Dr Radoslav Raković

BEZBEDNOST INFORMACIJA - OSNOVE I SMERNICE

Beograd, 2017.

Dr Radoslav Raković

BEZBEDNOST INFORMACIJA - OSNOVE I SMERNICE

Recenzenti:
Dr Ljubomir Lazić
Dr Miodrag Mesarović

Izdavač:
„Akademska misao“ doo Beograd

Glavni i odgovorni urednik:
Marko Vujadinović

Priprema:
Dr Radoslav Raković

Štampa:
Planeta print, Beograd

Tiraž:
500 primeraka

ISBN 978-86-7466-711-8

„Uspeh nije u onome dokle si stigao,
već u putu koji si prešao od onoga odakle si krenuo.“

Booker Washington

Slavici i Jasmini

Autor

PREDGOVOR

U našem okruženju postoji veliki razlog ZA nastajanje ove knjige i drugi veliki razlog PROTIV da ona bude napisana!

Ako već moram da se pravdam zašto sam se u to upustio, najbolja „odbrana" je sve ono što se dešava u vezi sa informacijama kako na globalnom nivou tako i neposredno oko nas. Tema je veoma aktuelna, i nažalost, ostaće aktuelna i ubuduće. Zato je veoma važno da se o toj temi priča i da se pronalaze načini kako se sa problemom bezbednosti informacija izboriti. U ovoj knjizi u prvom planu je bezbednost informacija u organizaciji, kako informacije vezane za aktivnost organizacije zaštititi od onih koji joj ne misle dobro. S obzirom na zaoštrenu tržišnu konkurenciju logično je očekivati da te informacije budu ugrožene spolja, od onih koji pokušavaju na razne načine da ostvare prednost u odnosu na organizaciju na tržištu. Nažalost, u ovoj oblasti može se primeniti čuvena izreka u obliku molitve: „Bože, sačuvaj me od prijatelja, od neprijatelja ću se sam sačuvati!". Dakle, i unutar same organizacije ima onih koji joj ne misle dobro, a pošto su njen deo, utoliko su opasniji u svom delovanju. Statistike u svetu pokazuju da se najveći broj ugrožavanja bezbednosti informacija dešava od strane insajdera, dakle onih koji su tu oko nas. To naravno ne znači da treba da skrenemo u paranoično ponašanje gledajući popreko ljude sa kojima radimo, već treba da se organizujemo tako da uredimo proces kako bi bio što je moguće više otporan i na tu vrstu ugrožavanja.

Razlog PROTIV razumeće pre svega oni koji su bar jednom prošli kroz proces pisanja knjige „od ideje do realizacije" (autor je to već prošao sedam puta) i ono što je sledilo nakon toga. Uložite ogromnu energiju i vreme, na radno vreme koje je „8+" dodate svakoga dana još po par sati, sve dok oči ili kičma mogu da izdrže, neretko odvajate vreme od sna ... Na kraju, kada se knjiga pojavi, podvučete crtu i zaključite kako se pisanje apsolutno ne isplati, a još kad čujete neke komentare padnete u iskušenje da se upitate: „A šta će to meni?". U današnje vreme to je Sizifov posao. Međutim, kada nakon nekog vremena kroz citiranje vidite da su ljudi koristili knjigu, kada se susretnete sa onima koji su je čitali i čujete poneku lepu reč (a neki put i primedbu) shvatite da napor nije bio uzaludan i da ste uradili nešto što će drugima biti od koristi. Upravo to zadovoljstvo komunikacije sa čitaocima predstavlja nešto što vas pokreće i vodi kroz buru današnjeg vremena.

Ovom prilikom želim da se zahvalim onima koji su doprineli da se ova knjiga pojavi i da izgleda baš onako kako je vide čitaoci.

Zahvaljujem se recenzentima dr Ljubomiru Laziću i dr Miodragu Mesaroviću na korisnim sugestijama koje su pomogle formiranju finalne verzije teksta.

Posebnu zahvalnost autor duguje preduzeću Energoprojekt Entel a.d. i direktoru Mladenu Simoviću što su imali razumevanja i kroz finansijsku podršku pomogli izdavanje ove knjige.

