

AGILNI MENADŽMENT E-RIZIKA KAO DEO INTEGRALNOG UPRAVLJANJA RIZICIMA

prof. dr Zoran Keković, Fakultet bezbednosti, Beograd,

zorankekovic@yahoo.com

Vesna Nikolić, Kriminalističko-policijska akademija, Beograd,

vesnan0812@yahoo.com

Apstrakt: *Integralni pristup upravljanju rizicima postavlja menadžment e-rizika u kontekst menadžmenta operacionalnih rizika, sa ciljem kreiranja adekvatnih akcionih odgovora na prepoznate bezbednosne rizike. Novi model agilne bezbednosti dodaje ovom opštem modelu proaktivnu i adaptibilnu komponentu, u skladu sa zahtevima da se bezbednosni menadžment integriše u poslovne funkcije organizacije. Agilni menadžment rizika ima za cilj očuvanje organizacijskih šticećenih vrednosti, razvojem bezbednosnih strategija i planova, na osnovu izgrađenih profila pretnji i identifikovanih slabosti u bezbednosnoj infrastrukturi. Softverska rešenja usklađena sa principima agilnog menadžmenta pružaju nam integrisanost administriranja, olakšanu kontrolu i monitoring, kao i brži akcioni odgovor sistema.*

Ključne reči: *integralno upravljanje rizicima, e-rizik, agilni menadžment*

AGILE E-RISK MANAGEMENT AS PART OF THE INTEGRAL RISK MANAGEMENT

Abstract: *The integral risk management approach has established e-risk management in context of the operational risk management, aiming to create proper action response on recognized security risks. New model named agile security adds proactive and adaptive component to that common model, regarding to requirements for integrating security management into bussines functions of the organization. Agile risk management aims to preserve organizational assets, by security strategies and plans development, based on established threat profiles and identified weaknesses in security infrastructure. The software solutions adjusted regarding to agile management principles provide us integrated administration, facilitated control and monitoring, and faster action response of the system.*

Keywords: *integral risk management, e-risk, agile management*

UVOD

Bezbednost, zajedno sa ostalim poslovnim funkcijama, mora postati sastavni deo paradigme savremenog upravljanja rizicima. Upravljanje rizicima je dinamički proces, a ne projekat ograničenog trajanja. Proces menadžmenta rizika obuhvata upravljanje neizvesnostima, pretnjama i slabostima, hazardima i rizicima, a u cilju postizanja najboljih mogućih ishoda za organizaciju. Važnost ovog procesa proizilazi iz same konstatacije da organizacija koja analizira rizike i kreira odgovor na njih, štiti sama sebe od loših konsekvenci rizika i pozicionira se tako da ima prednost među konkurencijom na tržištu. Jasno je dakle da se rizici ne smeju ignorisati, te da se proces upravljanje rizicima mora odvijati u svakoj organizaciji.

Rizik nije ni nešto dobro, ni nešto loše, već je jednostavno mera devijacije od očekivanog ishoda. Po standardu IEEE 1540:2001 rizik je »frekvencija pojavljivanja događaja, hazarda, pretnji ili situacija i njihovih neželjenih konsekvenci; potencijalni problem«. Posledice (konsekvence) rizika mogu biti dobre ili loše. Loše posledice crpe resurse, ometaju funkcije i procese, utiču na finansijsku stabilnost i sposobnost ispunjavanja misije organizacije. Dobre posledice proizvode bolje od očekivanih rezultata i (ili) neočekivane mogućnosti (prednosti) za organizaciju.

Na slici 1 prikazan je bezbednosni sistem na čijem se vrhu piramide nalazi sistem za podršku odlučivanju, kao sublimacija podsistema za analizu i izveštavanje, upravljanje rizikom, baza podataka, sistem obaveštavanja.

Integralni pristup upravljanju rizicima podrazumeva holistički koncept - proaktivnu tehniku menadžmenta koja identifikuje kritične procese i metodologiju za kontrolisanje i monitoring identifikovanih rizika.



