mr. sc. Kristian Saletović

SIGURNOST POSLOVNIH INFORMACIJSKIH SUSTAVA

priručnik

2015.

Nakladnik:
Grupa VERN d.o.o.,
Trg bana Josipa Jelačića 3, Zagreb

Za nakladnika:
Branko Štefanović

Urednik:
Tomislav Štuka

Recenzenti:
prof. dr. sc. Mario Spremić
dr. sc. Ozren Kubelka, v. pred.

Lektura:
Vicko Krampus

Grafičko oblikovanje:
BIP d.o.o.

CIP zapis dostupan u računalnom katalogu Nacionalne i sveučilišne knjižnice u Zagrebu pod brojem 000900814

ISBN
978-953-99244-9-0

SADRŽAJ

PREDGOVOR

Ovaj je priručnik ponajprije namijenjen studentima specijalističkoga diplomskog studija IT menadžmenta na Veleučilištu VERN'. Osim toga, zasigurno će biti koristan i ostalim studentima diplomskih studija iz područja informacijskih tehnologija i sustava, računarstva, menadžmenta, ekonomije poduzetništva i poslovnog upravljanja te onima koji žele steći ili osvježiti znanja o informacijskoj sigurnosti i sustavu upravljanja informacijskom sigurnošću.

Osnovni su ciljevi priručnika osvijestiti važnost informacijske sigurnosti u današnjem poslovnom okruženju, upoznati studente s osnovnim pojmovima i konceptima informacijske sigurnosti te potaknuti studente na daljnje samostalno proučavanje stručne i znanstvene literature iz izrazito propulzivnog područja informacijske sigurnosti.

Priručnik obuhvaća osam poglavlja. U prva se dva uvodna poglavlja definiraju i pojašnjavaju pojmovi *informacija* i *informacijska sigurnost* te prikazuju osnovna svojstva informacije i razlozi zašto je informacije potrebno štititi i zašto je informacijska sigurnost nužna u poslovanju. Najveći dio priručnika zauzima treće poglavlje pod naslovom *Sustav upravljanja informacijskom sigurnošću (ISMS)* u kojem se detaljno prikazuju pojedinačni koraci uvođenja sustava upravljanja informacijskom sigurnošću u poslovanje te uloga obitelji standarda ISO/IEC 27000 u tome. Važni pojedinačni aspekti sustava upravljanja informacijskom sigurnošću zasebno se obrađuju u poglavljima koja slijede. Četvrto je poglavlje posvećeno dokumentaciji, odnosno hijerarhiji dokumentacije sustava. Poglavlje pod naslovom *Upravljanje rizicima* obrađuje postupak procjene rizika, ranjivosti i prijetnje, načine procjene vjerojatnosti i štete te opcije za obradu rizika. Postupak klasificiranja informacija i klasifikacijske razine informacija obrađuju se u šestom poglavlju. Sedmo je poglavlje posvećeno

fizičkoj sigurnosti, odnosno aspektu informacijske sigurnosti koji je u praksi često zapostavljen. Završno je poglavlje posvećeno održavanju poslovanja u kriznim situacijama.

Sva su poglavlja strukturirana na sličan način. Na početku se nalazi popis informacija i znanja koja će studenti steći nakon što obrade određeno poglavlje. Cilj je studentima olakšati snalaženje u tekstu i pomoći im da se prilikom učenja usmjere na najvažnije. Postupci, procesi i podjele koje se opisuju u tekstualnom dijelu poglavlja u pravilu su uvijek prikazani i u obliku slika ili tablica. Na taj se način dvostrukim kodiranjem želi olakšati usvajanje novih znanja i informacija te potaknuti studente da prilikom proučavanja stručne i znanstvene literature iz područja na sličan način organiziraju informacije kako bi ih bolje razumjeli i brže usvajali. Uz ključne nazive na hrvatskome jeziku u zagradama su kurzivom navedeni engleski termini jer je veliki dio literature iz područja informacijske sigurnosti na engleskome jeziku. Osim olakšavanja snalaženja u literaturi na engleskome jeziku, cilj je ukazati na mogućnost i važnost stvaranja hrvatskog nazivlja. Na kraju se poglavlja nalaze prijedlozi za daljnje čitanje za one koji žele produbiti svoja znanja o pojedinim aspektima i elementima informacijske sigurnosti te za one koji iz navedenih područja žele izraditi specijalistički diplomski stručni rad.

Nadamo se da će priručnik biti koristan studentima te da će im poslužiti kao pregledan uvod i poticaj za stjecanje dodatnih znanja iz područja informacijske sigurnosti.

INFORMACIJA

U OVOME ĆEMO POGLAVLJU NAUČITI:

- ŠTO JE INFORMACIJA
- ZAŠTO JE POTREBNO ŠTITITI INFORMACIJU
- KOJA SU OSNOVNA FUNKCIONALNA SVOJSTVA INFORMACIJE.

INFORMACIJA

Riječ informacija često susrećemo u različitim situacijama u svakodnevnome životu. Hrvatski jezični portal **informaciju** definira kao: 1. obavijest o činjenicama, izvještaj o nečemu i 2. novost koju prenosi koja izvjestiteljska agencija, radio ili televizija.[1] Osim svakodnevne uporabe, riječ informacija zastupljena je u specijaliziranim znanstvenim područjima. Informacija je jedan od ključnih pojmova u informacijskim znanostima, u kojima se u načelu definira kao svaki podatak koji u određenome kontekstu ima vrijednost za vlasnika i korisnike. Hrvatski jezični portal uz treće značenje riječi informacija navodi leksikografsku odrednicu *inform.* kojom se upućuje na područje informatike i informacijskih znanosti u kojem riječ ima svoje specifično značenje: rezultat obrade podataka i podaci u bilo kojem stupnju obrade.

Polazeći od navedenoga specifičnog značenja riječi informacija, možemo postaviti pitanje je li 24519 informacija. Odgovor na pitanje je negativan jer se podatak koji nije smješten u kontekst u informacijskim znanostima ne smatra informacijom. Kada podatak stavimo u kontekst, koji može biti i naša pretpostavka, onda on postaje informacija i dobiva vrijednost za vlasnika i korisnike informacije. Ako uz broj 24519 poznajemo kontekst, primjerice ako smo na određeni način došli do saznanja da je riječ o posljednjih pet znamenki broja kreditne kartice neke osobe, onda 24519 postaje informacija i dobiva određenu vrijednost.

Komunikacijski, računalni ili drugi elektronički sustavi koji obrađuju, pohranjuju ili prenose podatke kako bi bili dostupni ovlaštenim korisnicima i kako bi ih oni mogli upotrebljavati nazivaju se **informacijskim sustavima** (*information system,* skraćeno IS)**.**

[1] Hrvatski jezični portal http://hjp.novi-liber.hr

I**nformacijska tehnologija** (*information technology,* skraćeno IT) je tehnologija koja se koristi za upravljanje i obradu informacija (računala, telekomunikacije i sl.)

Važno je razumjeti da ne postoji znak jednakosti između informacijskog sustava i informacijske tehnologije jer je informacijski sustav, kao što je vidljivo iz prethodno navedenih definicija, širi koncept od same informacijske tehnologije.

Već smo naglasili da informacije imaju određenu vrijednost za korisnike i stoga ih je potrebni štititi kao i svaku drugu vrstu imovine. Primjerice, u konferencijskim dvoranama, sobama za sastanke i predavaonicama obično se nalaze projektori (fizička imovina) koji se štite različitim mjerama. Obično su pričvršćeni za nosače, na ulazu u zgradu nalaze se portiri i/ili djelatnici zaštitarskih tvrtki, a često postoji i videonadzor. Informacija se kao vrsta imovine razlikuju od projektora i ostale pokretne imovine, te stoga postoje specifičnosti u načelima i metodama zaštite informacijske imovine. Informacijska sigurnost se u članku 2. Zakona o informacijskoj sigurnosti[2] određuje kao stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Povjerljivost, cjelovitost i **raspoloživost** smatraju se **glavnim funkcionalnim svojstvima informacija**. U literaturi na engleskome jeziku često se rabi naziv **C I A** koji je sastavljen od početnih slova navedenih svojstava na engleskome jeziku: povjerljivost (***c****onfidentiality*), cjelovitost (***i****ntegrity*) i raspoloživost (***a****vailability*). Hrvatsko nazivlje za područje informacijskih znanosti nije do kraja ujednačeno pa se uz termine *povjerljivost*, *cjelovitost* i *raspoloživost* kao istoznačnice rabe *tajnost*, *integritet* i *dostupnost*. U ovome priručniku rabimo termine *povjerljivost*, *cjelovitost* i *raspoloživost* jer se oni rabe u Zakonu o informacijskoj sigurnosti.

Hrvatska norma HRN ISO/IEC 27001 definira **povjerljivost** kao svojstvo informacije koja nije dostupna ili otkrivena neovlaštenim osobama, entitetima i procesima. Drugim riječima, informacija ne smije biti dostupna ili doći u ruke nikome tko za to nije ovlašten ili kome nije namijenjena. Primjerice, elektroničke poruke (*e-mail*) u pravilu su namijenjene isključivo primatelju i mnoge od njih sadrže izjave o odricanju

[2] *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07

odgovornosti. U njima se, između ostaloga, naglašava da je sadržaj poruke i priloženih dokumenata povjerljiv i namijenjen isključivo osobama ili subjektima koji su navedeni kao primatelji. Ako je uslijed greške u adresiranju ili prijenosu poruka pogrešno upućena, „neželjeni" se primatelji mole da obavijeste pošiljatelja te poruku zajedno s priloženim dokumentima trajno i bez prethodnog uvida u sadržaj uklone sa svoga računala. Povjerljivost kao svojstvo informacije najlakše je povezati s konceptom informacijske sigurnosti, a primjeri vođenja brige o povjerljivosti informacija zabilježeni su još u doba Rimljana. Julije Cezar koristio je tehniku osiguravanja povjerljivosti poruka koje je slao putem svojih izaslanika, danas poznatu pod nazivom Cezarov enkripcijskih algoritam. Riječ je o razmjerno jednostavnom zamjenskom algoritmu na osnovi kojeg bi se sva slova abecede pomaknula za određeni broj mjesta, pa bi se primjerice umjesto A rabilo B, umjesto B C itd.[3]

Osnovne su metode osiguravanja povjerljivosti informacija kontrola pristupa (fizička ili logička) te enkripcija. U praksi se često rabe zajedno. Jedan od najčešćih primjera narušavanja povjerljivosti informacija u poslovnome okruženju odnosi se na neovlašteni uvid u dokumente koji se nalaze na radnom stolu ili na zaslonu računala.

Hrvatska norma HRN ISO/IEC 27001 definira **cjelovitost** kao svojstvo očuvanja točnosti i kompletnosti informacije. Informacije nije dopušteno mijenjati bez odgovarajućeg ovlaštenja, što znači da neovlaštene osobe ne smiju mijenjati informacije te da ovlaštene osobe smiju unositi samo one izmjene i promjene za koje imaju ovlaštenje. U praksi su zabilježeni različiti primjeri narušavanja cjelovitosti informacija: brisanje dijelova dokumenata, maliciozni kod koji briše dokumente ili mijenja dijelove datoteka, namjerne ili nenamjerne pogreške u radu osoba ovlaštenih za pristup informacijama. Cjelovitost informacija osigurava se na isti način kao i povjerljivost – kontrolom pristupa, enkripcijom ili kombinacijom navedenih metoda.

Hrvatska norma HRN ISO/IEC 27001 definira **raspoloživost** kao svojstvo dostupnosti i upotrebljivosti informacije na zahtjev ovlaštenog entiteta. Ovlašteni entitet može biti korisnik, računalni sustav, tvrtka, organizacija, državno tijelo i slično. Raspoloživost nije nužno vezana uz razdoblje u kojemu je informaciju moguće dobiti na uvid i uporabu.

[3] Detaljnije o Cezarovom enkripcijskom algoritmu u Kahate, A. (2008), 41–43

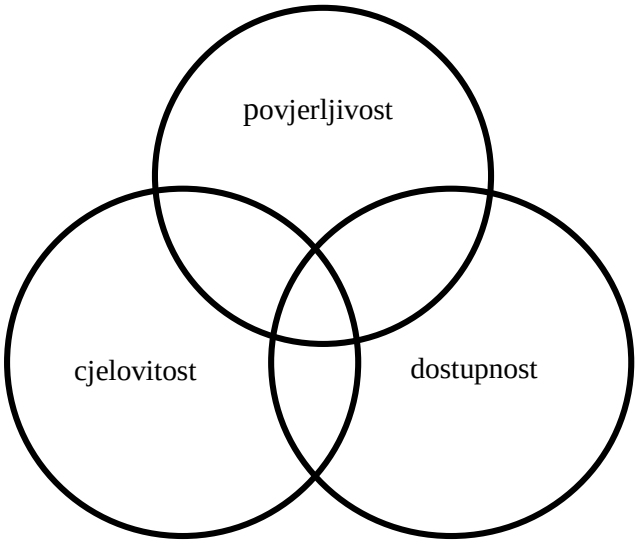
Postoje sustavi visoke raspoloživosti (*high availability systems*) kod kojih razina raspoloživosti iznosi do 99,99999%. Takvi se sustavi temelje na tehničkim rješenjima (duplo napajanje na serverima, diskovi spojeni u RAID polje, itd.) kojima se redundantnošću te kvalitetom izvedbe i materijala postiže izrazito nizak stupanj ispada sustava, što je prikazano u tablici 1. Takvi se sustavi rabe u vojsci, policiji, zrakoplovstvu, telekomunikacijama i djelatnostima u kojima je to uvjetovano vrstom posla koji obavljaju.

Raspoloživost %	**Vrijeme ispada tijekom godine**
90% („jedna devetka“)	36,5 dana
95%	18,25 dana
97%	10,96 dana
98%	7,30 dana
99% („dvije devetke“)	3,65 dana
99,5%	1,83 dana
99,8%	17,52 sati
99,9% („tri devetke“)	8,76 sati
99,95%	4,38 sati
99,99% („četiri devetke“)	52,56 minuta
99,999% („pet devetki“)	5,26 minuta
99,9999% („šest devetki“)	31,5 sekundi
99,99999% („sedam devetki“)	3,15 sekundi

Tablica 1. Razine raspoloživosti i pripadajuće vrijeme ispada na godišnjoj razini

S druge pak strane, postoje slučajevi u kojima informacija ne mora ili ne može biti odmah raspoloživa. Ponekad se dostupnost mjeri u satima ili danima, posebice ako se informacije nalaze pohranjene duboko u arhivima.

Granice među svojstvima povjerljivosti, cjelovitosti i raspoloživosti nisu apsolutne te među njima postoje određena preklapanja, kao što je vidljivo na slici 1.



Slika 1. Glavna funkcionalna svojstva informacije

U poslovnome su okruženje učestale situacije u kojima su istovremeno narušena dva ili tri svojstva informacije. Kao jednostavan primjer može nam poslužiti situacija u kojoj zaposlenik, za vrijeme razgovora sa zaposlenikom odjela ljudskih potencijala, na zaslonu njegova računala vidi ugovor o radu nekoga drugog zaposlenika, odnosno dio ugovora o radu koji se odnosi na financijske i ostale uvjete. Budući da su navedene informacije poslovna tajna, u opisanom je slučaju istovremeno došlo do narušavanja svojstva povjerljivosti i dostupnosti.

U prethodnim smo odlomcima prikazali glavna funkcionalna svojstva informacija. Ako su ona narušena, riječ je o razotkrivanju (*disclosure*), promjeni (*alternation*) i/ili prekidu (*disruption*). Razotkrivanje se odnosi na narušavanje povjerljivosti, promjena na narušavanje cjelovitosti, a prekid na kratkotrajnu ili dugotrajnu neraspoloživost informacija. Opisane su situacije zasigurno nepoželjne u poslovnome okruženju i cilj je svake organizacije svesti ih na najmanju moguću mjeru. Stoga ćemo u poglavljima koja slijede prikazati osnovna načela, elemente i obilježja sustava upravljanja informacijskom sigurnošću.

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Andress, J. (2011). *Basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (poglavlje 1). Waltham: Elsevier.
2. Kahate, A. (2008). *Cryptograophy and network security* (poglavlje 2). New Delhi: Tata McGraw-Hill.
3. Krausz, M. (2010). *Managing information security breaches: Studies from real life* (poglavlje 3). Cambridgeshire: IT Governance Publishing.

PITANJA ZA PONAVLJANJE:

1. Definirajte informaciju i osnovna funkcionalna svojstva informacije.
2. Zašto je potrebno štititi informacijsku i fizičku imovinu tvrtke?
3. Navedite po dva primjera narušavanja:
    a. povjerljivosti
    b. cjelovitosti i
    c. raspoloživosti.

INFORMACIJSKA SIGURNOST

U OVOME ĆEMO POGLAVLJU NAUČITI:

- ŠTO JE INFORMACIJSKA SIGURNOST
- ZAŠTO JE POTREBNA INFORMACIJSKA SIGURNOST.

INFORMACIJSKA SIGURNOST

U prethodnome smo poglavlju definirali **informacijsku sigurnost** kao stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Informacijska je sigurnost potrebna iz nekoliko razloga. Jedan je od razloga činjenica da informacija, kao što smo prikazali u prethodnome poglavlju, ima određenu vrijednost za vlasnika i korisnike. Ona može predstavljati intelektualno vlasništvo, ako je primjerice riječ o zaštićenom programskom kodu, ili može uključivati poslovne tajne, kao što su podaci o zaposlenicima, kupcima, dobavljačima, marketinškim i financijskim planovima. Osim toga, informacijska sigurnost u velikoj mjeri ovisi o informacijskoj tehnologiji (IT), koja je podložna čestim promjenama. Zbog toga su moguće pogreške, a prilikom povezivanja različitih sustava često dolazi do nekompatibilnosti.

