Заштита информационих система и пословна политика

Момчило Кокић
MD - Perić Company,
Bijeljina, Република Српска-Босна и Херцеговина
kokicm@gmail.net

Садржај—**Рачунарски информациони системи су инкорпорирани у све процесе привредних и друштвених система. Они су задужени за процесе у вези са снабдијевање корисника адекватним подацима и информацијама. Један од веома значајних процеса у информационом систему је и процес заштите података и иннформација. Он се остварује кроз свеобухватан процес заштите информационих система као цјелине. Политика заштите информационих система мора бити инкорпорирана у пословну политику, јер се само на такав начин може дати важност заштити података и информација која им, с обзиром на њихов значај као стратешких ресурса, припада. У овом раду ће се указати на објективне разлоге који захтијевају да се заштити информационих система, кроз политику заштите као дијела пословне политике, да заслужена пажња.**

Кључне ријечи-рачунарски информациони систем; податак, заштита, политика заштите, пословна политика.

I. УВОД

Ниједна активност није у ближој вези са успјехом од ефикасног прикупљања и ширења информација. Ниједна награда не смије бити већа од оне која се даје онима који доносе суштинске информације. Ниједна операција не смије бити у већој тајности од оне која је у вези са информацијама.[1] У савременим пословним системима информације су веома значајан ресурс и продукт су информационих система. Значај података потврђује и један од принципа менаџмента системом квалитета, који каже да се ефективне одлуке заснивају на чињеницама. Нема ваљане одлуке без чињеница. Чињенице, поред што обезбјеђују доношење ваљаних одлука оне подстичу доношење одлука. До одговарајућих чињеница се долази анализом података и информација уз помоћ информационе технологије. Благовремена и тачна информација је жила куцавица успјешне конкуренције.[1] Зато се подаци и информациони системи (ИС) морају штитити од неовлашћеног приступа због кога може настати крађа података, брисање или промјена података. Основни циљ заштите информација је обезбјеђење континуитета пословања и смањење штета које настају као посљедица неовлашћеног коришћења података.

Крађа материјалних ресурса се знатно лакше уочава од крађе података. Крађа података и информација је специфична и по томе што су украдени подаци најчешће и послије крађе на располагању власнику тако да је он врло често несвјесан крађе података све до њихове злоупотријебе. Неовлашћено уништавање података, брисањем, није ништа друго до уништавање значајних пословних ресурса. Промјена података се ради због навођења корисника тих података на погрешне акције које се доносе нао основу података. Штете изазване неовлашћеним приступом подацима могу бити немјерљиве. Зато се заштити информационих система (ИС) и података који они продукују мора дати заслужујућа пажња, а она је велика. То опредјељење мора бити изражено кроз пословне политике јер само тако заштита података добија заслужену пажњу. У раду се жели скренути пажња на значај схватања заштите информационих сисстема и неопходност да се процедуре заштите нађу међу правилима према којима се корисници информационих система понашају у току реализације планских циљева уз експлоатацију података и информација, а то захтијева да политука заштите ИС-а буде сатавни дио пословне политике.

II. ОПШТИ КОНТЕКСТ ПОСЛОВАЊА

Прилагођавање промјенама у окружењу и управљање промјенама је постао један од основних задатака на путу остваривања постављених циљева свих система. То се данас дешава у условима опште глобализације, условима аутоматизације пословних процеса на Интернет платформи и опште координације и сарадње на тој платформи, која остварује повезивање пословних партнера. Краће речено, то се дешава кроз стварање услова за електронско пословање на глобалном тржишту као предуслова опстанка на том тржишту. Интернет окружење и електронско повезивање пословних партнера по свим основама су доминантна карактеристика пословног окружења и неопходан услов опстанка пословних система (ПС). ПС су практично постали саставни дио глобалне мреже. Ни друштвени системи нису у дригачијој позицији.

Тржишни услови који заоштравају конкурентску борбу, функционисање и развој ПС-а, повећани ризици пословања и одлучивања, те развој све комплекснијих структура, елемената и веза система, неминовно воде ка постављању све већих захтјева у односу на информационе системе.[2] Информациони систем ПС-а као његов подсистем је јако интегрисан у све остале подсистеме и као такав бива праћен итекако видљивим манифестацијама на реализацију свих пословних процеса. Квалитет и информационе технологије се данас сматрају највећим покретачем напретка у свим сферама. Према истраживањима која је спровела Свјетска Банка (*The Investment Climate Survey*) још јануара 2006. године,

компаније које у већој мјери користе информационе и комуникационе технологије расту по стопи од 3,8% што је у поређењу са 0,4% за око 10 пута више у односу на оне које то не користе То се дешава захваљујући подацима као једном од веома битних ресурса у свим системима.