Slika 1 Integrirani sistem bezbednosti

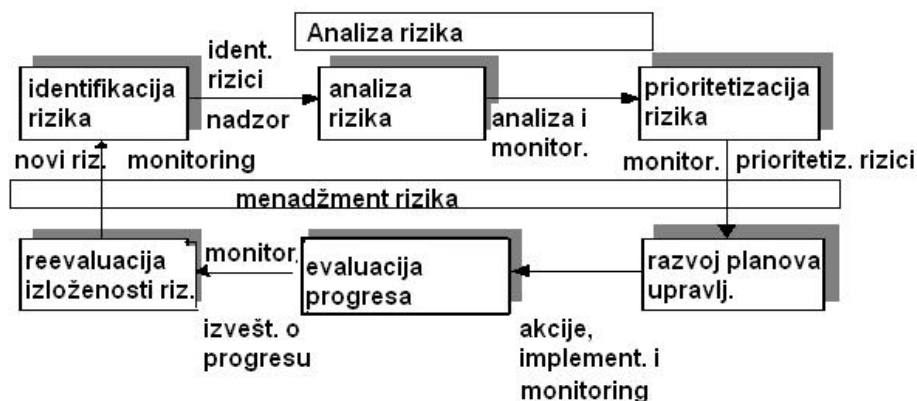
Model integralnog upravljanja rizicima

Menadžment rizika uključuje procese:

- Analiza rizika – identifikovanje rizika, analiza potencijalnih posledica, postavljanje prioriteta u akcijama
- Odgovor na rizik – razvoj i implementiranje akcionog plana koji tretira rizike.

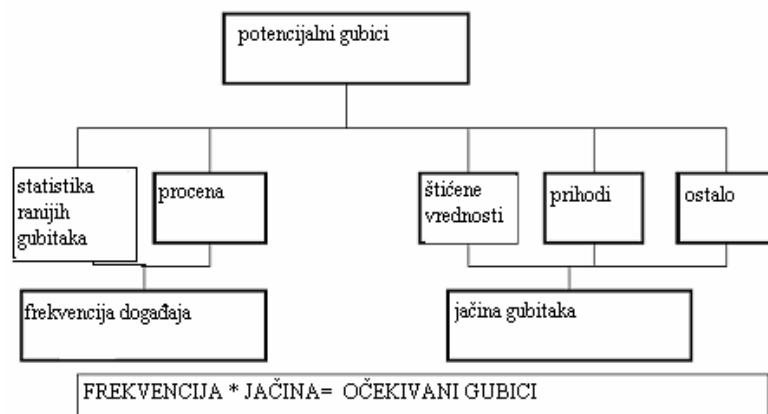
Elementi menadžmenta rizika podrazumevaju upravljanje operacionim rizicima, ljudskim resursima, tehnološkim rizicima/e-rizicima, kontinuitetom poslovanja,

oporavkom od katastrofa, kreditnim i tržišnim rizicima itd. Na slici 2 prikazan je inkrementalno-iterativni ciklus integralnog upravljanja rizicima, sa obavezno uspostavljenom povratnom spregom u sistemu, koja naglašava dinamički i adaptibilni karakter ovakvog načina menadžmenta.



Slika 2 Integralni proces upravljanja rizicima

Analize bezbednosti jesu metode za evaluaciju postojećih hazarda i rizika u sistemu i način za njihovo minimizovanje. Prvi stadijum u analizi je analiza hazarda, u kojoj se sistem analizira sa aspekta situacija u kojima potencijalna šteta može rezultovati i frekvencija sa kojima se pojavljuju ove situacije. Analiza rizika je drugi stadijum, u kome pokušavamo da determinišemo moguće ishode hazarda i frekvencija pojavljivanja svakog ishoda. Integralno upravljanje omogućava prioritizaciju potencijalnih šteta u sistemu i povećanje nivoa bezbednosti sistema. Mnogi standardi se bave određivanjem prihvatljivog nivoa bezbednosti, u različitim industrijama i biznis procesima, ali zapravo ih kratko možemo opisati kao procenu da je "sistem siguran". Sigurnost sistema zavisi od predefinisane bezbednosne politike i štićenih vrednosti sistema. Savremeni koncepti integralnog menadžmenta rizika pomeraju se iz navedenog determinističkog pristupa u probablistički pristup, koji pokušava da nađe i odgovor na pitanje koliko je verovatno da se incident dogodi, osim procene njegove jačine i konsekvenci. Na slici 3 prikazana je metrika rizika navedenog kombinovanog probablističkog i determinističkog pristupa



