UDK: 343.137:347.734:061.1
Biblid 1451-3188, 10 (2011)
Год X, бр. 35–36, стр. 214–223
Изворни научни рад

Др Владимир УРОШЕВИЋ[1]

ОДГОВОР ЕВРОПСКЕ УНИЈЕ И САВЕТА ЕВРОПЕ НА ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ И БАНКАРСКО ПОСЛОВАЊЕ У *CLOUD COMPUTING* ОКРУЖЕЊУ

ABSTRACT

Cloud computing can enable banks to reuse IT resources more efficiently - whether they are purchased up - front or rented without any long term commitment. However, cloud computing is much more than simply renting servers and storage on-demand to reduce infrastructure costs. In fact, the cloud offers a host of opportunities for banks to build a more flexible, nimble and customer-centric business model that can drive profitable growth. At the same time, cloud computing raises many issues at many levels and it might constitute a real danger for users and data subjects, especially in the field of high-tech crime.

Key words: Cloud computing, high-tech crime, financial banks.

I) СВРХА

Окружење *cloud computing-a*, представља много значајнију појаву од самог изнајмљивања сервера или рачунарских ресурса за складиштење података на захтев корисника, и није само техничко питање или тема, као што се до скора мислило у стручној и научној јавности. Као информатичко окружење, *cloud computing* нуди могућност банкама да изграде флексибилнији, бржи пословни модел који је посвећен корисницима услуга и који може довести до повећања профита. Због ове чињенице *cloud computing* окружење у пословању треба да буде појава коју ће доносиоци одлука у банкама који нису *IT* експерти разумети и ценити као могућност за побољшање и унапређење рада у банкама. Стални пораст употребе ових

[1] Министарство унутрашњих послова Републике Србије.

сервиса и значај који овај концепт има потиче из чињенице да се уклапа у неколико приоритета модерног пословања: омогућава задовољавање потреба пословања на флексибилним основама и помаже у исплатљивом одговору на променљиве услове пословања и захтеве који се постављају компанијама у смислу сталне надоградње IT ресурса. Банке као финансијске институције које највише послују у области платног промета посебно су угрожене од стране криминалаца из области високотехнолошког криминала. Пошто употреба *cloud computing*-а са собом носи знатну редукцију трошкова пословања и низ других предности у односу на класичну *IT* структуру овој теми је у научној и стручној јавности посвећена посебна пажња. Поред Конвенције о високотехнолошком криминалу (CETS No.: 185) који је Савет Европе донео у Будимпешти 23.11.2001. године а која се бави питањима везаним за појаву високотехнолошког криминала и даје препоруке за његово спречавање и сузбијање и сл., Савет Европе је теми безбедности употребе *cloud computing*-а посветио значајну пажњу у оквиру пројекта под називом: "*Project on Cybercrime"* у оквиру кога је дана 5. марта 2010. године објављена студија под називом "*Cloud computing and its implications on data protection*" која не представља званичан став Савета Европе али значајно указује на проблеме у овој области.[2] Европска агенција за сигурност рачунарских мрежа и информација – *The European Network and Information Security Agency (ENISA)* такође је у току 2009. године објавила извештај под називом "*Cloud computing – Benefits, risks and recommendations for information security*" у коме се између осталог дају и одређене препоруке за заштиту система, као и правне препоруке Европској комисији. [3]

II) ПОЈАМ *CLOUD COMPUTING*-а СА АСПЕКТА УПОТРЕБЕ У БАНКАРСКОМ ПОСЛОВАЊУ

Cloud computing се најчешће дефинише као динамичко обезбеђивање ИТ ресурса као што су хардвери, софтвери или усуге од стране трећих лица путем рачунарских мрежа. Израз "*cloud computing*" је релативно новијег датума, али поједини елементи овог концепта, као што су нпр. виртуелне

[2] "Cloud computing and its implications on data protection", Савет Европе, објављено 05.03.2010. Интернет извор: www.coe.int/t/dghl/cooperation/.../2079_reps_IF10_yvespoullet1b.pdf доступно 05.04.2011. године.

[3] "Cloud Computing – Benefits, risks and recommendations for information security", The European Network and Information Security Agency (ENISA), објављено 20.11.2009. Интернет извор: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, доступно дана 05.03.2011. године.

