KLASIFIKACIJA GREŠAKA U INFORMACIONIM SISTEMIMA

CLASSIFICATION OF ERRORS IN INFORMATION SYSTEMS

Katarina Predojević[1)], Dušan Drenovac[2)]

Rezime: *Brojne ekonomske transakcije, donošenje odluka i kreiranje poslovne politike većine organizacija počiva na pravilnoj upotrebi i upravljanju informacionim sistemima. S obzirom na njihovu važnost u svakodnevnom poslovanju organizacija razvijani su različiti koncepti za poboljšanje njihovih performansi, održavanje i otklanjanje potencijonalnih uzroka otkaza. Neki od njih su: adaptilnost, fleksibilnost, kapacitet sistema za oporavak, stabilnost. U ovom radu predstavljena je klasifikacija grešaka u informacionim sistemima kao i načini na koji se treba nositi sa njima. Činjenica da postoji način za ranu identifikaciju grešaka i otkaza, može se znatno unaprediti poslovanje i otkloniti rizici po organizaciju.*
Ključne reči: *klasifikacija grešaka,otkazi,informacioni sistemi*

Abstract: *Numerous economic transactions, making decision and creating business policy of most organizations is based on proper use and management of information systems. Their importance in the daily operations of organizations has developed various concept to improve their perfomance,maintenance and removal of potential causes of failure. Some of them are: adaptability,flexibility,system capacity for recovery,stability. In this paper we propose a classification of errors in information systems and the way they should deal with them. The fact that there is a way for the early identification of faults and failures,we can significantly improve operations and eliminate risks to the organization.*
Key words: *classification errors, failure, information systems*

1. UVOD

Menadžment informacionih sistema mora stalno da iznalazi odgovore u sve turbulentnijem poslovnom okruženju. Jedan od odgovora je razvoj sopstvene strategije u oblasti [1] :

- Poslovanja,
- Automatizacije,
- Integracije,
- Informacija i
- Iskorišćenja resursa.

U svim promenama na ulazu u poslovni sistem evidentan je uticaj elemenata informacionih sistema,a posebno u oblasti tehnologije, metoda, standard i informacionih sistema u uzem smislu. Pritisak konkurencije može se, takođe, ogledati i u primeni savremenih informacionih rešenja.
Informacioni sistemi u užem smislu obuhvataju:

- hardver,
- softver,
- procese i podatke,
- baze podataka,
- metode i tehnike(znanja zaposlenih),
- procedure i
- mreže.

Informacioni sistem obuhvata ljude, hardver, softver, podatke i mrežne resurse za ostvarivanje ulaza,obrade,izlaza,memorisanja i upravljanja performansama sistema čime se dobijaju informacioni proizvodi. S obzirom na raznolikost informacionih sistema ,nivoa organizacije koji podržavaju,osnovne oblasti poslovanja na koje se odnose,vrstu podrške i arhitekture,primenjuju se različite podele IS.
Prvi IS su bili TPS (Transaction Processing System)sistemi koji su obuhvatali prikupljanje, skladištenje, obradu i distribuciju informacija.
Softver predstavlja skup instrukcija ili programa na osnovu kojih hardver izvršava određene zadatke(obrada podataka,ulaz,izlaz,itd). Dok je hardver predviđen za opste namene, softver se

1) Katarina Predojević, Mašinski fakultet Kragujevac, mail: pandica1812@gmail.com
2) Dušan Drenovac, Mašinski fakultet Kragujevac, mail: drenovac88@gmail.com

može odnositi na specifične namene. Softver se deli u dve velike grupe:

- sistenski softver i
- aplikativni softver.

