Проблеми на подготовката за преминаване към Cloud computing за нуждите на информационното обслужване на административната структура на университетите в България

Биляна Стойнова, Кънчо Иванов

Abstract*: *Problems of preparation for switching to Cloud computing for the information service of the administrative structure of universities in Bulgaria: *In this paper, we will review what the cloud computing infrastructure will provide in the educational arena, especially in the universities where the use of computers are more intensive and what can be done to increase the benefits of common applications for students and teachers. This paper examines the broad topic of data security in the cloud computing along with data protection methods and approaches.*

***Key words**: Cloud computing, Data security, Cloud security, Universities, Virtualization.*

ВЪВЕДЕНИЕ

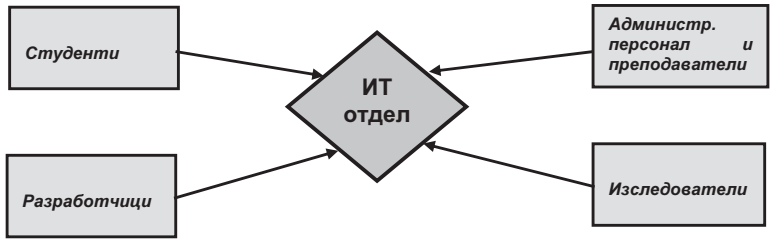
Една от най - новите тенденции в IT индустрията е концепцията на "облачните изчисления" или Cloud Computing. Важна роля в тази концепция заема виртуализацията. С нейна помощ може да се структурира ефективен "облак" т.е. създаване на изолирани виртуални групи потребители, които реализират отделни IT услуги, а също така и разделение на ресурсите на логическо ниво за по-гъвкаво управление. Основните й характеристики са приемлива стойност, ефективно управление на ресурсите и гарантирано ниво на обслужване на потребителите. Cloud Computing представлява набор от апаратни ресурси или IT услуги, които се представят на потребителите по изискване от страната на глобална (External Cloud) или локална (Internal Cloud) мрежа по такъв начин, че потребителите на IT ресурси не се замислят за характера им и мястото, където те се случват. Internal Cloud е Cloud computing модел за услуга, която се осъществява чрез IT ресурсите на дадена организация [7]. В Internal Cloud се прилагат механизми за виртуализация, споделен storage и мрежови ресурси за улесняване на пълен контрол над "облачната" среда в организацията. Internal Cloud предоставя компютри, съхранение и софтуерни услуги на всеки отдел в рамките на организацията. Вътрешният облак (Internal Cloud) предоставя следните предимства: пълна Cloud сигурност; намалени разходи за инфраструктура; намалени изисквания към хардуера. Концепцията Internal Cloud е подобна на изчислителната технология Private Cloud, когато се използва в рамките на една организация. Разликата е в това, че един частен облак (Private Cloud) може да се отнася за специализираните ресурси до трета страна - доставчик, докато вътрешният облак (Internal Cloud) използва собствената си инфраструктура. Поради тази причина е препоръчително за преминаването към глобална (External Cloud) във Висшите учебни заведения в България, които все още не са се възползвали от тази технология, да се подходи чрез предварително експериментиране в локална (Internal Cloud) мрежа. Целта е обучаване на персонала за работа в новата среда и придобиване на увереност в удобствата и сигурността на съответните университетски администрации, преподаватели и студенти.

Терминът Cloud computing съвместява понятия като софтуер като услуга (software as a service, SaaS), инфраструктура като услуга (infrastructure as a service, IaaS), платформа като услуга (platform as a service, PaaS) и други съвременни технологии, които под формата на онлайн бизнес приложения, достъпни през уеб браузър задоволяват изчислителни потребности,докато съхраняват софтуера и потребителските данни на свои сървъри [5].

Благодарение на Cloud Computing и виртуализацията на изчислителните ресурси, се очаква да се развият понятия "сървър" и "система за управление на бази от данни" до термини като "приложение" (application) и "услуга" (service).

ПОДГОТОВКАТА ЗА ПРЕМИНАВАНЕ КЪМ CLOUD COMPUTING НА УНИВЕРСИТЕТИТЕ В БЪЛГАРИЯ

В настоящият момент всички административни и образователни дейности в даден ВУЗ се контролират от отделна структура, занимаваща се с информационното осигуряване и обслужване на всички звена и потребители (фиг. 1) [1].

