HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

ISO/IEC 17799:2005

CCERT-PUBDOC-2005-09-133

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Koncept informacijske sigurnosti ne odnosi se isključivo na tehničke mjere zaštite (korisnička imena, zaporke, enkripciju, prava pristupa i sl.), već podrazumijeva administrativne (sigurnosne politike, pravilnici, procedure) i fizičke (video nadzor, zaštita prostorija, fizička kontrola pristupa itd.) mjere.

Obzirom da je za adekvatnu zaštitu informacijskog sustava gotovo neizostavno potrebna kombinacija svih tih mjera, pogotovo kada je riječ o većim organizacijama, efikasna implementacija i nadzor svih potrebnih mjera zaštite i sigurnosnih kontrola zahtjeva dobro definiran sustav za upravljanje sigurnošću.

Sustav za upravljanje sigurnošću moguće je uspostaviti *ad-hoc*, na temelju vlastitih iskustava, korištenjem vlastite metodologije i primjenom proizvoljnih mjera, no vrlo je često nužno sagledati sve moguće (i potrebne) mjere.

U cilju kompletne zaštite informacijskih sustava definirani su različiti standardi koji na različite načine nastoje obuhvatiti kompletni sustav za upravljanje sigurnošću, ili neke njegove aspekte.

Rainbow series nastali su iz potreba američke vojske i administracije, na temelju kojih je kasnije nastao međunarodni ISO 15408 standard. Zatim, brojni američki zakoni koji se odnose na određene gospodarske sektore npr. Health Insurance Portability And Accountability Act (HIPAA) u zdravstvu ili Gramm-Leach-Bliley Act (GLBA) u financijskom sektoru. Nadalje, tu su standardi formirani od organizacija koje se bave revizijom (informacijskih) sustava kao što su SAS70 ili COBIT koji predstavlja skup mjera i ciljeva, a razvijen je od strane ISACA-e, međunarodne udruge revizora informacijskih sustava. Isto tako, koncepti informacijske sigurnosti pokriveni su i ISO 13335, koji je tek 2004 prihvaćen kao međunarodni standard, iako je godinama postojao kao ISO tehnički dokument (eng. TR – *technical report*). Konačno, postoji i IT Baseline Protecion Manual (u originalu IT-Grundschutz - die Basis für IT-Sicherheit), njemačkog ureda za informacijsku sigurnost.

Među svim tim standardima, na međunarodnom planu ipak se sve više i više prihvaća ISO17799/BS7799, što ponajviše se odnosi na Europu i Japan, a donekle i Australiju. Razlog prihvaćenosti ovih standarda jest što osiguravaju fleksibilnost, definiraju upravljački okvir, a ne zadiru u konkretnu tehničku implementaciju, što ih čini primjenjivim u organizacijama različitih tehničkih sustava, iz različitih sektora te različitih veličina.

Ovaj dokument opisuje ISO 17799:2005, novu inačicu ISO 17799 standarda, službeno objavljenu u lipnju 2005, godine, koja nadograđuje prvu inačicu standarda iz 2000. godine. Opisan je razvoj ISO 17799 standarda, razlike između inačica iz 2005. i 2000. godine, te povezanost ISO 17799 s BS7799 standardom.

