# POLITIKA INFORMACIONE BEZBEDNOSTI KAO ELEMENT PREVENCIJE KRIZNIH SITUACIJA

# INFORMATION SECURITY POLICIES AS PREVENTION ELEMENT OF CRISIS SITUATIONS

Slobodan R. Petrović[1],
Zoran Čekerevac[2],
Zoran J. Milanović[3]

**Rezime:** Razrešavanje informacione bezbednosti predstavlja izuzetno ozbiljan i složen zadatak koji postaje praktično nerešiv ili neadekvatno rešiv ukoliko mu se ne pristupi na strateški osmišljen način. Upravo iz tih razloga u radu se, kroz definisanje politike informacione bezbednosti, razmatraju polazne osnove, pravci i načini razrešavanja ovog problema.

**Ključne reči:** informaciona bezbednost, politika, zaštita

**Summary:** Resolving information security is very serious and complex task that becomes practically unsolvable or inadequately solvable if it is not conceived in a strategic manner. For these reasons, the paper, through the definition of information security policy, considers starting points, directions and ways of resolving this problem.

**Keywords:** information security, policy, protection

## 1. UVOD

U poslednjih nekoliko dekada mogućnosti informacione tehnologije da olakša poslovne procese organizacionih entiteta dramatično su se uvećale, zbog čega je širenje njihove primene dostiglo neočekivane razmere. Upravo iz tih razloga biznis postaje sve zavisniji od ove tehnologije, pa je posledično nastala i rapidno se širila i potreba zaštite informacionih dobara. Ta potreba se vremenom transformisala u zahtev koji je postao imperativan u sadašnjem, ali za verovati je da će takav ostati i u budućem korišćenju ove tehnologije.

U ranijim vremenima, dok su sistem i računarska mreža bili izolovani od spoljnih uticaja, zaštitom su se bavila tehnička lica, takoreći van vidnog polja ostalih zaposlenih. Za njih se znalo samo ako dođe do ispada sistema i prekida u radu. Međutim, kada su organizacioni entiteti izašli iz svog lokalnog okruženja i počeli da se povezuju sa drugim mrežama i sistemima – problem zaštite je dobio sasvim nove dimenzije. Broj mogućnosti i broj pretnji se dramatično uvećao i pitanje zaštite je moralo da izađe iz informatičkog sektora i da se proširi na ceo organizacioni entitet.

[1] batop@beotel.net
[2] Univerzitet "Union" Beograd Fakultet za industrijski menadžment, Kruševac, zoran.cekerevac@hotmail.com
[3] Kriminalističko-policijska akademija, Beograd, mzt@eunet.yu

Za top-menadžment informaciona bezbednost postaje jedno od strateških pitanja čije uspešno razrešavanje obezbeđuje stabilno i perspektivno funkcionisanje kompanije. Imajući tu činjenicu u vidu jasna je potreba da se ovo pitanje razrešava osmišljeno, kvalitetno i celovito. Navedene konstatacije su i jasne i obavezujuće, ali kada je reč o konkretizaciji ostaje i dalje otvoreno pitanje KAKO? Odgovori na ovo pitanje, posebno kada je reč o praksi, veoma su raznoliki, često nelogični, nerazumljivi, kontradiktorni, nerealni, neprimenjivi, ...

Ovaj rad pokušava da odgovori na postavljeno pitanje na način koji bi bio, pre svega, jasan putokaz odakle početi, šta raditi i u kom pravcu se kretati. Zbog ograničenog prostora autori će se u svom izlaganju zadržati samo na ključnim stavovima, konstatacijama i sugestijama.

## 2. O INFORMACIONOJ BEZBEDNOSTI

Termin *informaciona bezbednost* podrazumeva stanje u kojem je obezbeđen ***integritet*** hardvera, procesa i podataka, njihova ***raspoloživost*** i ***poverljivost*** podataka i informacija.

***Integritet*** u razmatranom kontekstu podrazumeva tačnost i kompletnost podataka i informacija koji se nalaze na sistemu i samog sistema u njegovoj celosti, uključujući i procese koji se na njemu odvijaju.

Da bi se smatrali ***raspoloživim*** podaci, informacije i sistem moraju biti na svom mestu, dostupni i upotrebljivi za obaljanje funkcija koje si im namenjene. U tom kontekstu termin *raspoloživost* povezan je i sa *kontinuitetom* usluga.

