RAZVOJ INFORMACIONIH SISTEMA- IZVORI RANJIVOSTI

DEVELOPMENT OF INFORMATION SYSTEMS - THE VULENARBILITY SOURCES

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

Rezime: *Poslovanje u 21. veku je postalo nezamislivo bez primene informacionih i komunikacionih tehnologija, pomoću kojih se vrše kompleksni inženjerski proračuni., vrše eknomske transkakcije, dizajniraju realni modeli, itd. S obzirom na to, poslednjih dvadesetak godina je porasla svest o značaju informacionih sistema za svakodnevni život kao i to koliko njihovi otkazi mogu ugroziti normalno funkcionisanje organizacije i pojedinca. U ovom radu će biti predstavljeni izvori ranjivosti informacionih sistema kao i to kako se nositi sa njima na odgovarajući način. Pored toga ukazano je na spregu upravljanja rizikom i upravljanja ključnim ranjivostima informacionog sistema*
Ključne reči: *razvoj, informacioni sistemi, izvori ranjivosti*

Abstract: *Business in the 21st century has become unthinkable without the use of IT and communication technologies, by which complex engineering calculations are made, also economical transactions, designing realistic models, and so on. During the last twenty years the awareness about the importance of IT systems for everyday life has increased and how their failures can threaten the normal functioning of organizations and individuals. This paper will present the sources of vulnerability of IT systems and how to deal with them appropriately. Furthermore, it points to the connection of risk management and management of key vulnerabilities of IT system.*

Key words: *Development, information systems, vulnerability sources*

1. UVOD

Informacioni sistem je skup komponenata organizovanih tako da omogućavaju registrovanje, prikupljanje,prenos, obradu, skladištenje, analaizu i distribuciju informacija za različite namene. Prema opštoj teoriji sistema, svaki sistem sadrži elemente na ulazu i izlazu , odnosno input i output i odgovarajuće upravljanje. Kod IS sistema upravljanje se ostvaruje preko povratne sprege koja utiče na ulaze, transformacije i izlaze. Uticaj okruženja se takođe manifestuje na sve elemente informacionog sistema [1].

Savremeno poslovanje karakterišu brze promene u okruženju i sve veći pritisak konkurencije. Promene okruženju odnose se na promene: uslova poslovanja, tehnologija, metoda, standarda i informacionih sistema.

Menadžment poslovnih sistema mora stalno da nalazi odgovore u sve turbulentnijem poslovnom okruženju. Jedan od odgovora je razvoj sopstvene strategije u oblasti: Poslovanja, automatizacije, integracija, informacija i iskorišćenja resursa. Osnovni razlog primene IS je u visokoj produktivnosti koju obezbeđuju savremena tehnološka rešenja.

Polazeći od osnovne definicije IS, koja upućuje na angažovanje različitih poslovnih i informacionih resursa, tako da je moguće na osnovu ove analogije definisati životni ciklus razvoja IS pomoću drugih organizacionih i tehničkih sistema, koji se sastaoji iz faza ili procesa planiranja, analize, projektovanja, primene i podrške IS.

2. PREGLED LITERATURE

Da bi IS bio uspešno projektovan i ekspolatisan, potrebno je još u fazi dizajna identifikovati sve potencijalne izvore ranjivosti. U cilju postizanja navedenog, veliki broju istraživača je doprineo rasvetljavanju ove oblasti.

Neki od tih istraživača kao što su Yeu-Pong La, Po-Lun Hsia, govore o tome kako poslednjih godina problem sigurnosti postoje sve važniji svim korisnicima računara. Međutim ranjivosti na računarima se tako često javljaju da menadžeri ne mogu da postignu da sve podatke pošalju glavnom

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

hostu za mrežu u kratkom vremenskom roku. Oni moraju da izvrše procenu rizika kako bi mogli da odrede priorite zakrpa ranjivosti. Pored toga oni ne moraju imati administratorska prava za sve hostove u mreži, već samo na određene mrežne uređaje. Da bi se ove ranjivosti zadržale na hosta, menadžeri sistema mogu da podese ACL skripte na mrežne uređaje. Rešenje poboljšava sigurnost mreže momentalno, jer su su preteći servisni portovi na hostu blokirani za pristup. Ovde možemo videti i način kako unaprediti sigurnost mreže, koji uključuje menadžment mreže, skeniranje ranjivosti, procene rizika, kontrolu pristupa, i obaveštavanje u slučaju ne željenih situacija. Posmatrajući topologiju mreže, procena rizika ukazuje da preteći servisni portovi trebaju biti blokirani pomoću ACL skripte. Ove procedure ne zahtevaju dodatna novčana sredstva za dodatnu opremu. Sa predloženom metodom, bezbednost mreže je poboljšana za skoro 40% sa samo 8% blokiranih pretećih porotova u ispitivanoj mreži klase B [2].