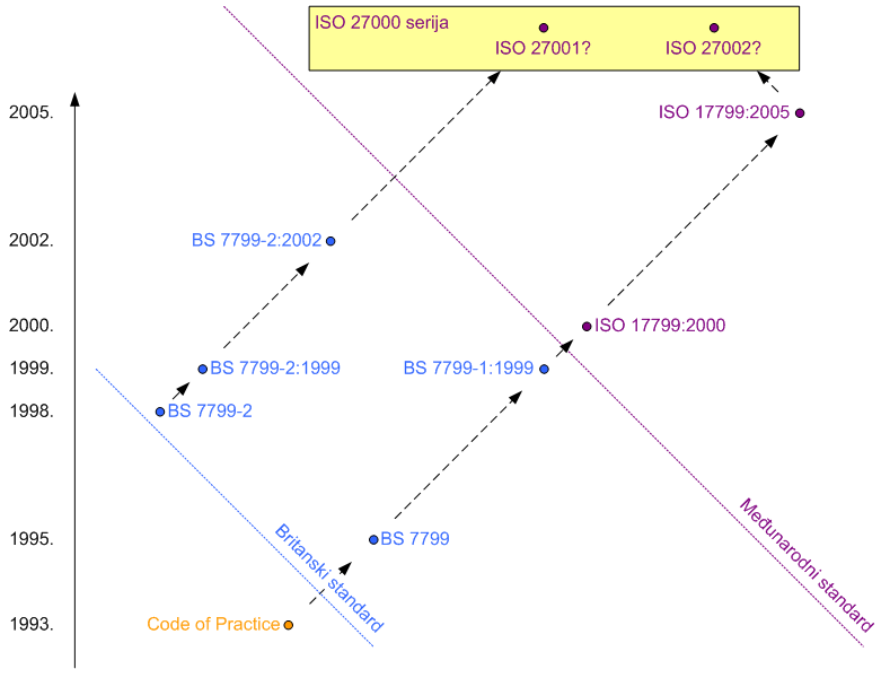
2. Razvoj ISO 17799 standarda

ISO 17799 čvrsto je povezan s BS 7799 standardom, od kojeg je i nastao. British Standards Institute (BSI) je prvi dokument o sigurnosti, odnosno o dobroj praksi u sigurnosti (*Code of Practice*) objavio još 1993. godine. Dokument je dorađen i 1995. postao je britanski standard 7799, no i dalje je definirao isključivo dobru praksu. 1998. objavljen je i BS7799-2 koji specificira sustav za upravljanje sigurnošću (eng. *Information Security Management System – ISMS*), baziran na ciljevima i kontrolama BS 7799-1 standarda. Godinu dana nakon toga, 1999., oba standarda, BS7799-1 i BS7799-2 su revidirana ne bi li se osigurala njihova konzistentnost.

Konačno, 2000. godine BS7799-1, odnosno *code of practice* prihvaćen je kao međunarodni standard ISO 17799:2000. BS 7799-2 koji nije prihvaćen kao međunarodni standard, doživio je još jednu reviziju, tako da je trenutno aktualna inačica BS 7799-2:2002.

Prihvaćanje samo dijela standarda uglavnom je vezano uz, u to vrijeme nepomirene interese zemalja članica ISO komiteta. Rezultat toga je da se organizacije ne mogu certificirati prema ISO 17799 standardu, kako je npr. slučaj s ISO 9001 standardom, pošto ISO 17799 predstavlja samo dobru praksu, dok je specifikacija ISMS sustava definirana u BS7799-2 standardu. Zbog toga je zasad moguća isključivo certifikacija prema BS7799-2 standardu u skladu s ISO 17799 normom.

Obzirom da se područje informacijske sigurnosti, koje pred desetak godina gotovo da i nije postojalo, razvija velikom brzinom, tako da su se ciljevi i kontrole definirani ISO17799:2000 standardom vrlo često smatrali nedostatnim, u lipnju 2005. objavljena je nova inačica ISO 17799 standarda; ISO 17799:2005 koja je unijela neke promjene i dodatke u odnosu na inačicu iz 2000. godine. *Slika 1* prikazuje razvoj ISO 17799 standarda i neka buduća predviđanja.



Slika 1: Razvoj ISO 17799 standarda

3. ISO 17799:2000

Obzirom da je inačica ISO 17799 standarda iz 2000. godine bila prvi međunarodni (ISO) standard vezan uz upravljanje informacijskom sigurnošću, koncepti definirani u tom dokumentu postali su široko prihvaćenima, tako da je za opis i razumijevanje ISO 17799:2005 standarda prvo potrebno opisati njegovu prethodnu inačicu.

Osnovni elementi informacijske sigurnosti koje ISO17799:2000 definira jesu (*Slika 2*):

- povjerljivost (eng. *confidentiality*) – mora osigurati da su informacije dostupna samo ovlaštenim osobama,
- integritet (eng. *integrity*) – mora osigurati točnost i kompletnost informacija i načina njihove obrade,
- raspoloživost (eng. *availability*) – mora osigurati da je informacija raspoloživa kada je to potrebno.

Slika 2: Osnovni elementi informacijske sigurnosti

Ti pojmovi su sami po sebi razumljivi i ne treba ih detaljnije pojašnjavati. Osim toga, ISO 17799:2000 definira i pojmove procjene rizika, kao i upravljanja rizikom.
Procjena rizika je definirana kao procjena prijetnji informacijama, njihovog utjecaja na informacije i ranjivosti informacija i informacijskih sustava, te vjerojatnost njihove pojave.
Upravljanje rizikom je definirano kao proces identificiranja, kontrole i umanjivanja ili eliminacije sigurnosnih rizika koji mogu utjecati na informacijske sustave, koji mora biti financijski opravdan.
Iako razumljivi, ovi pojmovi su donekle preopćeniti.
Također, standard u uvodnom dijelu donosi i kritične faktore uspjeha za implementaciju sustava za upravljanje informacijskom sigurnosti:

- sigurnosna politika, ciljevi i aktivnosti koji odražavaju poslovne ciljeve,
- pristup implementaciji sustava za upravljanje sigurnošću koji odgovara organizacijskoj kulturi,
- podrška uprave,
- razumijevanje sigurnosnih zahtjeva, procjena rizika i upravljanje rizikom,
- efikasno prezentiranje sigurnosti upravi i zaposlenicima,
- distribucija svih relevantnih dokumenata,
- osiguranje odgovarajuće naobrazbe i
- balansiran sustav za mjerenje i evaluaciju sustava sigurnosti, te njegovo unapređivanje.

