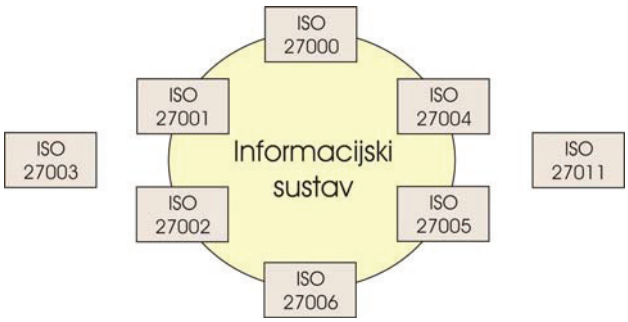
2. NORME SIGURNOSTI INFORMACIJSKIH SUSTAVA

Kako bi se organizacijama javnog i privatnog poslovnog sektora pomoglo pri uvođenju sustava informacijske sigurnosti u svrhu prevencije od zlouporabe, gubitka ili oštećenja podataka i informacija, u Velikoj Britaniji razvijen je standard BS 7799 pod nazivom *"Industry Code of Practice"*. Iz standarda BS 7799 proizašle su ISO/IEC 17799, odnosno ISO/IEC 27002 te ISO/IEC 27001 kao međunarodne norme. Razlog usvajanja standarda BS 7799 kao međunarodne norme je taj što osigurava fleksibilnost, definira upravljački okvir, a ne zadire u konkretnu tehničku implementaciju što je čini primjenjivom u organizacijama različitih tehničkih sustava bez obzira na njihovu veličinu.

Ovo nisu tehničke norme, nego norme upravljanja, a sadrže strukturirani set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću (ISMS – *Information Security Management System*). ISMS predstavlja sistemski pristup u upravljanju sigurnošću informacija prisutnih u organizaciji, a uključuje procese, djelatnike, IT sustav i politiku.

ISO (*engl. International Organization for Standardization*) i IEC (*engl. International Electrotechnical Commission*) zajedno čine sustav za međunarodnu standardizaciju. Organizacija ISO objavila je veći broj normi vezanih uz zaštitu i sigurnost informacijskog sustava:

- ISO 27000 – Pregled normi iz ISO 27k serije;
- ISO 27001 – (2006) Sustav upravljanja informatičkom sigurnošću (ISMS);
- ISO 27002 – (2007) Kodeks postupaka za upravljanje sustava informacijske sigurnosti;
- ISO 27003 – Vodič za uvođenje sustava informacijske sigurnosti;
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti;
- ISO 27005 – (2006) Upravljanje rizicima informacijske sigurnosti;
- ISO 27006 – (2007) Zahtjevi za postupkom analize i certificiranja standarda;
- ISO 27011 – Upute za uspostavu sustava informacijske sigurnosti u telekomunikacijskom sektoru.



Slika 1: Norme informacijske sigurnosti

U pripremi je još normi koje reguliraju pitanja sustava informacijske sigurnosti:

- ISO 27007 – Upute za analizu sustava informacijske sigurnosti;
- ISO 27008 – Upute za upravljanje informacijskom sigurnošću revizije (s naglaskom na sigurnosne kontrole);
- ISO 27013 – Upute o integriranoj primjeni ISO / IEC 20000-1 i ISO / IEC 27001;
- ISO 27014 – Okvir za upravljanja sigurnošću informacija;
- ISO 27015 – Upravljanje sigurnošću informacija - upute za sektor financija i osiguranja;
- ISO 27031 – Specifikacije za informacijsko-komunikacijski kontinuitet ;
- ISO 27032 – Upute za internetsku sigurnost;
- ISO 27033 – Upute za mrežnu sigurnost;
- ISO 27034 – Upute za sigurnost aplikacija;
- ISO 27799 – Sigurnosni sustav u zdravstvu.

2.1. ISO/IEC 27001; ISO/IEC 27002

Od navedenih normi za upravljanje sigurnošću informacijskih sustava najveću važnost imaju ISO/IEC 27002 i ISO/IEC 27001. Primjena ovih normi osigurava usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, kao i povećanje pouzdanosti sustava u slučaju katastrofe te pridonosi povećanju svijesti o nužnosti obuke i osvješćivanja djelatnika vezanim uz informacijsku sigurnost.