машине, у употреби су више деценија. Оно што *cloud computing* чини стварно новом појавом су повећање употребе Интернет технологија, виртуелизација, стандардизација хардверске опреме и софтвери типа *open source* (отвореног извора, слободни за употребу од стране корисника без наплате). Главни узроци коришћења *cloud computing*-а су успеси које су употребом овог модела постигле велике компаније као што су *Google*, *Amazon* и *Microsoft*. На овим платформама велике компаније изградиле су моћне сервисе за Интернет претраге, електронску трговину, социјалне мреже и друге форме Интернет сервиса.

Главне карактеристике *cloud computing*-а су следеће:

– Потребна су веома мала улагања а понекад она и нису неопходна пошто постоје бесплатне услуге које нуде различите компаније које се баве пружањем ових услуга;
– плаћање по принципу употребе сервиса од стране корисника;
– брза доступност и примена сервиса;
– нижи оперативни трошкови;
– прилагодљивост потребама корисника и могућност сталне надоградње и побољшања услуга.

Cloud computing појављује се у две форме тзв. облака: приватни и јавни. За велики број банака први важнији корак употребе ових платформи био је везан за форму „приватни облак". Ова форма настаје у оквиру компанијских ресурса као нпр. у центрима података и направљена је за сврхе обезбеђивања и дистрибуције виртуелних апликација, инфраструктуре и комуникационих сервиса за употребу у компанијама. Овакви сервиси имају еластичну структуру и широку примену на нивоу услуга. За разлику од „приватног облака" други облик под називом „јавни облак" има такву форму да центри података могу да буду одржавани од треће стране – провајдера преко пружања ИТ услуга путем мреже. Такви сервиси су нпр. "*software-as-a-service*" (софтвер као услуга), *platform-as-a-service* (платформа као услуга) и *infrastructure-as-a-service* (инфраструктура као услуга). Сви ови модели су направљени по моделу виртуелизације заснованим на моделу наплате у зависности од количине услуга ових сервиса. Ови модели све се више користе и представљају важне елементе нове генерације ИТ ресурса. Стални пораст употребе ових сервиса и значај који овај концепт има потиче из чињенице да се уклапа у неколико приоритета модерног пословања: омогућава задовољавање потреба пословања на флексибилним основама, и помаже у исплатљивом одговору на променљиве услове пословања и захтеве

који се постављају пред компанијама у смислу сталне надоградње IT ресурса. Комбиновањем виртуелизације и неке од информационих архитектура пословних модела по принципу плаћања по употреби од стране корисника, cloud computing представља нову појаву која ће значајно утицати на начин на који ће бити обезбеђиване, достављане и одржаване компоненте ИТ стуктуре као што су платформа, апликације и пословни процеси.

Једна од најбитнијих користи које су настале појавом *cloud computing*-а посебно у кратким роковима јесу нижи трошкови. Употреба *cloud computing*-а такође може значајно смањити време потребно да банке избаце нове апликације. Уштеде које настају употербом *cloud computing*-а, руководиоци банке не би требало да схвате као просту чињеницу, већ је потребно да на основу постојећих уштеда на различитим студијама покушају да установе који ће им модел уштедети највише новца. Требало би да сагледају критичке студије случаја употребе ових сервиса, пре него што почну да рачунају уштеду која ће настати употребом нових модела као што је *cloud computing.* Потребно је да се у фазама примене *cloud computing*-а врши константна евалуација од стране руководилаца и финансијских служби банке у вези са трошковима одржавања и употребе и уштеде која настаје применом модела. Само овакав приступ може да укаже на обим уштеде. Постоји велики број фактора који играју значајну улогу у томе колико банка може уштедети употребом овог модела:

– Усвајање стандарда који чине размену и кретање података лакшим,
– коришћење правила да сервис одговара одређеној сврси, као и нивоу услуга колико је то могуће, а у складу са захтевима банке за дату апликацију,
– примена заштите приватности података на одговарајући начин, а са друге стране стандардизација различитих нивоа употребе што је више могуће,
– превазилажење питања власништва над подацима од стране различитих одељења у банци ради њиховог смештања у заједнички „облак”,
– вођење рачуна о томе да се одржи флексибилност набавки како би се избегло фиксирање за одређеног добављача.

