

КРЕИРАЊЕ РЕЗЕРВНИХ КОПИЈА БАЗА ПОДАТАКА У ФУНКЦИЈИ ОСИГУРАЊА КОНТИНУИТЕТА ПОСЛОВАЊА

CREATING A DATABASE BACKUP IN THE FUNCTION OF ENSURING CONTINUITY OF THE BUSINESS

Раде Божић

Универзитет у Источном Сарајеву, Факултет пословне економије Бијељина,
Република Српска, Босна и Херцеговина
rade.bozic@fpe.unssa.rs.ba

Борислав Дракул

Универзитет у Источном Сарајеву, Факултет пословне економије Бијељина,
Република Српска, Босна и Херцеговина
borislav.drakul@fpe.unssa.rs.ba

Апстракт: Конкурентност у модерном пословању условљена је имплементацијом савремених информационих технологија. Компаније које у својој организацији имају интегрисан пословни информациони систем, у великој су мјери ослободени на његово исправно функционисање. Предуслов томе је и активна база података која мора имати осигурану непрекидну доступност. Из тог разлога неопходно је креирати резервне копије података како би се информације сачувале од посљедица нежељених догађаја. Уколико дође до оштећења или губитка пословних података, то ће директно утицати на неповољнији финансијски положај, па чак и могуће гашење пословног субјекта. Инвестирање у креирање копија база података представља мали новчани износ у поређењу са потенцијалном штетом која би могла да настане уколико се не предузму потребне мјере. Значај оваквог информационог процеса препознале су и државе, па су законским регулативама условиле поједине врсте привредних субјеката на адекватно креирање резервних копија пословних база. Ревизијом пословног информационог система настоји се постићи исправно функционисање и заштита података у сваком тренутку. Како би предузеће обављало несметано своје свакодневне пословне активности, потребно је препознати значај правилног копирања база података и његову улогу у комплетном информационом систему.

Кључне ријечи: база података, копија, осигурање, континуитет, пословање

Abstract: Competitiveness in modern business is conditioned with implementation of information technologies. Companies that have integrated business information

system are dependent of its functionality. One of main requirements for its functionality is business database which has to be active all the time. For that reason, it is necessary to create database backup to keep information safe from consequences of the accidental events. Damaged or lost data will affect negatively on financial result, or even causing the end of the business. Creating database backup is small investment comparing to potential damage which could happen without it. Governments have realized importance of this IT process for some types of business and created laws which insure proper use of this technology. Auditing of business information systems provides its correct functionality and protection of business data in every moment. In order for the company to carry out its daily business activities without any problems, it is necessary to recognize the importance of database backup and its role in the information system.

Key Words: *database, backup, ensuring, continuity, business*

УВОД

Одавно је уочено да информација у 21. вијеку постаје најважнији ресурс за развој свих дисциплина и организација. Имплементирајући савремене информационе технологије и дигитализацију у своје пословање, привредни субјекти настоје да искористе предности које им пружа управљање великом количином података. Без обзира да ли се они односе на саме потрошаче или на пословне процесе унутар организације, постају моћно оружје у борби против конкуренције. Уједно постају и пресудни елемент за опстанак на тржишту. Препознавање потреба и преференција потрошача, као основна фокусна тачка у плану развоја сваке организације, неостварива је без адекватног информационог система, који је задужен за прикупљање података. Поред адекватног софтвера који је задужен за њихово прикупљање, неопходна је и хардверска подршка, која може својим перформансама допринијети несметаном функционисању наведеног процеса, а уједно и чувати податке. Скоро да не постоји пословна организација која у свом портофлију не располаже одређеним базама података складиштеним у оквиру информационог система. У зависности од намјене и величине, рангира се и њихов значај за саму организацију. Оне које се односе на потрошаче и пословне партнере су стриктно законски регулисане и подлијежу кривичној одговорности. Посебан акценат стављен је на прикупљање и чување оваквих врста података. Када би се ове информације компромитовале у јавности, новчана казна би била најмањи проблем када се сагледају посљедице. Углед организације би био нарушен, а самим тим и пословни положај на тржишту. Поред објелодањивања, оштећење или брисање оваквих информација има примарни утицаја на будуће пословање предузећа. Да би се спријечио настанак оваквог догађаја, неопходно је креирати резервне копије и складиштити их на одговарајућим физичким компонентама информационог система. Цјелокупни пословни процеси су засновани на овим базама података, а њихова недоступност или неисправност спрјечава организацију да несметано

обавља своје пословне активности. Из тог разлога је важно учити значај креирања резервних копија података и њихов утицај на континуитет пословања.