Uz norme ISO 27001 (BS 7799-2) i ISO 27002 (ISO 17799) koja detaljnije opisuje na koji način provesti pojedine mjere zaštite iz ISO 27001, kasnije su nastale i norma BS 7799-3 koja detaljno propisuje proces procjene rizika te norme BS 25999-1/BS 25999-2 koje detaljno opisuju upravljanje kontinuitetom poslovanja.

Norma ISO/IEC 27001 usvojena je kao hrvatska norma HRN ISO/IEC 27001:2006 pod nazivom "Sustavi upravljanja informacijskom sigurnošću – Zahtjevi", a norma ISO/IEC 27002 usvojena je kao hrvatska norma HRN ISO/IEC

17799:2006 pod nazivom "Kodeks postupaka za upravljanje informacijskom sigurnošću".

2.1.1. ISO/IEC 27002; ISO/IEC 17799

Norma ISO/IEC 17799 preuzeta je iz prvog dijela BS 7799 standarda *"Code of Practice for Information Security Management"*. Od 1. srpnja 2007. godine ime norme je promijenjeno u ISO/IEC 27002 i predstavlja međunarodnu osnovu za razumijevanje i upravljanje informacijskom sigurnošću, a sastoji se od 11 domena koje opisuju sigurnosne kontrole.

Navedene domene sastoje se od 39 kontrolnih ciljeva i ukupno 133 kontrola koje pomažu u identifikaciji, upravljanju i smanjenju cijelog niza prijetnji kojima su informacije svakodnevno izložene.

2.1.2. ISO/IEC 27001

Drugi dio norme BS 7799-2 "*Specification for Information Security Management systems*", međunarodne oznake ISO/IEC 27001 opisuje sustav upravljanja informatičkom sigurnošću i daje specifikacije za primjenu prvog dijela norme i izgradnje ISMS-a, a sastoji se od četiri osnovna poglavlja:

- sustavi za upravljanje informacijskom sigurnošću (*engl. ISMS - Information Security Management System*);
- odgovornost uprave (*engl. Management Responsibility*);
- ispitivanje sustava upravljanja (*engl. Management Review*);
- poboljšanje sustava za upravljanje informacijskom sigurnošću (*engl. ISMS Improvement*).

S motrišta upravljanja ova četiri poglavlja mogu se sažeti u dva bloka i to:

- sustav za upravljanje sigurnošću koji obuhvaća dokumentiranje, pregled, ispitivanje, odgovornost uprava, korektivne i preventivne mjere te stalno poboljšanje sustava i
- upravljanje informacijskom sigurnošću koji je ciklus uspostave, implementacije, rukovanja, pregledavanja, ispitivanja i poboljšanja sustava za upravljanje informacijskom sigurnošću (ISMS), a koji je opisan modelom PDCA (*engl. Plan-Do-Check-Act*). Navedeni model predstavlja osnovu za pregled norme BS 7799-2. Faze PDCA ciklusa su:
  - PLAN: Uspostava sustava za upravljanje informacijskom sigurnošću;
  - DO: Upravljanje sustavom informacijske sigurnosti;
  - CHECK: Nadzor i ispitivanje sustava informacijske sigurnosti;
  - ACT: Poboljšanje sustava informacijske sigurnosti;

Slika 2: Shema PDCA ciklusa

Iz slike 1 vidljivo je da Plan-Do-Check-Act ciklus nikada ne završava, nego se njegove aktivnosti ciklički ponavljanju kako bi se osigurala ažurnost upravljanja sigurnošću informacijskog sustava.

Uvođenje norme ISO 27001 koja se sastoji od 11 područja, 39 kontrolnih ciljeva i ukupno 133 kontrole koje pomažu u identifikaciji, upravljanju i smanjenju cijelog niza prijetnji kojima su informacije svakodnevno izložene. Pomaže organizaciji kod osiguranja zaštite svoga informacijskog sustava. Primjenom norme osigurava se usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, kao i povećanje pouzdanosti sustava u slučaju katastrofe. Obuci i osvješćivanju djelatnika posvećena je velika pozornost.