Čitav standard, osim dva uvodna poglavlja, baziran je na 10 sigurnosnih kategorija (poglavlja) kojima se nastoji pokriti sve aspekte informacijske sigurnosti:

- *Sigurnosna politika* (eng. *Security Policy*),
- *Organizacijska sigurnost* (eng. *Organizational Security*),
- *Klasifikacija i upravljanje resursima* (eng. *Asset Classification and Control*),
- *Osobna sigurnost* (eng. *Personnel Security*),
- *Fizička sigurnost* (eng. *Physical and Environmental Security*),
- *Upravljanje komunikacijama i operacijama* (eng. *Communications and Operations Management*),
- *Kontrola pristupa* (eng. *Access Control*),
- *Razvoj i održavanje sustava* (eng. *Systems Development and Maintenance*),
- *Upravljanje kontinuitetom poslovnih procesa* (eng. *Business Continuity Management*),
- *Usklađenost sa zakonskim i drugim propisima* (eng. *Compliance*).

Svaka od navedenih 10 sigurnosnih kategorija definira sigurnosne ciljeva koje treba ispuniti (eng. *control objectives*), te kontrole (eng. *controls*) koje se mogu primijeniti za ispunjenje tih ciljeva. Standard ukupno definira 36, odnosno 37 ciljeva i 127 mogućih kontrola za njihovo ispunjavanje.
Tijekom vremena, obzirom da su se tehnologije, ali i ukupni pogled na informacijsku sigurnost ubrzano mijenjali, standard je u nekim svojim dijelovima postajao nedostatan, bez obzira što ni u jednom svom dijelu ne definira tehnološke zahtjeve, već samo koncepte sigurnosti, te je njegova revizija postala nužna.

4. ISO 17799:2005

Nova revizija ISO 17799 standarda, ISO 17799:2005 objavljena je u lipnju 2005. godine. Standard je zadržao sličnost s prethodnom inačicom, ali dodao je i neke nove elemente.

4.1. Pojmovi i definicije

Kao prvo, standard proširuje popis pojmova koje definira, pa tako definira sljedeće pojmove i definicije:

- resurs (eng. *asset*) – bilo što, što ima vrijednost za organizaciju,
- kontrola (eng. *control*)– načini upravljanja rizicima, što podrazumijeva politike, procedure, upute, organizacijske strukture koje mogu biti administrativne, tehničke, upravljače ili pravne,
- uputa (eng. *guideline*) – opis koji pojašnjava što i kako se treba činiti da se postignu ciljevi definirani politikama
- sustavi za obradu informacija (eng. *information processing facilities*) – svaki sustav za obradu informacija, servis, infrastruktura ili fizička lokacija,
- informacijska sigurnost (eng. *information security*) – uključuje tri osnovna elementa sigurnosti (povjerljivost, integritet i raspoloživost), a također može uključivati i druge elemente kao što su autentičnost, mogućnost praćenja, neporecivost i pouzdanost.
- sigurnosni događaj (eng. *information security event*) – svaki događaj koji može indicirati narušavanje sigurnosne politike ili dosad nepoznata situacija koja može biti relevantna sa stanovišta sigurnosti,
- sigurnosni incident (eng. *information security incident*) – pojedinačni ili niz sigurnosnih događaja koji mogu narušiti poslovanje i ugroziti informacijsku sigurnost,
- politika (eng. *policy*) – opća namjera i usmjerenje formalno oblikovano od uprave,
- rizik (eng. *risk*) – kombinacija (produkt) vjerojatnosti nekog događaja i njegovih posljedica,
- analiza rizika (eng. *risk analysis*) – sistematično korištenje relevantnih izvora da bi se procijenio rizik,
- vrednovanje rizika (eng. *risk evaluation*) – proces usporedbe procijenjenih rizika obzirom na dane kriterije, a u cilju određivanja ozbiljnosti rizika,
- procjena rizika (eng. *risk assessment*) – proces analize i vrednovanja rizika,
- upravljanje rizikom (eng. *risk management*) – koordinirane aktivnosti koje imaju cilj usmjeravati organizacijske aktivnosti i osigurati kontrolu rizika; upravljanje rizikom tipično uključuje procjenu rizika, umanjivanje rizika, prihvaćanje rizika i komunikaciju,
- umanjivanje rizika (eng. *risk treatment*) – proces odabira i implementacije mjera za umanjivanje rizika,
- treća strana (eng. *third party*) – osoba ili organizacija neovisna od strana koje rješavaju neko pitanje,
- prijetnja (eng. *threat*) – potencijalni uzrok neželjenog događaja koji može rezultirati štetom za sustav ili organizaciju,
- ranjivost (eng. *vulnerability*) – ranjivost resursa ili grupe resursa koja može biti iskorištena od strane prijetnji.