Nadalje, postoji zakonska regulativa koja poslovne subjekte obvezuju na zaštitu informacija i osobnih podataka, na održavanje kontinuiteta poslovanja i slično. Zakonska regulativa razlikuje se od države do države. U Republici Hrvatskoj postoji Zakon o informacijskoj sigurnosti[4] kojim se utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti te nadležna tijela nadležna za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. On se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, na pravne osobe s javnim ovlastima koje u svome djelokrugu koriste klasificirane i neklasificirane podatke te na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. Pojam

[4] *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07

klasificiranih i neklasificiranih podataka, stupnjeve tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima te njihovu zaštitu utvrđuje Zakon o tajnosti podataka.[5] Zakon o zaštiti osobnih podataka[6] uređuje zaštitu osobnih podataka i nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj. Zakon o kreditnim institucijama[7] i Odluka Hrvatske narodne banke o primjerenom upravljanju informacijskim sustavom[8] uređuju način na koji su banke i stambene štedionice obvezne upravljati svojim informacijskim sustavom. Za poslovne subjekte važan je i Zakon o zaštiti i spašavanju koji ih u članku 18.[9] obvezuje na izradu plana kontinuiteta poslovanja (*business continuity plan*). Nadalje, članak 19. Zakona o zaštiti tajnosti podataka[10] koji propisuje pojam, vrste i stupnjeve tajnosti te mjere i postupke za utvrđivanje, uporabu i zaštitu tajnih podataka, određuje da poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese. Iz gore navedene zakonske definicije proizlazi da je poslovnu tajnu potrebno regulirati internim aktom organizacije. U protivnom nije moguće poduzeti stegovne mjere protiv osoba koje su poslovnu tajnu učinile javno dostupnom ili otuđile. Tehničke mjere zaštite podataka, kao što su kriptiranje ili autorizacija pristupa, nisu dostatne ako zaštita nije pravno regulirana. Internim se aktima o poslovnim tajnama, između ostaloga, propisuje način na koji se djelatnici i vanjski suradnici obvezuju na čuvanje poslovne tajne. To uključuje potpisivanje ugovora o povjerljivosti (*non-disclosure agreement*), aneksa ugovora i posebnih izjava. Slika 2. prikazuje tehničke i pravne elemente zaštite poslovne tajne.

[5] *Zakon o tajnosti podataka,* Narodne novine 79/07

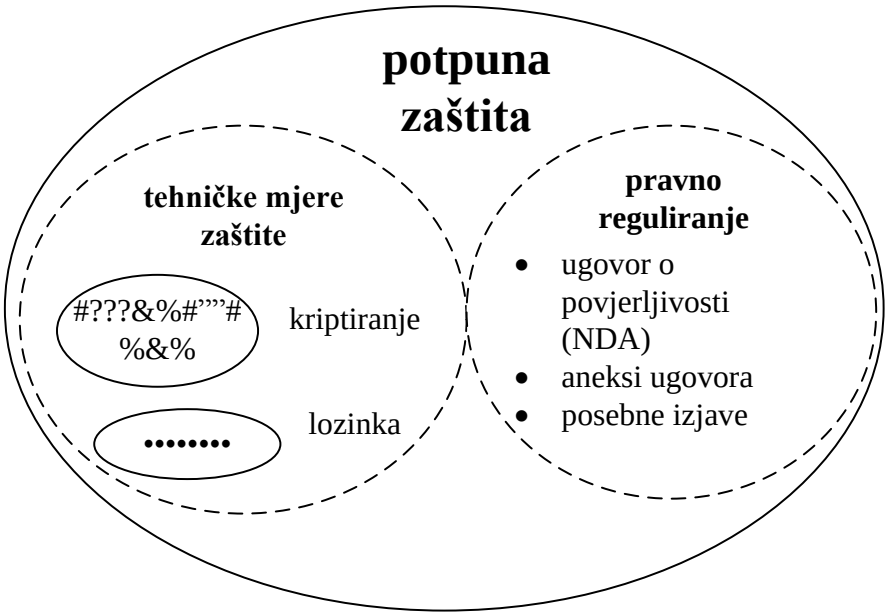
[6] *Zakon o zaštiti osobnih podataka*, Narodne novine 103/03

[7] *Zakon o kreditnim institucijama*, Narodne novine 117/08

[8] *Odluka Hrvatske Narodne banke o primjerenom upravljanju informacijskih sustavom*, Narodne novine 37/10

[9] *Zakon o zaštiti i spašavanju*, Narodne novine 174/04

[10] *Zakon o zaštiti tajnosti podataka*, Narodne novine 108/96



Slika 2. Tehnički i pravni elementi zaštite poslovne tajne

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management standard* (poglavlje 2). Norwood: Artech House.
2. *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07
3. *Zakon o tajnosti podataka*, Narodne novine 79/07
4. *Zakon o kreditnim institucijama*, Narodne novine 117/08, 74/09, 153/09 i 108/12

PITANJA ZA PONAVLJANJE:

1. Kako se može postići potpuna zaštita poslovne tajne?
2. Kojim se zakonom regulira informacijska sigurnost i na koga se on primjenjuje?

SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU (ISMS)

U OVOME ĆEMO POGLAVLJU NAUČITI:

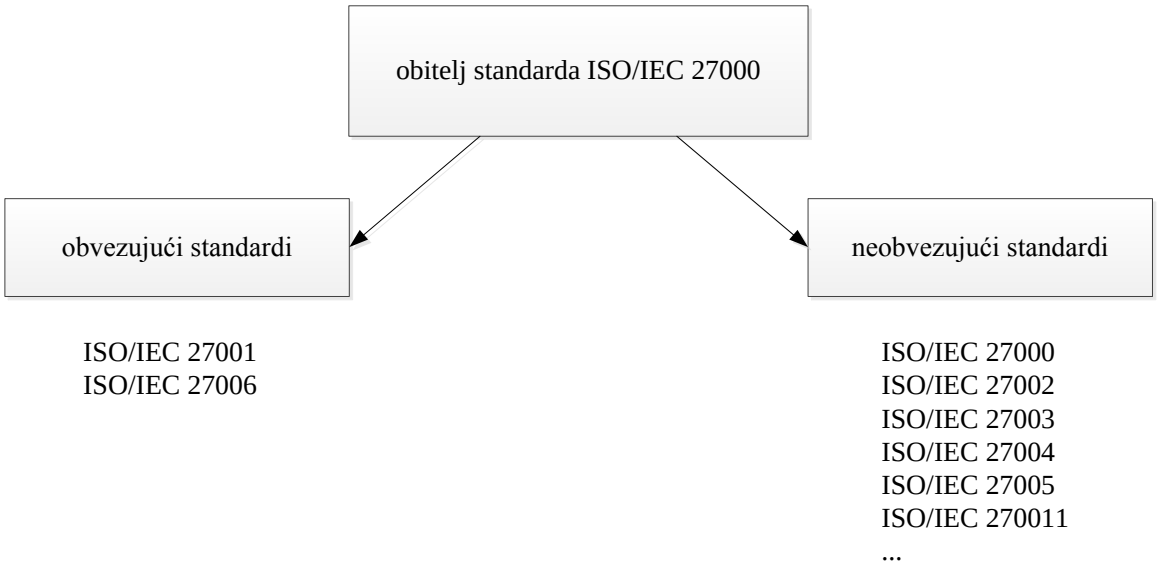
- ŠTO JE ISMS
- ZAŠTO SE ISMS UVODI U POSLOVANJE
- ŠTO JE OBITELJ STANDARDA ISO/IEC 27000
- OSNOVNA OBILJEŽJA STANDARDA ISO/IEC 27001
- KORAKE U UVOĐENJU SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU U POSLOVANJE I OSNOVNO O SVAKOM POJEDINAČNOM KORAKU.

SUSTAV UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU (ISMS)

Sustav upravljanja informacijskom sigurnošću (*Information Security Management System*) skup je politika i procedura koje imaju za cilj očuvanje osnovnih svojstava informacije. U literaturi je uvriježena kratica ISMS koja se sastoji od početnih slova termina na engleskome jeziku.

Sustav upravljanja informacijskom sigurnošću uvodi se u poslovanje iz različitih razloga. Uz zakonsku regulativu koju smo ukratko prikazali u prethodnome poglavlju, jedan od razloga za uvođenje sustava upravljanja informacijskom sigurnošću želja je i potreba poslovnih subjekata da mogućnost štete u poslovanju svedu na najmanju moguću mjeru. Na taj se način podiže razina konkurentnosti te razina povjerenja kupaca i vanjskih suradnika, osigurava se kontinuitet poslovanja itd.

Iskustva najbolje prakse i preporuke za osmišljavanje, uvođenje i održavanje sustava za upravljanje informacijskom sigurnošću pretočena su u obitelj standarda ISO/IEC 27000. ISO (*International Organization for Standardization*) je Međunarodna organizacija za normizaciju, a IEC (*International Electrotechnical Commission*) je Međunarodna komisija za elektrotehniku. ISO i IEC tvore specijalizirani sustav za normizaciju na svjetskoj razini. Države članice organizacija ISO i IEC sudjeluju u razvijanju međunarodnih normi radom u tehničkim povjerenstvima za pojedinačna područja tehnike. Obitelj standarda ISO/IEC 27000 prikazana na slici 3. obuhvaća obvezujuće i neobvezujuće standarde.



Slika 3. Obitelj standarda ISO/IEC 27000

Obvezujući standardi propisuju što je potrebno učiniti za dobivanje certifikata. Neobvezujući standardi prikazuju kako se ono što je potrebno za dobivanje certifikata može učiniti, što znači da sadrže preporuke i smjernice na osnovi najbolje prakse, no ne propisuju da se to mora učiniti upravo na takav način.

Obvezujući standardi unutar obitelji ISO/IEC 27000 su:

- standard ISO/IEC 27001 i
- standard ISO/IEC 27006.

Standard ISO/IEC 27001 obvezan je za sve poslovne subjekte koji se žele certificirati za sustav upravljanja informacijskom sigurnošću. Certifikat ISO/IEC 27001 potvrđuje da je sustav upravljanja informacijskom sigurnošću uveden u poslovanje sukladno standardu ISO/IEC 27001. Standard ISO/IEC 27006 obvezan je za tvrtke koje se bave certificiranjem za standard ISO 27001.

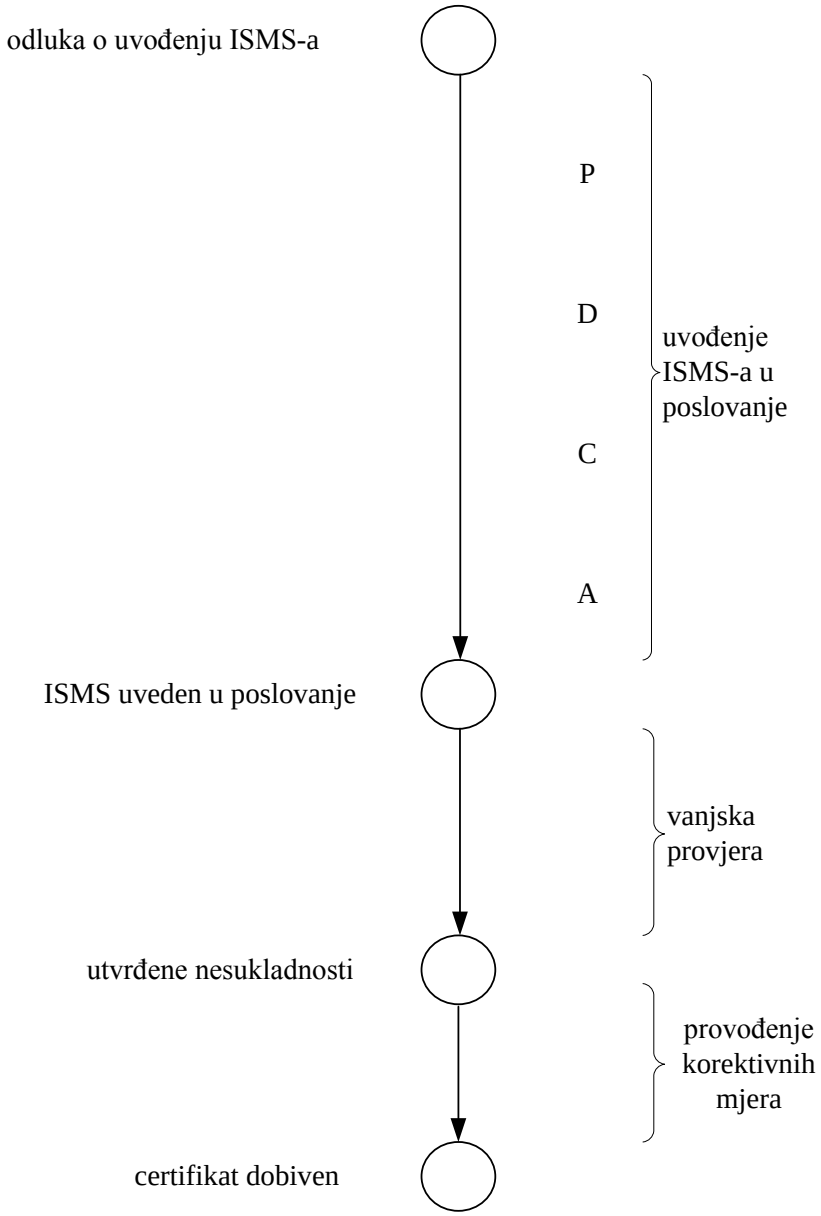
U skupinu neobvezujućih standarda spadaju sljedeći standardi:

- ISO/IEC 27002
- ISO/IEC 27003
- ISO/IEC 27004
- ISO/IEC 27005 i

- ISO/IEC 27011.

Standard ISO/IEC 27002 obuhvaća smjernice za zadovoljavanje kriterija standarda ISO/IEC 27001, a standard ISO/IEC 27003 smjernice za uvođenje sustava upravljanja informacijskom sigurnošću. Smjernice za metriku sustava upravljanja informacijskom sigurnošću sadržane su u standardu ISO/IEC 27004, a smjernice za upravljanje rizicima u standardu ISO/IEC 27005. Standard ISO/IEC 27011 donosi smjernice za uvođenje sustava upravljanja informacijskom sigurnošću u telekomunikacijskoj industriji. Organizacije ISO i IEC sustavno rade na promišljanju, osmišljavanju i objavi novih standarda u okviru obitelji standarda ISO/IEC 27000. Stoga je skupina neobvezujućih standarda otvorena, što je prikazano i na slici 3.

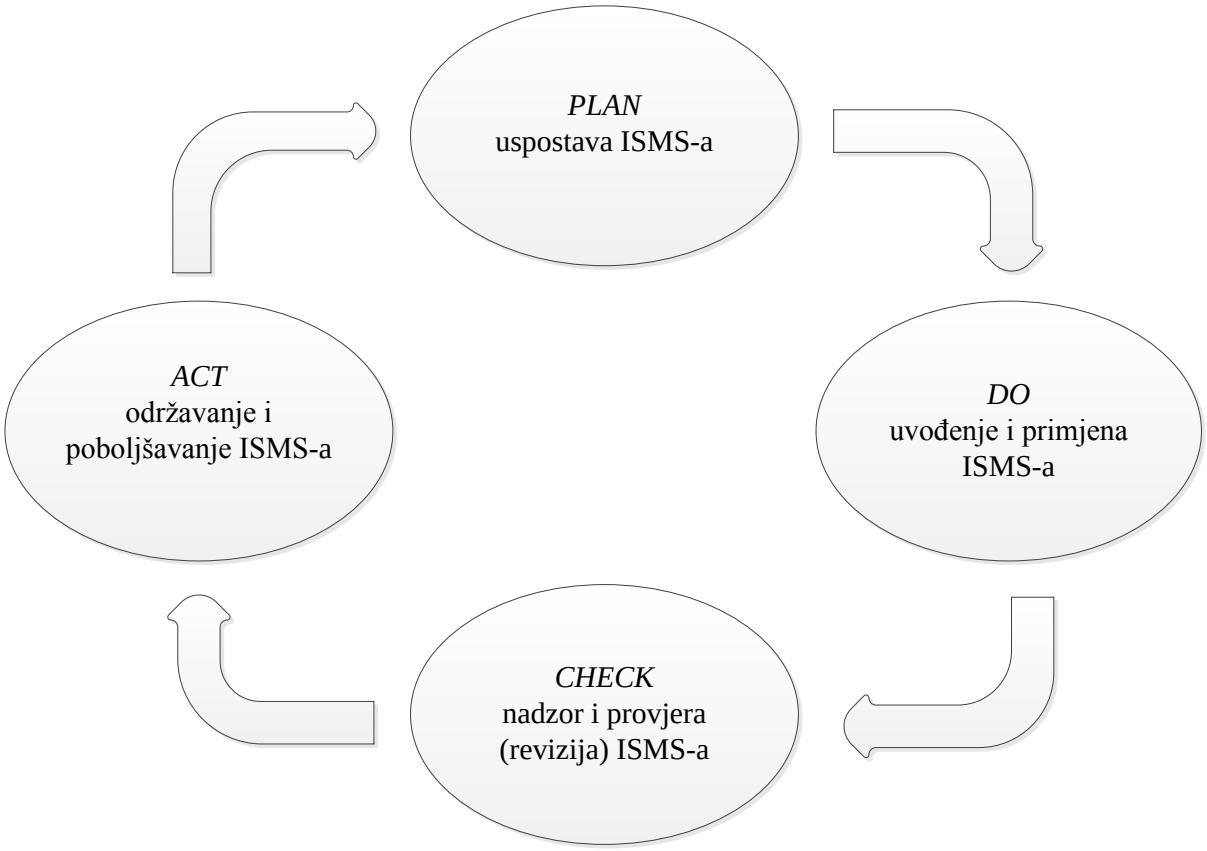
Standard ISO/IEC 27001 okvir je za uspostavu, uvođenje, primjenu, nadzor, provjeru (reviziju), održavanje i poboljšavanje sustava upravljanja informacijskom sigurnošću te kao takav predstavlja specifikaciju navedenoga sustava upravljanja. Generičkog je karaktera, što znači da se može primijeniti na različite vrste organizacija i poslovnih subjekata, neovisno o njihovoj veličinu, djelatnosti i ostalim obilježjima. Prvi korak za dobivanje certifikata ISO/IEC 27001 je uvođenje sustava upravljanja informacijskom sigurnošću u poslovanje.