1. Имплементација резервних копија база података и утицај на пословну организацију

Као саставни дио информационог система сваке привредне организације неизоставне су базе података. Својим функционисањем прате ток пословања, пружајући подршку у остваривању задатих циљева. Превелики је ризик посједовати само оперативну базу података и ослањати се на њену поузданост и доступност. Без креирања резервних копија (енг. *data backup*), знатно би се повећао пословни ризик, а на тај начин би директно проузроковао настанак губитка. Због тога, стручњаци запослени у сектору информационих технологија морају да уоче важност наведених процеса и да захтјевају од менаџмента довољна инвестициона улагања за имплементацију система за креирање резервних копија база података. Према истраживањима компаније CloudBerry, више него трећина пословних организација (36%) уопште не креира резервне копије база података. На нашем подручју, мала предузећа нису довољно информисана о значају овог проблема. Подизање свијести, нарочито предузетника, допринјело би знатном повећању броја организација које воде рачуна о својим подацима. У зависности од природе посла саме организације, ствара се и одговарајући број резервних копија базе. Према великом броју мишљења, креирање само једне резервне копије није довољно за постизање довољне сигурности за непрекидан рад система. Око 49% компанија креира само једну резервну копију база података, ризикујући да дође и до њеног оштећења. Поједине пословне организације као што су банке, креирају копије података у реалном времену, често на дислоцираним серверима ради елиминисања могућности уништења података због дјеловања елементарних непогода (Beeler Jr, D. E. 1999). Примјењује се правило 3-2-1, које налаже да се креирају најмање три копије података, на најмање два различита медијума (диск, cloud, итд.), док се једна копија чува на удаљеној локацији у случају природних катастрофа. Такође, важан фактор је и временски период у којем се подаци копирају. Уколико је природа посла динамична, онда је период између два процеса копирања краћи. Код организација које свакодневно имају промјене у базама података, неопходно је правити копије минимално на дневном нивоу, али и чешће. Примјењује се и креирање копија у реалном времену гдје се истовремено промјене биљеже и у оперативној бази, као и у резервним копијама наведене базе. Такође, према истраживању наведене компаније, 42% пословних организација које обављају копирање података, то одрађују с времена на вријеме, не вршећи константно наведену операцију. Ово може бити велики проблем уколико дође до отказа оперативне базе. Нова база не би била довољно ажурна што би изискивало додатне напоре да се доведе у адекватно стање уколико би то уопште било могуће.

У организацијама које немају имплементирано креирање резервних копија база података, приликом увођења наведеног поступка потребно је анализирати значај сваке врсте података и одредити приоритет њиховог копирања. Један од разлога је и што су ресурси за складиштење копија података (нпр. интернет или процесор сервера), често заузети другим операцијама. Овај процес је потребно укључити у саму политику правила и процедура сваког сектора информационих технологија, што доводи до смањења могућности настанка непредвиђеног догађаја, а уједно и саму технику и методе креирања резервних копија јасно дефинише и одређује. Често се у самом процесу ангажују партнерске фирме у постављању комплетне стратегије *backup*. Оно што је важно, а у пракси често изостављено, јесте свакако тестирање резервних копија. У великом броју случајева оне због одређених проблема, као што су недостатак меморије на диску или прекид процеса копирања, постају неупотребљиве. Примјењује се аутоматска провјера исправности, али често се то обавља и ручно (Crighton, I. P. 2001). За организацију је од великог значаја исправност саме резервне копије или лог фајла који се креира. Процењује се да 60% резервних копија података није правилно до краја одрађено, а око 50% покушаја да се ти подаци рестаурирају заврши неуспјешно (истраживање организације Gartner). Када је ријеч о самој техници чувања података, *backup* у облаку (eng. cloud) привлачи највише пажње. Јако је погодан за мала и средња предузећа јер не изискује куповину хардвера, а плаћање се врши на мјесечном нивоу. Сву одговорност за надоградњу и чување података преузима пружаоц услуге. Такође, обезбијеђена је и подршка уколико дође до проблема приликом самих операција. Интернет веза је предуслов који мора бити испуњен, како би сам процес копирања и приступа подацима био могућ и довољно брз.