***Poverljivost*** se koristi u kontekstu osetljivosti na otkrivanje (obelodanjivanje) podataka i informacija.[4]

## 3. POLITIKA INFORMACIONE BEZBEDNOSTI

Uspešna realizacija namere da se ovlada obimnim i složenim problemom kakav je informaciona bezbednost pretpostavlja postojanje polazne osnove koja će to omogućiti, a takvu osnovu predstavlja ***bezbednosna politika***. Dakle, bezbednosna politika je neophodan temelj na kojem se može razviti jedan efikasan i sveobuhvatan bezbednosni program.

U poslovnom svetu, bezbednosna politika je definicija onoga šta znači bezbednost za organizaciju (preduzeće, ustanovu, instituciju), za sistem ili za neki drugi entitet. U grubom, za organizaciju, ona označava ograničenja na ponašanje njenih članova, kao i ograničenja nametnuta od strane protivnika, a realizovana mehanizmima kao što su kamere, vrata, brave, ključevi, zidovi i dr. Za sisteme, bezbednosna politika označava ograničenja na funkcije i na protok između njih, ograničenja na pristup spoljnih sistema i protivnika, uključujući i programe, i pristup podacima od strane ljudi.

Politika informacione bezbednosti u osnovi definiše odnos organizacije prema informacionim dobrima i u tom kontekstu njena primarna svrha jeste da informiše rukovodioce, tehnička lica i korisnike o bitnim zahtevima za zaštitu informacione imovine, uključujući ljude, hardverske i softverske resurse i podatke. Dakle, politika informacione bezbednosti pribavlja okvir za najbolju praksu koju mogu razumeti i ispratiti svi zaposleni, čime presudno pomaže da se obezbedi minimiziran rizik i da se na bilo koji bezbednosni incident efikasno odgovori. [5]

---

[4] Developing a Security Policy, Sun Microsystems, Inc, 2001, http://www.sun.com/blueprints/1201/secpolicy.pdf; HMG Security Policy Framework, v.3.0 Oct 09, http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf; Information Security: How To Write An Information Security Policy, http://www.berr.gov.uk/files/file49963.pdf; FFIEC IT Examination Handbook, Information Security Booklet, July 2006, http://www.ffiec.gov/ffiecinfobase/booklets/information_ security/information_security.pdf

[5] Danchev D., *Building and Implementing a Successful Information Security Policy*, http://www.windowsecurity.com/pages/security-policy.pdf; Developing a Security Policy, op. cit; Information Security: How To Write An Information Security Policy, op. cit; Security policy, From Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Security_policy

Bezbednosna politika bi trebalo da udovolji mnogim potrebama. Ona bi trebalo da:

- zaštiti ljude i informacije;
- propiše pravila za očekivano ponašanje korisnika, tehničkog osoblja, menadžmenta i bezbednosnog osoblja;
- autorizuje bezbednosni personal da nadgleda, proverava i istražuje;
- definiše i odobri konsekvence narušavanja bezbednosti;
- pomogne u minimiziranju rizika.

Razrada realizacije ovako ocrtanih ciljeva bezbednosne politike sadržinski bi morala biti prikladna poslovnom, pravnom, regulatornom i tehničkom ambijentu u kojem organizacioni entitet deluje. U tom smislu mora da se uspostavi konzistentan pojam šta jeste a šta nije dozvoljeno u odnosu na pristup do i postupanje sa podacima i resursima obrade. S tim u vezi proces razvoja ove politike omogućiće i razvijanje operativnih postupaka (procedura), uspostavljanje pravila kontrole pristupa i različite aplikacijske, sistemske, mrežne i fizičke kontrole i parametre.

Kroz politiku informacione bezbednosti organizacioni entitet definiše stav organizacije prema informacijama i obznanjuje da su informacije njeno dobro, odnosno imovina koja treba da bude zaštićena od neovlašćenog pristupa, modifikacije, otkrivanje i destrukcije.