2. PREGLED LITERATURE

U vremenu kada informacione i komunikacione tehnologije dobijaju sve veći značaj za poslovanje, proučavanje izvora ranjivosti i otkrivanje grešaka postaju veoma značajne oblasti u teoriji i praksi. U ovoj oblasti je zbog toga napisano dosta radova. Autori Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum i Michael
Frantzene sproveli su analizu ranjivosti internet Firewall-a. [2] Analiza je zasnovana na ispitivanju zaštite poverljive mreže od neproverenih mreža, filtriranjem saobraćaja u skladu sa određenom politikom za bezbednost. Različiti setovi firewalls-a se koriste danas. Pošto je nemoguće ispitati i testirati svaki farewalls za sve moguće potencijalne probleme, taksonomiji je potrebno da razume ranjivosti firewalls-a u kontekstu firewall operacije. Ovaj rad opisuje roman metodologije za analizu ranjivosti internet firewalls. Ranjivost firewalls-a je definisana kao greška napravljena tokom firewalls projekcije, implementacije, ili konfiguracije koje mogu biti iskorišćene za napad na pouzdanu mrežu koju firewall treba da štiti. Mi smo ispitivali unutrašnjost firewall-a i unakrsne reference svakog firewall-a sa uzrocima i posledicama slabosti u toj operaciji, analizirajući dvadeset prijavljenih problema sa mogućim firewalls. Rezultat naše analize je skup matrica koje ilustruju distribuciju uzroka ugroženosti firewall-a i posledice preko firewall operacije. Ove matrice su korisne u izbegavanju i otkrivanju nepredviđenih problema tokom obe implementacije firewall-a i firewall testiranja. Dva studija slučaja Firewall-a 1 i Raptor ilustuju našu metodologiju.
Nan Feng i Minqiang Li navode da postoji mnogo nesigurnosti tokom procene rizika u procesu bezbednosti informacionih sistema(ISS), upravljanje neizvesnosti je od velikog značaja za efikasnost procene rizika[3]. U ovom radu, predlažemo ISS-modele procene rizikana osnovu poboljšanih dokaza teorije. Prvo, mi smo uspostavili indeks sistema ISS I kvantifikovali težinu indeksa, na čijoj osnovi je izgrađen dokazni dijagram. Kako bi se izborili sa neizvesnim dokazima pronađenim u ISS proceni rizika, ovaj model pruža novi način da se definiše osnovni zadatak u fuzzy merenju. Štaviše, model takođe pruža I metod testiranjadokazne doslednosti, što može neizvesnost koja proizilazi iz sukoba dokaza. Konačno, model je dodatno prikazan i proveren preko studije slučaja, u kojem je analiza zadužena za proveru pouzdanosti predloženog modela.

3. KLASIFIKACIJA OTKAZA U INFORMACIONIM SISTEMIMA

U informacionim sistemima se često dešavaju otkazi koji mogu imati dalekosežne posledice. Jedan od najčešćih otkaza je otkaz servisa. On je definisan kao pojava koja se dešava kada se isporučeni servis,razlikuje od ispravnog, odnosno tačnog servisa. Razni načini na koje se razlike manifestuju su sistemski načini suvišnih otkaza. Svaki od tih načina, može imati više od jednog nivoa ozbiljnosti.

SERVISNE GREŠKE

Servisne greške su definisane sa poštovanjem funkcija sistema, ali bez poštovanja opisa funkcije, navedenog u funkcionalnoj specifikaciji: saglasnost servisa isporuke može biti neprihvatljiva za korisnika, pa tako otkrivanje specifikacione greške, otkriva činjenicu da specifikacija ne opisuje funkciju sistema na adekvatan nacin. Takve specifikacione greške mogu biti ili propusti ili greške komisije (pogrešne interpretacije, neopravdane pretpostavke, nedoslednosti, tipografske greške) u takvim okolnostima, činjenica da je događaj nepoželjan može biti prepoznata, tek nakon sto se ona dogodi npr, preko njenih posledica. Otkaz može biti subjektivan i osporavan, on svakako može da zahteva sud o svojoj korektnosti da bi njegovo definisanje i karakterizacija uopšte bili mogući. Otkazi servisa i njihovi načini rada mogu se okarakterisati u svojoj nekorektnosti, i to preko četiri tačke gledišta [4] :
1-domen otkaza;
2-mogućnost otkrivanja;
3-doslednost grešaka i
4-posledice otkaza po okolinu.
Domen otkaza, kao tačka gledišta, dovodi nas do razlika:

- Sadržajni otkazi - Sadržaj informacija isporučen interfejsu servisa odstupa od sprovođenja funkcije sistema.
- Vremenski otkazi - vreme pristizanja ili trajanje informacija koja je isporučena interfejsu servisa odstupa od sprovođenja funkcije sistema.