Савремени трендови пословања су усмјерени ка повећању општег просперитета, задовољства људи, очувања природе и природних ресурса. Зато су потребни знање и информације. Знање и управљање знањем постали су најзначајнији капитал конкурентске предности. Вриједност неке организације више не одређују само мјерљива материјална и финансијска средства, него и нематеријалне вриједности и квалитет људских ресурса. Ово је ера података, информација, знања и мудрости. [3] Зато борба за ове рсурсе не бира средства ни у процесу њиховог прибављања ни у процесу њихове заштите.

III. ПОЛИТИКА ЗАШТИТЕ ИС-А

Изнесене чињенице су довољни докази за опредељење да се изградњи информационих система посвети пажња, а њиховој безбједности, у свакој фази живота, посвети додатна пажња. Ово опредјељење се мора системски спроводити, а најбољи ефекти ће се постићи ако је то дио пословне политике, то јест ако је дио правила према којима ће се ПС понашати у току изградње и експлоатације ИС-а. Зато је неопходно планирати пословне политике, пословне стратегије и израдити низ програма и планова усмјерених ка очувању интегритета информационог система, па тиме и интегритета података као ресурса. У овом контексту, планирање је примарна функција која обухвата дефинисање: циљева, политика, стратегија, програма и планова којима се омогућује усмјеравање и прилагођавање сигурносних процедура информационог система окружењу у којем функционише. Овакав приступ обезбјеђује оптималан однос степена заштите и утрошка ресурса за те намјене.

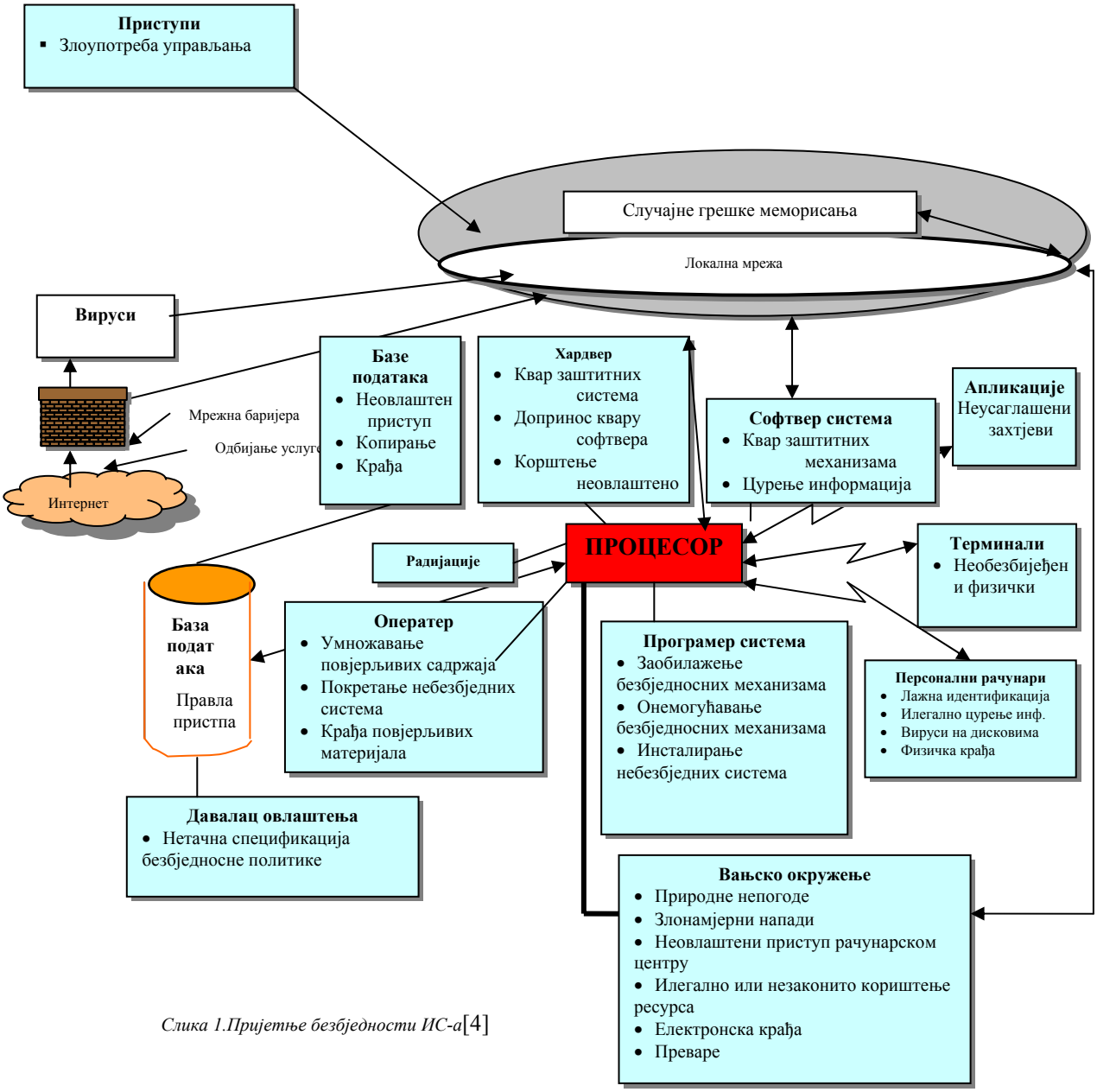
Сваки подсистем пословног система, па и подсистем заштите информационог система, мора имати властити процес планирања, дефинисања политика заштите, који представљају систематизовано сагледавање прошлости, садашњости и будућности у циљу предузимања активности у садашњости, ради остварења постављених циљева у блиској и даљој будућности. Основни циљеви система заштите морају бити благовремена заштита од неовлашћеног приступа ресурсима информационог система. То се реализује кроз предузимање низа превентивних и корективних мјера и поступака. Одговарајућа заштита информационих ресурса подразумијева, поред техничке и физичке заштите, и низ организационих мјера за њихову безбједност. Колико је заштита важан сегмент за ИС говори и то што се ова проблематика третира у низу законских прописа многих земаља. Ево неких закона из те области које је усвоио Парламент САД :