U odnosu na prethodnu inačicu standarda iz 2000. godine, očito je da je popis pojmova i definicija znatno proširen. Pri tom se standard referencira na druge postojeće standarde sigurnosti (ISO/IEC 13335-1:2004, ISO/IEC Guide 73:2002 i ISO/IEC Guide 2:1996). Direktna posljedica detaljnije definicije pojmova i definicija jest točnija specifikacija procesa upravljanja informacijskom sigurnosti, koji je u prvoj inačici standarda bio prilično nedorečen (sam proces upravljanja informacijskom sigurnošću bio je definiran isključio u BS 7799-2 standardu). Očita je tendencija (i potreba) da se svi procesi pri upravljanju informacijskom sigurnošću mogu što bolje i jednoznačnije opisati.

4.2. Ključni faktori uspjeha

Iako se na prvi pogled ne čini važnim, popis kritičnih faktora uspjeha koji je već u prethodnoj inačici standarda definirao opće uvjete koje je potrebno ispuniti da bi sustav za upravljanje informacijskom sigurnošću bio funkcionalan i efikasan, proširen je sljedećim:

- određivanjem budžeta za upravljanje informacijskom sigurnosti i

– uspostavom efikasnog sustava za upravljanje sigurnosnim incidentima.

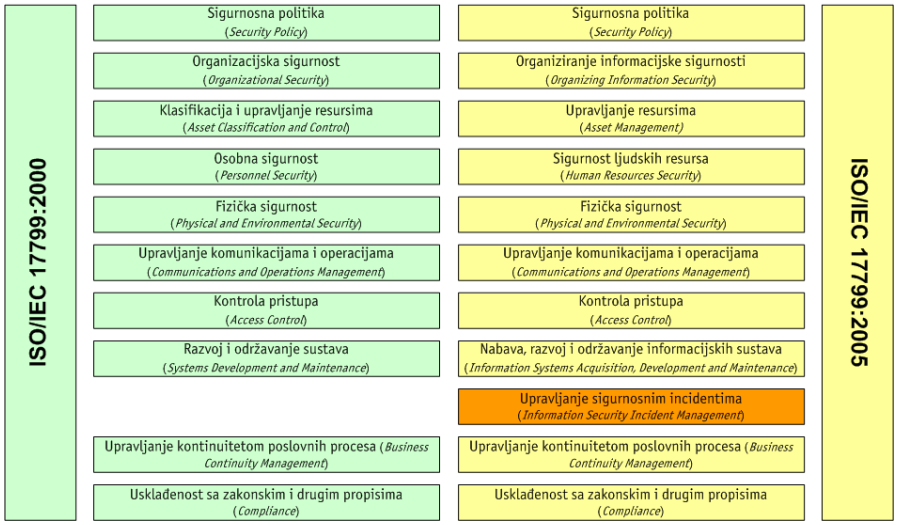
Uvrštavanje ovih faktora u popis kritičnih faktora uspjeha očito je posljedica toga što je praksa pokazala da bez tih faktora sustavi za upravljanje informacijskom sigurnošću ne mogu biti funkcionirati.

4.3. Struktura standarda

ISO 17799:2005 strukturiran je slično kao i njegova inačica iz 2000. godine. Za razliku od prethodne inačice, standard definira 11 glavnih sigurnosnih kategorija (prije 10):

– Sigurnosna politika (eng. *Security Policy*),
– Organiziranje informacijske sigurnosti (eng. *Organizing Information Security*),
– Upravljanje resursima (eng. *Asset Management*),
– Sigurnost ljudskih resursa (eng. *Human Resources Security*),
– Fizička sigurnost (eng. *Physical and Environmental Security*),
– Upravljanje komunikacijama i operacijama (eng. *Communications and Operations Management*),
– Kontrola pristupa (eng. *Access Control*),
– Nabava, razvoj i održavanje informacijskih sustava (eng. *Information Systems Acquisition, Development and Maintenance*),
– Upravljanje sigurnosnim incidentima (eng. *Information Security Incident Management*),
– Upravljanje kontinuitetom poslovnih procesa (eng. *Business Continuity Management*) i
– Usklađenost sa zakonskim i drugim propisima (eng. *Compliance*).