Ревизијом пословних информационих система, односно база података, врши се контрола тренутног стања саме базе, као и креирања њених резервних копија. Уколико су процедуре правилно успостављене, онда се провјерава да ли су оне испоштоване. Могуће је кориговати и саме процедуре уколико се установи да нису адекватно постављене или да уопште нису ни донешене. Иако неопходно свакој организацији, ово је примјењено само у пракси великих компанија, чији сектор информационих технологија има велики број запослених и широк опсег радних задатака.

Важна компонента успостављања овог процеса је свакако сарадња свих сектора, укључујући и топ менаџмент саме компаније који мора бити информисан о значају константне доступности података. Сваки појединачни сектор захтијева различите врсте података, који користи у току свог редовног пословања, те је с тога потребно обавијестити руководиоце и упутити их на правила чувања података. Процес доношења одлука зависи од података којима компанија располаже и њихове доступности. Било који отпор приликом имплементације самог система за креирање резервних копија база података може да изазове застоје у пословању. На нашем подручју, првенствено неинформисаност топ менаџмента представља проблем приликом планирања

инвестиција за овај пословни подухват и често се приоритет ових операција погрешно процијени и стави у други план. Тек када дође до оштећења, у том случају се спозна величина проблема, али је често касно за дјеловање. Пословне организације у сјеверном и источном дијелу Босне и Херцеговине, као географског подручја, које је често погођено поплавама као елементарном непогодом, у свој *backup* систем морају да имплементирају и чување података на другој локацији, која мора бити удаљена од примарне базе минимално 15 километара. Анализом плавног подручја може да се установи на ком терену би било погодно држати резервне копије података, а да не буду угрожене истим таласом елементарне непогоде. Основни утицај резервне копије базе података на саму организацију односи се на успостављање сигурности да је у сваком тренутку могуће складиштење информација и обезбијеђена њихова доступност, а да се самим тим пословни процеси обављају неометано и у складу са планом.

2. Посљедице отказа базе података и утицај на континуитет пословања

Дјеловањем природних непогода, кваром рачунарске опреме, злоупотребом података, ненамјерним брисањем или осталим сличним радњама, може доћи до прелаза оперативне базе у њено неупотребљиво стање. Тада она не може да испоручи податке које корисник захтијева, али истовремено нови подаци не могу да буду похрањени у њу. На примјер, уколико дође до прекида напајања електричном енергијом, рачун није могуће прокуцати кроз касу, али и истовремено у базу због њене недоступности. Када дође до оштећења базе, сектор информационих технологија рјешава проблем рестаурирајући базу и омогућавајући да се пословни процес врати у нормалу. Из тог разлога резервна копија мора да се врати у оперативну без потешкоћа, па је потребно подесити аутоматску провјеру валидности *backup* фајлова или у одговарајућем периоду ручно провјерити исправност.

Постоје четири ситуације када дође до отказа базе података:

- Уколико компанија посједује најажурнију верзију базе и њеним опоравком администратор је врати у оперативно стање без потребе за додатним корекцијама.
- Када компанија посједује резервну копију базе, али у верзији која није најажурнија. У зависности од природе посла, такве базе се могу вратити у оперативно стање ручним уносом недостајућих података (нпр. уколико постоји документација која прати сваку промјену у пословном процесу која се догоди).
- Када компанија посједује резервну копију базе података, али она због застарјелости не одговара процесу опоравка.
- Уколико компанија уопште не посједује резервну копију базе података.