Поред тога што се употребом ових сервиса штеди новац постоји и много других разлога зашто је употреба *cloud computing*-а рентабилна. Постоје четири начина на који банке могу да употребе *cloud computing* сервисе како би направиле нове пословне моделе који ће бити

оријентисани ка клијентима, и који ће бити бржи и ефикаснији. Такође би могли да утичу на то да банке стварају већи профит.[4]

Први начин на који *cloud computing* може као окружење да утиче на развој банке је што се његовом употребом постиже стварање флексибилног система у окружењу које омогућава бржу размену података без беспотребних задржавања у току употребе и размене података у систему. Стварање *cloud computing* окружења које је оријентисано ка клијентима банке представља други начин којим банке могу да утичу на побољшање свог пословања. Употребом *cloud computing*-а привлаче се нови и задржавају стари клијенти кроз њихово веће ангажовање и одговарајуће корисничко искуство које им може омогућити лакши приступ и коришћење банкарских производа и услуга. У *cloud computing*-у олакшана је и употреба апликација које се могу успостављати и употребљавати у зависности од жеље корисника. Уједно, то је и трећи начин на који би банке могле унапредити своје пословање овим моделом. Употреба платформе као услуге веома је поједностављена и отворена за примену иновација. Уместо застарелих и ригидних система данас је применом овог модела охрабрена употребе модерних апликација заснованих на врсти података. Као четврти разлог за употребу *cloud computing* окружења може се навести и побољшање аналитичких перформанси система у банкама. Многе компаније стално траже иновативне начине да побољшају интеракцију са клијентима и омогуће бољи приступ производима или услугама. Ипак, многе компаније немају аналитичке могућности, најчешће зато што им недостају потребни ресурси или имају проблема са пријемом, интегрисањем и складиштењем огромне количине података. Као што је већ наведено, у *cloud computing* окружењу трошкови за овакве врсте послова знатно су умањени и олакшани у смислу приступа од стране корисника па је њихова примена економски оправдана због уштеде у новцу, времену и ресурсима.

III) РИЗИЦИ И ПРЕТЊЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА БАНКАРСКОМ ПОСЛОВАЊУ У *CLOUD COMPUTING* ОКРУЖЕЊУ

Употребом савремене технологије технолошки аспекти савременог, реалног света криминала и криминалне активности које се одвијају у њему,

[4] „Banking on the Cloud“, Accenture Ltd, објављено 25.03.2010. године, Интернет извор: www.accenture.com/.../PDF/Accenture_Banking_Cloud_Computing.pdf, доступно 06.04.2011. године.

представљају шири и веома комплексан друштвени проблем. Комерцијализација високотехнолошког криминала више се не односи само на трговину подацима, као што је то био случај у прошлости када су криминалци нудили осетљиве пословне податке најбољем понуђачу на Интернету, већ на пружање услуге којом се обухвата целокупан напад и процес инфекције рачунара, након чега се корисницима пружају филтрирани подаци који настају као „плод" целокупног напада. Важно је схватити да су теме везане за сигурност употребе *cloud computing*-а углавном новијег датума али да се најчешће ради о ризицима и претњама који су већ познати, с тим што у овом, новом окружењу постају све озбиљнији. Као пример, може се навести чињеница да су напади на виртуелне машине на Интернету и на Интернет *Web* сервисе постојали много пре појаве *cloud computing*-а, да су многе од ових тема и раније разматране у научној и стручној јавности, те да за њих већ постоје одређена решења.[5] Организоване криминалне групе данас се понашају по истим принципима као легалне организације, проналазе „тржишне" могућности и шире своје „пословне видике" помоћу технолошких иновација и присуства на Интернету (на пример постављањем својих Интернет сајтова, реклама на Фејсбуку и сл.), а све то раде у циљу стицања веће финансијске добити. Организоване криминалне групе из области високотехнолошког криминала схватају суштину бизнис модела на Интернету, знају како да у тој области функционишу и како да избегну кривично гоњење.[6] Чињеница је да је *cloud computing* идеалан простор за деловање криминалаца из области високотехнолошког криминала. У суштини, у оквиру „облака" Интернет саобраћај се прикупља на централизованој локацији, пружајући на тај начин криминалцима прилику да постигну критичну масу ресурса за нападе које желе да изведу. И док сви размишљају како да у таквој средини направе безбедно окружење за рад, прилика за напад од стране криминалаца и организованих криминалних група остаје отворена. Те тврдње засноване су на чињеници и идеји да што је више циљева за напад утолико постоји већа шанса да тај напад буде успешан. Заиста, скуп ботова тј. заражених рачунара формира најчешће

[5] Richard C., Philippe G., M., Ryusuke M., Jesus M., Elaine S., Jessica S., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", *CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security*, ACM New York, САД, 2009, стр. 85–90.