Politika, koja je u suštini izraz namera predstavljenih dokumentima trebalo bi da reguliše kako jedan organizacioni entitet koristi i štiti svoja informaciona dobra. Brojnost i raznovrsnost bezbednosnih tema, veličina i raznovrsnost auditorijuma, složenost informacionog ambijenta, kao i načini korišćenja politike informacione bezbednosti, znače da veličina, sadržina i oblik politike informacione bezbednosti može da varira od entiteta do entiteta, odnosno od jednog do drugog informacionog ambijenta, a njena arhitektura da se prostire od krajnje jednostavne do vrlo složene. Upravo iz tih razloga za različite ambijente moguća je različita razuđenost politike informacione bezbednosti.

Elementarni pristup podrazumeva da je politika informacione bezbednosti urađena na top-nivou u formi *jedinstvenog* dokumenta i da pokriva kompletnu organizacionu strukturu entiteta na koji se odnosi. Ovakav pristup se preporučuje samo za manje složene entitete. Međutim, za velike entitete, razvijanje jedinstvenog dokumenta politike koji se odnosi na sve kategorije korisnika unutar organizacije i označava sva bitna pitanja informacione bezbednosti može se pokazati nemogućim ili nepoželjno složenim.

Sledstveno tome, u kompleksnim organizacionim sistemima efikasniji koncept je da se ukupna politika bezbednosti razloži na jednu osnovnu politiku i na veći broj pod-politika. Osnovna politika, koja se razvija i usvaja na top nivou i koja se zbog toga naziva *upravljačka politika*, predstavlja "kapu" za sve pod-politike, objedinjavajući ih u jedinstvenu funkcionalnu celinu. Pod-politike, koje se nazivaju *tehničke politike,* obuhvataju parcijalne delove informacione bezbednosti, a usmerene su na specifične auditorijume – grupacije zaposlenih, čime se olakšava alociranje bezbednosnih mehanizama za sprovođenje konkretne pod-politike. [6]

Dakle, u kreiranju bezbednosne politike koriste se dva tipa politike:

- Upravljačka politika;
- Tehnička politika.

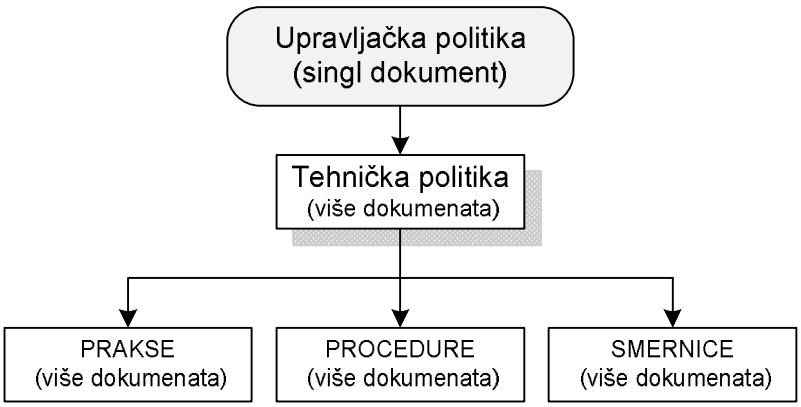
Oba ova tipa politike bila bi podržana proceduralnim dokumentima: *dokumentovanom praksom, procedurama* i *smernicama,* koji pokrivaju određene bezbednosne teme i odgovaraju različitim kategorijama korisnika.

Dokumenta ovih politika formiraju hijerarhijsku strukturu bezbednosne politike (šema 1) koja odražava hijerarhijsku strukturu uloga i odgovornosti zaposlenih u velikom organizacionom entitetu.

---

[6] Developing a Security Policy, op. cit; HMG Security Policy Framework, op. cit. Information Security: How To Write An Information Security Policy, op. cit; FFIEC IT Examination Handbook, Information Security Booklet, op. cit; Information Technology Security Policy, November 17, 2008, http://www.iowadnr.gov/legal/files/it_security_policy.pdf; U.S Department of Energy, *IT security architecture*, http://cio.energy.gov/DOE_Security_Architecture.pdf

Za one kompanije koje tek počinju razvijati politiku moguće je koristiti osnovni okvir koji podrazumeva da se inicijalno razvije upravljačka politika i manji broj tehničkih politika, a zatim da se uvećava broj politika i pratećih dokumenata, kao i složenost politika kako se bude napredovalo u razvoju.