Сваки радни сат који се проведе у ручном уносу недостајућих података, одузет је од редовних пословних активности и нема користи за компанију. Из тог разлога је неопходно што чешће правити резервне копије база података. За то

вријеме, пословне активности у великом броју случајева стагнирају, што директно утиче на приходе предузећа. Уколико се компанија бави трговином, сваки дан у којем нема приходовања смањује потенцијални пословни добитак. Нарочито уколико се ради о организованој распродаји или сезонској продаји, када се остварује највећи промет. Према истраживању, 93% компанија које изгубе своје податке у трајању од 10 дана сусрећу се са банкротством у току једне године, а 50% тих компанија непосредно након губитка базе (National Archives & Records Administration in Washington DC.). Са друге стране, законска регулатива приморава компаније да увијек презентују најсвјежије податке. Уколико је то изостављено, могу се врло лако суочити са правним посљедицама. Ако је уговором одређен рок за обављање одговарајућих обавеза према пословним партнерима, сваки застој у раду информационог система онемогућава да се оне обаве у предвиђеном року. Посљедице тога могу да буду пенали, које предузеће мора да исплати пословним партнерима.

Интерни подаци који служе за обављање пословних процеса унутар предузећа (као што су исплате плата, продужавање уговора запослених и сл.), такође имају утицаја на континуитет пословања. Спорије одвијање ових процеса директно се одражава на пословне активности, а кроз њих и на финансијски резултат. Уколико су базе потака о потрошачима недоступне у одговарајућим моментима или уништене, CRM (eng. Customer relation-ship management) систем неће моћи да функционише, како би пословање предузећа прилагодио жељама потрошача. Директан контакт са купцима био би онемогућен, као и приступ информацијама који говоре о њиховим преференцијама. Уколико не би било могуће повратити такве информације, улагање компаније у CRM систем би било неисплативо и утицало би на пословни резултат преко смањења продаје. Компаније које имају имплементиран систем за однос са потрошачима, углавном су свјесне посљедица које носи ризик од оштећења базе, те с тога инвестирају и у креирање резервних копија. Ако сектор информационих технологија није у могућности да поврати базу, постоје специјализоване агенције које се баве рестаурацијом података. Њихове услуге имају јако високу цијену и те их је због тога тешко приуштити. Веома је важно да предузеће увијек има доступне и ажурне базе података, а у случају њихових оштећења да их брзим реаговањем поново доведе у оперативно стање, јер сваки застој у похрањивању и читавању података директно утиче на пословни резултат. Тада се пословни процеси одвијају успорено или са прекидом, реметећи континуитет пословања, па чак проузрокујући и гашење компанија.

3. Оправданост инвестирања у креирање резервних копија база података

Као главна препрека у имплементирању система за креирање резервних копија база података јавља се отпорност према инвестирању у овај процес од стране менаџмента. Разлог томе је често неупућеност у могуће посљедице, које могу да се реализују уколико дође до непредвиђеног догађаја. Може се закључити да

оваква улагања представљају неминовност и потребу како би се обезбиједио континуитет пословања.

У развијеним привредама предузећа су свјесна овог проблема и издвајају адекватна новчана средства за имплементацију наведеног поступка, као и едукацију својих запослених. На нашем подручју, веома мали број компанија издваја новчана средства у ову сврху.

Наведени проблеми који могу да се јаве уколико дође до отказа базе, изазивају много веће финансијске губитке у односу на новчана средства која је потребно издвојити за имплементацију креирања резервних копија база података. У зависности од врсте *backup*-а, инвестирање може да обухвати куповину хардверске опреме, софтвера, па и ангажовање спољних сарадника за обављање процеса имплементације, уколико компанија не посједује стручни кадар. *Backup* у облаку не захтијева куповину хардвера, него се плаћа на мјесечном нивоу у зависности од искоришћености. За велики број малих и средњих предузећа ово представља најефикасније рјешење. Око 70% малих и средњих предузећа која доживе већи губитак података престаје са пословањем (DTI/Price Waterhouse Coopers). Према истраживању из 2014. године, открива да им је отказ базе података произвео губитак у просјеку од 50.000 до 5.000.000 долара (Disaster Recovery Preparedness Council). У појединим земљама, законска регулатива предвиђа казне за губитак података, које се крећу до 5% оствареног прихода компаније.