Ove funkcije mogu biti specijalizirane:

1) sadržaj može biti numerički ili nenumerički podešen i

2) vremenski otkaz može biti preuranjen ili okasneo.

Otkazi,u slučaju kada su obe informacije i vreme netačni,spadaju u dve klase:

- Greška zastoja - ili jednostavno zastoj kada je sisitem otvoren (eksterni-spoljašnji status je konstantan), npr.aktivnost sistema, ako je uopšte ima nije više primetna korisniku.
  Poseban slučaj zastoja,**ćutanje**,je slučaj u kome nema aktivnosti ni isporuke servisa,u interfejsu. To doslovno znači da u sistemu distribucije nema poslatih poruka.

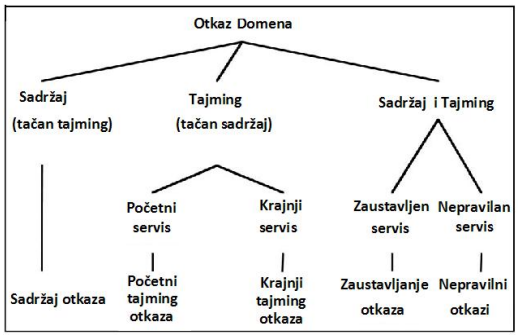
- Nerealni otkazi - ili slučaj kada je servis isporučen,ali je nestvaran što se u žargonu informacionih sistema izražava kao zamor.

Tačka gledišta, omogućava otkrivanje i korak usmeravnja i signalizaciju otkaza servisa prema korisniku. Signalizacija servisnog interfejsa potiče od otkrivanja mehanizama u sistem u koji proverava tačnost isporučenih servisa. Kada su gubici primećeni i signalizirani od strane signala upozorenja, tada se dešava signalizirani otkaz. U svakom drugom slučaju to su nesignalizirani otkazi. Sami mehanizmi otkrivanja otkaza odnosno grešaka imaju dva načina rada:
1)Signaliziranje gubitka funkcije, je proces koji se manifestuje kao greška koja se u stvarnosti nije dogodila, što pretstavlja lažni signal;
2)Nesignaliziranje gubitka funkcije što je u stvari nesignalizirani otkaz.
U trenutku kada se događa otkaz servisa u smanjenom obimu, sistem signalizira degradirani način servisa korisniku. Degradirani načini mogu imati obim od manje redukcije do hitnog servisa i sigurnosnog isključivanja.

Doslednost grešaka vodi nas do razlika, kada sistem ima dva ili više korisnika:

- Dosledne greške-nekorektan servis svi korisnici doživljavaju isto.
- Nedosledne greške-neki ili svi korisnici servisa doživljavaju sistem drugačije. Može se desiti da korisnici mogu u stvari da ga dožive i kao korektan servis.

Najčešće se nazivaju nedoslednim greškama po ,"Byzantine" otkazima. Ocenjivanje posledica otkaza na sistemnom okruženju omogućava da ozbilljne greške budu definisane. Modovi grešaka su poređani po ozbiljnim nivoima koji su obično u vezi sa maksimalno prihvatljivom verovatnoćom događaja. Broj, označavanje i definisanje ozbiljnih nivoa , kao i prihvatljiva verovatnoća događaja su u vezi sa primenom, i uključuju pouzdanost i sigurnost atributa za razmotrenu primenu.



Slika 1- Sumnja na otkaze servisa i njihove načine rada poštujući tačku gledišta domena otkaza

Primeri za određivanje vrsta ozbiljnih grešaka su:

1. za raspoloživost-prekid trajanja;
2. za sigurnost- mogućnost da ljudski životi budu ugroženi;
3. za poverljivost-tip informacije koji može biti neopravdano iskazan i
4. za integritet-merenje nepravilnosti podataka i sposobnost da se oporavi od ovih nepravilnosti.

Uopšteno govoreći ,dva limitirajuća nivoa mogu biti definisana prema relaciji između koristi sve vrednosti koje nisu ograničene ekonomskim pitanjima a koje su ujedno obezbeđene od strane servisa isporučenog u nedostatku otkaza, i posledica otkaza.