Slika 3 Metrika rizika

Agilna (adaptibilna) bezbednost

Nova bezbednosna filozofija agilne (adaptibilne) bezbednosti zahteva ne samo ispunjavanje ciljeva sigurnosti, već i ukrštanje misije održivog razvoja i kompetitivnog poslovanja sa tehnologijom. Bezbednosni menadžment danas je prerastao, razvio se, u IT menadžment (rizika). Nova filozofija bezbednosti je inteligentni pristup upravljanju, u smislu formiranja bezbednosnih komandnih centara, ICT vođenih, koji redukuju redundansu, agregiraju i koreliraju bezbednosne podatke iz različitih tehnoloških rešenja. Agilni sistemi upravljanja e-rizicima pokušavaju da prioritetizuju velike količine informacija iz različitih delova bezbednosnog sistema i pretvore ih u inteligentne, upotrebljive informacije, radi kreiranja akcionog odgovora.

U teoriji planirana integrisanost i adaptibilnost, agilnost i proaktivnost, pojedinih sofisticiranih rešenja (*firewall*, menadžment identiteta, upravljanje sadržajem, fizička sigurnost, kontrola pristupa, mostovi između aplikacija i tsl.) izgubila se u praksi. Nestalo je deljenje informacija između proizvođača. Bezbednost je dostigla nivo odnosa signal/šum kojim se ne može upravljati, tako da je opala brzina reagovanja sistema na incidenteⁱⁱ.

Agilni bezbednosni menadžment stoga podrazumeva:

- jedinstvenu komandu i kontrolu (jedinstvena centralizovana konzola za daljinsko upravljanje)
- poboljšanu operacionu i situacionu svesnost (ubrzano i poboljšano otkrivanje, istraživanje i ubrzan odgovor na procese, pretraživanje detalja po zahtevu, pronalaženje korenog uzroka problema, izgradnja modela stanja bezbednosti)
- širinu i dubinu pokrivanja sistema (produkti treće generacije koji podržavaju integritet i transparentnost)
- podršku konceptu totalnog kvaliteta bezbednosnog menadžmenta ("Vidi sve i upravljaj svim").

Savremene teorije, kao što je OCTAVE koncept bezbednosti informacijaⁱⁱⁱ, bazirane su na komponenti rizika zvanom štice vrednost, pa tek potom na pretnjama i slabostima, kao dodatnim tretiranim komponentama rizika. Bezbednost informacija zahteva od tima za rizik da identifikuje štice vrednosti povezane sa informacijama (podatke i sisteme) koji su važni za organizaciju, usredsredi aktivnosti analize rizika na one vrednosti koje su procenjene kao najkritičnije za organizaciju, da odredi veze među kritičnim vrednostima, pretnje tim vrednostima i slabosti koje mogu izložiti vrednosti pretnjama (organizacione i tehnološke). Od tima se zahteva da evaluiira rizike u operacionom kontekstu.