На тај начин се предузеће може сусрести и са финансијским посљедицама проузрокованим дејством правне природе. Када дође до отказа базе, компаније, прије свега, не могу да обављају све или дио својих редовних пословних активности попут продаје, набавке, производње, регулисања обавеза и слично. Уколико је потребно поново похранити базу са одговарајућим групама података, искориштено радно вријеме за ову врсту активности се одузима од обављања редовних послова. Тако да утрошен рад запослених за обављање редовних пословних активности бива испод очекиваног нивоа за тај временски период. Најгори сценарио представља, прије свега, немогућност опоравка пословне организације што у крајњој ситуацији доводи до престанка пословања.

Предузеће, такође може да се сусретне и са правним санкцијама. Улагање у систем за креирање резервне копије база података за мала и средња предузећа зависи од количине података коју треба *backupovati* као и од врсте *backup*-а који се примјењује. Основне инвестиције су у сервер, дискове или простор у облаку који се закупује. Чак је могуће подесити самосталан виртуелни сервер на постојећем физичком, тако да нема потребе за набавку новог сервера. Софтверска рјешења немају високу цијену и могуће их је самостално креирати уколико компанија посједује адекватан стручни кадар. Комплетан систем се аутоматизује укључујући и контролу. Цијена куповине дискова уколико се посједује сервер кошта до пар стотина конвертибилних марака, што је мала

цијена за постизање адекватне сигурности. Простор у облаку такође се плаћа у зависности од простора који се користи. У табели 1. су наведене цијене на мјесечном нивоу неколико пружаоца услуга у облаку.

Табела 1. Цијена *cloud* простора на мјесечном нивоу у конвертибилним маркама (ВМ)

Назив пружаоца услуге	Меморијски простор	Цијена на мјесечном нивоу
Sync	500 GB	7,12 KM
PCloud	500 GB	6,96 KM
Hetzner	500 GB	9,55 KM
OneDrive	1 TB	12,2 KM
GoogleDrive	1 TB	17,43 KM
Tresorit	1 TB	19,5 KM

Извор: <https://www.ictbusiness.info/internet>

Довољан меморијски простор, у сврху похране резервних копија база податка, за мала и средња предузећа је углавном до 500 GB. На годишњем нивоу ови трошкови износе од 85,5 KM, па навише, у зависности од потреба пословне организације. Цијеновно посматрано, ови трошкови су занемарљиви у односу на сигурност, коју резервне копије базе података пружају у пословању.

ЗАКЉУЧАК

Циљ управљања подацима је да у сваком тренутку располажемо оперативном и ажурном базом. Уколико дође до њеног отказа, посљедице могу да буду веома штетне за предузеће, доводећи чак и до престанка пословања. Нормалан ток пословања, раста и развоја стагнира или чак назадује уколико дође до наведене ситуације. Да би се ово избјегло, потребно је креирати резервне копије база података. Оне морају да буду прилагођене пословању предузећа и самим подацима којим предузеће манипулише.

Вријеме копирања, број копија, поставке сервера на удаљеним локацијама, *backup* у облаку, провјера валидности фајлова, само су неке од категорија које је потребно сагледати приликом његове имплементације. За ово је надлежан сектор информационих технологија и администратори база податка. Уколико компанија не посједује стручни кадар, увијек може ангажовати партнерске организације, које са баве пружањем оваквих услуга. Оне су често и савјетодавне, нарочито уколико се јави специфична ситуација у овој области.