Slika 4. Put do dobivanja certifikata ISO/IEC 27001

Put do dobivanja certifikata, kao što je vidljivo na slici 4., obuhvaća četiri koraka. Nakon donošenja odluke o uvođenju sustava upravljanja informacijskom sigurnošću slijedi najduži korak, odnosno samo uvođenje. Kao što smo naveli u prethodnim odlomcima, smjernice i preporuke za zadovoljavanje kriterija i uvođenja sustava navedene su u neobvezujućim standardima ISO/IEC 27002 i ISO/IEC 27003. Uvođenje se temelji na procesnom pristupu čije je temeljno polazište da je za učinkovito funkcioniranje organizacije nužno utvrditi međusobno povezane procese te njima upravljati na jednostavan i efikasan način. Načelo koje je izravno povezano s procesnim pristupom upravljanju je načelo neprekidnog poboljšanja. Metodologiju neprekidnog poboljšanja

razvio je Walter Shewhart, a danas je poznata i u širokoj je uporabi pod nazivom *Demingov krug*.[11] *Demingov krug* obuhvaća sljedeće radnje: **P** (P*lan*), **D** (*Do*), **C** (*Check*) i **A** (A*ct*).[12] **P** se odnosi na planiranje i uspostavljanje procesa nužnih za ostvarivanje ciljeva, **D** označava primjenu procesa, **C** nadziranje i mjerenje procesa s obzirom na postavljenje ciljeve, a **A** poduzimanje radnji za daljnja poboljšanja procesa. *Demingov krug*, odnosno **model PDCA** primijenjen na sustav upravljanja informacijskom sigurnošću prikazan je na slici 5.



Slika 5. Model PDCA primijenjen na sustav upravljanja informacijskom sigurnošću

Faza *Plan* uključuju uspostavu politika, procedura i mjera s ciljem poboljšanja informacijske sigurnosti. **Faza *Do*** obuhvaća uvođenje kontrola (sigurnosnih protumjera) i unaprjeđenje poslovnih procesa i procedura. U **fazi *Check*** provode se procjena i mjerenje učinkovitosti uvedenih procedura te se pripremaju izvještaji potrebni za unutarnju i vanjsku provjeru sustava upravljanja informacijskom sigurnošću. U **fazi *Act*** se na osnovi provjera i ocjena menadžmenta poduzimaju

[11] Detaljnije o tome u Swamidassu, P. M. (2000), 156

[12] Detaljnije o tome u Kreitner, M. (2009), 481–483

korektivne i preventivne aktivnosti u cilju poboljšanja sustava upravljanja informacijskom sigurnošću.

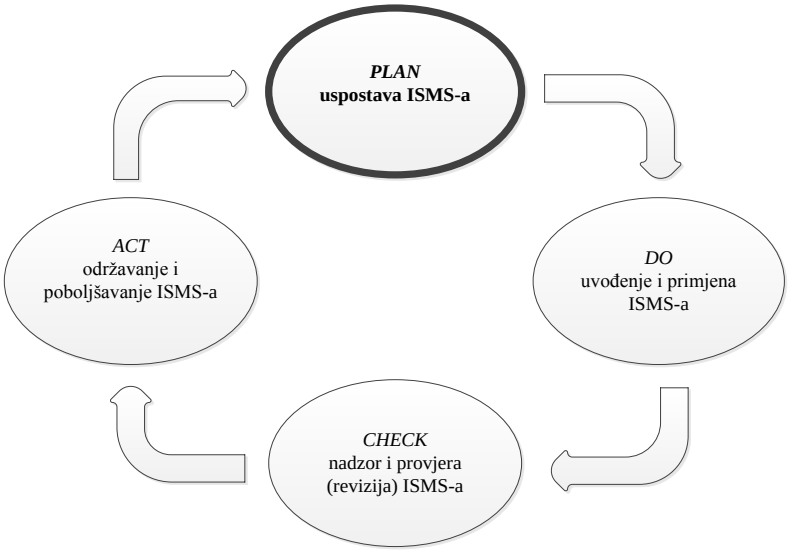
Nakon uvođenja ovog sustava, tvrtka ovlaštena za certificiranje provodi vanjsku provjeru usklađenosti sustava upravljanja informacijskom sigurnošću sa zahtjevima norme ISO/IEC 27001. U većini slučajeva daje preporuke za provođenje korektivnih mjera. Ako se korektivne mjere provedu na odgovarajući način, poslovni subjekt dobiva certifikat ISO/IEC 27001. Certifikat se u pravilu dobiva na razdoblje od tri godine nakon čega slijedi postupak ponovnog dobivanja certifikata. U međuvremenu je poslovni subjekt obvezan provoditi unutarnje provjere na godišnjoj razini, a tvrtka ovlaštena za certificiranje na godišnjoj razini provodi vanjske nadzorne provjere.

Osim ISO/IEC 27001 okvira postoje i drugi standardi za upravljanje informacijskom sigurnošću ili pojedinim područjima sigurnosti, a specifični su u svojoj namjeni i području:

- PCI DSS – standard koji u sklopu zakonske regulative osigurava okvir za uspostavu čvrstih procesa za prijenos podataka u kartičnom poslovanju, uključivši prevenciju, detekciju i prikladnu reakciju na sigurnosne ispade.
- CobiT – okvir za vođenje IT-a (*IT Governance*). Razvio ga je Institut za vođenje IT-a (*IT Governance Institute*). CobiT je otvoreni standard neovisan o tehnološkim platformama te omogućuje kontrolu nad informacijskom tehnologijom.
- NSIT (*National Institute of Standard and Technology*) je glavna udruga SAD-a za standarde i jedna od svjetskih standardizacijskih udruga. U svome opsegu sadrži nekoliko standarda vezanih uz upravljanje informacijskom sigurnošću.
- SANS institut (*SysAdmin, Audit, Networking, and Security*) je privatna tvrtka iz SAD-a koja se specijalizirala za sigurnost na internetu. Najviše se bavi školovanjem i certifikacijom ljudi u području sigurnosti.

USPOSTAVA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

U uvodnom smo dijelu poglavlju prikazali što je to sustav upravljanja informacijskom sigurnošću te iz kojih se razloga i na koji način uvodi u poslovanje. Prvi korak u okviru procesa uvođenja koji smo prikazali pomoću modela PDCA je **faza *Plan***, odnosno uspostava sustava upravljanja informacijskom sigurnošću, čime ćemo se, kao što je prikazano na slici 6., detaljnije baviti u ovome potpoglavlju.

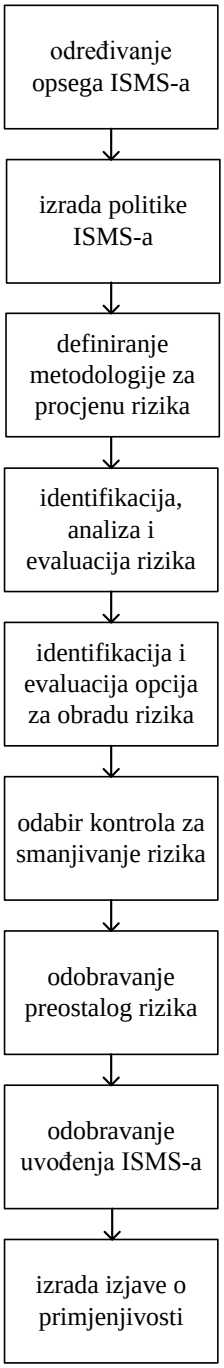


Slika 6. Faza Plan u okviru modela PDCA

Hrvatska norma HRN ISO/IEC 27001 određuje način uspostave sustava upravljanja informacijskom sigurnošću. Kao što je prikazano na slici 7., uspostava obuhvaća sljedećih devet koraka:

1. određivanje opsega sustava upravljanja informacijskom sigurnošću
2. izradu politike sustava upravljanja informacijskom sigurnošću
3. definiranje metodologije za procjenu rizika
4. identifikaciju, analizu i evaluaciju rizika

5. identifikaciju i evaluaciju opcija za obradu rizika
6. odabir kontrola za smanjivanje rizika
7. odobravanje preostalog rizika
8. odobravanje implementacije sustava upravljanja informacijskom sigurnošću,
9. izradu izjave o primjenjivosti.



Slika 7. Pojedinačni koraci za uspostavu sustava upravljanja informacijskom sigurnošću (vlastiti rad autora prema Marijanović, I. (2010), 64)

Prvi je korak **određivanje opsega sustava upravljanja informacijskom sigurnošću**. Određuju se granice sustava, odnosno precizno se definira područje nad kojim će se provesti postupak certifikacije. Prilikom definiranja opsega moguće je obuhvatiti cjelokupno poslovanje (sve poslovne procese ili usluge) ili samo dijelove poslovanja (pojedine poslovne procese ili usluge). U praksi se često kao opseg definira samo dio poslovanja jer je uvođenje sustava upravljanja informacijskom sigurnošću u cjelokupno poslovanje, posebice ako je riječ o velikim tvrtkama, vrlo zahtjevan i skup posao. Nakon određenog vremena ili zbog poslovnih potreba moguće je proširiti opseg certifikacije. U okviru definiranja opsega preporučljivo je sastaviti i popis imovine.

Sljedeći je korak **izrada politike sustava upravljanja informacijskom sigurnošću** (*information security management system policy* ili *ISMS policy*). Taj se dokument smatra ključnim dokumentom jer se u njemu definiraju ciljevi i smjernice za uspostavu sustava. Odobrava se na najvišoj razini menadžmenta poslovnog subjekta. Važno je naglasiti da politika mora biti u skladu sa strategijom upravljanja rizicima u okviru sustava upravljanja informacijskom sigurnošću.

Definiranje metodologije za procjenu rizika treći je korak u uspostavi sustava upravljanja informacijskom sigurnošću. Prilikom odabira metodologije potrebno je voditi računa o kriterijima jednoznačnosti, ponovljivosti i prikladnosti. Kriterij jednoznačnosti znači da je dobivene rezultate moguće međusobno uspoređivati, odnosno da oni nisu dvosmisleni. Kriterij ponovljivosti znači da se metodologija može primjenjivati više puta jer je sukladno normi rizik potrebno procjenjivati barem jednom godišnje te nakon svake značajnije promjene imovine koja je obuhvaćena opsegom sustava upravljanja informacijskom sigurnošću. Kriterij prikladnosti odnosi se na odabir kvantitativne ili kvalitativne metode procjene rizika.[13] Kvalitativna metoda procjene rizika prikladna je za procjenu rizika u poslovnim procesima i projektima, dok je kvantitativna metoda prikladna za financijske ustanove. Primjerice, baza podataka koja se nalazi na starom (knjigovodstveno amortiziranom) serveru primjenom kvantitativne metode ima nisku vrijednost, dok se primjenom kvalitativne metode, ako je riječ o poslovno vrijednim podacima, može utvrditi znatno veća vrijednost.

[13] Detaljnije o tome u Vellani, K. H. (2007), 109–119

Četvrti je korak **identifikacija, analiza i evaluacija rizika**. Provodi se na imovini koja spada u opseg sustava upravljanja informacijskom sigurnošću. Najprije se utvrđuju prijetnje za imovinu i ranjivost imovine. Slijedi procjena utjecaja prijetnji i ranjivosti na osnovna svojstva informacije i utjecaja na cjelokupno poslovanje. Na kraju se procjenjuju mogućnosti sigurnosnog incidenta, odnosno je li rizik prihvatljiv ili ga je potrebno obraditi. Primjerice, ako se utvrdi da postoji prijetnja otuđivanja prijenosnih računala koja sadrže povjerljive poslovne informacije, analizom se utvrđuje da se gubitak i zlouporaba takvih podataka može izrazito negativno odraziti na poslovanje te se rizik procjenjuje neprihvatljivim i potrebno ga je tretirati na određeni način.

Identifikacija i evaluacija opcija za obradu rizika je sljedeći korak u uspostavi sustava upravljanja informacijskom sigurnošću. Opcije za obradu rizika, odnosno njegovo tretiranje uključuju smanjivanje rizika, prihvaćanje rizika, izbjegavanje rizika i prenošenje rizika. U praksi se najčešće koristi smanjivanje rizika primjenom odgovarajućih kontrolnih procedura. Prisjetimo li se prethodnog primjera s prijetnjom otuđivanja prijenosnih računa, odgovarajuća kontrola bila bi kriptiranje podataka na prijenosnim računalima ili bolja kontrola prostora u kojima se oni nalaze (nadzorne kamere, alarmi, zaštitari, itd.). Prihvaćanje rizika odnosi se na svjesno i objektivno prihvaćanje rizika u skladu s politikom sigurnosti i kriterijima za prihvaćanje rizika. Izbjegavanje rizika odnosi se na izbjegavanje situacija u kojima može doći do pojave rizika, primjerice privremena zabrana rada na daljinu ako se procjeni da je takav rad visokorizičan. Prenošenje rizika odnosi se na prebacivanje rizika na treću stranu, primjerice osiguravajuća društva, dobavljače, podugovarače itd. Radi postojanja visokog rizika od krađe, poslovni subjekti često za prijenos većih količina novca s jedne lokacije na drugu angažiraju zaštitarske tvrtke i na taj način rizik prenose na njih.

Sljedeći korak je **odabir kontrola za smanjivanje rizika**. Kontrole za smanjivanje rizika navedene su u Aneksu A Norme ISO/IEC 27001.[14] Aneks sadrži 114 kontrola, no broj nije konačan i može se po potrebi proširivati. Odabir kontrola mora biti usklađen s kriterijima za prihvaćanje rizika te pravnim, regulatornim i ugovornim zahtjevima. Primjer kontrole za smanjivanje rizika je politika čistog stola (*clear desk policy*), koja

[14] Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission*.

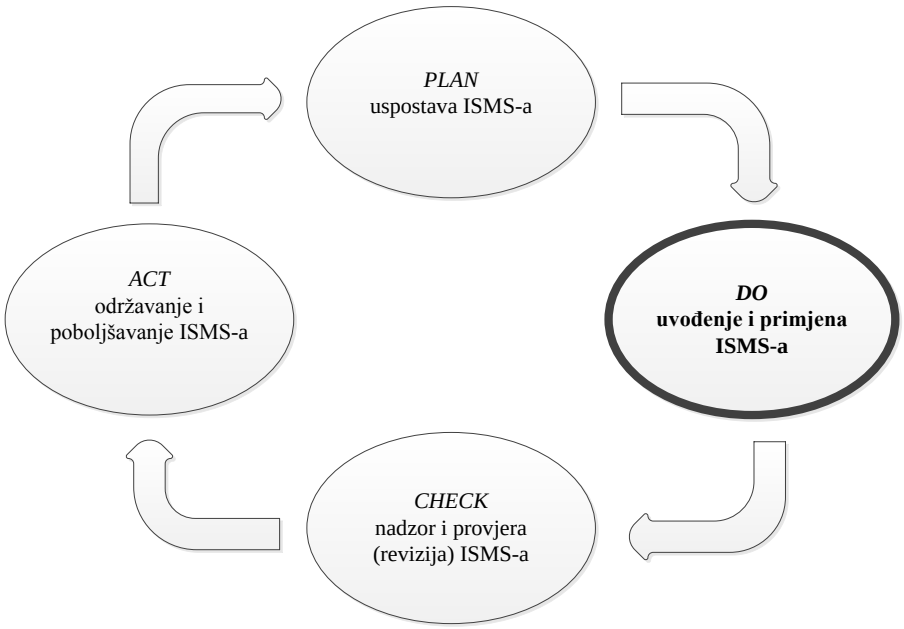
propisuje da djelatnici sa svoga radnog stola moraju ukloniti sve povjerljive dokumente kada nisu na svome radnom mjestu.

Za sljedeća dva koraka u uspostavi sustava upravljanja informacijskom sigurnošću potrebno je odobrenje uprave poslovnog subjekta. Riječ je o **odobravanju uvođenja kontrola** i **svjesnom prihvaćanju određenih rizika**, odnosno o odobravanju uvođenja sustava upravljanja informacijskom sigurnošću.

Posljednji korak je **izrada izjave o primjenjivosti** (*statement of applicability*). U literaturi se učestalo rabi kratica **SoA**. Ona sadrži ciljeve i razloge uporabe kontrola i razloge isključenja nekih kontrola. Nakon uspostave sustava slijedi faza *Do*, tj. drugi korak u postupku uvođenja sustava upravljanja informacijskom sigurnošću, koji ćemo prikazati u sljedećem potpoglavlju.

UVOĐENJE I PRIMJENA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

Drugi korak u procesu uvođenja sustava upravljanja informacijskom sigurnošću koji smo prikazali pomoću modela PDCA je **faza *Do***. Ona uključuje prvotno uvođenje i primjenu sustava, što ćemo, kao što je vidljivo na slici 8., detaljnije prikazati u ovome potpoglavlju.

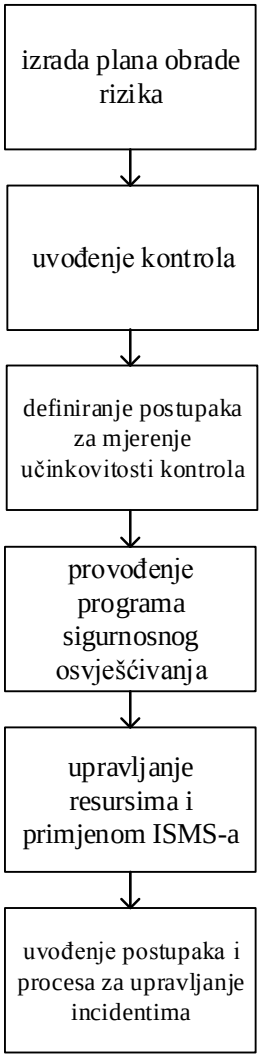


Slika 8. Faza Do u okviru modela PDCA

Hrvatska norma HRN ISO/IEC 27001 definira način prvotnog uvođenja i primjene sustava upravljanja informacijskom sigurnošću. Slika 9. prikazuje pojedinačne korake:

1. izradu plana obrade rizika
2. uvođenje kontrola
3. definiranje postupaka za mjerenje učinkovitosti kontrola
4. provođenje programa sigurnosnog osvješćivanja

5. upravljanje resursima i primjenom sustava upravljanja informacijskom sigurnošću
6. uvođenje postupaka i procesa za upravljanje incidentima.