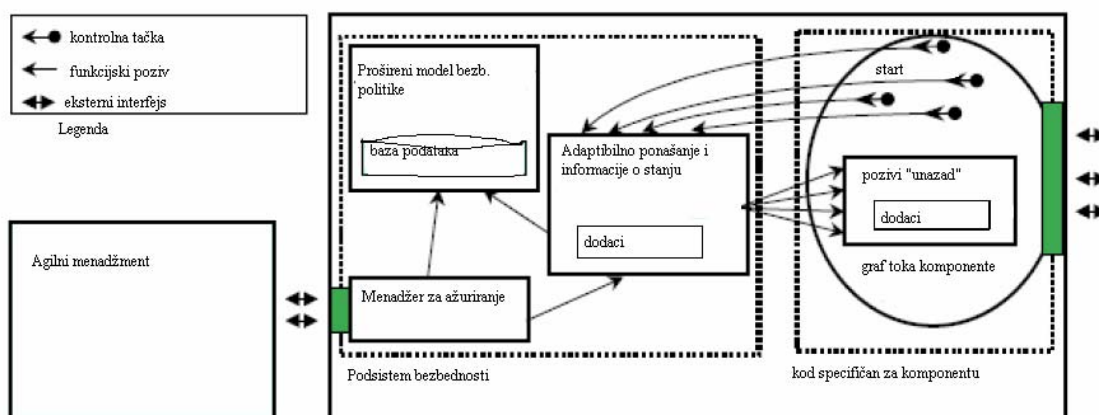
Adaptibilna bezbednosna infrastruktura jeste dinamički, prilagodljiv odgovor na bezbednosne događaje i način obezbeđivanja automatskih metoda za pouzdano uspostavljanje nivoa poverenja, detekciju upada u sistem, usklađivanje bezbednosne politike sa novim situacijama i oporavka od kritičnih uslova sigurnosti. Ispunjavanje ovih misija moguće je izgradnjom inteligentnih tehnika koje agilno reaguju na bezbednosne potrebe dinamičkog okruženja. Glavni cilj je identifikovanje problema i njihova automatska korekcija. Tradicionalni mehanizmi kontrole su često bazirani na statičkoj konfiguraciji kontrole pristupa, tako da ne pružaju agilnu bezbednost. U konceptu adaptibilne bezbednosti, bezbednost se ne odnosi samo na statičke konfiguracije sistema definisane od strane administratora, već na tekuće procese ažurirane u skladu sa definisanim bezbednosnom politikom, radi stvaranja dinamičke automatske konfiguracije za upravljanje bezbednosnim događajima.

Bezbednosni menadžment sledi iste povratne sprege obuhvaćane mrežnim i sistemskim menadžmentom, koje uključuju monitoring, dijagnostiku/analizu i primenu korektivnih akcija-odgovora. Faza monitoringa uključuje nadzor i detekciju promena u okruženju. Faza analize uključuje dijagnostiku i identifikaciju promena koje vode do vanrednih događaja, kao i odlučivanje u vezi sa korektivnim akcijama koje će se

sprovести. Faza odgovora uključuje sprovođenje izmena u konfiguraciji diktiranih politikom ili odlukama tokom faze analize (akcijama upravljanim od strane analitičara).

Moguća rešenja agilne bezbednosti

Problem koji treba prevazići modelima agilne bezbednosti jeste nedovoljna interoperabilnost između različitih servisa za nadzor bezbednosti (firewall, alati za detekciju upada, kontrola pristupa, nadzor web servisa i dr. imaju zasebne bezbednosne funkcije). Ovi nezavisni proizvodi nemaju međusobnu interakciju, svaki ima zasebnu konzolu menadžmenta i administrira se individualno. Efikasnije rešenje bi integrisalo ova rešenja radi minimizovanja bezbednosnih pretnji.



Slika 4 Arhitektura komponenti agilne bezbednosti ^{iv}

Kao primer nekih rešenja koja počinju da usvajaju koncept adaptibilne bezbednosti navodimo *Tivoli Risk Manager* i *Intelligent Security Infrastructure Management Systems*.

Tivoli Risk Manager razvijen je da upravlja bezbednosnim pretnjama i slabostima širom organizacije, korelirajući bezbednosne informacije i upozorenja iz mnoštva uređaja i kontrolnih uređaja, uključujući sisteme za detekciju upada, firewall-ove, rutere i mrežu. Tivoli Risk Manager dolazi sa inteligentnom mašinom, koja korelira sve informacije sa više senzora i potom daje upozorenje za svaki napad, na jedinstvenoj konzoli.

Tivoli Risk Manager pokušava da dostigne sledeće projektovane ciljeve:

- obezbediti jedinstvenu centralizovanu kontrolnu tačku-jedinstvena web zasnovana bezbednosna konzola za monitoring i upravljanje bezbednosnim alarmima širom rganizacije
- integrisati bezbednosne aplikacije, mrežu i operativni sistem da bi se obezbedilo sveobuhvatno upravljanje okruženjem
- pomagati administratrima sistema da identifikuju tipove pretnji, šablone upada i napada, koristeći tehnike korelacije, agregacije i sumiranja, radi ubrzanja vremena odgovora i redukovanja lažnih uzbuna.
- obezbediti različite predefinisane poslove odgovora radi rešavanja hitnih ili lakih napada kao što je npr. neautorizovani pristup.