- Beznčajni otkazi - oni se mogu definisati kao štetne posledice sa istovetnim troškovima nasuprot koristi obezbeđenoj od strane servisa isporuke.
- Katastrofalni otkazi - ova vrsta otkaza podrazumeva da je magnituda posledica po troškove jednaka ili veća na mesečnom nivou od koristi obezbeđene od strane servisa isporuke.

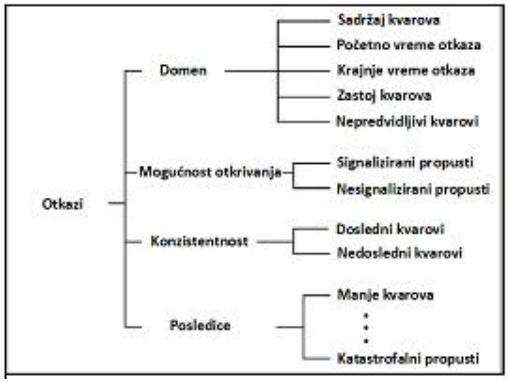
Sistemi koji su dizajnirani i sprovedeni tako da imaju otkaze samo u specifičnim načinima otkaza, opisanu su u zavisnosti i u sigurnosnoj

speicifikaciji i prihvatljivi su samo u opsegu u kom je otkaz kontrolisan od strane sistema. Haotične vrednosti u isporučenom sistemu nasuprot zamoru su konstantno suprotstavljene nedoslednim otkazima. Sistem u kome su otkazi u prihvatljivom obliku odnosno svi beznačajniotkazi su sigurni po sistem. Isporuka nekorektnog servisa traje do restartovanja servisa i njegovog obnavljanja. Prekid trajanja može značajno da varira u zavisnosti od aktivnosti povazanih sa obnavljanjem servisa nakon sto se dogodila greška:

1)automatsko ili obnavljanje u kom operator insistira restartovanje ili rebutovanje;

2)ispravno održavanje - ispravka razvojnih grešaka se obično izvodi u oflajn modu, nakon obnavljanja servisa, i nadograđene komponente dobijene od ispravke greške su onda predstavljene u prikladnom vremenskom intervalu sa ili bez prekidanja sistemskih operacija.

Preventivno prekidanje sistemskih opreacija radi nadogradnje ili prevencije je gašenje sistema takođe poznato i kao planirano prekidanje.



Slika 2 - Sumira načine otkaza servisa

RAZVOJNI OTKAZI

Razvojni otkazi mogu biti predstavljeni u sistemskom izražavanju i razvoju od strane njegove okoline posebno od strane ljudskih dizajnera, razvojnih alatki i produkcionih postrojenja [4]. Takvi razvojni otkazi mogu doprineti delimičnom ili kopletnom razvojnom otkazu ili mogu ostati neindetifikovani do faze korišćenja. Kompletni razvojni neuspeh prouzrokuje gašenje razvojnog procesa pre nego što je prihvaćen i postavljen u servis.

Postoje dva aspekta razvojnih otkaza:

1)budžetski otkaz - sredstva ustanovljena na početku razvoja su iscrpljena pre nego što je sistem prošao testiranje prihvatljivosti.

2)otkaz rasporeda - projektovani raspored isporuke zapada u tačku u budućnosti u kojoj će sistem biti tehnološki zastareo,neupotrebljiv ,ili funkcionalno neadekvatan za potrebe korisnika.

Osnovni razlozi razvojnih grešaka su: nekompletna ili manjkava specifikacija prevelik broj izmena specifikacije inicirane od strane korisnika; neadekvatan dizajn sa poštovanjem funkcionalnosti i ciljevi performansi; previše razvojnih grešaka neadekvatan pristup otklanjanju otkaza; i loša procena razvojnih troškova. Kompletan postupak se dovodi u vezu sa procenom složenosti sistema koji će biti razvijen. Postoje dve vrste delimičnih razvojnih otkaza, npr. otkazi manjih različitosti u odnosu na okončanje projekta. Budžetni ili rasporedni previdi se dešavaju kada je razvoj okončan ali su sredstva ili vreme potrebno za završetak prekoračili kompletan napor da se dođe do krajnog cilja. Druga forma parcijalnog razvojnog otkaza je smanjivanje: Razvijen sistem je isporučen kao manje funkcionalan,sa lošim performansama, ili je predviđeno da ima manju sigurnost nego što je zahtevano u originalnoj sitemskoj specifikaciji. Razvojni otkazi, povećčavanje ili smanjivanje imaju veoma negativan udar na korisničku zajednicu.