Slika 9. Pojedinačni koraci u okviru faze Do (vlastiti rad autora prema Marijanović, I. (2010), 67)

Prvi je korak **izrada plana obrade rizika** (*risk treatment plan*). Taj dokument sadrži popis kontrola koje su odabrane u fazi *Plan* te su povezne s imovinom, aktivnostima i resursima na kojima se kontrole provode, popis osoba koje su odgovorne za provođenje kontrola i popis prioriteta. Primjerice, u fazi *Plan* odabrana je kontrola iz Aneksa Hrvatske norme HRN ISO/IEC 27001[15] pod nazivom *politika čistog stola i čistog zaslona.* Ona se navodi u planu obrade rizika te povezuje s imovinom na koju se

[15] Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission*.

primjenjuje (npr. radni stolovi i zasloni računala odjela za upravljanje ljudskim potencijalima).

Sljedeći je korak **uvođenje kontrola** koje su definirane u planu obrade rizika. Primjerice, *politika čistog stola i čistog zaslona* može se uvesti postavljanjem dodatnog stola koji ne služi kao radni stol, već za razgovore s djelatnicima, čime se mogućnost neovlaštenog uvida u dokumente povjerljivog sadržaja znatno smanjuje.

Razumljivo je da je način provođenja i učinkovitost odabranih kontrola potrebno redovito nadzirati. Stoga je sljedeći korak **definiranje postupaka za mjerenje učinkovitosti kontrola**. Mjerenja se provode periodički i služe za stalno unaprjeđenje procesa. Poslužimo li se gore navedenim primjerom postavljanja dodatnog stola, potrebno je utvrditi je li navedena mjera utjecala na smanjenje neovlaštenoga uvida u sadržaje povjerljivih dokumenata.

Četvrti je korak **provođenje programa sigurnosnog osvješćivanja zaposlenika**. Ciljevi sigurnosnog osvješćivanja (*information security awareness training*) uključuju: upoznavanje zaposlenika s politikama i procedurama sustava upravljanja informacijskom sigurnošću te zakonskom regulativom, podizanje razine svijesti zaposlenika o vrijednosti informacija i načinima kako ih je potrebno štititi, upoznavanje zaposlenika sa sigurnosnim prijetnjama, rizicima i kontrolama za tretiranje rizika te utjecanje na način razmišljanja i poticanje zaposlenika da u obavljanju poslovnih aktivnosti odluke donose uzimajući u obzir sigurnost informacija.

Peti korak, tj. upravljanje resursima i primjenom sustava upravljanja informacijskom sigurnošću odnosi se na osiguravanje i vođenje brige o resursima potrebnim za sve četiri faze uvođenja.

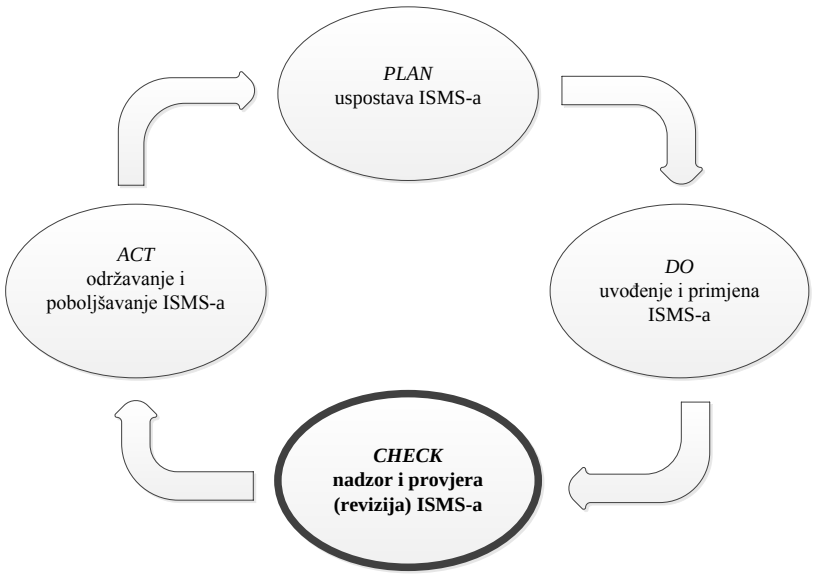
Završni korak u fazi *Do* je **uvođenje postupaka i procesa za upravljanje sigurnosnim incidentima**. Sigurnosni je incident svaki događaj koji narušava povjerljivost, cjelovitost i raspoloživost informacija unutar sustava upravljanja informacijskom sigurnošću.[16] Ciljevi postupaka i procedura za upravljanje sigurnosnim incidentima su osigurati prijavu incidenata, dosljednu i učinkovitu reakciju nakon prijave incidenta te upravljanje slabostima koje potencijalno mogu dovesti do incidenta putem

[16] Detaljnije o tome u Gregory, P. (2009), 212

pravovremenog provođenja korektivnih mjera. Razlika između incidenta i slabosti informacijskog sustava je u tome što se incident odnosi na samo narušavanje sigurnosti, dok slabost predstavlja potencijalni izvor za narušavanje sigurnosti. Primjer slabosti je navika zaposlenika da ne zaključavaju vrata svoga ureda za vrijeme pauze za ručak, što ne mora nužno dovesti do sigurnosnog incidenta, ali značajno povećava mogućnost nastanka sigurnosnog incidenta. Primjer sigurnosnog incidenta je situacija u kojoj djelatniku ne radi lozinka za ulazak u operativni sustav Windows. Prvi je korak prijava sigurnosnog incidenta. Sljedeći je korak poduzimanje propisanih procedura za nastalu situaciju koje u gore opisanom slučaju, između ostaloga, mogu uključivati provjeru je li riječ o pogrešci korisnika ili sistemskoj pogrešci te provjeru logova. Sigurnosni incident mogu prijaviti zaposlenici, vanjski suradnici, vlasnici imovine koja je obuhvaćena opsegom sustava upravljanja informacijskom sigurnošću i nadzorni sustavi (alarmi, kamere itd.).

NADZOR I PROVJERA (REVIZIJA) SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

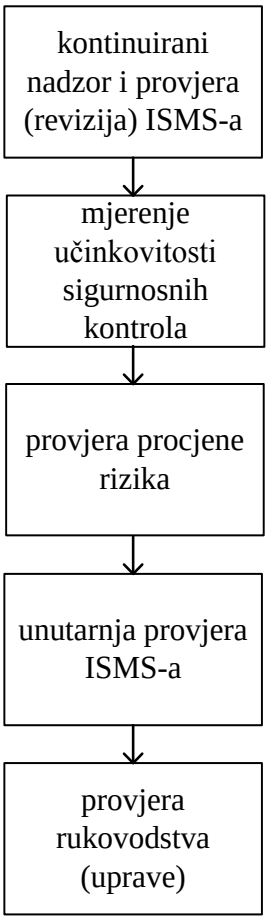
Treći korak u okviru procesa uvođenja koji smo prikazali pomoću modela PDCA je **faza *Check***, odnosno nadzor i provjera sustava upravljanja informacijskom sigurnošću, čime ćemo se, kao što je vidljivo na slici 10., baviti u ovome potpoglavlju.



Slika 10. Faza Check u okviru modela PDCA

Hrvatska norma HRN ISO/IEC 27001 definira provođenje nadzora i provjere (revizije) sustava upravljanja informacijskom sigurnošću. Na slici 11. prikazani su koraci koji se provode u okviru faze *Check*. Riječ je o sljedećih pet koraka:

1. kontinuirani nadzor i provjera sustava upravljanja informacijskom sigurnošću
2. mjerenje učinkovitosti sigurnosnih kontrola
3. provjera procjene rizika
4. unutarnja provjera sustava upravljanja informacijskom sigurnošću
5. provjera uprave.



Slika 11. Pojedinačni koraci za nadzor i provjeru (reviziju) sustava upravljanja informacijskom sigurnošću; (vlastiti rad autora prema Marijanović, I. (2010), 69)

Nakon uspostave sustava upravljanja informacijskom sigurnošću sustav je potrebno **kontinuirano nadzirati i provjeravati** jer se promjene unutar organizacije (poslovnog subjekta) odražavaju i na sustav upravljanja informacijskom sigurnošću. Riječ je o promjenama u poslovnim procesima (npr. dobavljač je uvođenjem digitalnih potpisa promijenio način rada i komunikacije), promjenama u organizaciji poslovanja (npr. poslovni subjekt zbog povećanja opsega poslovanja osniva nove podružnice), kadrovskim promjenama (npr. inženjer zadužen za *backup* podataka odlazi iz tvrtke i na njegovo mjesto dolazi nova osoba) te promjenama hardvera i softvera (npr. nova tehnologija koju će organizacija implementirati u postojeću infrastrukturu). Radi usklađivanja gore opisanih promjena i sustava upravljanja informacijskom sigurnošću, potrebno je kontinuirano nadzirati poslovne procese, pratiti promjene, analizirati prijedloge za poboljšanja te pratiti razvoj tehnologija. Osim toga, važno je nadzirati

pogreške u radu, pokušaje narušavanja ili slučajeve narušavanja informacijske sigurnosti te provođenje postupaka trajnog rješavanja sigurnosnih incidenata.

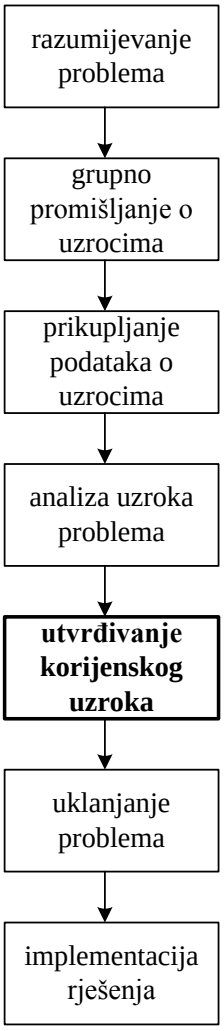
Sukladno zahtjevu Hrvatske norme HRN ISO/IEC 27001 za **mjerenje učinkovitosti sigurnosnih kontrola** potrebno je uspostaviti odgovarajuću metriku. Metrika predstavlja skup alata za prikupljanje, analiziranje i izvještavanje o relevantnim informacijama koje se odnose na učinkovitost. Metrika informacijske sigurnosti jedan je od važnih čimbenika u donošenju odluka o različitim aspektima informacijske sigurnosti, primjerice za osmišljavanje sigurnosne arhitekture i kontrola. Ona pruža kvantitativnu i objektivnu osnovu za procjenu sigurnosti. Rabi se u različite svrhe (primjerice kao strateška potpora poslovnim procesima).[17] Metričkim se alatima u propisanim vremenskim intervalima prikupljaju i analiziraju podaci o mjestu, broju i učestalosti sigurnosnih incidenata te njihovom utjecaju na poslovanje, podaci o pokušajima narušavanja sigurnosti, o pridržavanju propisanih sigurnosnih mjera i slično.

Provjera procjene rizika provodi se periodično te nakon svake važne promjene, primjerice, nakon promjena u vlasničkoj strukturi, promjene dobavljača određene opreme ili promjene vatrozida.

Unutarnja provjera (revizija) sustava upravljanja informacijskom sigurnošću provodi se barem jednom godišnje, a preporučljivo je dva puta godišnje: nakon prvih šest mjeseci i prije eksternog audita revizorske kuće. Često se za unutarnju provjeru koriste izrazi *interna revizija* i/ili *interni audit*. Potrebno je naglasiti da internu provjeru provodi skupina djelatnika, a preporučljivo je da barem voditelj skupine posjeduje odgovarajući certifikat za internog auditora (*lead auditor certificate*). Mogu je provoditi i djelatnici koji nisu stalno zaposleni u organizaciji. Ciljevi unutarnje provjere su procjena sukladnost sustava upravljanja informacijskom sigurnošću sa zahtjevima norme HRN ISO/IEC 27001, utvrđivanje učinkovitost sustava i ispitivanje zadovoljava li sustav zahtjeve definirane u politici upravljanja informacijskom sigurnošću. Voditelj skupine zadužen je za pripremu unutrašnje provjere, što znači da sastavlja pitanja i određuje što će točno provjeravati. Obično se unutarnja provjera usredotočuje na one dijelove

[17] Detaljnije o tome u Jansen, W. (2009), 1–2

sustava za koje se smatra da slabije funkcioniraju i da u praksi slabije provode ono što je propisano politikama i procedurama informacijske sigurnosti. Nakon završetka unutarnje provjere voditelj skupine sastavlja izvješće koje sadržava sve utvrđene nesukladnosti. Na temelju izvještaja voditelj informacijske sigurnosti izrađuje plan za uklanjanje nesukladnosti. Proces uklanjanja nesukladnosti, odnosno rješavanja problema uključuje (vidi sliku 12): razumijevanje problema, grupno promišljanje o uzrocima problema (*problem cause brainstorming*), prikupljanje podataka o uzrocima problema, analizu uzroka problema, utvrđivanje korijenskog uzroka (*root cause*), uklanjanje problema i implementaciju rješenja.[18]



Slika 12. Proces rješavanja problema
(vlastiti rad autora prema Andersen, B. i Fagerhaugu. T. (2006), 7)

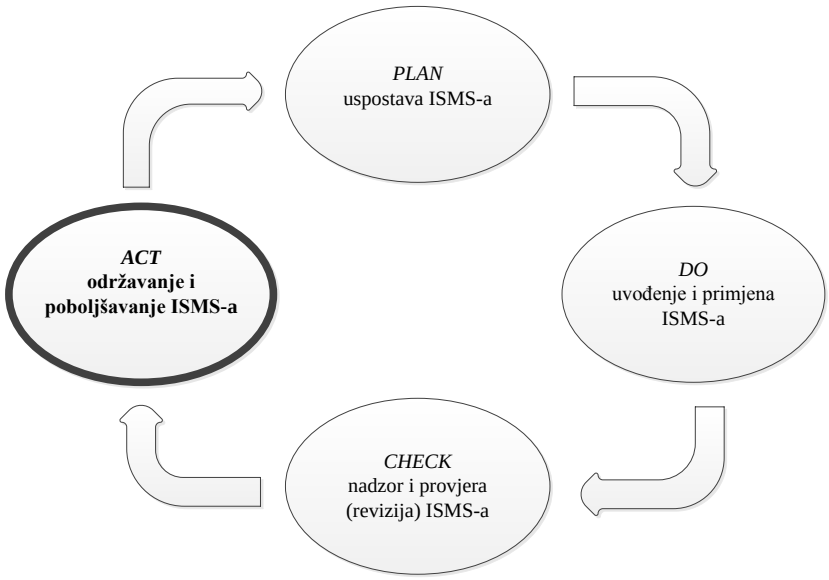
[18] Detaljnije o tome u Andersen, B., Fagerhaug, T. (2006), 3–8

Mnogi autori smatraju da je utvrđivanje korijenskog uzroka ključ za rješavanje problema i da bez utvrđivanja korijenskog uzroka nema trajnih rješenja. Andersen i Fagerhaug (2006., str. 12) analizu korijenskih uzroka (*root cause analysis*) definiraju kao strukturiranu istragu čiji su ciljevi utvrditi istinski uzrok problema i utvrditi mjere koje je potrebno poduzeti za uklanjanje problema. Primjerice, unutarnjom provjerom utvrđena je nesukladnost u smislu neprovođenja analize rizika prije uvođenja novog servera. Jedan od mogućih razloga je da djelatnik zadužen za uvođenje novog servera nije bio svjestan što je sve potrebno učiniti prije samog uvođenja jer nije prošao odgovarajuću edukaciju. Korijenski uzrok pak može biti propust u planiranju edukacije djelatnika o sustavu upravljanja informacijskom sigurnošću u smislu da je edukacija djelatnika provedena prilikom uvođenja sustava, ali se nije vodilo računa o novim djelatnicima koji su zaposleni naknadno. Opisani korijenski uzrok može biti uzrokom i drugih problema u okviru sustava upravljanja informacijskom sigurnošću te ako se ne ukloni može dovesti i do novih problema.

Uprava organizacije također **provodi provjeru (reviziju) sustava upravljanja informacijskom sigurnošću**. Provjera se provodi barem jednom godišnje, obuhvaća čitav sustav upravljanja informacijskom sigurnošću i temelji se na podacima dobivenim unutarnjom provjerom, od vanjskih partnera i djelatnika obuhvaćenih opsegom sustava. Ciljevi provjere uprave su strateško usmjeravanje sustava upravljanja informacijskom sigurnošću, usklađivanje sustava s poslovnim ciljevima i kontinuirano poboljšanje sustava. Važno je naglasiti da pravo na nadzor i provjeru sustava upravljanja informacijskom sigurnošću imaju interni auditori, eksterni auditori i uprava organizacije.

ODRŽAVANJE I POBOLJŠAVANJE SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

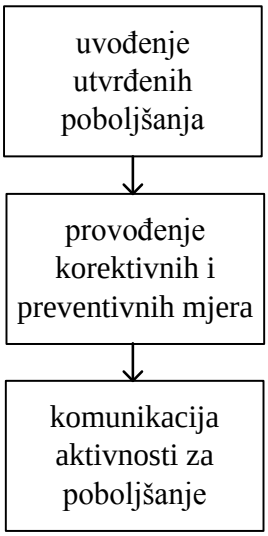
Četvrti korak u procesu uvođenja sustava upravljanja informacijskom sigurnošću koji smo prikazali pomoću modela PDCA je **faza *Act***. Ona uključuje održavanje i poboljšavanje sustava, što ćemo detaljnije prikazati u ovome potpoglavlju (vidi sliku 13).



Slika 13. Faza Act u okviru modela PDCA

Hrvatska norma HRN ISO/IEC 27001 definira potrebu održavanja i poboljšavanja sustava upravljanja informacijskom sigurnošću. Kao što je prikazano na slici 14., održavanje i poboljšavanje sustava obuhvaća sljedeće korake:

1. uvođenje utvrđenih poboljšanja
2. provođenje korektivnih i preventivnih mjera
3. komunikaciju aktivnosti za poboljšanje.