- obezbediti analitičke izveštaje iz proteklih perioda, kao podršku odlučivanju i menadžmentu rizika.

Arhitektura *Tivoli* menadžera rizika obuhvata komponente za generisanje događaja, *real-time* komponente upozorenja (uključujući mašinu za korelaciju podataka, zasnovanu na normalizaciji informacija, agregaciji pravila i situacionoj analizi), izveštajne komponente (sadrže data mining deo i mehanizme analize za podršku odlučivanju).

Inteligentni sistemi menadžmenta bezbednosne infrastrukture (*Intelligent Security Infrastructure Management Systems (iSIMS)*) je tehnološka platforma razvijena od strane kompanije *Symbiot*, slična konceptu *Tivoli Risk Manager*-a. Naime *iSIMS* interoperabilan je sa drugim bezbednosnim infrastrukturna kao što su *firewalls*, detekcija upada/prezentacioni sistemi i *Virtual Private Networks*, koje akumuliraju bezbednosne događaje u realnom vremenu, pa na osnovu njih izgrađuju model rizika. Model rizika pruža informacije o težini napada (kako ugrožava napadač) i uticaju na sistem (cena ako napad uspe).

Mere pretnji su definisane koristeći skor rizika. Korišćena metrika rizika slična je kreditnom skor koji računaju kreditni biro i banaka. Skorovi rizika koriste platformu *iSIMS* i *Symbiot.NET* skladište da obezbede odgovornost, konzistentnost i standardizaciju. *Symbiot.NET* je centralno skladište podataka koje sadrži profile i obeležja napada i incidenata u sistemu, zasnovane na kooperativnom nadzoru i prepoznavanju, podacima "izvidnice" na mreži. Baza znanja *iSIMS* je ažurirana koristeći podatke iz *Symbiot.NET*. Ovi podaci se koriste radi identifikovanja napadača, razloga incidenata, evaluacije metoda i namera i preporuka odgovarajuće kontramere.

Očekivana mera rizika, $EV(R)$ je funkcija sledećih subjekata integrisanih tokom vremena:

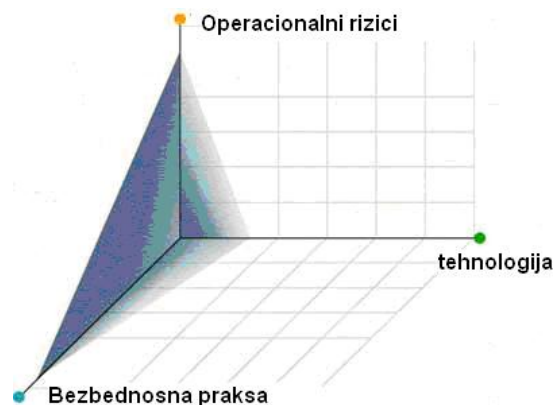
$$EV(R) = \int [P_{treat}(t) * P_{vulnerability}(t) * Value(t)] dt \quad (1)$$

Verovatnoća pretnji $PTREAT(t)$ je estimacija derivirana iz kumulativnih alarma generisanih od postojećih bezbednosih komponenti i može biti samo-generisana od *iSIMS* platforme (zasnovana na anomalijama, ponašanju i analizi "živog" saobraćaja na mreži). Verovatnoća slabosti, $PVULNERABILITY(t)$, je estimacija zasnovana na evaluaciji o tome kako mreža reaguje i kako odgovara na pretnje. Vrednost (Value) je determinisana koristeći troškove, imovinu i sadašnje vrednosti prihoda povezanih sa infrastrukturom izloženoj pretnji.

Symbiot.NET pruža model graduiranog odgovora na bezbednosne incidente, od jednostavnih tehnika kao što su blokiranje mrežnog saobraćaja pa do agresivnih mera, uključujući blokiranje saobraćaja, limitiranje protoka, skretanje saobraćaja i karantin.