ZAVISNOST I SIGURNOSNI OTKAZI

Očekivano je da otkazi različitih vrsta utiču na sistem u toku trajanja njegove korisničke faze. Greške mogu prouzrokovati neprihvatljivo degradiranje performansi ili totalni otkaz isporuke posebnog servisa. Iz ovog razloga,zavisnost i sigurnosna specifikacija se slažu u ciljevima za svaki atribut: mogućnost, sigurnost, poverljivost integritet i održivost. Specifikacija tačno indentifikuje vrste otkaza koje su ocekivane i korisnickom okruženju u kom će sistem raditi. Specifikacija može takođe zahtevati sigurnost protiv određenih neželjenih ili opasnih stanja, inkluzija specifičnih otkaza i njihova prevencija ili tolerisanje otkaza može biti zahtevana od strane korisnika. Zavisnost ili sigurnosni otkazi se dešavaju kada sistem pretrpi servisne otkaze češće ili različitije nego sto je to prihvatljivo. Druga vrsta otkaza je neopravdan izvor veoma visokih zahteva za jedan ili više atributa koji povećavaju cenu razvoja i mogu voditi do povećanja troškova ili čak dootkaza razvoja. Na primer, početni AAS limit od tri sekunde godišnje je promenjen na pet minuta godišnje za novi ugovor 1994.

GREŠKE

Greške su definisane kao deo sistemskog stanja koje može voditi do otkaza - otkaz se dešava kada greška izazove do odstupanja sistema isporuke od korektnog servisa. Uzrok greške se naziva otkaz. Greška je uočena ako je njeno prisustvo povezano sa porukom greške ili signalom greške. Greške koje su prisutne ali nisu uočene su latentne greške. Pošto se sistem sastoji od seta interaktivnih komponenti totalno stanje je set komponenti stanja. Definicija implicira da otkaz prvobitno izaziva grešku u stanju jedne (ili više) komponenti, ali otkaz servisa se neće desiti dok spoljašnje stanje te komponente ne postane deo spoljašnjeg stanja sistema. Uglavnom greška postaje deo spoljasnjeg stanja komponente, otkaz servisa te komponente se dešava, ali greška ostaje unutrašnja stvar celokupnog sistema.
Da li će ili ne greška ustvari voditi do otkaza servisa zavisi od dva faktora:

1. struktura sistema a pogotovo prirode bilo kog viška koja postoji u njemu:
    - Zaštitni višak, predstavljen da obezbedi toleranciju otkaza, što prvashodno ima za zadatak da spreči grešku od stvaranja servisnog otkaza.
    - Nenamerni višak (u praksi je teško ako ne i nemoguće izgraditi sistem bez ikakve forme viška) koje može imati iste-neočekivane-rezultate kao namerni višak.
2. Ponašanje sistema: deo stanja koji sadrži grešku ne mora nikad da bude potreba za servis ili greška može biti eliminisan pre nego što dovede do otkaza.

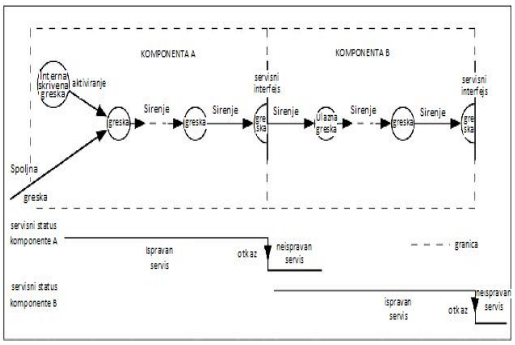
Prikladna klasifikacija grešaka je opisivanje njih samih u uslovima osnovnih servisnih otkaza koje oni sami izazivaju, koristeći terminologiju: sadržaj nasuprot vremenskih grešaka, lociranje nasuprot latentnim greškama, dosledno nasuprot nedoslednim greškama kada servis ide od dva ili više korisnika, beznačajno nasuprot katastrofalnim greškama. Na polju kontrolnih kodova grešaka, greške sadržaja su dalje klasifikovane prema obrascu štete: sam, dupli, trostruki, aritmetički, itd. Neki otkazi mogu simultano izazvati greške na više od jedne komponente. Takve greške se nazivaju višestruko povezane greške. Usamljene greške su greške koje utiču samo na jednu komponentu.