Slika 14. Pojedinačni koraci u održavanju i poboljšavanju sustava upravljanja informacijskom sigurnošću (vlastiti rad autora prema Marijanović, I. (2010), 71)

U okviru faze *Check*, odnosno prethodne faze u procesu uvođenja sustava upravljanja informacijskom sigurnošću, prikazali smo unutarnju provjeru (reviziju) sustava na temelju koje se sastavlja izvješće o utvrđenim nesukladnostima i način na koji voditelj informacijske sigurnosti sastavlja plan za uklanjanje nesukladnosti. Nesukladnosti se pojavljuju ako nisu zadovoljeni neki od zahtjeva standarda prema kojem je uspostavljen sustav upravljanja informacijskom sigurnošću, ako nisu zadovoljeni zahtjevi internih politika, procedura, pravilnika i radnih uputa te ako nisu zadovoljeni zakonski, regulatorni i ugovorni zahtjevi. Nesukladnosti je potrebno korigirati **uvođenjem utvrđenih poboljšanja**, koja se mogu odnositi na procedure, tehnologije, način izvještavanja i vođenja bilješki, djelatnike, ugovorne obveze itd. Prisjetimo li se primjera iz prethodnoga poglavlja s djelatnikom koji nije proveo procjenu rizika prije uvođenja novog servera, potrebno je uvesti poboljšanja koja se odnose na proceduru provođenja edukacije o sustavu upravljanja informacijskom sigurnošću za nove djelatnike.

Sljedeći je korak **provođenje korektivnih i preventivnih mjera**. Korektivne se mjere primjenjuju za uklanjanje uzroka postojećih nesukladnosti, nedostataka sustava upravljanja informacijskom sigurnošću i neželjenih situacija unutar opsega sustava. Preventivne se mjere poduzimaju za uklanjanje uzroka potencijalnih nesukladnosti, nedostataka i neželjenih situacija unutar sustava upravljanja informacijskom sigurnošću.

Treći korak **komuniciranje aktivnosti za poboljšanje** razumljiv je sam po sebi, no praksa je pokazala da se na njega učestalo zaboravlja, čime se uvelike umanjuju pozitivni učinci uvođenja poboljšanja te korektivnih i preventivnih mjera. Stoga je izrazito važno da svi djelatnici obuhvaćeni opsegom sustava upravljanja informacijskom sigurnošću budu pravovremeno obaviješteni o aktivnostima koje se provode u cilju poboljšanja sustava. Takve aktivnosti često dovode do promjena politika, procedura i ostale dokumentacije zbog čega je potrebno redovito ažuriranje i označavanje verzija.

Kao što je vidljivo iz prethodnih potpoglavlja, nakon utvrđivanja nesukladnosti, potrebno je uvesti poboljšanja. Uvođenje poboljšanja ponovo nas dovodi do prve faze u kojoj je aktivnosti (ovoga puta aktivnosti poboljšanja) potrebno planirati, zatim u sljedećoj fazi pod nazivom *Do* uvesti i primijeniti, u fazi pod nazivom *Check* nadzirati i provjeravati te, ako se ponovo utvrde nesukladnosti, u fazi *Act* raditi na njihovome uklanjanju. Može se zaključiti da je sustav upravljanja informacijskom sigurnošću projekt u koji je potrebno kontinuirano ulagati i na čijem je unaprjeđenju potrebno kontinuirano raditi. Projekt ne završava uvođenjem sustava i ako se na njemu kontinuirano ne radi, njegovi su dosezi i mogućnosti ograničeni.

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Calder, A. (2008). *ISO 27001/ISO 27002: A pocket guide* (poglavlja 2, 3 i 15). Cambridgeshire: IT Governance Publishing.
2. Hrvatski zavod za norme (2013). *International Standard ISO/IEC 27000, International Organization for Standardization and International Electrotechnical Commission.*
3. Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission*.
4. Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27005, International Organization for Standardization and International Electrotechnical Commission*.
5. Gregory, P. (2009). *CISSP guide to security essentials* (poglavlje 1). Boston: Course Technology.
6. Marijanović, I. (2010). ISO/IEC 27001: 2005 norma. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 59-72). Zagreb: Algebra.
7. Strahonja, V. i Saletović, K. (2007). Proactive approach to the problem management in communication network. *Journal of Information and Organizational Sciences*, *31/1*, 245–259.
8. Andersen, B. i Fagerhaug, T. (2006) *Root cause analysis: Simplified tools and techniques* (poglavlja 1 i 2). Milwaukee: Quality Press.
9. Jansen, W. (2009). *Directions in security metrics research* (poglavlja 1, 2 i 3). Gaithersburg: National Institute of Standards and Technology.
10. Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management standard* (poglavlje 3 i 6). Norwood: Artech House.

PITANJA ZA PONAVLJANJE:

1. Zašto tvrtke uvode ISMS u svoje poslovanje?
2. Što tvrtke dokazuju posjedovanjem međunarodnog standarda informacijske sigurnosti?
3. Skicirajte PDCA krug i u par riječi objasnite osobitosti pojedinih dijelova.
4. Kojim korakom započinje PDCA krug i što se njime definira?
5. Što je to sigurnosno osvješćivanje i kada se primjenjuje?
6. Što se smatra sigurnosnim incidentom i koji je cilj procesa upravljanja sigurnosnim incidentima?
7. Koja je razlika između sigurnosnog incidenta i slabosti informacijskog sustava?
8. Koje se sve godišnje provjere informacijske sigurnosti provode?

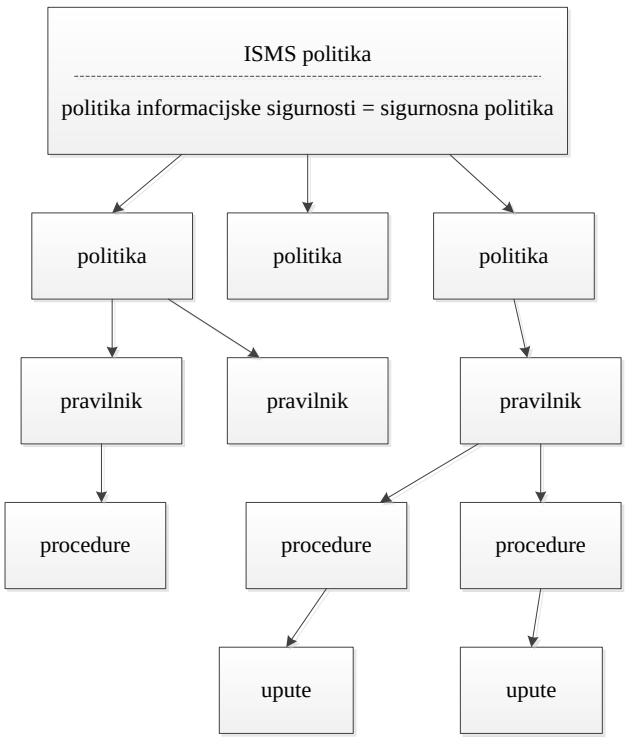
DOKUMENTACIJA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

U OVOME ĆEMO POGLAVLJU NAUČITI:

- HIJERARHIJU DOKUMENTACIJE U OKVIRU SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU
- ŠTO JE POLITIKA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU
- ŠTO JE POLITIKA INFORMACIJSKE SIGURNOSTI, ODNOSNO SIGURNOSNA POLITIKA
- ŠTO SU POLITIKE NIŽE RAZINE
- ŠTO SU PRAVILNICI
- ŠTO SU PROCEDURE
- ŠTO SU UPUTE.

DOKUMENTACIJA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU

U prethodnim smo poglavljima pomoću modela PDCA prikazali četiri osnovne faze procesa uspostave sustava upravljanja informacijskom sigurnošću. Prva **faza** pod nazivom ***Plan*** obuhvaća devet koraka, a jedan od njih je izrada politike sustava upravljanja informacijskom sigurnošću, koja se smatra krovnim dokumentom na području informacijske sigurnosti (vidi sliku 15).



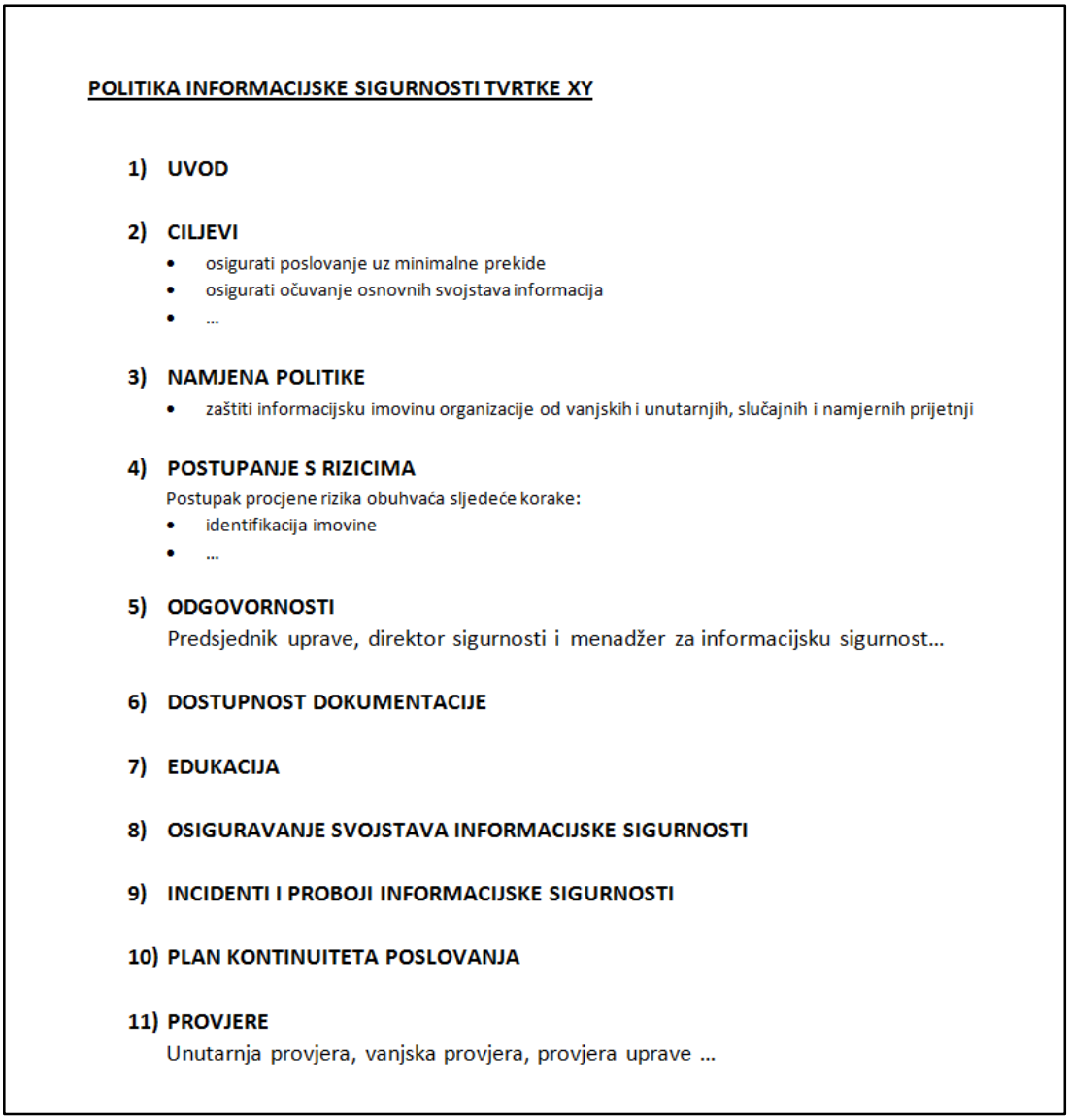
Slika 15. Hijerarhija dokumentacije u okviru sustava upravljanja informacijskom sigurnošću; (vlastiti rad autora prema Marijanović, I. (2010), 91)

U politici sustava upravljanja informacijskom sigurnošću (*information security management system policy* ili *ISMS policy*) načelno se definiraju ciljevi i smjernice za uspostavu sustava. Mnoge organizacije politiku sustava upravljanja informacijskom

sigurnošću proglašavaju javnim dokumentom i objavljuju na svojim mrežnim stranicama.

Politika informacijske sigurnosti (*information security policy*), koja se u literaturi često naziva i sigurnosna politika (*security policy*) predstavlja dokument koji je hijerarhijski podređen politici upravljanja informacijskom sigurnošću. U njemu se detaljnije razrađuju očekivanja, smjernice i namjere uprave poslovnog subjekta ili organizacije u smislu informacijske sigurnosti. Namijenjen je svim djelatnicima. U praksi je taj dokument često sadržan u istom dokumentu s politikom sustava upravljanja informacijskom sigurnošću, što na slici 15. označava isprekidana linija. Velike globalne organizacije zbog opsega poslovanja i broja zaposlenika u pravilu imaju dva odvojena dokumenta, dok su u manjim organizacijama politika sustava upravljanja informacijskom sigurnošću i politika informacijske sigurnosti sadržane u zajedničkom dokumentu. To je u skladu Hrvatskom normom HRN ISO/IEC 27001 u kojoj se precizira da je navedena dva dokumenta moguće objediniti i prikazati u okviru jednog dokumenta. Smjernice za izradu politike upravljanja informacijskom sigurnošću navedene su u Hrvatskoj normi HRN ISO/IEC 27001 i Hrvatskoj normi HRN ISO/IEC 27002, dok Zakon o informacijskoj sigurnosti,[19] između ostaloga, definira mjere i standarde informacijske sigurnosti (u člancima 3., 4., 5., 6. i 7.) te područja informacijske sigurnosti za koja se mjere i standardi primjenjuju (u člancima 8., 9., 10., 11., 12. i 13.). Politika informacijske sigurnosti sadrži osnovne ciljeve, namjenu politike, postupanje s rizicima, odgovornosti za provođenje politike, dostupnost dokumentacije, način provođenja edukacija, načine osiguravanja osnovnih svojstava informacija i postupanja u slučaju incidenata i problema, načine nadzora i provjera sustava itd. Primjer koncepcije politike informacijske sigurnosti prikazan je na slici 16.

[19] *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07



POLITIKA INFORMACIJSKE SIGURNOSTI TVRTKE XY

1) **UVOD**

2) **CILJEVI**
- osigurati poslovanje uz minimalne prekide
- osigurati očuvanje osnovnih svojstava informacija
- ...

3) **NAMJENA POLITIKE**
- zaštiti informacijsku imovinu organizacije od vanjskih i unutarnjih, slučajnih i namjernih prijetnji

4) **POSTUPANJE S RIZICIMA**

Postupak procjene rizika obuhvaća sljedeće korake:
- identifikacija imovine
- ...

5) **ODGOVORNOSTI**

Predsjednik uprave, direktor sigurnosti i menadžer za informacijsku sigurnost...

6) **DOSTUPNOST DOKUMENTACIJE**

7) **EDUKACIJA**

8) **OSIGURAVANJE SVOJSTAVA INFORMACIJSKE SIGURNOSTI**

9) **INCIDENTI I PROBOJI INFORMACIJSKE SIGURNOSTI**

10) **PLAN KONTINUITETA POSLOVANJA**

11) **PROVJERE**

Unutarnja provjera, vanjska provjera, provjera uprave ...

Slika 16. Primjer koncepcije politike informacijske sigurnosti

U uvodnom se dijelu u kratkim crtama opisuje organizacija i navode njena strateška opredjeljenja, primjerice usklađenost sa smjernicama iz najbolje prakse, jačanje pozicije na tržištu i slično. U dijelu pod naslovom *Postupanje s rizicima* definiraju se procjena i obrada rizika, što ćemo detaljnije prikazati u sljedećem poglavlju. Dio *Odgovornosti* prikazuje osnovne uloge u sustavu upravljanja informacijskom sigurnošću organizacije (predsjednik, uprave, direktor sigurnosti, menadžer za informacijsku sigurnost itd.), njihove obveze, ovlaštenja i prava te odgovornosti djelatnika i podugovarača. Važan element je provođenje edukacija i obuka te podizanje razine svijesti djelatnika o informacijskoj sigurnosti. U točki 8. načelno se opisuju načini očuvanja povjerljivosti, cjelovitosti i raspoloživosti informacija, dok točka 9. prikazuje postupanje s incidentima i probojima informacijske sigurnosti. Politika informacijske

sigurnosti u pravilu sadrži i plan kontinuiteta poslovanje, čime ćemo se baviti u posljednjem poglavlju. Nadzor i provjeru sustava, kao što smo prikazali u prethodnim poglavljima, obavljaju interni auditori, vanjski auditori i uprava organizacije. Potrebno je naglasiti da je koncepcija politike informacijske sigurnosti prikazana na slici 16. samo jedan od mogućih načina koncipiranja i da se u praksi može naići na politike informacijske sigurnosti koje su koncipirane na drugačiji način.

Za razliku od politike informacijske sigurnosti koja je dostupna svim djelatnicima, dokumenti niže razine prikazani na slici 15. (politike za pojedina područja informacijske sigurnosti, pravilnici, procedure i upute), dostupni su samo pojedinim djelatnicima, ovisno o prirodi njihova posla i ovlaštenjima u okviru sustava upravljanja informacijskom sigurnošću.

Na osnovi politike informacijske sigurnosti izrađuju se politike za pojedina područja informacijske sigurnosti (primjerice politika klasifikacije informacija, politika kontrole pristupa, politika za mobilno računarstvo) koje su namijenjene za operativnu uporabu. Politike izražavaju namjeru i pružaju smjernice za pojedina područja informacijske sigurnosti, a u pravilnicima se definiraju i razrađuju pravila koja proizlaze iz nadređene politike. Jedna politika može se razraditi i u nekoliko pravilnika, kao što je strelicama prikazano na slici 15. Primjerice, politika zaporki propisuje da su svi djelatnici, u okviru sustava upravljanja informacijskom sigurnošću, odgovorni za odabir sigurnosne zaporke i brigu o njoj. Pravilnikom o zaporkama precizno se definira kako zaporka treba izgledati (minimalan broj znakova, velika i mala slova, specijalni znakovi, brojevi). Ako je riječ o većoj organizaciji, politika zaporki može se precizno definirati u okviru dvaju ili više pravilnika, npr. u okviru pravilnika o zaporkama na osobnim računalima i pravilnika o zaporkama na serverima. Politike se u pravilu vrlo rijetko mijenjaju, dok se pravilnici mijenjaju kako bi bili usklađeni s poslovnim procesima, tehnologijama itd.