Zahvaljujem se izdavaču ove knjige, kompaniji „Akademska misao“, koja je istrajala u opredeljenju da podrži izdavanje ove vrste literature.

Na kraju, jedno VELIKO HVALA supruzi Slavki i kćerki Jasmini, koje su imale dovoljno ljubavi, strpljenja, podrške i razumevanja za ono što sam radio.

Autor

U Beogradu, novembra 2017.

SADRŽAJ

Sadržaj

Sadržaj

Sadržaj

SPISAK SLIKA **Glava / Poglavlje**

Sadržaj

SPISAK TABELA **Glava / Poglavlje**

Sadržaj

Glava 1:
UVOD

**"Knjiga je vrednija od svih spomenika,
jer ona sama gradi spomenike u srcu onoga ko je čita!"**
Egipatski zapis iz Novog carstva

Pristojno ponašanje prema čitaocima nalaže da se u početku daju uvodne napomene, kako bi znali šta ih u nastavku čeka, iako se to već moglo naslutiti iz sadržaja knjige. Uostalom, u svemu što se radi uvek je korisno sagledati smisao, celinu, širi kontekst, da bismo u nastavku mogli lakše da se suočimo sa nekim detaljima. Nadam se da će nagoveštaj onoga što se nalazi na narednim stranama biti dovoljno privlačan i da nećete odustati od onoga što sledi. Bilo bi šteta za autora (zašto se uopšte trudio), a verujem (možda neskromno) i za vas.

Poslednje tri decenije obeležene su burnim razvojem u nekoliko oblasti, od kojih je svakako najvidljiviji onaj u oblasti informaciono-komunikacionih tehnologija. Pre samo dvadesetak godina bilo je nezamislivo imati mobilni telefon, računari su bili veoma spori, a njihove memorije nekoliko puta manje od današnjih USB-ova, na telefonski priključak fiksne telefonije čekalo se godinama, kablovska TV bila je tek u začetku pa su stambene zgrade na terasama i krovovima bile "ukrašene" mnoštvom antena kojima je bilo teško pronaći položaj da svi kanali (od njih nekoliko) imaju prihvatljiv kvalitet slike, itd. U poslovanju organizacija automatizovanost procesa bila je retka, sve se svodilo na obračun ličnih dohodaka, knjigovodstvo i računovodstvo i složenije proračune, a sve ostalo radilo se "peške".

Verujem da je navedeno podsećanje kod vas izazvalo blagi smešak, a možda i nevericu, iako ste bili savremenik ovih promena. Očigledno je da je napredak informaciono-komunikacionih tehnologija omogućio niz pogodnosti i olakšao nam svakodnevni život, kako u privatnoj sferi tako i u poslovanju. Nažalost, kao i mnoge stvari u životu i ove pogodnosti imaju i "tamniju" stranu, jer su upravo zahvaljujući tehnologijama informacije postale dostupne mnogima sa lošim namerema, spremnim da te informacije zloupotrebe iz materijalnih i mnogih drugih razloga.

Bez obzira na to u koje svrhe se koriste informacije, očigledno je da je neophodno razviti mehanizme koji će omogućiti da one budu dostupne samo onima kojima su i namenjene, da informacija bude kompletna i tačna (bez neovlašćenih izmena u sadržaju) i da bude raspoloživa onda kada nam je potrebna. Očuvanje navedenih osnovnih svojstava informacije – poverljivosti, tačnosti i raspoloživosti – predmet je oblasti koja je poznata kao "bezbednost infomacija" (engl. *Information Security*).

Iza naziva "bezbednost informacija" krije se veoma složena tema, koja je povezana sa mnoštvom oblasti tehničke i organizaciono - pravne prirode. U tehničkom segmentu tu su računari, računarske mreže, softveri, telekomunikaciona oprema, komunikacioni sistemi i sl. U organizaciono – pravnom segmentu tu su relevantni standardi i preporuke, kako za tehnički tako i za menadžment deo, zakonska i podzakonska regulativa i sl. Da bi se suočili sa ovako kompleksnom temom potrebno je da imate neka osnovna znanja i vladate nekim osnovnim pojmovima iz svih navedenih oblasti, bez obzira na to šta je vaša osnovna struka.