*Šema 1 – Hijerarhijska struktura dokumenata bezbednosne politike*

Ono što bi svakako trebalo imati u vidu jeste činjenica da ne postoji jedinstvena metoda za razvoj bezbednosne politike(a). Mnogi faktori moraju biti uzeti u obzir, uključujući brojnost i raznovrsnost zaposlenih, vrste poslova i veličinu organizacionog entiteta, nivo ostvarene automatizacije i dr.[7]

## 4. AUDITORIJUM

Auditorijum kojem je namenjena politika informacione bezbednosti u globalu čine svi zaposleni. Međutim, jasno je da njihova interesovanja i potrebe za poznavanjem delova i cele politike nisu identična. Iz tih razloga ceo auditorijum bi se mogao razvrstati (podeliti) na tri pod-grupe (interesne grupe, kategorije zaposlenih). Glavne grupe su: [8]

- menadžment – svih nivoa;
- tehničko osoblje;
- krajnji korisnici.

Svi korisnici spadaju bar u jednu kategoriju (*end-user*), a neki će biti u dve ili čak sve tri grupe.

## 5. UPRAVLJAČKA POLITIKA

Upravljačka politika trebalo bi da pokrije sve aspekte bezbednosti na višem, širem nivou od detalja koji će biti sadržani u tehničkim politikama. Sve glavne, bazne bezbednosne teme moraju biti pokrivene. Ovo je mesto da se izlože osnovni stavovi organizacionog entiteta o ovim pitanjima.

Upravljačka politika trebalo bi da pokriva koncepte informacione bezbednosti na visokom nivou, definisanje tih koncepata, objašnjenja zašto su važni, i detaljno kakav je odnos organizacionog entiteta prema njima. Upravljačku politiku će čitati menadžeri, tehnička lica i krajnji korisnici, jer sve ove grupe će koristiti politiku da bi razumeli ukupnu filozofiju bezbednosne politike entiteta. [9]

Upravljačka politika je podržana tehničkim politikama koje pokrivaju teme u više detalja. U smislu nivoa detalja, upravljačka politika bi trebalo da označi ***"šta treba"*** u terminima bezbednosne politike.

---

[7] FFIEC IT Examination Handbook, Information Security Booklet, op. cit; Information Technology Security Policy, op. cit.

[8] Danchev D., op. cit; Developing a Security Policy, op. cit.

[9] FFIEC IT Examination Handbook, Information Security Booklet, op. cit; U.S Department of Energy, *IT security architecture*, op. cit.

## 6. TEHNIČKA POLITIKA

Tehnička politika trebalo bi da bude korišćena od strane tehničkih lica dok obavljaju svoje bezbednosne odgovornosti za sisteme sa kojima rade. One će biti mnogo detaljnije od upravljačke politike i odnosiće se na sistem ili specifičan problem.

Tehničke politike će prekriti mnogo od istih tema koje pokriva i upravljačka politika, kao što su neke dodatne teme specificirane u sveukupnoj tehničkoj temi. One su priručnik za to kako bi jedan operativni sistem ili mrežni uređaj trebalo da bude zaštićen. One opisuju šta se mora uraditi, ali ***ne i kako*** da se to uradi – to je rezervisano za proceduralna dokumenta koji su sledeći nivo detalja od upravljačke i tehničke politike.[10]

U smislu nivoa detalja, Tehnička politika bi trebalo da označi ***"šta"*** (u više detalja), ***"ko", "kada"*** i ***"gde"*** u odnosu na bezbednosnu politiku.

## 7. PROCEDURALNA DOKUMENTA

Proceduralna dokumenta daju ***korak-po-korak*** uputstva ***"kako"*** da se sprovode nalozi bezbednosne politike i trebalo bi da budu pisani na sledećem nivou granularnosti, opisujući kako nešto treba biti urađeno. Oni obezbeđuju sistematske praktične informacije o tome kako implementirati zahteve navedene u dokumentima politike. To može biti napisano od strane različitih grupa u celoj firmi i može, ali ne mora da se poziva na relevantnu politiku, zavisno od zahteva.

Proceduralna dokumenta mogu biti pisana kada je potrebno da se podrže ostali tipovi dokumenata politike, kako bi čitaocima kroz proširena objašnjenja pomogli u razumevanju šta je značajno u politici. Neće sve politike zahtevati podržavajuća dokumenta.