Ako je potrebno, u procedurama se definira način provođenja aktivnosti koje su navedene u pravilnicima. U njima se opisuju pojedinačni koraci pojedinih aktivnosti, a važno je da sadrže dovoljno informacija kako bi korisnici mogli provoditi aktivnosti. Prisjetimo li se gore navedenog primjera pravilnika o zaporkama, onda je moguće imati proceduru za promjenu zaporke u kojoj se opisuju pojedinačni koraci promjene (prijava u sustav, odabir postavki korisničkog računa, unos stare zaporke, unos nove zaporke

itd.). U praksi se često koriste samo pravilnici ili samo procedure, a ne nužno jedno i drugo. Kao što je vidljivo na slici 15., procedure se mogu razjasniti u obliku uputa za pojedinačne korake. Često je riječ o uputama proizvođača ili alatima koje je moguće koristiti.

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Calder, A. (2008). *ISO 27001/ISO 2700: A pocket guide* (poglavlje 8). Cambridgeshire: IT Governance Publishing.
2. Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission*.
3. Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27002, International Organization for Standardization and International Electrotechnical Commission*.
4. Marijanović, I. (2010). ISO/IEC 27001: 2005 norma. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 59–72). Zagreb: Algebra.
5. Whitman, M. E. i Mattord, H. J. (2010). *Management of information security* (poglavlje 4). Boston: Course Technology.

PITANJA ZA PONAVLJANJE:

1. Koji se dokument smatra krovnim u informacijskoj sigurnosti tvrtke?
2. Objasnite hijerarhiju dokumenata u sustavnom upravljaju informacijskom sigurnošću.
3. Gledajući iz perspektive hijerarhije dokumenata, bi li šteta za tvrtku bila veća ako bi javno objavili politiku informacijske sigurnosti ili radne upute?

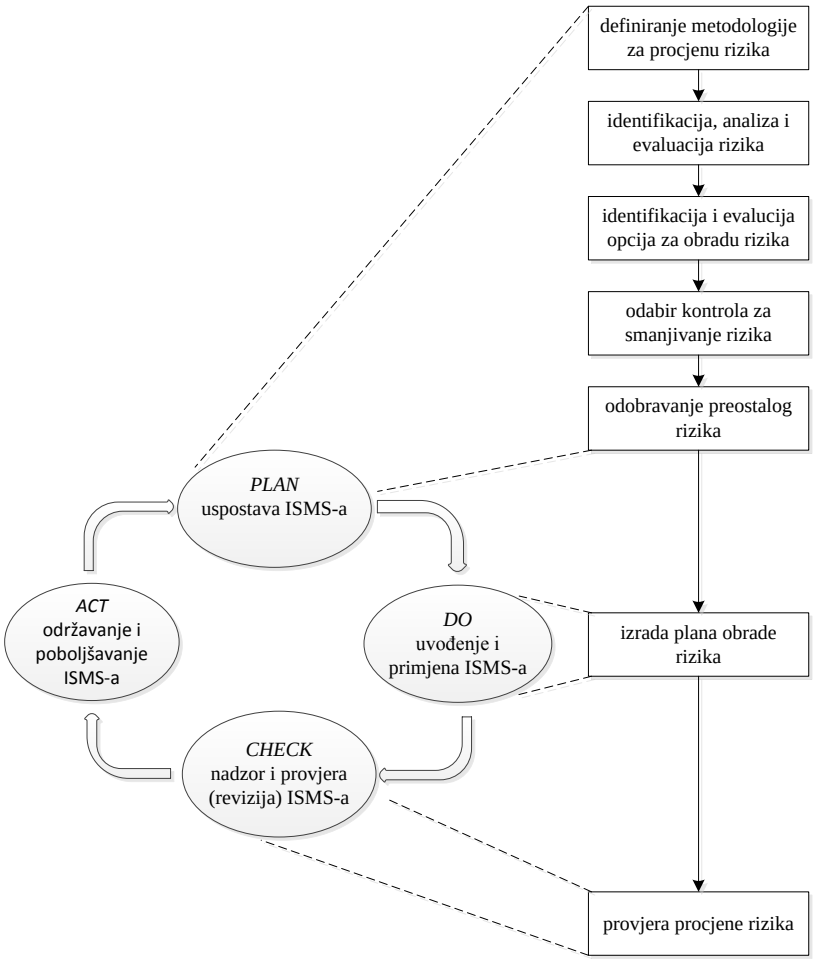
UPRAVLJANJE RIZICIMA

U OVOME ĆEMO POGLAVLJU NAUČITI:

- POSTUPAK PROCJENE RIZIKA
- ŠTO SU RANJIVOST I PRIJETNJE
- NAČINE PROCJENE VJEROJATNOSTI I PROCJENE ŠTETE
- OPCIJE ZA OBRADU RIZIKA.

UPRAVLJANJE RIZICIMA

Upravljanje rizicima (*risk management*) jedan je od osnovnih preduvjeta za upravljanje informacijskom sigurnošću. Cjelokupni se proces upravljanja informacijskom sigurnošću u velikoj mjeri oslanja na proces upravljanja rizicima. U prethodnim smo poglavljima upravljanje rizicima spominjali u okviru triju faza sustava upravljanja informacijskom sigurnošću (vidi sliku 17.).



Slika 17. Upravljanje rizicima u okviru sustava upravljanja informacijskom sigurnošću

Rizik je vjerojatnost da će prijetnja u određenim okolnostima iskoristiti ranjivost (slabost) sustava i dovesti do štete po imovinu. **Upravljanje rizicima** je pojam koji podrazumijeva procjenu rizika i definiranje protumjera kojima se procijenjeni rizik može obrađivati (smanjiti, prihvatiti, zaobići ili prenijeti na nekoga drugog). Iz perspektive odvijanja poslovanja koje je u ovisnosti o informacijskom sustavu, potrebno je naglasiti pojam informatičkog rizika. On podrazumijeva rizike koji proizlaze iz intenzivne uporabe poslovnih informacijskih sustava i tehnologije kao važne podrške odvijanju i unaprjeđenju poslovnih procesa i općenito poslovanja.

Upravljanje rizicima izrazito je važno u okviru uspostave sustava (faza *Plan* na slici 17.) jer se u okviru te faze definira metodologija za procjenu rizika, identificiraju, analiziraju i utvrđuju rizici, identificiraju i evaluiraju opcije za tretiranje rizika, odabiru kontrole za smanjenje rizika te odobravaju preostali rizici. U sklopu uvođenja i primjene sustava upravljanja informacijskom sigurnošću (faza *Do* na slici 17.) izrađuje se plan obrade rizika. Provjera procjene rizika provodi se kao dio nadzora i provjere (revizije) sustava (faza *Check* na slici 17.).

Sigurnosni rizik je rizik za imovinu organizacije koji je potrebno obraditi.[20] U kontekstu informacijske sigurnosti sigurnosni se rizik odnosi na mogućnost neželjenog događaja koji može štetno utjecati na povjerljivost, cjelovitost i raspoloživost informacijske imovine. Upravljanje rizicima omogućuje postizanje ravnoteže između ostvarenja poslovnih ciljeva i minimiziranja štete zbog neželjenih događaja.

Postoje različite metodologije za procjenu rizika. U ovome ćemo poglavlju prikazati postupak procjene rizika koji se u velikoj mjeri temelji na preporukama Američkog nacionalnog instituta za standarde i tehnologiju (*National Institute of Standards and Technology*).[21] Postupak obuhvaća sljedećih osam koraka (vidi sliku 18.):

1. identifikaciju imovine
2. identifikaciju ranjivosti
3. identifikaciju prijetnji koje mogu iskoristiti ranjivosti

[20] Detaljnije o tome u Landoll, D.J. (2011), 8

[21] Detaljnije o tome u Stoneburner, G., Goguen, A. i Feringa, A. (2002), 8–26

4. identifikaciju i analizu sigurnosnih kontrola
5. procjenu vjerojatnosti ostvarivanja prijetnji
6. procjenu štete koja nastaje ostvarivanjem prijetnji
7. izračun rizika
8. prijedlog kontrola za umanjivanje rizika.

Slika 18. Postupak procjene rizika

Na samome je početku potrebno **identificirati imovinu** nad kojom će se provesti procjena rizika. U tu se svrhu rabi popis imovine definiran prilikom određivanja opsega sustava upravljanja informacijskom sigurnošću.

Sljedeći je korak **identifikacija ranjivosti**. Stoneburner, Goguen i Feringa (2002., str. 15) ranjivost definiraju kao pogreške ili slabosti u procedurama, dizajnu i implementaciji sigurnosnog sustava ili internih kontrola koje mogu uzrokovati i dovesti do sigurnosnih incidenata ili povrede politike informacijske sigurnosti. Riječ je o slabostima imovine koje se odnose na tehničke karakteristike (primjerice nekvalitetno osmišljen sustava) i procedure (primjerice neadekvatno definirana procedura). Ostali primjeri ranjivosti uključuju nezaštićena spremišta, nekontrolirano kopiranje dokumenata, nedostatak dokumentacije, loše kabliranje, napuštanje radnog mjesta bez odjave (*log out*) i slično. Ranjivost se u pravilu promatra u kombinaciji s prijetnjama koje se, kao što je prikazano na slici 18., identificiraju u sljedećem koraku.

Stoneburner, Goguen i Feringa (2002., str. 12) **prijetnju** definiraju kao potencijalni izvor rizika za pojedinu ranjivost. **Prijetnja iskorištava ranjivost i nanosi štetu imovini.** Ako ne postoji prijetnja koja može iskoristi ranjivost, tada ne postoji ni sigurnosni rizik. Nezadovoljni djelatnik predstavlja jednu od najvećih prijetnji. Prijetnje koje mogu iskoristi prethodno navedene ranjivosti su otuđivanje dokumentacije ili medija (nezaštićena spremišta, nekontrolirano kopiranje dokumenata, napuštanje radnog mjesta bez odjave), zloupotreba prava (napuštanje radnog mjesta bez odjave, nekontrolirano kopiranje dokumenata), greška prilikom uporabe (nedostatak dokumentacije) i ispadi komunikacijske opreme (loše kabliranje, nedostatak dokumentacije) itd.

Četvrti korak uključuje **identifikaciju i analizu sigurnosnih kontrola** koje se rabe za smanjenje vjerojatnosti da će prijetnja iskoristiti ranjivost ili za smanjenje štete u slučaju da prijetnja iskoristi ranjivost. Kontrole mogu biti tehničke (enkripcija, kontrola pristupa, vatrozid), administrativne (procedure kojima se definiraju pravila) ili fizičke (videonadzor, alarmni sustav, protupožarni sustav).

Peti korak **procjena vjerojatnosti** odnosi se na procjenu vjerojatnosti da će prijetnja iskoristi ranjivost. Često se izražava u obliku skale s tri razine vjerojatnosti, kao što je prikazano u tablici 2.

Vjerojatnost	Opis
1 – niska	• adekvatne sigurnosne kontrole • niska motivacija potencijalnog napadača • dešava se rijetko (manje od jednom godišnje)
2 – srednja	• mogućnost za iskorištavanje ranjivosti • postojanje sigurnosnih kontrola to otežava • srednja motivacija potencijalnog napadača • dešava se do dva puta godišnje (poznati su slučajevi u prošlosti)
3 – visoka	• ne postoje implementirane sigurnosne kontrole ili nisu adekvatne • visoka motivacija potencijalnog napadača • dešava se češće od dva puta godišnje

Tablica 2. Primjer kvalitativnog izražavanja vjerojatnosti

Broj 1 označava nisku razinu vjerojatnosti jer postoje adekvatne sigurnosne kontrole te je motivacija potencijalnog napadača niska. Sigurnosni incident ili povrede sigurnosne politike dešavaju se rijetko, manje od jednom godišnje. Broj 2 se odnosi na srednju razinu vjerojatnosti u kojoj postoji mogućnost za iskorištavanje ranjivosti, no postoje sigurnosne kontrole koje to otežavaju. Motivacija potencijalnog napadača je srednje jaka. Slučajevi iskorištavanja ranjivosti zabilježeni su u prošlosti i dešavaju se do dva puta godišnje. Visoka razina vjerojatnosti označava se brojem 3. Potencijalni napadač je izrazito motiviran, a ne postoje implementirane sigurnosne kontrole ili one nisu adekvatne. Mogućnost za iskorištavanje ranjivosti se pojavljuje više od dva puta godišnje.

Procjena štete odnosi se na procjenu potencijalnih gubitaka u slučaju da prijetnja iskoristi ranjivosti. Prilikom procjene štete u obzir je potrebno uzeti namjenu imovine u poslovnim sustavima, važnost imovine za organizaciju, osjetljivost informacija na pokretnoj imovini i vrijednost imovine koja je navedena u popisu imovine. Tablica 3. prikazuje kvalitativno izražavanja štete. Kratica **C I A** u tablici označava osnovna svojstva informacija (*confidentiality*, *integrity* i *availability*).

Šteta	Opis
1 – niska	Utjecaj ostvarenja prijetnje na C I A-u je malen ili zanemariv: • zanemariva šteta na imovini • nisu narušeni poslovni ciljevi organizacije.
2 – srednja	Utjecaj ostvarenje prijetnje na C I A-u postoji, ali nije kritičan: • djelomični gubitak ili oštećenje imovine • djelomično narušeni poslovni ciljevi organizacije.
3 – visoka	Utjecaj ostvarenje prijetnje na C I A-u je vrlo velik: • gubitak ili uništenje imovine • potpuno narušavanje poslovnih ciljeva organizacije.

Tablica 3. Primjer kvalitativnog izražavanja štete

Broj 1 označava nisku razinu štete jer je utjecaj ostvarenja prijetnje na osnovna svojstva informacije malen ili zanemariv. Srednja razine štete označava se brojem 2, a visoka razina štete brojem 3. Visoka razina štete znači da je utjecaj ostvarenja prijetnje na osnovna svojstva informacije vrlo velik što dovodi do gubitka ili uništenja imovine i/ili potpunog narušavanja poslovnih ciljeva organizacije.

Prilikom **izračuna rizika** za pojedinačnu imovinu u okviru sustava upravljanja informacijskom sigurnošću, u obzir je potrebno uzeti vjerojatnost da prijetnja iskoristi ranjivost, štetu u slučaju ostvarenja prijetnji te implementirane sigurnosne kontrole koje mogu umanjiti vjerojatnost ostvarenja prijetnje ili štetu.

Na osnovi izračuna rizika sastavlja se **prijedlog kontrola za umanjivanje rizika**. Prilikom odabira kontrola u obzir se uzimaju različiti čimbenici, primjerice sigurnosna politika, učinkovitost pojedinih kontrola, troškovi uvođenja i održavanja kontrola, korporativna kultura i reakcije korisnika.

Nakon postupka procjene rizika potrebno je obraditi rizike što uključuje izradu plana obrade rizika te analizu, evaluaciju i uvođenje kontrola. Važno je naglasiti da se rizik u pravilu ne može u potpunosti ukloniti, već se rizik umanjuje do razine koja je prihvatljiva za pojedinu organizaciju. Odluku o tome na koji način i u kojoj mjeri se umanjuje rizik donosi menadžment organizacije. Opcije za obradu rizika (vidi tablicu 4.) uključuju smanjivanje rizika primjenom odgovarajućih kontrola, svjesno prihvaćanje rizika u skladu s politikom sigurnosti i kriterijima za prihvaćanje rizika, izbjegavanje rizika,

odnosno situacija u kojima može doći do pojave rizika te prenošenje rizika na treću stranu (primjerice dobavljače ili osiguravajuća društva).

Opcije za obradu rizika
1. smanjivanje rizika
2. prihvaćanje rizika
3. izbjegavanje rizika
4. prenošenje rizika

Tablica 4. Opcije za obradu rizika

Budući da je imovina u opsegu sustava upravljanja informacijskom sigurnošću podložna promjenama, potrebno je konstantno nadzirati rizike te ih periodički evaluirati. U praksi se procjena rizika često provodi nakon promjena unutar opsega sustava upravljanja informacijskom sigurnošću, kao što su promjene opreme ili djelatnika.

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management standard* (poglavlje 4). Norwood: Artech House.
2. Hrvatski zavod za norme (2013). *International Standard ISO/IEC 27005, International Organization for Standardization and International Electrotechnical Commission*.
3. Landoll, D. J. (2011). *The security risk assessment handbook: A complete guide for performing security risk assessment* (poglavlja 1, 2 i 4). Boca Raton: CRC Press.
4. Marijanović, I. (2010). Upravljanje rizikom. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 73-85). Zagreb: Algebra.
5. Stoneburner, G., Goguen, A. i Ferniga, A. (2002). *Risk management guide for information technology systems: Recommendations of the National institute of standards and technology* (poglavlje 3). Gaithersburg: National Institute of Standards and Technology.
6. Vellani, K. H. (2007). *Strategic security management: A risk assessment guide for decision makers* (poglavlja 6 i 7). Oxford: Butterworth-Heinemann.
7. Whitman, M. E. i Mattord, H. J. (2010). *Management of information security* (poglavlja 8 i 9). Boston: Course Technology.

PITANJA ZA PONAVLJANJE:

1. Što je to rizik u kontekstu informacijske sigurnosti?
2. Koja rečenica je ispravna?
3. Ranjivost koristi prijetnju i nanosi štetu na imovini tvrtke ili

   prijetnja iskorištava ranjivost i nanosi štetu imovini tvrtke.
4. Navedite koje su mogućnosti obrade rizika i objasnite ih na primjeru?