[6] Владимир Урошевић, „Коришћење Интернет сервиса који пружају злоћудне програме као услугу при извршењу кривичних дела из области високотехнолошког криминала у Републици Србији", *Безбедност*, Министарство унутрашњих послова Републике Србије, Београд, 2011, стр. 177–190.

добру мрежу рачунарских ресурса криминалцима, који потом своје услуге продају на тржишту преко Интернет сервиса на којима нуде „злоћудне програме као услугу" (CaaS).[7] Софтверски пакети „злоћудних програма" (на енглеском *crimeware toolkits*) почињу да се појављују као део услуге "*Software-as-a-Service*". Побољшани економски ефекти и размере које *cloud computing* и SaaS модел доносе у пословању такође су повећале и број могућности које криминалци из области високотехнолошког криминала имају по питању нове рањивости у којој криминалци не обављају директно послове који се односе на податке који су компромитовани. Овај тренд представља нове изазове за провајдере у погледу безбедности софтвера који пружају такве услуге.[8]

Уколико се сервиси одржавају од стране трећих лица онда организација која користи тај сервис губи одређену контролу над сигурношћу својих података. Банке које користе *cloud computing* окружење за веома озбиљне функције као што је нпр. пословање са платним и кредитним картицама *online* банкарство и сл., морају у свом пословању посебно да обрате пажњу на следећа кључна питања употребе *cloud computing*-а:

– Да ли су подаци у „облаку" и код провајдера довољно безбедни;
– да ли се чува приватност података који се налазе у „облаку" и код провајдера;
– да ли други клијенти одређеног провајдера чије се услуге користе такође могу да прићу подацима банке;
– како све претходне ставке утичу на усклађивање потреба банке;
– шта ако постоје безбедоносни пропусти који доводе до угрожавања података банке;
– да ли се врши складиштење података, њихово чување и сл. онолико дуго колико је то банци потребно?

Наведена питања банке морају постављати константно, ради флексибилног одговора на све врсте претњи по безбедност њиховог пословања и података који су им од виталног значаја у раду.

---

[7] „Cloud computing sets perfect scene for cyber crime", објављено 28.07.2010. Интернет: http://www.asiacloudforum.com/content/cloud-computing-sets-perfect-scene-cyber-crime доступно 04.02.2011.

[8] ASIS International Councils: the Information Technology Security Council and the Physical Security Council (2010): Cloud Computing and Software as a Service (SaaS): An Overview for Security Professionals, ASIS International, SAD, стр. 1–49.

Европска агенција за сигурност рачунарских мрежа и информација – *The European Network and Information Security Agency (ENISA)* у извештају под називом "*Cloud computing – Benefits, risks and recommendations for information security*" у делу под називом Правне препоруке указује на проблеме везане за правна питања у вези са склапањем уговора са провајдерима. Ови уговори нису стандардни као код класичних Интернет услуга, и у великој мери зависе од природе самог *cloud computing* као појаве. Уговорне стране би требало да обрате пажњу на њихова права али и обавезе у случају нарушавања сигурности, преноса података, промене врсте посла у току реализације и приступа подацима од стране полиције. Пошто се у овој врсти окружења често налазе подаци интерног карактера, у овом извештају се наводи и да је потребно да се размотре начини ограничења приступа на различитим нивоима. Управо из наведених разлога у овим препорукама се наводи да би уговорне стране посебно требало да воде рачуна о безбедоносним ризицима. Такође су дате и правне препоруке за Европску комисију да се проуче или разјасне следеће ставке:

– Питања везана за Директиву о заштити података и препорука из чл. 29 о заштити података;
– обавеза провајдера *cloud computing* услуга да обавесте клијенте о нарушавању безбедности њихових података и безбедносним пропустима;
– како се обавезе изузећа за посреднике које произилазе из Директиве о електронској трговини из чланова од 12 до 15 примењују на провајдере који пружају ове услуге;
– како да се на најбољи могући начин подржи минимум стандарда заштите и шеме за сертификацију приватности која је заједничка за све државе чланице Европске уније.