Kwo-Jean Farna, Shu-Kuo Lina, Andrew Ren-Wei Fung govore kako je sigurnost informacionih sistema kao lanac, a lanac je jak koliko je jaka njegova najslabija karika. Kako možemo postići100% Informacioni Sigurnosni Menadžment Sistema(ISMS) bezbednosti, moramo pažljivo popuniti sertifikat i akreditaciju informacione bezbednosti. U ovo radu je analizirana, proučavana procena znanja i veština potrebnih za revizije sertifikata za tri aspekta ISMS-a sredstva, pretnje i ranjivosti [3].

Sledeći veliki korak je bilo prepoznavanje bezbednosti kao kompozitnog atribuda, pouzdanosti, integriteta i dosupnosti i dodavanje klase ne zlonamernih grešaka, zajedno sa analizom problema ne adekvatne sistemske specifikacije [4], iako ovaj nalog pruža samo pregled klasifikacije pouzdanih pretnji.

Informacioni sistemi imaju sve veći strategijski značaj, a intenzivnijim korišćenjem Interneta, ekstranetova i internetova od strane organizacija povećava se i pitanje sigurnosti informacionih sistema. Frekventnost i veličina aktivnosti kompjuterskog kriminala je u rapidnom porastu pa je teško i skupo postavljati zaštitu protiv svih mogućih pretnji za IS sisteme, zbog toga je neophodno obavljati analize ekonomičnosti pre donošenja odluke o tome koliko i koje kontrole treba usvojiti.

3. SISTEMSKE FUNKCIJE, PONAŠANJE, STRUKTURA I SERVISI

Sistem u našem obračunskom sistemu je entitet koji interaktuje sa drugim entitetima ili sistemima, uključujući hardver, softver, ljudski faktor i fizički svet sa svojim prirodnim fenomenima [5]. Ovi drugi sistemi su okruženje datih sistema. Sistemska granica jeste uobičajena granica između sistema i okoline. Računanje i sistemi komunikacije su okarakterisani od strane fundamentalnih osobina: funkcionalnost, performanse, zavisnost, sigurnost i koštanje. Druge važne osobine sistema koje utiču na pouzdanost i sigurnost uključuju korisnost, upravljivost i adaptivnost. Funkcija takvih sistema je ono za šta je sistem namenjen da radi i opisuje se funkcionalnim specifikacijama u smislu funkcionalnosti i performansi. Ponašanje sistema je ono šta sistem radi kako bi implementirao svoje funkcije i opisuje se sekvencama stanja. Ukupno stanje datog sistema jeste set sledećih stanja: računanje, komunikacija, poznte informacije, unutrašnje veze i fizičko stanje.

Usluga koju pruža sistem (kao provajder) jeste njegovo ponašanje koje se prikazuje korisniku: korisnik je drugi sistem koji prima usluge od provajdera. Deo provajderovih sistemskih granica gde se odvija dostavljanje informacija jeste provajerov servisni interfejs. Deo provajderovog ukupnog stanja koje se dostavlja u servisnom interfejsu jeste njegovo spoljašnje stanje, ostatak predstavlja unutrašnje stanje. Dostavni servis je sekvenenca provajderovog spoljašnjeg stanja. Primećujemo da sistem može postepeno ili odjednom biti provajder i korisnik uporedo sa drugim sistemima, na primer da dostavlja i prima usluge od drugih servisa sa drugh sistema. Interfejs korisnika na kojem korisnik prima informacije jeste korisnički interfejs. Do sada smo koristili jedninu za funkcije i servise. Sistem u suštini implementira više od jedne funkcije i prosleđuje je na više od jednog servisa. Time se funkcije i servisi mogu videti kao sastavni deo funkcija i servisa. Zarad pojednostavljenja pojednostavićemo množinu funkcija i servisa kada je to neophodno da bi razlikovali više funkcijskih ili servisnih delova.