- Закон о уређајима за неовлашћени приступ рачунарској превари
- Закон о рачунарској превари и злоупотреби
- Закон о рачунарској безбједности
- Закон о електронском трансферу новца
- Закон о е- трговини,
- Закон о електронском потпису

Све ово обавезује да се, поред низа заштитних мјера, предузму многе организационе мјере и организационо предвиди спречавање и отклањање посљедица остварених безбједностних пријетњи. Да би се то остварило треба предузети мјере које ће за посљедицу имати управљање ризицима у циљу свођења ризика на прихватљиву мјеру. Прихватљива мјера ризика је мјера спремности организације да улаже материјална и финансијска средства у смањење ризика од остварења појединих пријетњи на прихватљив ниво. Треба се бити свјестно да апсулутно безбједних информационих система нема, те стога, тежња ка свођењу ризика на нулу је неостварљива, зато је уведен појам прихватљивог ризика чије се последице, с обзиром на уложена средства у заштиту ИС-а, могу или морају прихватити.

Велики проблем за добру заштиту ИС ресурса представља дисперзија ИС ресурса. Пословни системи имају велику дисперзију у свим погледима, као што су: дисперзија ресурса, дисперзија клијената, дисперзија производа, итд. Ово за посљедицу има велику дисперзију ИС ресурса, већи број пријетњи, па и теже успостављање ефикасне заштите ИС ресурса. Они могу бити угрожени на разне начине, намјерно и ненамјерно. На намјерно изазване проблеме отпада око 30% свих проблема у рачунарским системима.[4] На Сл. 1. су приказани могући извори пријетњи по безбједност информационих система. Свакој од ових пријетњи се мора посветити довољно пажње. Пријетње се морају уочити, проценити ризик њиховог остварења, уочити штете које могу проузроковати, треба се предвидјети одговарајућа заштита-предвидјети превентивне мјере да се не би пријетња-пријетње реализовале, а ако се реализују морају се имати дефинисане процедуре опоравка. О захтјевима у овом погледу говори се и у серији стандарда ИСО 20000- *Information technology -- Service management*. [5]

Систем заштите подразумијева инкорпорацију одбранбених механизама у циљу спречавања случајних ризика, одвраћања од намјерних радњи, предвиђање и унапријеђење процеса опоравка од оштећења те уочавања извора будућих безбједносних проблема. Главни циљ система заштите је управљање ризиком у циљу његовог смањења. Ризик са овог становишта је специфичан за сваки информациони систем те се заштити информација мора приступити на такав начин да се обезбиједи рентабилан и адекватан систем заштите за процијењени профил ризика уз оптималне трошкове заштите. Да би се обезбиједила адекватна заштита информационих система, при дефинисању политике заштите, као добар алат могу послужити разни стандарди који регулишу ову област, као што је серија стандарда ИСО 27000- *Information security managament system*[6] и ИСО 31000- *Risk management*[7]. У овим процесима се могу користити различити примјери најбоље праксе.