IV) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Република Србија је чланица Савета Европе и држава која је ратификовала Конвенцију о високотехнолошком криминалу (CETS No.: 185) који је Савет Европе донео у Будимпешти 23.11.2001. године, а која се бави питањима везаним за појаву високотехнолошког криминала и даје препоруке за његово спречавање и сузбијање и сл. У нашој кривично-правној регулативи имплементиране су препоруке из ове Конвенције. У оквиру Министарства унутрашњих послова Републике Србије формирано је Одељење за борбу против високотехнолошког криминала, а у оквиру Вишег јавног тужилаштва Одељење за борбу против вишег јавног

тужилаштва које са организационог аспекта у својој надлежности врше преткривичну истрагу у вези са овим кривичним делима ради њиховог откривања и расветљавања. Управо из наведених разлога од кључног је значаја да се у домаћој литератури обрати посебна пажња на чињеницу да је Савет Европе теми безбедности употребе *cloud computing*-а посветио значајну пажњу у оквиру пројекта под називом: *Project on Cybercrime* у оквиру кога је 5. марта 2010. године објављена студија под називом "*Cloud computing and its implications on data* protection" која не представља званичан став Савета Европе, али значајно указује на проблеме у овој области. Такође је важно и да је Европска агенција за сигурност рачунарских мрежа и информација - The European Network and Information Security Agency (ENISA) у току 2009. године објавила извештај под називом "Cloud computing – Benefits, risks and recommendations for information security" у коме се између осталог дају и одређене препоруке за заштиту система, као и правне препоруке Европској комисији.

Угроженост финансијског сектора високотехнолошким криминалом, а посебно банака и њихових клијената, као тема у Републици Србији требала би да има посебан значај због безбедности економског система државе. Чињеница је да *cloud computing* представља окружење у коме се рад банака у знатној мери унапређује и да се захваљујући овом окружењу знатно смањују трошкови за набавку и одржавање хардверске опреме као и софтвера и других ИТ ресурса потребних за обављање банкарских послова. Међутим, потребно је јасно указати и на чињеницу да би ова област морала да се регулише на правилан начин како би се подаци заштитили од утицаја извршилаца кривичних дела из области високотехнолошког криминала којима је *cloud computing* донео ново подручје за деловање. Уколико се то не учини на адекватан начин угрожавање банкарског сектора тј. банака које користе *cloud computing* окружење у свом пословању могло би да буде све чешће, а последице све опасније. Врло чест мотив криминалаца из области високотехнолошког криминала – стицање противправне имовинске користи – посебно је изражен у области злоупотреба и фалсификовања платних картица, електронске трговине и *online* банкарства па је познавање начина функционисања банкарског пословања у овом окружењу и ризика и претњи који се у њему скривају од виталног значаја за државне органе Републике Србије, банке које послују у овом окружењу али и за клијенте банака – предузећа, физичка лица и друге.

V) ИЗВОРИ

- „Конвенције о високотехнолошком криминалу (CETS No.: 185)", Савет Европе, Будимпешта, 23.11.2001.
- Richard C., Philippe G., M., Ryusuke M., Jesus M., Elaine S., Jessica S., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", *CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security*, ACM New York, САД, 2009, стр. 85–90.
- Владимир Урошевић, „Коришћење Интернет сервиса који пружају злоћудне програме као услугу при извршењу кривичних дела из области високо-технолошког криминала у Републици Србији", *Безбедност*, Министарство унутрашњих послова Републике Србије, Београд, 2011, стр. 177–190.
- ASIS International Councils: the Information Technology Security Council and the Physical Security Council (2010): Cloud computing and Software as a Service (SaaS): An Overview for Security Professionals, ASIS International, SAD, стр. 1–49.
- "Cloud computing and its implications on data protection", Савет Европе, објављено 05.03.2010. Интернет извор: www.coe.int/t/dghl/cooperation/.../2079_reps_IF10_yvespoullet1b.pdf доступно 05.04.2011. године.
- "Cloud computing – Benefits, risks and recommendations for information security" The European Network and Information Security Agency (ENISA), објављено 20.11.2009. Интернет извор: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, доступно дана 05. 03. 2011. године.
- "Banking on the Cloud" Accenture Ltd, објављено 25.03.2010. године. Интернет извор: www.accenture.com/.../PDF/Accenture_Banking_Cloud_Computing.pdf, доступно 06.04.2011. године.