2.1.3. Koraci za implementaciju norme ISO/IEC 27001

Za implementaciju norme ISO/IEC 27001 potrebito je uspostaviti i dokumentirati područje upravljanja sigurnošću organizacije. Pod točkom b) članka 3. poglavlja 3.2. navodi se da je potrebno definirati opseg ISMS-a čije granice treba definirati u skladu s karakteristikama organizacije, njene lokacije, vrijednosti i tehnologijom.

Implementacija norme ISO/IEC 27001 provodi se kroz 8 glavnih koraka koje je potrebno slijedno provoditi.

*1. **Započinjanje projekta**.*

Za započinjanje projekta potrebno je osigurati potporu višeg menadžmenta i odabrati i obučiti članove inicijalnog projektnog tima. U ovom koraku nužno je usvojiti sigurnosnu politiku.

*2. **Definiranje ISMS-a**.*

Za implementaciju norme ISO/IEC 27001 potrebito je uspostaviti i dokumentirati područje upravljanja sigurnošću organizacije. Pod točkom b) članka 3. poglavlja 3.2. navodi se da je potrebno definirati opseg ISMS-a čije granice treba definirati u skladu s karakteristikama organizacije, njene lokacije, vrijednosti i tehnologijom.

Inicijalni projektni tim mora definirati okvir upravljanja informacijskom sigurnošću kako bi se fokusirao na ključne elemente. Sigurnosni opseg može pokriti pojedine odjele organizacije ili cjelokupnu organizaciju. Kod utvrđivanja ISMS-a potrebno je jasno utvrditi:

- Cilj i svrhu informacijskog sustava;
- Opseg;
- Granice i ograničenja;
- Međusklopove;
- Ovisnosti;
- Izuzeća i opravdanja;
- Strateški kontekst;
- Organizacijski kontekst.

*3. **Procjena rizika**.*

Potrebno je provesti početnu procjenu sukladnosti statusa sustava za upravljanje informacijskom sigurnošću u okviru kontrola, procesa i procedura zahtijevanih normom ISO 27001.

Idući korak je utvrđivanje imovine i njenog vrednovanja, odnosno utvrđivanje kritičnih i povjerljivih podataka.

Nakon toga potrebno je utvrditi i vrednovati prateću i potpornu imovinu (kvantitativno i/ili kvalitativno), a to je neopipljiva imovina kojom se rukuje i komunicira, koja se obrađuje, pohranjuje, ispisuje, te procesuira i odlaže kroz opipljiva sredstva.

Na kraju se provodi utvrđivanje i vrednovanje prijetnji i ranjivosti, gdje je od velike važnosti prepoznati slabosti svakog dijela imovine koji podržava kritične informacije organizacije. Takve su slabosti ranjive na prijetnje i zbog toga mogu imati negativan učinak na podatke i informacije.

Općenito, **rizik** kao pojam predstavlja kombinaciju vjerojatnosti nekog događaja i utjecaja, odnosno (negativne) posljedice tog događaja u slučaju realizacije prijetnji koje iskorištavaju neku od ranjivosti.

Kad se govori o informacijskoj sigurnosti, rizik (R) za pojedini resurs procjenjuje se procjenom njegove vrijednosti (*engl. asset value* – AV), ranjivosti tog resursa (*engl. vulnerability* – V), prijetnji koje mogu iskoristiti te ranjivosti (*engl. threat* – T), vjerojatnosti ostvarenja prijetnji (*engl. probability* – P) i posljedicama (*engl. impact* – I) koje se mogu dogoditi ukoliko se određena prijetnja ostvari. Dakle, matematički rizik predstavlja funkciju navedenih varijabli.

$$R = f\,(AV, V, T, P, I\,)$$

Također, da bi se rezultati procjene rizika mogli smatrati valjanima, sam proces mora zadovoljiti sljedeće kriterije:

- jednoznačnost;
- objektivnost;
- pouzdanost i
- repetabilnost. (Šegudović,2008.,6)

*4. **Upravljanje rizikom**.*

Prilikom upravljanja rizikom treba izabrati neku od sljedećih opcija:

- smanjenje rizika;
- prihvaćanje rizika;
- izbjegavanje rizika;
- prijenos rizika.