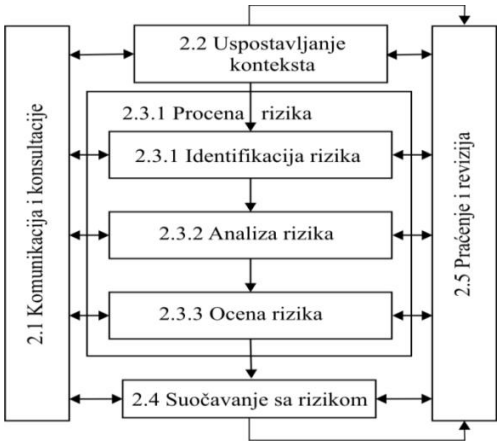
3.1Pretnje po zavistnost i sigurnost: otkazi, greške i prekršaji

Pravilne usluge se dostavljaju kada usluge mogu da se implementiraju u sistemske funkcije[5]. Otkaz sistema, koji se često naziva i pad, jeste događaj koji se dešava kada se dostavljena usluga razlikuje od pravilne usluge. Pad usluga se događa ili zbog nekompatibilnosti sa funkcionalnim specifikacijama ili zbog toga što date specifikacije ne prikazuju adekvatno sistemske funkcije. Otkaz sistema jeste prelaz sa pravilnih usluga na nepravilne usluge. Vreme

primanja nepravilnih informacija se naziva odsutnost sistema. Prelaz sa nekorektnih servisa na pavilne naziva se restauracija sistema. Devijacija sa pravilnih servisa može imati različite forme koje se nazivaju modovi pada i rangiraju se po težini problema.. Pošto je servis sekvenca sistemskih spoljašnjih stajna, pad sistema znači da je bar jedno spoljašnje stanje sistema različito od pravilnog stanja. Razlika se naziva greška. Razlog greške se naziva prekršaj. Prekršaj može biti unutrašnji ili spoljašnji u okviru sistema. Prethodno prisustvo ranjivosti sistema je neophodno kako bi spoljašnj prekršaj napravio grešku i mogući pad sistema. U većini slučajeva prekršaj prvo napravi grešku u komponenti sistema koja je deo unutrašnjeg stanja sistema i spoljašnje stanje sistema nije isprva oštećeno. Iz ovog razloga definisanje greške je deo celog sistema koji može da dovede do pada celokupnog sistema. Važno je napomenuti da mnogi prekršaji ne dopru do spoljašnjeg dela sistema i dovedu do greške. Prekršaj je aktivan kada dovede do greške, u suprotnom je neaktivan. Kada funkcionalne specifikacije sistema uključuju set nekoliko funkcija, otkaz jedne ili više funkcija unutar servisa mogu da degradiraju funkcionalnost sistema koji će i dalje nuditi određene usluge korisniku. Specifikacije mogu identifikovati nekoliko takvih modova, na primer: usporen rad sistema,... U tom slučaju možemo reći da je sistem doživeo delimičan pad funkcionalnosti ili performansi.

3.2Suočavanje sa izvorima ranjivosti

Tok poslovnih informacija bi trebalo integrisati na način koji je u skladu sa propisima, standardizacijom i harmonizacijom.



Slika 1 – Proces upravljanja rizikom

Integracija mehanizama za izveštavanje u procesu upravljanja rizikom donosi višestruku korist i doprinosi usklađenosti poslovnih procesa i povećanju efikasnosti. Procesi upravljanja rizikom su opisani standardom ISO 31000.Organizacija u okviru lanca snabdevanja bi trebalo da uspostavi mehanizme interne komunikacije i izveštavanja. Oni treba da sadrže procedure za konsolidaciju rizika i informacije iz različitih izvora unutar organizacije. Oragnizacija bi takođe trebalo da razvije i sprovede plan komunikacije sa spoljnim stejkholderima [6].