Slika 3 ilustrira sličnosti i razlike nove i stare inačice ISO 17799 standarda.



Slika 3: Usporedba ISO 17799:2005 i ISO17799:2000 standarda

U načelu, sigurnosne kategorije koje su postojale u prethodnoj inačici standarda su dopunjene, a nekima su, u skladu s tim dopunama, nazivi donekle i izmijenjeni. Jedina značajna dopuna sigurnosnih kategorija odnosi se na upravljanje sigurnosnim incidentima, koje u prethodnoj inačici standarda nije bilo. Ono je prepoznato kao ključna sigurnosna kategorija, iako se u nekoliko kategorija marginalno spominjalo.

Nova inačica standarda zadržava definiciju sigurnosnih ciljeva i kontrola, no dodaje i dva nova elementa: upute za implementaciju (eng. *implementation guidance*) i općenitu kategoriju "ostalih informacija" koja sadrži dodatne informacije koje mogu biti relevantne za pojedinu kontrolu.

4.3.1. Sigurnosna politika

Definicija sigurnosne politike i kontrole u ovoj kategoriji nisu značajno promijenjene u odnosu na inačicu standarda iz 2000. godine. Jedina značajna razlika jest u tome da nova inačica naglašava da

sigurnosna politika može biti dio opće politike organizacije, a ne mora nužno predstavljati poseban dokument.

4.3.2. Organiziranje informacijske sigurnosti

Kategorija *Organiziranje informacijske sigurnosti* (u staroj inačici standarda *Organizacijska sigurnost*) doživjela je određene promjene. Terminološki; umjesto pojma *treće strane* (eng. *third parties*) iz stare inačice standarda sada se koristi pojam *vanjski partneri* (eng. *external parties*).
Također, nova inačica standarda kao posebne kontrole definira kontakte s vlastima (ili odgovornim osobama) i kontakte sa specijaliziranim interesnim (sigurnosnim i profesionalnim) grupama, za razliku od stare inačice gdje je kontakt s vlastima bio spomenut marginalno, dok kontakti sa specijaliziranim sigurnosnim grupama nisu bili uopće spomenuti.
Standard je ustvari prihvatio već postojeće stavove da se sigurnost (i sigurnosni incidenti) ne prikrivaju pod svaku cijenu, već je njihovo rješavanje u nekim slučajevima nužno kroz ovlaštene institucije, a komunikacija s drugim stručnjacima kroz sigurnosne i profesionalne grupe i organizacije može uvelike pomoći pri rješavanju internih incidenata ili pri sprječavanju istih.
Također, sigurnosni cilj iz stare inačice standarda, koji se odnosio na obradu informacija kod vanjskih partnera (eng. *outsourcing*), u novoj inačici standarda uključen je u poglavlje *Vanjski partneri*, što je i logično.

4.3.3. Upravljanje resursima

Ova kategorija, iako joj je iz naziva izbačena riječ *klasifikacija* (*Klasifikacija i upravljanje resursima*), i dalje obuhvaća iste ciljeve kao i u staroj inačici standarda.
Nova inačica u tom dijelu ipak donosi neke promjene. Kao prvo, nova inačica naglašava da se moraju identificirati SVI (informacijski) resursi, a nakon toga izdvojiti lista BITNIH informacijskih resursa (stara inačica inzistirala je samo na bitnim informacijskim resursima). Također, još važnije, nova inačica prepoznaje i eksplicitno definira nove kategorije resursa: ljude, njihovo znanje, stručnost i kvalifikacije te *image* i reputaciju organizacije. Konačno, dodane su nove kontrole *Vlasništva nad resursima* (eng. *Ownership of assets*) i *Primjerene uporabe resursa* (eng. *Acceptable use of assets*) kojima se eksplicitno definira odgovornost vlasnika i korisnika resursa, što u prethodnoj inačici standarda nije bilo jasno definirano. Isto tako, nova inačica uvodi i pojam odgovorne osobe (eng. *custodian*) kojoj vlasnik resursa može delegirati određene odgovornosti.