Слика 1.Пријетње безбједности ИС-а[4]

IV. ЗНАЧАЈ ПОСЛОВНЕ ПОЛИТИКЕ

Одавно је менаџмент информационог система ушао у ранг топ менаџмента у великом броју организација. По истраживању, које је спровео ИБМ са сарадницима 2007. године у оквиру истраживања унапређења професије менаџера информационог система у коме је учествовало 175 менаџера информационих система из 18 индустрија са шест континената из 27 земаља, малих и великих компанија, владиних и научних сектора, 80% менаџера ИС-а у 2007. години је постало пуноправан члан сениорских менаџерских тимова. Ово представља пораст од 10% у односу на 2006. годину. Истовремено, 70% менаџера ИС-а имају званичну улогу у извршном комитету ПС-а[8]. У многим компанијама менаџер ИС-а заузима још неку веома значајну функцију у топ менаџменту.Са становишта потврде значаја који се придаје ИС-у, ово сазнање је веома битно.

Пошто се пословне политике креирају на нивоу топ менаџмента, резултати наведеног истраживања потврђују могућност значајне партиципације менаџера информационих система у креирању пословне политике. Они са позиције у топ менаџменту могу значајно допринијети да дио пословне политике буде и заштита података и информација које су основни продукт процеса у информационом систему и стратешки су ресурс цијелог система. Ови резултати потврђују да у пракси великих система менаџмент информационих система има заслужену позицију, а она је у топ менаџменту. Ово априори не значи да ти системи имају успостављен

адекватан систем заштите, односно системски приступ заштити ИС-а, али су створени значајни организациони предуслови да се то оствари. Многи системи имају низ заштитних мјера за ИС, али без адекватног системског приступа на чему инсистирају помињани стандади, а потребу таквог приступа потврђују многи примјери добре праксе. Системски приступ у заштити ИС-а је усмјерен на успостављање: политике, циљева, планирања, управљања, обезбјеђења и побољшања система заштите информационих система. Зато менаџмент ИС-а мора бити лидер у стратегијском размишљању и одлучивању, јер се само тако може обезбиједити јединство политика, стратегијских циљева ПС-а и циљева ИС-а. [9] Сагласност ових циљева је трећа по значају мјера ИТ услуге у ПС-у. Као мјера нивоа ИТ услуга се користи: задовољство корисника у 69% организација; достигнути ниво услуга у 58%; сагласност са пословном стратегијом 53%,.. итд.[10]

Менаџер ИС-а никада не смије бити задовољан постигнутим степеном информатизације пословних процеса и безбједношћу података и информација. Да би се задовољили истакнути или подразумијевани циљеви заштите потребна је реализација низа процеса и обезбјеђење значајних ресурса за њихово испуњење. Из опште пословне политике ПС-а мора произаћи, између осталих, и политика у погледу ресурса, а из политике ресурса мора произаћи и политика у погледу ресурса неопходних за системску заштиту ИС-а. Из те политике посебно се може издвојити онај сегмент који се односи на заштиту података и информација. Овај дио пословне политике мора бити јасно саопштен и доступан свим запосленим, јер су сви запослени у ситуацији да располажу одређеним подацима и информацијама које заслужују адекватан степен сигурности.

Изражавање појединих политика обично није опширно, али је зато потребно да буде врло јасно. Обично се са неколико реченица у оквиру политике ПС-а декларише политика заштите ИС-а, док се она посебно разрађује у документима заштите. У оквиру политике заштите се саопштавају опредјељења менаџмента у односу на све ресурсе заштите.

Сљедећих неколико примјера би се могло користити за изражавање оног сегмента политике заштите који се односи на људске ресурсе који су битан сегмент система заштите.

- Доследном бригом о људским ресурсима обезбиједићемо потребан ниво знања, стручности и оспособљености свих запослених из домена заштите података и информација, за шта су одговорни менаџери сектора.
- Задовољење захтјева у погледу безбједности ИС-а обезбиједиће стручни и квалитетни менаџери који су одговорни за стални раст укупних знања и вјештина својих запослених.
- Примјена савремених информационих технологија у нашим процесима је наше пословно опредјељење те у циљу задовољења потреба у погледу заштите ИС-а одговорни ће бити наши менаџери, зато њиховом знању посвећујемо посебну пажњу, итд.