3.4 Pouzdanost, Bezbednost, i njihovi Atributi

Originalna definicija pouzdanosti je mogućnost da se isporuci servis kome se opravdano može verovati. Ova definicija naglašava potrebu za opravdanim poverenjem. Alternativna definicija koja obezbeđuje kriterijum za odlučivanje ukoliko je servis pouzdan, pouzdanost sistema je mogućnost da se izbegnu neuspesi servisa koji su sve češći i sve ozbiljniji nego što je to prihvatljivo. Uobičajeno je reći da je pouzdanost sistema dovoljna za zavisnost tog sistema. Zavisnost sistema A na sistem B, dakle, predstavlja stepen zavisnosti sistema A koji utiče (ili će uticati) na sistem B. Koncept zavisnosti vodi do toga da od poverenja, koje može veoma zgodno definisati kao prihvatljiva zavisnost. Kao što je razvijena u poslednje tri decenije, pouzdanost je integrirajući koncept koji obuhvata sledeće attribute: Dostupnost- spremnost za ispravan servis., Pouzdanost-kontinuitet ispravnog servisa., Bezbednost- odsustvo katastrofalnih posledica na korisnika kao i na okolinu. Integritet-odustvo nepravilnih izmena sistema. Sposobnost održavanjaa- Sposobnots za modifikacije i popravke.

Kada se radi o bezbednosti, atribut od velike popularnosti je tajnost, odnosno odsutnost ne dozvoljenog otkrivanja informacija. Bezbednost sastavljena od atributa poverljivosti, integriteta i dostupnosti, zahtevajući postojanje 1) dostupnost samo za ovlaćenje radnje 2) poverljivost, 3) integritet sa “nepravilnim” značenjem “neovlašćenim”

3.5 Sredstva za postizanje pouzdanost i bezbednost

Tokom poslednjih pedeset godina mnoga sredstva su razvijena da dostignu različite atribute pouzdanosti, Ta sredstva možemo svrstati u četri glavne kategorije:

- Prevencija grešaka u cilju sprečavanja pojave grešaka,

- Tolerancija grešaka u cilju da se izbegne pad sistema u slučaju prisustva grešaka,
- Uklanjanje grešaka u cilju redukcije grešaka i ozbiljnosti grešaka,
- Prognoziranje grešaka znači procenu sadašnjih, predvđanje budućih učestalih, i mogućih posledica grešaka.

Prevencija grešaka i tolerancija grešaka imaju cilj da obezbede mogućnost dostavljanja servisa od poverenja, dok uklanjanje grešaka i predviđanje grešaka imaju za cilj da dobiju poverenje u tu sposobnost, zadovoljavajući funkcionalne, pouzdane i sigurnosne specifikacije na adekvatan način pa će i sistem najverovatnije prihvatiti tu sposobnost.