Nakon odabira opcije potrebito je postaviti ciljeve i implementirati kontrole te izraditi plan upravljanja rizikom koji treba sadržavati: zadatke i odgovornosti, imena sudionika, prioritet uprave i drugo. Plan upravljanja rizikom mora se provesti i treba ga nazirati definiranim kontrolama.

*5. **Obuka i osvješćivanje**.*

Organizacija mora osigurati da su svi članovi kojima je dodijeljena odgovornost pri uspostavi ISMS-a osposobljeni za obavljanje svojih zadataka. Uzimajući tu činjenicu u obzir organizacija mora:

- Utvrditi potrebne vještine za rad na informacijskoj sigurnosti;
- Pružiti odgovarajuću obuku i, po potrebi, zaposliti iskusno osoblje za ovaj zadatak;
- Ocijeniti učinkovitost pružene obuke i poduzetih aktivnosti;
- Čuvati zapis o programu obuke za svakog zaposlenika, uključujući i njihove vještine, iskustvo i kvalifikacije.

*6. **Priprema za reviziju**.*

Prije same revizije mora biti izrađena **Izjava o primjenjivosti**. Taj dokument pruža opravdanja o primjenjivosti ili neprimjenjivosti svake od ISO/IEC 27001 kontrola ISMS-a za koju se vrši revizija. Dokument također uključuje, gdje je primjenjivo, te trenutni implementacijski status svake kontrole.

Ukratko, u tom su dokumentu objašnjeni ciljevi, odabrane kontrole i razlozi za njihov odabir, kao i razlozi izuzimanja bilo koje od kontrola propisanih normom ISO/IEC 27001.

*7. **Revizija**.*

Revizija se provodi kroz dva dijela, a to su revizija dokumentacije i revizija implementacije.

*8. **Neprekidno osvješćivanje**.*

Nakon što je implementirano upravljanje sigurnošću informacijskim sustavom, važno je redovito provjeravati i unaprjeđivati upravljački okvir.

3. SVRHA PRIMJENE NORMI SIGURNOSTI INFORMACIJSKIH SUSTAVA

Kao rezultat implementiranja normi informacijske sigurnosti dobiva se jasno definiran okvir nadležnosti, odgovornosti i ovlasti unutar informacijskog sustava. One su, kao rezultat sigurnosnih zahtjeva, prevedene u procedure unutar sigurnosnih pravilnika i ostalih dokumenata. Njihova primjena nužna je za kvalitetnu, odgovornu i uspješnu provedbu sigurnosnih procedura. Njima trebaju detaljno biti određene odgovornost, zaštita i klasifikacija podataka, područje sustava, uporaba interneta i intraneta te suradnja s korisnicima izvan sustava. Planom kontinuiteta poslovanja, koji je također rezultat implementacije normi, definirana su postupanja koja treba provoditi u slučajevima postojanja sigurnosnih rizika. Implementacijom normi procjenjuju se rizici koji ostaju nepokriveni planiranim sigurnosnim mjerama te se analizira mogućnost njihovog ostvarenja i njihov utjecaj na sustav, kao i aktivnosti u slučaju njihovog nastanka. Planom se definira provedba procedura, određuju se osobe za njihovu provedbu, te se utvrđuju potrebna tehnička sredstva za provedbu određenog plana.

Svi korisnici sustava trebaju biti na nesumnjiv način identificirani. Stoga je potrebno definirati plan upravljanja identitetima. On obuhvaća definiciju svih procesa i aktivnosti u kojima se korisnicima sustava dodjeljuju prava i ovlasti pristupa resursima informacijskog sustava, kao i osnove za njihovu dodjelu. Za svaki resurs utvrđuju se uvjeti za dodjelu prava pristupa, ovlasti i opseg prava, te se definira način i slijed postupaka za dodjelu prva pristupa. Izrađuju se precizne procedure koje se moraju poštivati prilikom provedbe, a koje su ključne za uspješnost upravljanja sigurnošću informacijskog sustava.