4.3.4. Sigurnost ljudskih resursa

Iako samo donekle promijenjenog imena, ova kategorija značajno je promijenjena. U prethodnoj inačici standarda toj kategoriji (*Osobna sigurnost*) bili su definirani ciljevi sigurnosti u definiciji poslova (eng. *Security in job definition and resourcing*), obuci korisnika (eng. *User training*) i ponašanju u slučaju sigurnosnih incidenata (eng. *Responding to security incidents*).
Nova inačica standarda sigurnosne ciljeve i odgovarajuće kontrole definira kronološki: *Prije zapošljavanja* (eng. *Prior to employment*), *Tijekom radnog odnosa* (eng. *During employment*), *Prestanak radnog odnosa* (eng. *Termination or change of employment*). Neke sigurnosne kontrole preuzete su u manje izmijenjenom obliku iz prethodne inačice standarda, a uz ciljeve koji se odnose na trajanje radnog odnosa i prestanak radnog odnosa, dodane su kontrole koje se odnose na odgovornost uprave, odgovornosti pri prestanku radnog odnosa, vraćanje resursa i uklanjanje prava pristupa.
Može se uočiti da je standard uvažio primjere iz prakse, gdje se pokazuje da pri prestanku ili prekidu radnog odnosa sigurnosni zahtjevi uglavnom nisu sagledani u potpunosti. To se posebno se odnosi na uklanjanje prava pristupa informacijskim sustavima.
Cilj koji se odnosi na ponašanje u slučaju sigurnosnih incidenata u novoj inačici standarda izbačen je iz ove kategorije, te se u izmijenjenom obliku sad nalazi u novo dodanoj kategoriji *Upravljanje sigurnosnim incidentima*.

4.3.5. Fizička sigurnost

Ova kategorija nije značajno izmijenjena u odnosu na prethodnu inačicu standarda. Može se uočiti da su neki ciljevi i kontrole detaljnije i preciznije specificirani, dodana je nova kontrola koja eksplicitno definira zaštitu od vanjskih i prirodnih prijetnji (eng. *Protecting against external and environmental threats*), te je izbačen cilj iz stare inačice standarda koji se odnosio na općenite zahtjeve (eng. *General controls*), koji je bi prilično neujednačen, s tim da je dio kontrola ostao i dalje uključen u ovu kategoriju, a dio koji se odnosio na Sigurno korištenje radnog okruženja (eng. *Clear desk and clear screen policy*) prebačen je u kategoriju *Kontrola pristupa*, cilj *Korisnička odgovornost* (eng. *User responsibilities*), što je i mnogo logičnije.

4.3.6. Upravljanje komunikacijama i operacijama

Upravljanje komunikacijama i operacijama najopsežnija je kategorija nove inačice standarda, a u odnosu na prethodnu inačicu standarda doživjela je značajne promjene. Od sigurnosnih ciljeva iz prethodne inačice standarda uz određene promjene zadržani su sljedeći:

- *Operativna odgovornost i procedure* (eng. *Operational procedures and responsibilities*) – kontrola koja se odnosila na upravljanje incidentima (eng. *Incident management procedures*) u staroj inačici standarda, u novoj inačici spada u kategoriju *Upravljanje incidentima*. Također, kontrola koja se odnosila na upravljanje dijelovima informacijskog sustava koji održavaju vanjski partneri (eng. *External facilities management*) u novoj inačici standarda prepoznata je kao kompleksniji element sigurnosti, tako da predstavlja zaseban sigurnosni cilj koji treba ispuniti.
- *Planiranje novih sustava* (eng. *System planning and acceptance*) – ovaj cilj u novoj inačici nije značajnije izmijenjen u odnosu na staru inačicu standarda.
- *Zaštita od zlonamjernih programa* (eng. *Protection against malicious software*) – ovaj cilj dopunjen je kontrolama koje se odnose na zaštitu od mobilnih programa, pa je i naslov u tom smislu dopunjen – Zaštita od zlonamjernog i mobilnog koda (eng. *Protection against malicious and mobile code*). Standard je ovdje uvažio činjenicu da je korištenje mobilnog koda (ActiveX, Java i slične tehnologije) vrlo rašireno u legitimne, ali i zlonamjerne svrhe.
- *Zaštita mrežne infrastrukture informacijskog sustava* (eng. *Network management* – u staroj inačici, *Network security management* u novoj inačici) – ovaj cilj izmijenjen je utoliko što je dodana nova kontrola koja eksplicitno definira i zaštitu mrežnih servisa.
- *Sigurnost i rukovanje medijima* (eng. *Media handling*) – ovaj cilj nije značajnije izmijenjen u odnosu na staru inačicu standarda.