PATOLOGIJA OTKAZA : VEZA IZMEĐU PREKRŠAJA,GREŠAKA I OTKAZA

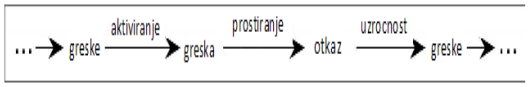
Stvaranje i manifestacioni mehanizmi prekršaja, grešaka i otkaza su ilustrovani na slici 3 i sumirani na sledeći način [4]:

1. Prekršaj je aktivan kada prozvodi grešku; inače je skriven. Aktivan prekršaj je ili unutrašnji prekršaj koji je predhodno bio skriven i koji je aktiviran procesom računanja ili uslovima okoline ili je spoljašnji prekršaj. Aktiviranje prekršaja i aplikacija ulaza u komponentu koja izaziva skriveni prekršaj i aktivira ga. Većina unutrašnjih prekršaja se odigrava između skrivenih i aktivnih stanja.
2. Veza greške u komponenti je izazvana procesom računanja: greška je uspešno transformisana u druge greške.

Otkaz servisa se dešava kada se greška propagira do servisnog interfejsa i izaziva isporučivanje servisa od strane sistema da odstupi od ispravnog servisa. Otkaz komponente izaziva permanentni prekršaj u sistemu u kom se nalazi komponenta. Otkaz servisa sistema izaziva permanentno spoljašnje kršenje za ostale sisteme koji primaju servis od datog sistema. Ovi mehanizmi omogućavaju ‘’lancu pretnji’’ da bude kompletiran, kao što je navedeno na slici 4. Strelice u ovom lancu izražavaju vezu između uzroka prekršaja, grešaka i otkaza. Oni bi trebali da budu generički interpretirani: po propagiranju, više grešaka može biti generisano pre nego što se otkaz desi. Važno je napomenuti da, od gore navedenih mehanizama, propagiranje i primeri ovog lanca mogu se desiti preko interakcije između komponenti ili sistema, sastavu komponenti u sistemu i kreaciji ili modifikaciji sisitema.



Slika 3 - Greška propagacije



Slika 4 - Osnovni lanac pouzdanosti i bezbednosne pretnje

4. ZAKLJUČAK

U ovom radu su predstavljene greške i otkazi u informacionim sistemima. Analizirana su pitanja koja se odnose na ranjivost internet Firewall-a i dati su zaključci o načinima suočavanja sa njima. Klasifikovani su otkazi u IS i kao jedan od nejčešćih otkaza se navodi otkaz servisa, on je definisan kao pojava koja se dešava kada se isporučeni servis,razlikuje od ispravnog servisa. Takođe su prikazani zavisnost otkaza i sigurnosni otkazi koji utiču na sistem u toku trajanja njegove korisničke faze.

5. LITERATURA

[1] Zora Arsovski, ‘’Informacioni sistemi’’, CIM Centar, Masinski Fakultet-Kragujevac 2002
[2] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum i Michael
Frantzen; ‘’Analysis of vulnerabilities in Internet firewalls’’, Center for Education and Research in Information Assurance and Security (CERIAS) Purdue University, 656 Oval Dr., West Lafayette, IN 47907–2039, USA
[3] Nan Feng, Minqiang Li, ‘’ An information systems security risk assessment model under uncertain environment ’’, Department of Information Management and Management Science, School of Management, Tianjin University, 92 Weijin Road, Nankai District, Tianjin 300072, PR China
[4] Algirdas Avižienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, Senior Member, IEEE, ‘’ Basic Concepts and Taxonomy of Dependable and Secure Computing’’, IEEE Transactions on dependable and secure Computing, vol. 1, no. 1, January-March 2004