Zaključak

Izgradnja fleksibilnog sistema, različitog od tipično tehnološki-fokusiranih sistema, koji će biti usredsređen na organizacijske rizike i strategije, sa poslovanjem povezane ciljeve, predstavlja novi koncept integrisanog menadžmenta e-rizika u operacionalni menadžment. Agilni model bezbednosti na pravi način balansira operacionale rizike, bezbednosnu praksu i tehnologiju (slika 5).



Slika 5 OCTAVE pristup operacionalnim rizicima i bezbednosnoj praksi^v

Većina predloga modela upravljanja rizicima fokusira se na integraciju postojećih bezbednosnih mehanizama ili proizvoda tj. detekciju upada u sistem i drugih vanrednih događaja, sa ciljem pružanja adaptibilnog ponašanja na izazove i pretnje. Pouzdaniji i fleksibilniji modeli uključivali bi mehanizme za izgradnju i opravdanost zahtevanog stepena sigurnosti, u vidu povećane održivosti i elastičnosti sistema, dinamičkih parametara bezbednosne politike i višeg stepena pouzdanosti.

Misija agilnih menadžera e-rizika i menadžera operacionalnih rizika, integriše se i transformiše u procese upravljanja rizicima koji poboljšavaju efikasnost sistema, redukuju gubitke i povećavaju vrednost organizacije.

LITERATURA

1. Alberts C. J., Dorofee A. J. (2001), "OCTAVE Criteria V2.0 (CMU/SEI-2001-TR-016, ADA3399229), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University,
<http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html>.
2. IBM (2002), "Tivoli Risk Manager, Problem Determination Guide",
<http://publib.boulder.ibm.com/tividd/td/RiskManager4.1.html>
3. IBM (2002), "Recommended Practices for Risk Management with Tivoli Risk Manager. RedBook",
<http://publibb.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/redp0202.html?Open>
4. Keković Z., Nikolić V. (2006), "Proces integralnog upravljanja rizicima u organizacijama", Bezbednost, 3/06, Beograd
5. Lupu E., Wilson M.D. (2006), "State of the art survey on trust, security and contract management in web services and Grid computing",
<http://epubs.cclrc.ac.uk/bitstream/909/RAL-TR-2006-008.pdf>
6. MoD (1996), "Interim Defense Standard 00-58 HAZOP Studies on Systems Containing Programmable Electronics.", <http://www.seasys.demon.co.uk/>
7. Nikolić V. (2005), "Analitika bezbednosnih pojava kao podrška odlučivanju", Bezbednost 4/05, Beograd
8. Petkac M., Badger L., Morrison W. (2001) "Security Agility for Dynamic Execution Environments", Proceedings of the DARPA Information Survivability Conference & Exposition Volume I of II, Hilton Head, South Carolina
9. Symbiot Security (2006), <http://www.symbiot.com/>

Fusnote:

ⁱ Raz T., Hillson D. (2005), "A Comparative Review of Risk Management Standards", *Risk Management:*

An International Journal, december 2005, Volume 7, No 4., page 54

ⁱⁱ Riyaz A. K. (2006), "Risk mitigation using comprehensive State of the art survey on trust, security and contract management in web services and Grid computing",

[http://www.intaj.net/storage%20folder/PDF/](http://www.intaj.net/storage%20folder/PDF/AKR%20presentation.pdf)
[/AKR%20presentation.pdf](http://www.intaj.net/storage%20folder/PDF/AKR%20presentation.pdf)

ⁱⁱⁱ Alberts C. A., Audrey J.D., (2001), "OCTAVE CriteriaVersion 2.0", *TECHNICAL REPORT-CMU/SEI-2001-TR-016-ESC-TR-2001-016*, Software Engineering Institute, Carnegie Mellon University , page 6

^{iv} Lupu E., Wilson M.D. (2006), "State of the art survey on trust, security and contract management in web services and Grid computing", <http://epubs.cclrc.ac.uk/>, page 307

^v Alberts C., Dorofee A., Stevens J., Woody C. (2003), "Introduction to the OCTAVE® Approach", Software Engineering Institute, Carnegie Mellon University, page 4