Ova knjiga namenjena je svima onima koji na ovaj ili onaj način dolaze u kontakt se oblašću bezbednosti informacija - menadžerima na različitim nivoima u organizaciji, projektnim menadžerima, specijalistima u oblastima računasrtva i telekomunikacija, zaposlenima bez obzira na delatnost organizacije, jer temu bezbednosti informacija nikako ne mogu izbeći, onima koji se bave proverama sistema menadžmenta bezbednošću informacija (internim i eksternim), studentima fakulteta ili visokih škola na kojima se ove teme izučavaju itd. Ako svima njima knjiga bude pomogla da lakše prepoznaju i razumeju neke pojmove i pojave, ako im to bar malo pomogne u svakodnevnom radu, ako ih usmeri na ključne stvari u ovoj oblasti ona će postići svoj cilj, a ako nekoga bude podstakla da nastavi da se bavi nekom od ovih oblasti i da proširi svoja znanja, onda će ga i premašiti.

Pored ove, uvodne glave, knjiga ima još 8 glava i dva priloga.

Glava 2 posvećena je osnovnim pojmovima vezanim za informacije i bezbednost informacija. Nakon definisanja pojma informacije i njenog odnosa sa drugim pojmovima, razmotreno je aktuelno stanje u oblasti bezbednosti informacija formirano na osnovu podataka iz literature. Razmotrena su osnovna i druga svojstva informacija, a zatim je ukazano na osnovne stvari koje je neophodno znati da bi se moglo delovati u ovoj oblasti.

Glava 3 posvećena je informacionim sistemima i telekomunikacijama. Razmotrene su osnovne karakteristike računarskih mreža, softvera kao specifične vrste proizvoda, osnovne vrste komunikacionih puteva za prenos infomacija i zakonska regulativa u Srbiji orijentisana ka elektronskim komunikacijama.

Organizacije koje posluju na tržištu imaju svoje poslovne ciljeve koji mogu biti ugroženi narušavanjem bezbednosti informacija. Iz ugla poslovanja organizacija, to predstavlja poslovni rizik, pa je oblast upravljanja rizicima tesno povezana sa aktivnostima organizacije u oblasti bezbednosti informacija. Zato je u **glavi 4** razmotren pojam rizika i menadžmenta rizicima, dat je prikaz serije standarda ISO 31000 koja se bavi tematikom rizika i detaljnije je prikazan proces menadžmenta rizicima, od identifikacije rizika preko njihove analize i vrednovanja, do predviđanja mera za postupanje sa rizicima i njihovog sprovođenja.

Glava 5 bavi se standardima za bezbednost informacija. U prvom planu je serija standarda ISO 27000. S obzirom da je reč o standardima koji su prvi prilagođeni budućoj jedinstvenoj strukturi menadžment standarda, prvo je prikazana ta jedinstvena struktura definisana ISO/IEC dokumentom poznatim pod skraćenim nazivom „Aneks SL", a zatim je napravljen pregled familije standarda ISO 27000 počev od pojmova, ključnih zahteva i ključnih faza i dokumenata u sistemu menadžmenta rizicima po bezbednost informacija. Posebna pažnja posvećena je problematici obezbeđenja kontinuiteta poslovanja, širem konceptu u okviru koga bezbednost informacija igra veoma važnu ulogu. Na kraju su razmotreni neki praktični aspekti bezbednosti informacija kao i zakonskli okvir za tu oblast u Srbiji.

Bezbednost mreža razmotrena je u **glavi 6**. Prvo je prikazan OSI referentni model komunikacionog sistema sa specifičnostima pojedinih nivoa, a zatim su razmotreni aspekti bezbednosti mreža u nekoliko oblasti koje su danas veoma aktuelne - u okruženju „oblaka" (engl. *Cloud*), u bežičnim komunikacijama i u mrežama koje primenjuju Internet protokol (IP).

U svim oblastima problematika bezbednosti informacija ima svoje specifičnosti, zavisno od posledica koje mogu nastati u slučaju njene ugroženosti. Zato su glave 7 i 8 posvećene aspektima bezbednosti informacija u dve specifične oblasti – telekomunikacije i elektroprivredni sistemi.