Osim navedenih ciljeva iz prethodne inačice standarda, novi standard definira ciljeve koje stari standard nije poznavao u tom obliku:

- *Upravljanje vanjskim sustavima* (eng. *External facilities management*) – kako je već spomenuto predstavlja u novom standardu, zbog uočene važnosti, poseban cilj, za razliku od stare inačice standarda gdje je bio definiran samo kao kontrola.
- *Sigurna pohrana podataka* (eng. *Back-up*) – predstavlja cilj koji je preciznije definiran u odnosu na cilj iz prethodnog standarda *Održavanje informacijskog sustava* (eng. *Housekeeping*), a koji je osim kontrola za sigurnosnu pohranu podataka sadržao i elemente vezane uz bilježenje informacija koji u novoj inačici predstavljaju poseban cilj (*Nadgledanje sustava*).
- *Razmjena informacija* (eng. *Exchange of information*) – iako ovaj cilj ima vrlo sličan naziv kao i u staroj inačici standarda: *Razmjena informacija i programske podrške* (eng. *Exchange of information and software*), konceptualno je prilično promijenjen tako da su u novoj inačici standarda predložene kontrole puno konzistentnije obzirom na cilj.
- *Elektroničko poslovanje* (eng. *Electronic commerce services*) – novi standard uočio je važnost sigurnosti ovog aspekta poslovanja, te ga navodi kao poseban cilj, za razliku od stare inačice koja je aspekte elektroničkog poslovanja prilično šturo definirala kroz posebnu sigurnosnu kontrolu vezanu uz *Razmjenu informacija i programske podrške*.
- *Nadgledanje sustava* (eng. *Monitoring*) – ovo poglavlje objedinjuje kontrole koje su se odnosile na različite ciljeve iz stare inačice standarda. Na taj način izbjegnuto je pojavljivanje sličnih elemenata u različitim dijelovima dokumenta (*Upravljanje komunikacijama i operacijama*, *Kontrola pristupa*), te je osigurana veća koherentnost.

4.3.7. Kontrola pristupa

Ova kategorija logički nije značajno izmijenjena u odnosu na staru inačicu standarda. Jedina značajna promjena jest da cilj *Nadgledanje pristupa i korištenja sustava* (eng. *Monitoring system access and use*) u novoj inačici standarda više nije dio kategorije *Kontrola pristupa*, već je dopunjen s nekim kontrolama iz drugih kategorija, sada dio kategorije *Upravljanje komunikacijama i operacijama*.
Također, u cilj *Korisnička odgovornost* dodana je kontrola Sigurno korištenje radnog okruženja (eng. *Clear desk and clear screen policy*), koja je u staroj inačici standarda bila dio *Općenitih zahtjeva* kategorije *Fizička sigurnost*.
Ostali ciljevi iz ove kategorije ostali su isti, dok su kontrole izmijenjene i osuvremenjene u tolikoj mjeri da bolje opisuju načine zaštite modernih informacijskih sustava.

4.3.8. Nabava, razvoj i održavanje informacijskih sustava

Kod ove kategorije promijenjen je naziv, tako da sada preciznije identificira na što se odnosi (u staroj inačici standarda *Razvoj i održavanje sustava*). Iz stare inačice standarda preuzeti su svi ciljevi, čije kontrole su u određenoj mjeri dopunjene i osuvremenjene. Najznačajnije promjene napravljene su kod cilja *Kriptografske kontrole* (eng. *Cryptographic controls*) gdje su preporuke za implementaciju preciznije nego u staroj inačici standarda i referenciraju druge vanjske izvore i standarde (ISO/IEC JTC1 SC27, IEEE P1363, OECD Guidelines on Cryptography, ISO/IEC 9796, ISO/IEC 14888).
Također, nova inačica standarda definira cilj *Upravljanje tehničkim ranjivostima* (eng. *Technical vulnerability management*) koji nije postojao u staroj inačici standarda, a u praktičnom održavanju sigurnosti današnjih informacijskih sustava je nezaobilazan.

4.3.9. Upravljanje sigurnosnim incidentima

Upravljanje sigurnosnim incidentima (eng. *Information security incident management*) je nova kategorija koja se pojavljuje u ISO 17799:2005 standardu. Kategorija definira dva cilja:

- *Prijavljivanje sigurnosnih incidenata i ranjivosti* (eng. *Reporting information security events and weaknesses*) i
- *Upravljanje sigurnosnim incidentima i unapređenjem informacijske sigurnosti* (eng. *Management of information security incidents and improvements*).