4. ZAKLJUČAK

Uvođenje sigurnosti informacijskog sustava prema zahtjevima normi iz ISO 27K serije je prilično složen postupak koji je uglavnom definiran kroz samu normu. Ono treba biti shvaćeno kao projekt kojega odlikuju sve opće karakteristike projekta, ako što su ciljevi, rokovi i troškovi, ali i neke posebnosti, poput uvjeta da određeni sudionici trebaju za određene aktivnosti imati specijalizirano i kvalitetno obrazovanje, te iznimno iskustvo kao i primjerena znanja za specifična područjima, poglavito prilikom procjene rizika. Sve sa ciljem čim kvalitetnijeg zadovoljavanja, očuvanja i unapređenja tri osnovana načela sigurnosti informacijskog sustava, a to su cjelovitost, dostupnost i povjerljivost podataka. Uvođenje ISMS-a izaziva troškove koji su ovisni o procjeni rizika. Što je procjena rigoroznija to su i troškovi uvođenja veći. No, s druge strane, preblaga procjena smanjuje troškove, ali je i sigurnost informacijskog sustava manja.

Kvalitetno proveden proces procjene rizika omogućuje rukovodnim strukturama sagledavanje stvarnog stanja sigurnosti te im olakšava donošenje odluka o načinu upravljanja sigurnošću informacijskih sustava. Uz iskustvo značajan je čimbenik kod procjene rizika i dostupna dokumentacija o sustavu za koji se radi procjena rizika, odnosno podaci koji govore o nastalim incidentima unutar sustava.

Među najvažnijim ciljevima svake organizacije je osiguranje neprekinutosti poslovanja, koje u velikoj mjeri ovisi o zaštiti informacijskih i ostalih poslovnih resursa. S tim ciljem, uvođenje sustava upravljanja sigurnošću informacijskog sustava predstavlja provedbu potrebnih mjera za postizanje zadovoljavajuće razine informacijske sigurnosti unutar organizacije. Tako se omogućava nesmetanost obavljanja djelatnosti organizacije, ali i organizacija postaje prepoznata kao pouzdan i moderan poslovni partner, koja se u svakom trenutku može suočiti s najnovijim sigurnosnim prijetnjama i na vrijeme reagirati na eventualne sigurnosne incidente.

LITERATURA

1. Brumec, J.: **Projektiranje i metodika razvoja informacijskog sustava**, Euro Data, Zagreb, 1996.
2. Bubić V., Šmidl, I.: **Risk Managment of Working Capital Requirements**, CECIIS 2008 Proceeedings, Faculty of Organization and Informatics, Varaždin, 2008.

3. ISO 27001 and ISO 27002* Plain English Information Security Managment Definititions, http://www.praxiom.com/iso-27001-definitions.htm (28. 12. 2008.)
4. ISO/BS 17799: 2000
5. ISO/IEC17799:2005,http://www.cert.hr/documents.php?lang=hr&page=4 (11. 7. 2008.)
6. ISO/IEC 27001: 2005
7. Košutić, D.: Norme za informacijsku sigurnost http://sigurnost.info/sto_je_infosec/norme-za-informacijsku-sigurnost.html, (17. 11. 2008.)
8. Kvadra Consluting, Hrvatski prijevod 133 kontrole po Aneksu A norme ISO/IEC 27001, http://www.kvadraconsulting.com/Download/Hrvatski_prijevod_kontrola_po_ISO_27001.pdf (10. 12. 2008.)
9. Nacionalni program informacijske sigurnosti, http://www.cert.hr/documents.php?lang=hr&page=6 (12. 8. 2008.)
10. Šehanović, J., Hutinski Ž., Žugaj M.: **Informatika za ekonomiste**, "Fakultet ekonomije i turizma "Dr. Mijo Mirković", Pula, 2002.
11. Uredba o mjerama informacijske sigurnosti («Narodne novine», broj 46/08)
12. Zakon o informacijskoj sigurnosti («Narodne novine», broj 79/07)
13. Zakon o tajnosti podataka («Narodne novine», broj 79/07)