Razvoj proceduralnih dokumenata ne mora bezuslovno biti realizovan od razvojnog tima koji razvija upravljačku i tehničke politike. Može biti efikasnije da individualne poslovne jedinice razvijaju vlastita prateća dokumenta po potrebi, zbog činjenice da tehničko osoblje u poslovnim jedinicama verovatno ima najcelovitija i *up-to-date* tehnička znanja o problematici koju radno pokrivaju i da će, zahvaljujući tome, moći lakše i kvalitetnije napisati njima potrebna dokumenta. Politike im daje okvir da slede ("šta", "ko", "kada" i "gde", u smislu bezbednosne politike) i oni jednostavno treba da prate ove putokaze i skiciraju "kako ". [11]

## 8. ZAKLJUČAK

Kao što je istaknuto na početku, u radu su dati samo grubi orijentiri u razrešavanju izuzetno obimnog i veoma složenog problema informacione bezbednosti. Međutim, i pored svoje opštosti u pristupu temi nije teško uočiti da izložen materija, inače, prvenstveno bazirana na preporukama međunarodnog standarda ISO/IEC 27001, omogućava racionalan *top-down* pristup u kojem se arhitektura sistema bezbednosti, po principu lego kockica, gradi od hijerarhijski (po vertikali) i funkcionalno (po horizontali) povezanih, ali sadržinski u velikoj meri nezavisnih komponenata.

Ova činjenica omogućava da se na sve promene u ambijentu, koje mogu u manjoj ili većoj meri negativno uticati na postojeći sistem zaštite, reaguje veoma brzo, bez velikih zahvata, tako što će se u postojeću bezbednosnu arhitekturu, na pripadajućem hijerarhijskom nivou, i na funkcionalno lociranoj poziciji, ugraditi nove komponente, sadržinski korigovati postojeće komponente ili jednostavno odstraniti komponente koje više nisu u funkciji politike informacione bezbednosti.

---

[10] Information Security: How To Write An Information Security Policy, op. cit; FFIEC IT Examination Handbook, Information Security Booklet, op. cit; Information Technology Security Policy, op. cit.

[11] Information Security: How To Write An Information Security Policy, op. cit; FFIEC IT Examination Handbook, Information Security Booklet, op. cit; NCSA Security Policies and Procedures, Updated June 26, 2009, http://www.ncsa.illinois.edu/UserInfo/Security/policy/NCSA_SPP.pdf.

Ovakva elastičnost predstavlja garanciju da će bezbednosni sistem moći uspešno, blagovremeno i u celosti da odgovori na sve potencijalne izazove koji mogu ugroziti bezbednost informacionih dobara.

## LITERATURA


[1] Danchev D., *Building and Implementing a Successful Information Security Policy*, http://www.windowsecurity.com/pages/security-policy.pdf
[2] Developing a Security Policy, Sun Microsystems, Inc, 2001, http://www.sun.com/blueprints/1201/secpolicy.pdf
[3] FFIEC IT Examination Handbook, Information Security Booklet, July 2006, http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf
[4] HMG Security Policy Framework, v.3.0 Oct 09, http://www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf
[5] Information Security: How To Write An Information Security Policy, http://www.berr.gov.uk/files/file49963.pdf
[6] Information Technology Security Policy, November 17, 2008, http://www.iowadnr.gov/legal/files/it_security_policy.pdf
[7] IT Security Policy, http://www.ruskwig.com/docs/security_policy.pdf
[8] IT Security Policy, Castlereagh Borough Council, August 2002, http://www.castlereagh.gov.uk/Documents/hr/IT%20Security%20Policy.pdf
[9] Milanović J. Z, Organizacija zaštite računarskih sistema, Magistarski rad, Mašinski fakultet, Beograd 2006.
[10] NCSA Security Policies and Procedures, Updated June 26, 2009, http://www.ncsa.illinois.edu/UserInfo/Security/policy/NCSA_SPP.pdf
[11] Security policy, From Wikipedia, http://en.wikipedia.org/wiki/Security_policy
[12] U.S Department of Energy, IT security architecture, http://cio.energy.gov/DOE_Security_Architecture.pdf