KLASIFICIRANJE INFORMACIJA

U OVOME ĆEMO POGLAVLJU NAUČITI:

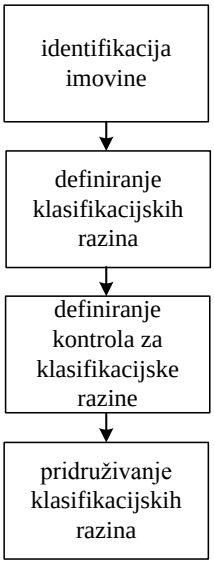
1. ZAŠTO JE POTREBNO KLASIFICIRATI INFORMACIJE
2. KORAKE U PROCESU KLASIFIKACIJE INFORMACIJA
3. KLASIFIKACIJSKE RAZINE INFORMACIJA.

KLASIFICIRANJE INFORMACIJA

Informacije je potrebno klasificirati iz više razloga. Informacije unutar pojedine organizacije imaju različite vrijednosti za organizaciju. Ako se za sve informacije primjenjuju iste mjere zaštite, pojedine će informacije biti previše, a pojedine premalo zaštićene. Otkrivanje vrijednih informacija može nanijeti značajnu štetu organizaciji. Odabir se odgovarajućih kontrola, između ostaloga, temelji na vrijednosti informacije. Nadalje, Zakon o tajnosti podataka Republike Hrvatske u članku 2.[22] propisuje da se odredbe Zakona primjenjuju na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe koje, u skladu s ovim Zakonom, ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Klasificiranje informacija je postupak utvrđivanja stupnjeva tajnosti informacija. Postupak obuhvaća četiri koraka i prikazan je na slici 19.

[22] *Zakon o tajnosti podataka*, Narodne novine 79/07



Slika 19. Postupak klasificiranja informacija

Riječ je o sljedećim koracima:

1. identifikacija imovine
2. definiranje klasifikacijskih razina
3. definiranje kontrola za pojedine klasifikacijske razine
4. pridruživanje klasifikacijskih razina pojedinačnim informacijama.[23]

Početni je korak **izrada registra informacija** u organizaciji. Registar se može izraditi na temelju anketa ili poslovnih analiza. Većina organizacija koristi popis imovine koji je definiran na početku uvođenja sustava upravljanja informacijskom sigurnošću. Informacijska imovina uključuje baze podataka, ugovore, dokumente i slično.

Drugi je korak **definiranje klasifikacijskih razina**. Državna tijela te tijela jedinica lokalne i područne (regionalne) samouprave Republike Hrvatske sukladno članku 4. Zakona o tajnosti podataka[24] podatke klasificiraju u četiri skupine: vrlo tajno, tajno, povjerljivo i ograničeno. Stupanj tajnosti *VRLO TAJNO* odnosi se na podatke čije bi neovlašteno otkrivanje nanijelo nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske. Stupnjem tajnosti *TAJNO* klasificiraju se podatci čije bi neovlašteno otkrivanje teško naškodilo nacionalnoj sigurnosti i vitalnim interesima Republike

[23] Proces klasificiranja informacija temelji se na opisu Marijanović, I (2010), 131, no četvrti je korak dorađen.

[24] *Zakon o tajnosti podataka*, Narodne novine 79/07

Hrvatske. Stupanj tajnosti *POVJERLJIVO* primjenjuje se za podatke čije bi neovlašteno otkrivanje naštetilo nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske. Podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova od sigurnosnog interesa za Republiku Hrvatsku u području obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva označavaju se stupnjem tajnosti *OGRANIČENO*. Poslovni subjekti informacije mogu klasificirati na različite načine, odnosno mogu imati broj razina i oznake koje su prikladne i potrebne za zaštitu informacijske imovine poslovnog subjekta. Tablica 5. prikazuje primjer oznaka i opisa klasifikacijskih razina.

Klasifikacijska razina	Opis
javno	• informacije namijenjene javnoj objavi • javna objava ne može naštetiti organizaciji
povjerljivo	• informacije čije otkrivanje neovlaštenim osobama može imati štetne posljedice za organizaciju • ugled, manja financijska šteta…
tajno	• informacije čije otkrivanje neovlaštenim osobama može imati značajne štetne posljedice za organizaciju • značajno narušavanje ugleda, veća financijska šteta…
vrlo tajno	• informacije čije otkrivanje neovlaštenim osobama može imati značajne štetne posljedice za organizaciju • tržišne, pravne…

Tablica 5. Klasifikacijske razine informacija

Klasifikacijska razina *javno* odnosi se na sve informacije koje su namijenjene javnoj objavi i čija javna objava ne može nanijeti štetu organizaciji. Primjer su takvih informacija informacije koje se navode na mrežnim stranicama, objave za medije i slično. Klasifikacijska razina *povjerljivo* rabi se za informacije čije otkrivanje neovlaštenim osobama može imati štetne posljedice za organizaciju, primjerice manje financijske štete ili nanošenje štete ugledu organizacije. Riječ je o općim informacijama o organizaciji, osobnim informacijama zaposlenika, informacijama o partnerima i slično. Klasifikacijska razina *tajno* označava informacije čije otkrivanje neovlaštenim osobama može imati značajne štetne posljedice za organizaciju. Otkrivanje financijskih

informacija, ugovora ili informacija o klijentima može dovesti do značajnog narušavanja ugleda organizacije i većih financijskih šteta. Informacije čije otkrivanje neovlaštenim osobama može dovesti do značajnih štetnih tržišnih i pravnih posljedica za organizaciju označavaju se klasifikacijskom razinom *vrlo tajno*. Primjeri su marketinške informacije, financijski planovi, informacije o tehničkim sustavima i slično.

Sljedeći je korak **definiranje kontrola za pojedine klasifikacijske razine**. One se definiraju na osnovi sigurnosne politike te regulatornih i ugovornih zahtjeva. Kontrole koje se često rabe uključuju: provjeru identiteta osobe koja pristupa informaciji, pristup podacima prema radnom mjestu (*role-based access*), kriptiranje i razne tehničke kontrole (antivirusni sustavi, segregacija mreže itd.). Za definiranje kontrola zadužen je vlasnik informacije.

Nadalje, vlasnik informacije zadužen je i za **pridruživanje klasifikacijskih razina pojedinačnim informacijama** i sukladno tome za određivanje prava pristupa informacijama. Pored toga, potrebno je provoditi periodičku provjeru pridruživanja klasifikacijskih razina s obzirom na zakonske promjene, promjene u poslovnim procesima i slično.

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Gifford, N. (2009). *Information security: Managing legal risks* (poglavlje 3). Sydney: CCH Australia Limited.
2. Marijanović, I. (2010). Klasifikacija informacija. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 129–134). Zagreb: Algebra.
3. *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07
4. *Zakon o tajnosti podataka*, Narodne novine 79/07

PITANJA ZA PONAVLJANJE:

1. Što je klasifikacija informacija?
2. Koliko razina tajnosti definira Zakon o tajnosti podataka i tko je obavezan primjenjivati takvu klasifikaciju?

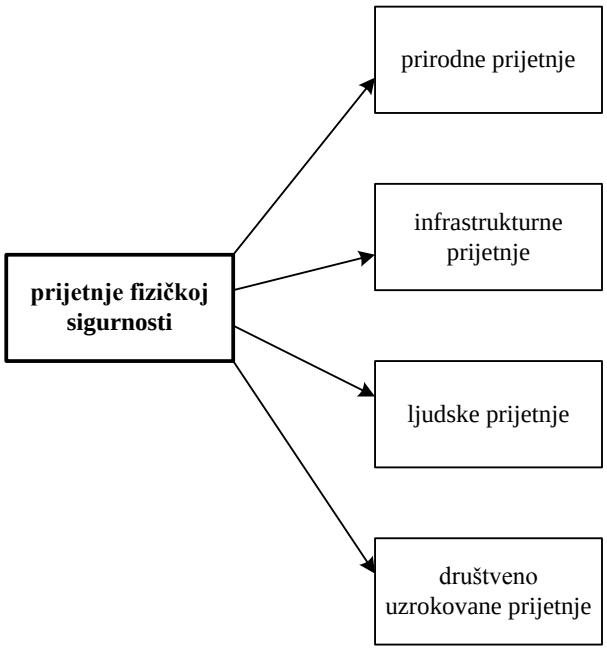
FIZIČKA SIGURNOST

U OVOME ĆEMO POGLAVLJU NAUČITI:

- KOJE SU PRIJETNJE FIZIČKOJ SIGURNOSTI INFORMACIJA
- ZA KOJU SE IMOVINU NAJČEŠĆE PROVODE MJERE FIZIČKE ZAŠTITE
- FIZIČKE KONTROLE ZA GRAĐEVINE I OKOLIŠ
- FIZIČKE KONTROLE ZA PROSTORIJE
- FIZIČKE KONTROLE ZA RAČUNALNU I MREŽNU OPREMU
- FIZIČKE KONTROLE ZA PAPIRNATE I ELEKTRONIČKE MEDIJE.

FIZIČKA SIGURNOST

Fizička sigurnost predstavlja aspekt informacijske sigurnosti koji se u praksi često zanemaruje. Stručnjaci za područje informacijske sigurnosti naglasak često stavljaju na logičke kontrole, primjerice politike, procedure i pravilnike, zaporke, antivirusnu zaštitu i slično, dok se fizičkim kontrolama posvećuje manja pozornost. Ne smije se zanemariti činjenica da je informacijski sustav siguran u onoj mjeri u kojoj je sigurna njegova najslabija karika. Stoga je u sklopu sustava upravljanja informacijskom sigurnošću potrebno osmisliti i implementirati i kontrole kojima se umanjuje fizičke prijetnje osnovnim svojstvima informacije (vidi sliku 20).



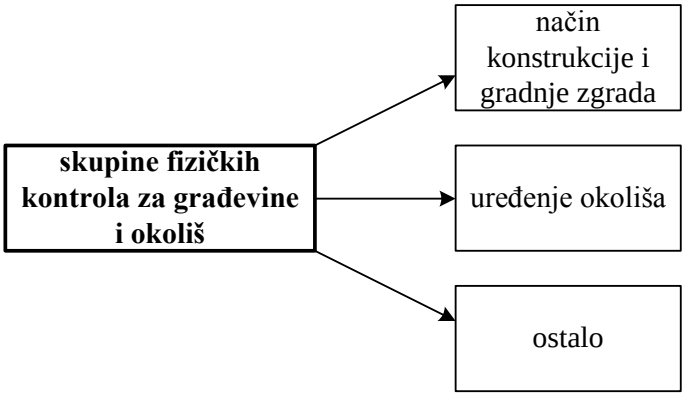
Slika 20. Prijetnje fizičkoj sigurnosti informacija

Prijetnje fizičkoj sigurnosti informacija prema Šegudoviću (2010., str. 106–107) uključuju prirodne prijetnje (poplave, potrese, oluje, ekstremne temperature i slično), infrastrukturne prijetnje (prekide napajanja električnom energijom, probleme s

plinskim i vodovodnim instalacijama itd.), ljudske prijetnje (neovlašteni pristup, nepažnju i nemar, vandalizam, krađe i slično) i društveno uzrokovane prijetnje (štrajk, rat, teroristički napad).

Fizičke mjere zaštite najčešće se provode nad građevinama i okolišem, prostorijama, računalnom i mrežnom opremom te papirnatim i elektroničkim medijima.

Građevine i okoliš prva su razina zaštite od različitih vrsta prijetnji. Prilikom procjene rizika za građevine i okoliš u obzir je potrebno uzeti konstrukciju i izgled građevine (izvedba infrastrukture, vodovodne, električne, plinske i telekomunikacijske instalacije, raspored i položaj prostorija, prozora i vrata, građevinske materijale i slično), okoliš i vanjske utjecaje (izgled zgrade i terena, stopu kriminaliteta na tom području, blizinu vatrogasaca i policije, dostupnost (cestovni pristup, gustoću prometa, blizinu zračne luke, autobusnog ili željezničkog kolodvora) te prirodne prijetnje (rizik od požara, potresa, poplava, oluja, odrona kamenja i klizišta). Fizičke kontrole za građevine i okoliš mogu se svrstati u tri osnovne skupine: način konstrukcije i gradnje zgrada, uređenje okoliša i ostalo (vidi sliku 21.).



Slika 21. Skupine fizičkih kontrola za građevine i okoliš

Prilikom konstrukcije i izrade zgrada potrebno je voditi računa o vatrootpornosti zidova, stropova i podova, posebice kada je riječ o prostorijama za arhiviranje i sistemskim salama. Takve se prostorije mogu dodatno zaštiti uporabom posebne armature, dvostrukim zidovima, ugradnjom protuprovalnih i protupožarnih vrata, prozora s rešetkama ili ojačanim staklima. Infrastrukturne instalacije također predstavljaju prijetnju, no one nisu u središtu interesa menadžera i/ili stručnjaka za

informacijsku sigurnost. Potrebno je osigurati njihovo redovito održavanje te znati gdje se nalaze sigurnosni ventili.

Najčešće kontrole koje se odnose na okoliš su postavljanje ograda, javne rasvjete, rasvjete, klupica za sjedenje te uklanjanje stabala u neposrednoj blizini građevina. Cilj je smanjenje rizika od kriminalnih aktivnosti. Uz spomenuto smanjenje rizika od kriminalnih aktivnosti videonadzor je izrazito koristan u naknadnim analizama.

U skupinu ostalo spadaju redoviti obilasci djelatnika zaštitarskih službi, trenirani psi koji čuvaju građevinu i okoliš i slično. Praksa je pokazala da takve mjere fizičke zaštite imaju snažan učinak odvraćanja potencijalnih provalnika.

Fizičke kontrole za prostorije obuhvaćaju kontrolu pristupa (identifikaciju posjetitelja, ograničavanje pristupa u određene prostorije i na određene katove), sustave za detekciju i alarmne sustave, sustave za zaštitu od požara (detektore dima, plamena i temperature) i adekvatno napajanje električnom energijom (odvajanje infrastrukturnih instalacija od instalacija informacijsko-komunikacijske tehnologije, generatore, uređaje za neprekinuto napajanje (*uninterruptable power supply,* skraćeno *UPS*) itd.). Sustavi za detekciju i alarmni sustavi imaju široku primjenu. Rabe se za otkrivanje provala i drugih slučajeva neovlaštenog pristupa. Nakon aktiviranja alarma potrebna je intervencija stručnog osoblja.

Fizičke kontrole za računalnu i mrežnu opremu najčešće se primjenjuju za sistemske sale. Pristup u njih imaju isključivo djelatnici kojima je pristup neophodan zbog prirode posla koji obavljaju. Takve prostorije u pravilu imaju protuprovalna vrata, visok stupanj protupožarne zaštite (vatrootporne zidove, detekciju požara, protupožarne uređaje), senzore za detekciju tekućine, antistatičke podove i uzemljenja. Nadalje, često se rabi i seizmička zaštita u obliku gumenih postolja i seizmičkih ormara koji smanjuju osjetljivost na vibracije. Potrebno je voditi računa o osjetljivosti računalne opreme na vlagu (potrebna je vlažnost zraka od 40 do 60%) i temperaturu (mora biti manja od 25^{o}C). Poslužiteljski ormari osiguravaju hlađenje i pravilan smještaj. Kabliranje mora biti provedeno prema pravilima struke, što podrazumijeva ispravnu uporabu odgovarajućih kablova (kablovi *UTP*, *FTP* i *STP* itd). Preporučljivo je ne ostavljati prijenosna računala na javnim mjestima, koristiti sigurnosne brave i detektore pokreta. Kao logička kontrola preporuča se kriptiranje podataka.

Sefovi, rezači papira i uništavači elektroničkih medija spadaju u fizičke kontrole za papirnate i elektroničke medije. Sefovi su tradicionalno rješenje koje pruža zaštitu od provala, požara i ostalih prijetnji iz okoline. Elektronički mediji uništavaju se demagnetizacijom ili fizičkim metodama. Na slici 22. prikazan je uređaj za demagnetizaciju elektroničkih medija.

Slika 22. Uređaj za demagnetizaciju tvrdih diskova i traka pod nazivom SV91M Degausser (www.eyecote.com/degausser/units/SV91M.htm)

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Andress, J. (2011). *Basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (poglavlje 7). Waltham: Elsevier.
2. Šegudović, H. (2010). Fizička sigurnost. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 105–128). Zagreb: Algebra.
3. Whitman, M. E. i Mattord, H. J. (2010). *Management of information security* (poglavlje 9). Boston: Course Technology.

PITANJA ZA PONAVLJANJE:

1. Koje su sve prijetnje fizičkoj sigurnosti informacija?
2. Za koju se imovinu najčešće provode mjere fizičke zaštite?
3. Što osoba zadužena za informacijsku sigurnost mora uzeti u obzir prilikom planiranja fizičke sigurnosti?

ODRŽAVANJE POSLOVANJA U KRIZNIM SITUACIJAMA

U OVOME ĆEMO POGLAVLJU NAUČITI:

- ŠTO JE UPRAVLJANJE KONTINUITETOM POSLOVANJA
- ŠTO JE PLAN KONTINUITETA POSLOVANJA
- KOJE KORAKE OBUHVAĆA PROCES PLANIRANJA KONTINUITETA POSLOVANJA
- ŠTO JE ANALIZA UČINKA NA POSLOVANJE I ŠTO ONA OBUHVAĆA
- KORAKE PROVEDBE PLANA KONTINUITETA POSLOVANJA NAKON ŠTO DOĐE DO PREKIDA POSLOVANJA.

ODRŽAVANJE POSLOVANJA U KRIZNIM SITUACIJAMA

Uslijed dugotrajnog nestanka napajanja, kvara na ključnom serveru ili kvara mrežne opreme, požara u sistemskoj sobi, potresa, poplave ili primjerice namjernog uništenja opreme može doći do djelomičnog ili potpunog prekida poslovanja. Stoga je potrebno na određeni način spriječiti ili kontrolirati posljedice prekida poslovanja. Hotchkiss (2010., str. XV) upravljanje kontinuitetom poslovanja (*business continuity management*) definira kao proces osmišljavanja i održavanja sveobuhvatnog plana kontinuiteta poslovanja (*business continuity plan*) koji osigurava kontinuitet poslovanja nakon što dođe do prekida poslovanja. Nadalje, Marijanović (2010., str. 270) navodi da upravljanje kontinuitetom poslovanja omogućuje otpornost organizacije na prekide, oporavak ključnih usluga i proizvoda na odgovarajuću razinu u odgovarajućem razdoblju te zaštitu poslovanja, ugleda i klijenata organizacije.