На сличан начин се могу изразити и остали сгменти политике заштите који се односе на остале рсурсе, организацију, менаџмент,... итд.

Може се рећи да је у процесу менаџмента заштитом ИС-а потребно ускладити политику заштите, са дефинисаним циљевима, ускладити процесе заштите и обезбиједити адекватне ресурсе који су неопходни за испуњење захтјева заштите. Колико се у томе успије показују резултати анализе реализације политике заштите и успостављеног система заштите. Ове анализе се обавезно морају радити, у нормалним околностима, када и анализа пословања, а ванредно у сваком случају када дође до нарушавања система заштите и неовлашћеног приступа подацима и информацијама. Уколико је овакво опредјељење дио пословне политике, оправдано је очекивати да ће се процеси анализе узрока и штета насталих као последица остварених пријетњи завршавати корективним мјерама које ће спријечити понављање таквих појава и повећати степен заштите ИС-а као цјелине.

V. ЗАКЉУЧАК

Системски приступ заштите података и информација се реализује кроз систем за управљање заштитом информација (*Information Security Management System* - ISMS). Потенцијални носиоци пријетњи по безбједност ресурса ИС-а су извршиоци напада и узроци су настанка фактора ризика. Ризик је процијењена мјера утицаја пријетњи на информационе ресурсе и може се дефинисати као вјероватноћа да ће носиоц пријетње искористити неку рањивост система и изазвати негативне посљедице за систем и организацију у цјелини. Зато се управљање безбједношћу информационог система реализује кроз процесе управљања ризиком. Ризик је директно пропорционалан порасту пријетњи те смањење пријетњи смањује ризик, а мањи ризик значи безбједнији систем. Због тога су анализа извора пријетњи и процјена ризика релевантни процеси за безбједност ИС-а. Процјена ризика укључује и избор различитих контрола заштите за смањење ризика на прихватљив ниво, смањењем рањивости и изложености у складу са захтјевима успостављене политике заштите. Политика заштите, ради своје ефикасности, мора бити јасно изражена кроз пословну политику цјелокупног система коме информациони систем кроз информационе процесе пружа неопходну подршку. За успјешну заштиту ресурса ИС-а неопходно је користити релевантне међународне стандарде и примјере добре праксе.

LITERATURA

[1] Перишић М., Управљање трошковима квалитете, Зборник радова. Оскар, Загреб, 2000

[2] Крсмановић С., Мандић П. Д., Менаџмент информационих система, Факултет за менаџмент "Браћа Карић" Београд, Београд 1995..

[3] Балабан Н., Информационе технологије и информациони системи, Универзитет у Новом Саду, Економски факултет Суботица, Суботица, 2007.

[4] Turban, McLean, Wetherbe, Информациона технологија за менаџмент, John Wiley, превод 3. издање Завод за уџбенике и наставна средства, Београд, 2003.

[5] Кокић М., "Значај примјене ИСО/ИЕЦ 20000 за квалитет ИТ услуга", Квалитет и изврсност, Година I Број 7-8/2012, FQCE-Београд, 2012.

[6] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements

[7] ISO/IEC 31000:2009 Risk management -- Principles and guidelines

[8] IBM, „Advancing the CIO profession through research and thought leadership", www.ibm.com, 2007.

[9] Кокић М., "Карактеристике менаџера савременог информационог система у пословним системима као допринос менаџменту", докторска дисертација, Универзитет у Источном Сарајеву, Факултет за производњу и менаџмент, Требиње, 2012.

[10] „Ready, Willing and Enabled: A Formula for Performance", Economist Intelligence Unit уз спонзорство Microsoft-a, јануар 2008.

ABSTRACT

Content - Computer information systems have been incorporated in all the processes of economic and social systems. They are responsible for processes related to supply users with adequate data and information. One of the most important processes in the information system is the process of protecting data and information. It is achieved through a comprehensive process of protecting information systems as a whole. Politics of protection information systems must be incorporated into the business policy, because only in this way it could be given an importance to the protection of data and information which, regard their importance as a strategic resource, belongs to them. This paper will point out the objective reasons that require protection of information systems, through the policy of protection as part of business policy that deserves attention.

Keywords: computer information system, data, protection, protection policies, business.

The Protection of Information Systems and Business Policy

Momčilo Kokić
MD - Perić Company,
Bijeljina, Republic of Srpska – Bosnia and Herzegovina
kokicm@gmail.net