Ova kategorija predstavlja skup ciljeva i sigurnosnih kontrola, od kojih je većina postojala i u prethodnoj inačici standarda no, međutim, te su kontrole bile definirane u različitim kategorijama i ciljevima, (*Osobna sigurnost – Prijavljivanje sigurnosnih incidenata i nepravilnosti u radu, Upravljanje komunikacijama i operacijama – Operativne procedure i odgovornosti, te Usklađenost sa zakonskim i drugim propisima – Sukladnost sa zakonskom regulativom*).
Standard je uočio da je upravljanje sigurnosnim incidentima jedinstven proces, te ga na taj način i definirao, što predstavlja znatno unaprjeđenje u odnosu na staru inačicu standarda.

4.3.10. Upravljanje kontinuitetom poslovnih procesa

Kategorija upravljanja kontinuitetom poslovnih procesa strukturalno gotovo da i nije promijenjena. U načelu kontrole koje nova inačica standarda predlaže gotovo da su identične kontrolama iz prethodne inačice. Sintaksa koja se koristi u novoj inačici standarda ipak je preciznija, a iz definicije sigurnosnog cilja koje se kontrole iz ove kategorije moraju ispuniti može se uočiti da je sigurnost ipak samo dio općenitijeg procesa upravljanja kontinuitetom poslovnih procesa, dok je prethodna inačica implicirala da je kompletno upravljanje kontinuitetom poslovnih procesa dio informacijske sigurnosti.
Može se zaključiti da je to posljedica višegodišnjih trendova kroz koje se informacijska sigurnost više ne promatra isključivo kao dio IT-a, već se sve više i više smatra integralnim dijelom u ukupnom odvijanju poslovnih procesa i poslovanju.

4.3.11. Usklađenost sa zakonskim i drugim propisima

Ova sigurnosna kategorija smisleno gotovo da i nije promijenjena. Kontrole su iste kao i u ranijoj inačici standarda. Kontrola *prikupljanje dokaza*, koja je izbačena u odnosu na inačicu standarda iz 2000. godine je u novoj inačici standarda dio kategorije *Upravljanje sigurnosnim incidentima*.

5. Zaključak

Nova inačica ISO/IEC 17799 standarda, iako ne donosi revolucionarne promjene, ipak prilično unaprjeđuje sigurnosne kategorije poznate iz prethodne inačice, a isto tako donosi i novu kategoriju *Upravljanja sigurnosnim incidentima*. Ostale kategorije, prenesene iz stare inačice standarda u većoj su ili manjoj mjeri promijenjene, dopunjene i modernizirane.

Također, u novoj inačici standarda određeni je broj kontrola pregrupiran i pridružen drugim ciljevima, odnosno kategorijama. Na taj način standard je postao koherentniji, a izbjegnuta su ponavljanja sličnih kontrola u različitim kategorijama i ciljevima (npr. kategorija *Upravljanje sigurnosnim incidentima* ili cilj *Nadgledanje sustava*). Dodani su i novi ciljevi, koje stara inačica standarda nije poznavala, iako je njihovo ispunjavanje u današnjim informacijskim sustavima bilo nužno (npr. *Upravljanje tehničkim ranjivostima*).

Predložene kontrole su u novoj inačici standarda bolje definirane i preciznije, iako i dalje omogućavaju fleksibilnost uporabe. Također, standard na više mjesta referencira i druge relevantne sigurnosne standarde i dokumente (npr. ISO/IEC 13335 i ISO/IEC 15408 serije itd.).

Najveći nedostatak standarda, međutim i dalje ostaje nepostojanje međunarodno priznatog standarda koji bi definirao implementaciju sustava za upravljanje sigurnošću u skladu s preporukama iz ovog standarda, nego je trenutno još uvijek aktualan britanski standard BS 7799-:2002.

U bliskoj budućnosti ipak se očekuje prihvaćanje ISO 27000 serije sigurnosnih standarda koji bi konačno trebali osigurati kompletni i međunarodno priznati okvir za uspostavu sustava za upravljanje informacijskom sigurnošću. ISO 27000 serija trebala bi se sastojati od 6 različitih dokumenata (ISO 27000, ISO 27001, ISO 27002, ISO 27003, ISO 27004 i ISO 27005), od kojih bi uskoro trebala biti prihvaćena tri: ISO 27000 – s popisom pojmova i definicija, ISO 27001 – specifikacija sustava za upravljanje informacijskom sigurnošću (trenutno je to BS 7799-2), te ISO 27002 – skup kontrola i preporuka, koji bi trebao zamijeniti ISO 17799.

6. Literatura

[1] International standard ISO/IEC 17799:2000 "Information technology – Code of practice for information security management"

[2] International standard ISO/IEC 17799:2005 "Information technology – Security techniques – Code of practice for information security management"

[3] British standard BS 7799-2:2002 "Information security management systems – Specification with guidance for use"

[4] ISO 27001 security, http://www.iso27001security.com