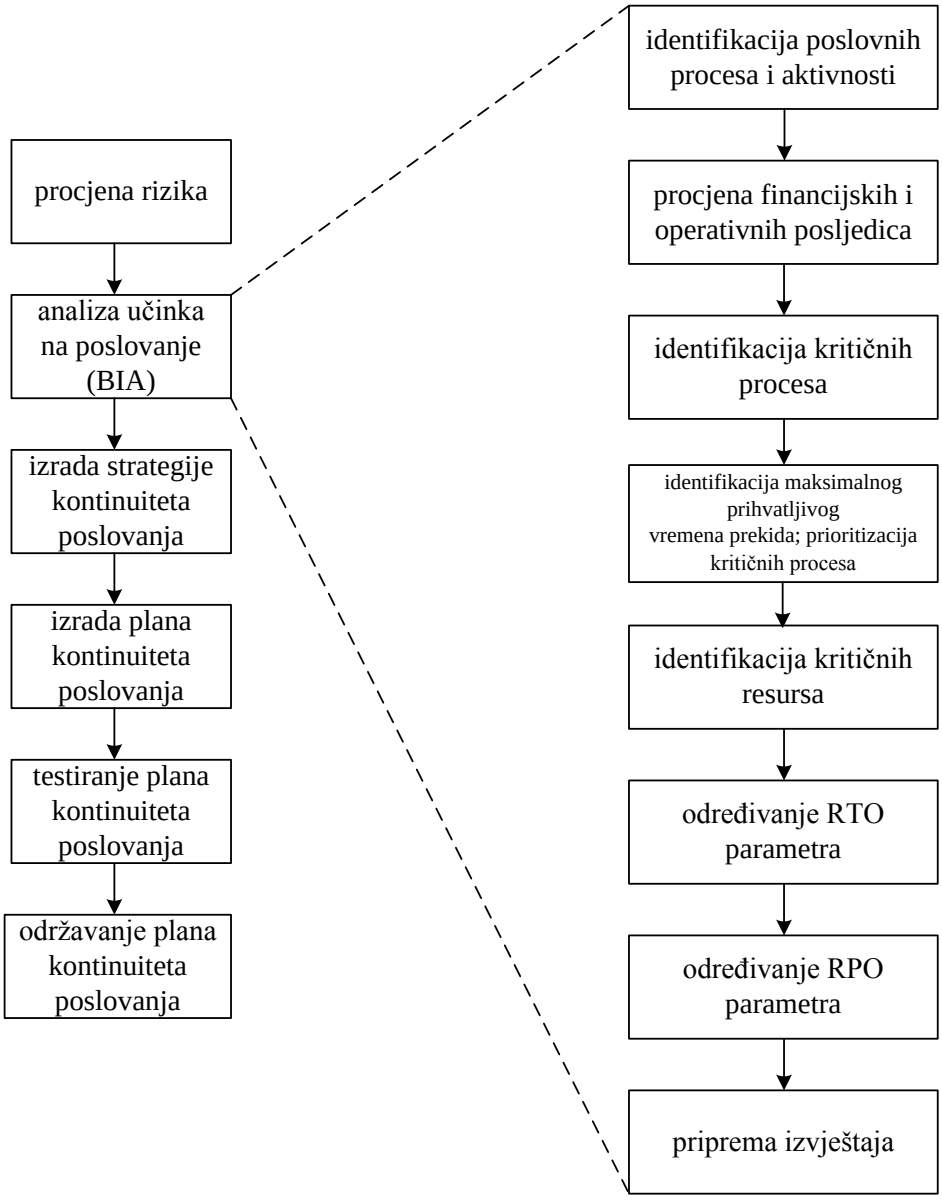
Plan kontinuiteta poslovanja (Hotchkiss, 2010., str. XV) dokumentirana je procedura kojom se određuje način djelovanja u slučaju ostvarenja rizika. On mora obuhvaćati sve scenarije i procedure te služiti kao vodič u slučaju prekida poslovanja. On se ažurira i održava u sklopu upravljanja kontinuitetom poslovanja.

Proces planiranja kontinuiteta poslovanja obuhvaća šest aktivnosti koje su prikazane na slici 22.[25] Prva je aktivnost **procjene rizika od prekida poslovanja**.

Slijedi **analiza učinka na poslovanje** (*business impact analysis*). Ona obuhvaća identifikaciju poslovnih procesa i aktivnosti, procjenu financijskih i operativnih posljedica, identifikaciju kritičnih procesa, identifikaciju maksimalnoga prihvatljivog

[25] Detaljnije o tome u Marijanović, I. (2010), 270–285

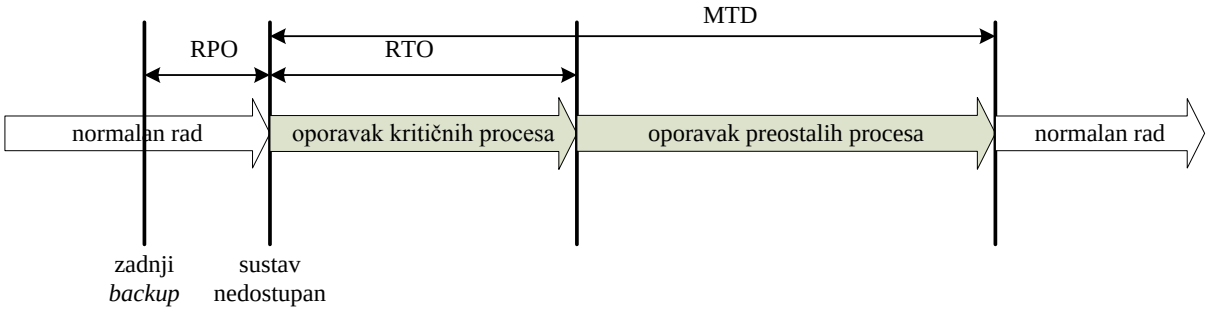
vremena prekida i prioritizacija kritičnih procesa, identifikaciju kritičnih resursa, određivanje parametara RTO i RPO te pripremu izvještaja (vidi sliku 22.).



Slika 22. Aktivnosti u okviru procesa planiranja kontinuiteta poslovanja

U okviru prvog koraka *identifikacije poslovnih procesa i aktivnosti* utvrđuju se poslovni procesi organizacije. Oni se u pravilu dijele u dvije skupine: primarne poslovne procese i procese podrške. Primarni poslovni procesi su oni koji nose osnovu poslovanja, dok procesi podrške omogućuju odvijanje primarnih procesa. Primjerice ako je riječ o marketinškoj tvrtki, onda se u primarne procese ubraja organiziranje promotivnih aktivnosti, osmišljavanje reklamnih kampanja i slično. Ako je pak riječ o tvrtki koja se bavi proizvodnjom medicinske opreme, onda prethodno navedeni procesi spadaju u

procese podrške. U drugom se koraku provodi *procjena potencijalnih financijskih i operativnih posljedica* u slučaju prekida poslovnih procesa. Na osnovi procjene *utvrđuju se kritični poslovni procesi*. Četvrti je korak *identifikacija maksimalnoga prihvatljivog vremena prekida i prioritizacija kritičnih procesa.* Maksimalno prihvatljivo vrijeme prekida (*maximum tolerable downtime – MTD*) označava maksimalno prihvatljivo trajanje prekida do oporavka poslovnog procesa na uobičajenu razinu. Na osnovi parametra MTD određuju se prioriteti za opravak kritičnih procesa. Nakon *identifikacije kritičnih resursa* potrebno je *odrediti parametre RTO* i *RPO*. RTO parametar (*recovery time objective*) označava vrijeme od prekida do opravka ključnih resursa. RPO parametar (*recovery point objective*) označava razdoblje prihvatljive količine izgubljenih podataka. Riječ je o razdoblju između zadnjeg *backupa* podataka i trenutka u kojem je došlo do neželjenog događaja. Slika 23. prikazuje parametre MTD, RTO i RPO.



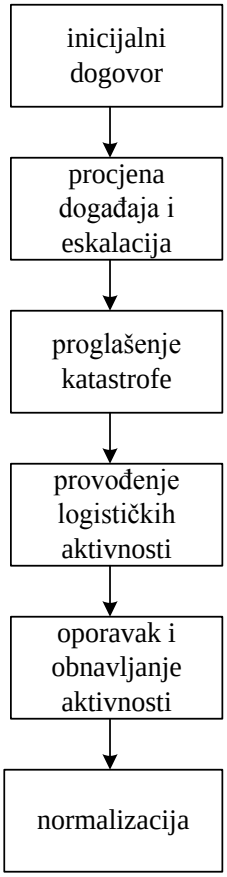
Slika 23. Parametri MTD, RTO i RPO
(vlastiti rad autora prema Snedaker, S. (2011), 220, i Marijanović, I. (2010), 64)

Posljednji korak u okviru analize učinka na poslovanje je *izrada izvještaja* koji sadrži informacije o kritičnim procesima, kritičnim resursima, parametrima MTD, RTO i RPO za pojedine poslovne procese te popis prioritetnih procesa za oporavak.

Treći je korak u procesu planiranja kontinuiteta poslovanja (vidi sliku 22.) **izrada strategije kontinuiteta poslovanja**. Strategijom se, između ostaloga, određuje kritični procesi i resursi za oporavak, način oporavka, vrijeme opravka i troškovi implementacije. Sljedeći je korak **izrada plana kontinuiteta poslovanja**. U planu se navode opseg i svrha plana, definicija neželjenog događaja, sažetak procjene rizika, sažetak analize utjecaja na poslovanje, sažetak strategije kontinuiteta poslovanja, članovi tima za provedbu plana te opis aktivnosti za provedbu plana. Hrvatska norma

HRN ISO/IEC 27001[26] određuje da je plan kontinuiteta poslovanja potrebno testirati. Nadalje, plan je potrebno redovito održavati.

Ako dođe do neželjenog događaja, odnosno incidenta potrebno je primijeniti plan održavanja kontinuiteta poslovanja. Faze provedbe plana kontinuiteta poslovanja prikazane su na slici 24.



Slika 24. Faze provedbe plana kontinuiteta poslovanja

Prva je faza *inicijalni dogovor*. Potrebno je obavijestiti koordinatora za provođenje plana kontinuiteta poslovanja i ostale članove time te izvršiti grubu procjenu posljedica. U okviru sljedeće faze *procjene događaja i eskalacije* procjenjuje se šteta, izrađuje izvještaj o šteti i po potrebi donosi odluka o eskalaciji u sljedeću fazu. Treća je faza *proglašenje katastrofe.* Katastrofa se proglašava na osnovi izvješća iz prethodne faze. Ona obuhvaća odabir strategije oporavka, izradu izjave o proglašenju katastrofe, pripremu priopćenja za javnost i okupljanje tima za provedbu plana kontinuiteta

[26] Hrvatski zavod za norme (2013). *Hrvatska norma HRN ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission*.

poslovanja. Faza *provođenja logističkih aktivnosti* odnosi se na pripremu okruženja za oporavak svih poslovnih aktivnosti (nabava hardvera, instalacija softvera i slično). U fazi *opravka i obnavljanja aktivnosti* obnavljaju se kritički resursi i uspostavljaju poslovni procesi. Završna je faza *normalizacije,* odnosno povratka na stanje prije neželjenog događaja.

PRIJEDLOZI ZA DALJNJE ČITANJE:

1. Blyth, M. (2009). *Business continuity management: Building an effective incident management plan* (poglavlja 1 i 2). New Jersey: John Wiley & Sons.
2. Hotchkiss, S. (2010). *Business continuity management: A practical guide*. Swindon: The Charted Institute for IT.
3. Marijanović, I. (2010). Održavanje poslovanja u kriznim situacijama. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 269–286). Zagreb: Algebra.
4. Snedaker, S. (2011). *Business continuity & disaster recovery for IT professionals* (poglavlja 1, 3 i 4). Burlington: Elsevier.

PITANJA ZA PONAVLJANJE:

1. U kojim situacijama može doći do potpunog prekida poslovanja?
2. Što je cilj upravljanja kontinuitetom poslovanja?
3. Kada se primjenjuje plan održavanja kontinuiteta poslovanja?
4. Što je potrebno uzeti u obzir prilikom planiranja rezervne (sekundarne) lokacije? Razmislite o odgovoru u kontekstu posla kojim se tvrtka bavi.

POPIS LITERATURE

1. Andersen, B. i Fagerhaug, T. (2006). *Root cause analysis: Simplified tools and techniques.* Milwaukee: Quality Press.
2. Andress, J. (2011). *Basics of information security: Understanding the fundamentals of InfoSec in theory and practice.* Waltham: Elsevier.
3. Blyth, M. (2009). *Business continuity management: Building an effective incident management plan.* New Jersey: John Wiley & Sons
4. Calder, A. (2008). *ISO 27001/ISO 2700: A pocket guide.* Cambridgeshire: IT Governance Publishing.
5. Gifford, N. (2009). *Information security: Managing legal risks*. Sydney: CCH Australia Limited.
6. Gregory, P. (2010). *CISSP guide to security essentials.* Boston: Course Technology.
7. Hotchkiss, S. (2010). *Business continuity management: A practical guide.* Swindon: The Charted Institute for IT.
8. Humphreys, E. (2007). *Implementing the ISO/IEC 27001 information security management standard.* Norwood: Artech House.
9. Jansen, W. (2009). *Directions in security metrics research.* Gaithersburg: National Institute of Standards and Technology.
10. Kahate, A. (2008). *Cryptograophy and network security.* New Delhi: Tata McGraw-Hill.
11. Krausz, M. (2010). *Managing information security breaches: Studies from real life.* Cambridgeshire: IT Governance Publishing.
12. Kreitner, M. (2009). *Management.* Boston: Houghton Mifflin Harcourt.
13. Landoll, D. J. (2011). *The security risk assessment handbook: A complete guide for performing security risk assessment.* Boca Raton: CRC Press.

14. Marijanović, I. (2006). ISO/IEC 27001: 2005 norma. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 59-72). Zagreb: Algebra.

15. Marijanović, I. (2006). Upravljanje rizikom. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 73–85). Zagreb: Algebra.

16. Marijanović, I. (2006). Klasifikacija informacija. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 129–134). Zagreb: Algebra.

17. Marijanović, I. (2006). Održavanje poslovanja u kriznim situacijama. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 269–286). Zagreb: Algebra.

18. Snedaker, S. (2011). *Business continuity & disaster recovery for IT professionals.* Burlington: Elsevier.

19. Stoneburner, G., Goguen, A. i Ferniga, A. (2002). *Risk management guide for information technology systems: Recommendations of the National institute of standards and technology.* Gaithersburg: National Institute of Standards and Technology.

20. Strahonja, V. i Saletović, K. (2007). Proactive approach to the problem management in communication network. *Journal of Information and Organizational Sciences*, *31/1*, 245–259.

21. Swamidass, P. M. (2000). *Encyclopedia of production and manufacturing management.* Norwell: Kluwer Academic Publishers.

22. Šegudović, H. (2010). Fizička sigurnost. U Silvija Jurak (ur.), *Sigurnost informacijskih sustava* (str. 105–128). Zagreb: Algebra.

23. Vellani, K. H. (2007). *Strategic security management: A risk assessment guide for decision makers.* Oxford: Butterworth-Heinemann.

24. Whitman, M. E. i Mattord, H. J. (2010). *Management of information security.* Boston: Course Technology.

MREŽNI IZVORI

1. Hrvatski jezični portal http://hjp.novi-liber.hr (pristupljeno 3. svibnja 2013.)
2. Tvrtka *Eyecote Media Security Specialists* www.eyecote.com (pristupljeno 19. svibnja 2013.)

ZAKONI, ODLUKE I NORME

1. Hrvatski zavod za norme (2013). Hrvatska norma HRN ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission.
2. Hrvatski zavod za norme (2013). Hrvatska norma HRN ISO/IEC 27002, International Organization for Standardization and International Electrotechnical Commission.
3. Hrvatski zavod za norme (2013). International Standard ISO/IEC 27000, International Organization for Standardization and International Electrotechnical Commission.
4. Hrvatski zavod za norme (2013). International Standard ISO/IEC 27005, International Organization for Standardization and International Electrotechnical Commission.
5. *Odluka Hrvatske Narodne banke o primjerenom upravljanju informacijskih sustavom*, Narodne novine 37/10
6. *Zakon o informacijskoj sigurnosti*, Narodne novine 79/07
7. *Zakon o kreditnim institucijama*, Narodne novine 117/08, 74/09, 153/09 i 108/12
8. *Zakon o tajnosti podataka*, Narodne novine 79/07
9. *Zakon o zaštiti i spašavanju*, Narodne novine 174/04, 79/07, 38/09 i 127/10
10. *Zakon o zaštiti osobnih podataka*, Narodne novine 103/03, 118/06, 41/08, 130/11 i 106/12
11. *Zakon o zaštiti tajnosti podataka*, Narodne novine 108/06

POPIS SLIKA

POPIS TABLICA

BIOGRAFIJA AUTORA

KRISTIAN SALETOVIĆ rođen je u Zagrebu 1977. godine. Magistrirao je informacijske znanosti na Fakultetu organizacije i informatike Sveučilišta u Zagrebu. Radio je u uglednim globalnim kompanijama na stručnim poslovima u telekomunikacijskoj industriji.

2010. godine izabran je u naslovno nastavno zvanje višeg predavača. Nositelj je i izvođač kolegija Modeliranje poslovnih procesa i Sigurnost poslovnih informacijskih sustava na diplomskom studiju IT menadžmenta na Veleučilištu VERN'. Radi u informatičkoj industriji kao direktor informatike i menadžer za informacijsku sigurnost.