U **glavi 7** razmotrena je bezbednost informacija u oblasti telekomunikacija kroz standard ISO 27011i ITU-T preporuke. U **glavi 8** razmotrena je ova tematika u elektroprivrednim sistemima, posebno u sistemima tipa SCADA i inteligentnim mrežama (engl. *Smart Grid*) kroz prikaz standarda institucija kao što su CIGRE, IEC, NIST, NERC, DoE, ENISA i ISO. Drugi standardi za bezbednost informacija prikazani su u **glavi 9** – okvir COBIT, IEEE standardi kao i bezbednost osnovnih aplikacija, elektronske pošte i veba.

S obzirom da je u knjizi primenjen pristup da se pojmovi objasne „svojim rečima", uz maksimalno izbegavanje zvaničnih definicija i stručnih izraza kako bi se pomoglo čitaocima da ih lakše razumeju i usvoje, u **Prilogu A** dat je rečnik sa definicijama osnovnih pojmova i skraćenicama korišćenim u tekstu, abecednim redom i uz navođenje izraza iz engleskog jezika.

Korišćena literatura (knjige, članci, dokumenti i sl.) navedena je na kraju svake od glava, zavisno od njene teme, i zbirno u **Prilogu B**, uključujući i interesantne Internet sajtove. Razlog za neku vrstu „dupliranja" je dvojak - sa jedne strane, to je u novije vreme uobičajena praksa u literaturi, a sa druge, omogućuje čitaocu da se posveti onom segmentu koji ga najviše interesuje i da ima sve na jednom mestu.

U cilju preglednijeg izlaganja i lakšeg snalaženja čitaoca, u tekstu je korišćena sledeća grafička simbolika:

PITANJE / DILEMA
Formuliše suštinu problema ili nedoumice. U većini slučajeva reč je o realnim pitanjima na koje je autor nailazio u kontaktu sa ljudima, koja su postavljena direktno ili su proistekla iz određenih aktivnosti.

ODGOVOR
Objašnjava suštinu problema ili nedoumice i kako ih prevazići. Dat je sa ciljem da bar delimično pomogne u otklanjanju problema ili nedoumice, bez pretenzija da bude jednoznačan i sveobuhvatan.

SAVET
Ukazuje o čemu bi trebalo posebno voditi računa u vezi sa razmatranim pitanjem. Ako se već daje, autor je nastojao da savet bude upotrebljiv.

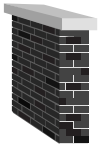
KLJUČNA STVAR
Ukazuje na ono što je najbitnije što uvek treba imati u vidu kad je reč o razmatranom problemu. Kada se naiđe na ovaj simbol, treba mu dati status „crvenog slova" u kalendaru!

UPOZORENJE
Mesto na kome se često greši. Ako se greška ne otkloni (tj. ako se fitilj ne ugasi), može imati veoma loše posledice (kad fitilj dogori, ne verujem da bi želeli da budete u blizini!).

NE ZABORAVITE
Navodi ono o čemu bi uvek trebalo voditi računa u vezi sa razmatranim pitanjem. Nije toliko važno kao „crveno slovo", ali ako se zaboravi ili zanemari, prelazi u kategoriju upozorenja.

PODSEĆANJE
Stav ili materija koji su potrebni za lakše razumevanje problema. Navedeni su u naznakama, a detaljnije su obrađeni u navedenoj literaturi.

DEFINICIJA
Određenje pojma u obliku koji je neophodan za praćenje materije u preostalom delu knjige. Nije idealna, ako takva uopšte postoji, ali je praktična, jer omogućuje da se (bar privremeno) premosti problem.



ZABLUDA
Ukazuje na pogrešan stav koji se povremeno ili često susreće u praksi. To se odnosi na samo neke od prepreka sa kojima se svakodnevno susrećemo. Da bi se premostile treba ih pre svega prepoznati kao zablude, a onda je već lakše!

Ukoliko vas nešto dodatno interesuje, ukoliko želite da ukažete na neku grešku ili iznesete svoju sugestiju vezanu za knjigu, slobodno pišite na jednu od ovih adresa elektronske pošte:

rrakovic@ep-entel.com **ili** rmrakovic@outlook.com

Budite strpljivi, odgovor će stići, pre ili kasnije.