Основни проблем је указати на важност посједовања резервних копија менаџменту или управним органима пословне организације. Посебна грана су предузетници и мала предузећа која често нису упућена у сам проблем. Одржавањем семинара или пословних презентација може се усмјерити на сам

проблем и предложити његово рјешење. Сарадња са осталим секторима у предузећу може да пружи допринос у имплементацији *backup*-а. Инвестирање у овакав подухват доноси користи, које су много веће у односу на саме трошкове. Циљ је омогућити да се пословање обавља неометано, односно без техничких проблема, што даље омогућава предузећу да се посвети планирању пословних потеза проматрајући тржишне прилике.

ЛИТЕРАТУРА

- [1] CARNet CERT., LS&S. (2006). *Osnove sigurnosnih kopija*. Zagreb: Nacionalno središte za sigurnost računalnih mreža i sustava,
- [2] Beeler Jr, D. E. (1999). *Real time backup system*. Washington, DC: U.S. Patent and Trademark Office
- [3] Crighton, I. P. (2001). *Data backup system*. Washington, DC: U.S. Patent and Trademark Office
- [4] Mehr, J. D., Murphy, E. E., Virk, N., & Sosnosky, L. M. (2015). *Hybrid distributed and cloud backup architecture*. Washington, DC: U.S. Patent and Trademark Office.
- [5] Dunham Scott R., (2001). *Virtual storage and block level direct access of secondary storage for recovery of backup data*. Washington, DC: Patent and Trademark Office
- [6] Kovačević Ž., (2018). *Modeliranje, implementacija i administracija baza podataka*. Zagreb: Tehničko veleučilište u Zagrebu
- [7] <https://www.unitrends.com/blog/what-are-the-consequences-of-data-loss> (pristupljeno sajtu 20.04.2019. god)
- [8] <https://consoltech.com/blog/10-common-causes-of-data-loss> (pristupljeno sajtu 21.04.2019. god)
- [9] <https://www.acronis.com/en-us/articles/data-backup-for-business> (pristupljeno sajtu 20.04.2019. god)
- [10] <https://www.itproportal.com/2016/04/22/a-third-of-businesses-dont-backup-crucial-data/> (pristupljeno sajtu 22.04.2019. god)
- [11] <https://www.ictbusiness.info/internet> (pristupljeno sajtu 19.04.2019. god)
- [12] <https://www.hetzner.com/cloud> (pristupljeno sajtu 19.04.2019. god)
- [13] <https://www.pcloud.com> (pristupljeno sajtu 20.04.2019. god)
- [14] <https://www.sync.com> (pristupljeno sajtu 20.04.2019. god)

SUMMARY

Information systems are necessary in modern business, and often they are crucial factor of competitive advantages. As a part of them, databases are one of the most important elements. They have to be available all the time for distribution and storage of data. Data loss is one of most dangerous problems in business. If that happens, business flow is interrupted and company has to solve those problems before they continue to reach business goals.

Consequences of data loss and database damage can be very serious. Some of them even cause bankrupt. By National Archives & Records Administration in Washington

research, 93% of business which experience data loss more than 10 days due data loss, face with bankruptcy. About 43% of them never reopen and 51% close within two years. Law regulates manipulation of data and data breaching can cause financial losses. To avoid all of these problems, database *backup* is must have solution. No matter how big is the company, they have to implement *backup* system in their IT strategy. Collaboration IT sector with other sectors in the company can contribute to the implementation of *backup*. If they do not have IT sector, they can engage it companies to help them. Price of implementing this system is very low comparing to consequences if data loss happens.

Depending on the type of the *backup*, the investment may include the purchase of hardware, software, or the engagement of external associates to carry out the implementation process if the company does not have a professional staff. *Backup* in the cloud does not require purchase of the hardware, but it's being paid on a monthly basis, depending on the utilization.

This is the most effective solution for a large number of small and medium-sized companies. Top level management has to realise problem of data loss and consider investing in *backup* system. Seminars or business presentations, can point to the problem itself and propose its solution.

The goal is to enable the business to be done smoothly, without any technical problems, which further allows the company to devote itself to the planning of business moves by observing market opportunities.