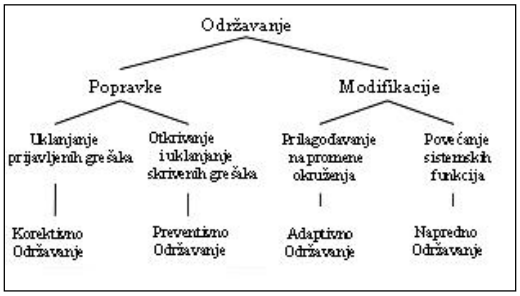
4. **Pretnje na pouzdanost bezbednost**

4.1 **Životni ciklus sistema:**

Pretnje po pouzdanost i sigurnost

Životni ciklus sistema: Faze i Okruženja
U ovom delu prestavićemo skup pretnji koje mogu da utiču na sistem tokom njegovog životnog ciklusa. Životni ciklus sistema sastoji se od dve faze: razvoja i upotrebe. Razvoj ovih faza uključuje sve faze prezentacije korisničkog koncepta do odluke da li je sistem prosao tačku prihvatljivosti i potrebne testove i spreman je da izvrši potrebne zadatke u korisničkom okruženju. Tokom faze razvoja, sistem je interaktivan sa razvojnim okruženjem i razvojne greške mogu predstavljene u sistem preko okruženja. Razvojno okruženje sistema sastoji se od sledećih elemenata:
1. Fizički svet sa prirodnim fenomenima
2. Ljudski razvojni timovi, sa mogućnosti postojanja sumnjivih ciljeva
3. Razvojni alati: software i hardware koji koriste programeri i koji im pomažu u razvojnom procesu.
4 . Postrojenja za proizvodnju i testiranje.
Upotrebna faza sistema počinje kada je sistem prihvaćen za upotrebu i kada počne da sluzi korisnicima. Upotreba se sastoji od naizmeničnih perioda usluge , prekida usluge i isključivanja usluge. Prekid usluge izazivaju kvarovi. To je period kada se netačan servis(usluga) dostavlja putem interfejsa servisa. Isključivanje servisa je nenameran zastoj servisa od strane ovlašćenog lica. Održavanje servisa se moze vršiti tokom sva 3 perioda upotrebne (korisničke) faze. Tokom korisničke faze sistem dolazi u kontakt sa korisničkom sredinom koja višestruko moze uticati na sistem greškama koje potiču iz nje. Korisnička sredina se sastoji od sledecih elemenata:
1. Fizički svet sa svojim prirodnim pojavama;
2. Administratori (uključujući i one koji održavaju system): tela (ljudi ili drugi sistemi)
koji imaju ovlašćenje da upravljaju, menjaju, popravljaju i koriste sistem; neki ljudi nisu
dovoljno kompetentni ili jednostavno imaju zle namere;
3. Korisnici: tela (ljudi ili drugi sistemi) koji dobijaju servis(uslugu) od sistema na njihovom korisničkom interfejsu;
4. Provajderi: tela(ljudi ili drugi sistemi) koji dostavljaju servis(uslugu) na korisnički interfejs.
5. Infrastruktura: tela koja pružaju specijalizovane usluge (servis) sistema, kao što su
izvor informacija (vreme, GPS, itd.), komunikacione veze, izvor napajanja, hladenje itd.
6. Uljezi: zlonamerna tela (ljudi ili drugi sistemi) koji pokušavaju da prekorače ovlašćenje
koje mozda imaju i izmene uslugu (servis) ili je zaustave, izmene funcionalnost ili performance
ili pristupe poverljivim informacijama. Primeri uljeza su hakeri, vandali, korumpirani radnici,
agenti neprijateljskih vlada ili organizacija i zlonameran software.

Održavanje je razvojni proces i prošla diskusija o razvoju se odnosi i na održavanje. Različite forme održavanja su: na slici 2.



Slika 2- Forme održavanja

Termin održavanje koji se ovde koristi ne uključuje samo popravke već i modifikacije sistema i dešava se tokom korisničke faze sistema.

5. ZAKLJUČAK

U radu su predstavljeni osnovi izvori ranjivosti IS, date su mere za suočavanje sa njima predlog održavanja IS. Važno je napomenuti da su popravka i tolerancija grešaka srodni koncepti; razlika između tolerancije grešaka i održavanja u ovom radu je da održavanje uključuje učešće spoljnog lica, npr. Majstora (servisera), opremu za testiranje, daljinsko učitavanje software-a. Pored toga, popravka je deo uklanjanja kvara (tokom korisničke faze) i prognoza kvara obično zahteva popravku. Popravka se može posmatrati kao aktivnost u okviru tolerancije greške većeg sistema koji uključuje popravku sistema i ljude i druge

sisteme koji vrše takve popravke. Iz navedenog se može zaklkjučiti da su informacioni sistemi izloženi dejstvu različitih uticaja i da je poznavanje svih pretnji po funkcionisanje IS neophodno za uspešano poslovanje bilo koje organizacije.

LITERATURA

[1] Zora Arsovski, ‘’Informacioni sistemi’’, CIM Centar, Mašinski Fakultet-Kragujevac 2002

[2] Yeu-Pong La, Po-Lun Hsia, „Using the vulnerability information of computer systems to improve the network security “ Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University,
Tauyuan 33509, Taiwan, ROC
Received 20 September 2006; received in revised form 7 March 2007; accepted 8 March 2007

[3] Kwo-Jean Farna, Shu-Kuo Lina, Andrew Ren-Wei Funga, „A study on information security management system evaluation—assets, threat and vulnerability“, Institute of Information Management, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan, ROC
b Internet Security Solutions International Co., Taiwan, ROC
cDCGS for Communications, Electronics and Information (J-6), Ministry of National Defense, Taiwan, ROC
Received 1 October 2003; received in revised form 11 March 2004; accepted 20 March 2004

[4] J.C. Laprie, “Dependability—Its Attributes, Impairments and Means,” Predictably Dependable Computing Systems, B. Randell et al., eds., pp. 3-24, 1995.

[5] Algirdas Avižienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL.1, NO.1, JANUARY-MARCH 2004.

[6] ISO/DIS 31000