Glava 2:
INFORMACIJA I BEZBEDNOST INFORMACIJA

"Ljudi greše, ali je za stvarno gadnu grešku potreban računar!"
Marfijev zakon

Razvoj informacionih tehnologija u poslednjih nekoliko decenija značajno je promenio način života i rada ljudi širom sveta. Proces prikupljanja informacija, nekada dugotrajan i često mukotrpan, postao je veoma brz i udoban za korisnika gde god da se nalazi, kod kuće ili na radnom mestu, u sredstvima prevoza ili na plaži. Da bi se u to uverili, dovoljno je da pogledate oko sebe – dok čitate ove redove (možda na vašem tablet računaru, ili kao klasičnu knjigu) mnogi oko vas su, kao opčinjeni, zagledani u svoj mobilni telefon, koji je sve manje telefon, a sve više računar čije karakteristike prevazilaze ono što smo pre dvadesetak godina mogli i da zamislimo. U kombinaciji sa deregulacijom tržišta, globalizacijom i ostalim trendovima u savremenom svetu informacione tehnologije uticale su da se stvore potpuno drugačiji uslovi poslovanja. Dakle, ove tehnologije počele su da se razvijaju pre svega kao sredstvo povezivanja na lokalnom i na globalnom nivou, a prerasle su u glavnog pokretača promena i faktor rešavanja privrednih, socijalnih i svih drugih problema savremenog sveta.

"Gde god je upotrebe, ima i zloupotrebe!"
Nepoznat izvor

Nažalost, blagodeti koje pružaju informacione tehnologije sve više su praćene pojavama koje nam stvaraju probleme. Pri tome ne mislimo na činjenicu da oprema brzo zastareva (a njeno modernizovanje ima svoju cenu), da je aplikacije koje se nude sve teže pratiti, a kamoli koristiti, ili da se ljudi međusobno sve više otuđuju. Mnogo teži problem je saznanje da je svet oko nas prepun onih koji pokušavaju (a često i uspevaju) da na različite načine zloupotrebe dostupnost informacija, i da ti pokušaji postaju sve bezobzirniji.

Sve veća primena informacionih tehnologija u poslovanju otvorila je pitanje bezbednosti informacija koje se koriste, čuvaju ili razmenjuju, kako u pogledu njihove poverljivosti (tajnosti), integriteta (tačnosti i celovitosti) i raspoloživosti. Informacije su izložene različitim pretnjama, kako spolja, tako i unutar same organizacije, one su u većoj ili manjoj meri ranjive i njihov gubitak, oštećenje, neovlašćena izmena, neraspoloživost itd. mogu naneti štetu poslovanju organizacije.

Informacija je danas postala veoma moćno oružje u borbi na tržištu, u politici, nauci ili sportu. Reč oružje uopšte ne stavljamo pod znake navoda - neki put je to sredstvo ubojitije od klasičnog naoružanja, jer moćnima omogućuje da postignu svoje ciljeve na mnogo suptilniji način!

Sve su to razlozi zbog kojih se problematici bezbednosti informacija mora posvetiti posebna pažnja. O ozbiljnosti problema svedoči i činjenica da na posledice upada nisu imuni ni vojni sistemi, uprkos mnoštvu mera koje su po prirodi svog funkcionisanja preduzimali da se to ne desi.

2.1 Pojam informacije

Pre nego što se posvetimo problematici koja se odnosi na bezbednost informacija, pozabavićemo se nekim osnovnim pojmovima oko kojih u praksi ima dosta nedoumica. To su komunikacija, informacija i njena zaštita, odnosno bezbednost.

Na slici 2-1 prikazan je model komunikacionog sistema koji će nam poslužiti da lakše objasnimo ove pojmove [Raković_B-10].

Komunikacija je razmena poruka koje sadrže neku informaciju.

Razmena poruka može se obavljati u različitim oblicima. U komunikaciji učestvuju „izvor" informacije (u komunikacionom smislu igra ulogu „predajnika") koji šalje informaciju, i „odredište" informacije, koje u komunikacionom smislu igra ulogu „prijemnika" koji tu informaciju prima. Pokretač „prenosa poruke" je ona strana koja želi da saopšti nešto onoj drugoj.