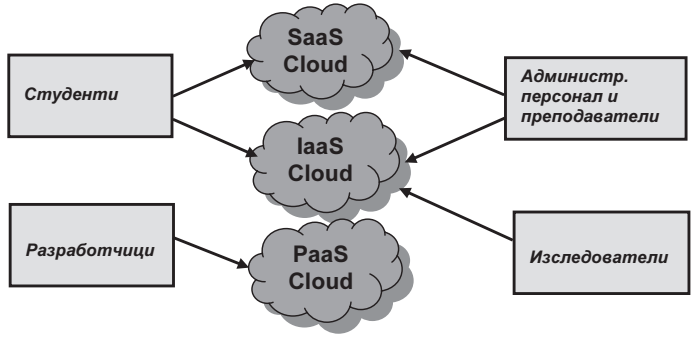


Фигура 1. Структура на основните потребители на ИТ услуги във ВУЗ

Cloud computing е технология, която се приема от много организации с динамичната си възможност за надграждане и използването на виртуализирани ресурси като услуга чрез Интернет. Тя вероятно ще има значително влияние върху образователната среда в бъдеще. Cloud computing е отлична алтернатива за висши учебни заведения (които обикновено са с бюджетен недостиг), за да работи на техните информационни системи ефективно, без да се изразходват повече средства за компютри и мрежови устройства. Университетите могат да се възползват от наличните cloud -базирани приложения, предлагани от доставчиците на услуги и това да позволи на техните потребители (студенти, преподаватели, административен персонал и др.) да извършват обичайните си академични задачи [3]. Новата технология позволява бързо и навременно получаване на финансовите отчети, автоматична обработка на данните и най-важното извършва насрещен контрол на информацията (фиг.2).

ХАРАКТЕРИСТИКИ НА CLOUD COMPUTING

-Utility Computing. Под това понятие се разбира употребата на IT ресурсите като нещо необходимо и използвано ежедневно [8] (фиг. 2).



Фигура 2. Структура на основните потребители на ИТ услуги във ВУЗ, използващи Cloud computing

-Software as a Service (SaaS). Това е фундаментално понятие на Cloud Computing и предполага промяна в доставката на софтуера към потребителите, при

който те спират да го закупуват като готово или решение и започват да го използват от облака на база абонамент.

-Виртуализация. Благодарение на нея е възможно създаването на изолираните виртуални групи потребители, които реализират отделни IT услуги, а също така и разделение на ресурсите на логическо ниво за по-гъвкаво управление [9].

ПРЕДИМСТВА НА ВИРТУАЛИЗАЦИЯТА

Виртуализацията представлява софтуер, който разделя приложенията и услугите от физическата инфраструктура [10]. Всяка организация разполага с набор от възможности по отношение на това какво се прави с наличните приложения. Има възможност да се използват голям брой приложения на много по-малък брой сървъри и по този начин се спестяват финансови средства. С технологията по виртуализация може да се автоматизира доставката на приложения и услуги. В миналото би отнело часове, за да бъде стартирана дадено приложение, и месеци да бъде поръчан или закупен хардуер. С виртуализацията това се случва веднага и отнема минути. Времето за начало на използването на ценни услуги е много по-кратко. В същото време могат да се преместват приложения между дата центрове и в облака.

В миналото едно приложение беше свързано с един компютър. Сега виртуалните машини позволяват на един компютър да има много приложения, което спестява много пари. Също така приложението може да бъде доставено много по-бързо. Това прави компаниите изключително гъвкави в доставянето на нови услуги, което предоставя и по-голяма надеждност. Ако възникне проблем с хардуера и трябва да бъде отстранен, можем да преместим приложението на друг компютър и всъщност потребителите никога не виждат нещо повредено. След като компютърът бъде поправен, приложението може да бъде върнато. Всички тези предимства водят до масовото навлизане на тази технология.

Очаква се пазарът на облачни технологии да нарасне с 19% през 2012г., превръщайки се в индустрия за 109 милиарда долара – с 18 милиарда повече от 2011г. До 2016 г. се очаква секторът да достигне 207 милиарда долара. За сравнение, анализаторите прогнозират ръст на целия ИТ пазар от 3%.

Предлагането на софтуер се променя от традиционна продажба на лицензи към инсталиране на приложения на място по SaaS модела. Закупуването на хардуер преминава от капиталови разходи за поддържането на хардуер в самата организация до оперативни разходи за изнесено към чужда фирма оборудване.

СИГУРНОСТ НА ИНФОРМАЦИЯТА ПРИ ИЗПОЛЗВАНЕТО НА CLOUD COMPUTING

Cloud сигурността на данните включва повече от криптиране на данните. Изисквания за сигурност на данните варират в зависимост на услугата модел (SaaS, PaaS и IaaS), на разполагане на модел (лично чрез публично), и на потребителя. Изпълнението на изискванията за сигурност на data Cloud води до прилагане на съществуващите техники за сигурност. Преместването на персоналните данни в “облака” и тяхната защита са класическите фактори, задържащи миграцията към Cloud модела [4,11].

Разпространението на облачните технологии решава множество проблеми, включително и такива, които съществуват отдавна и няма как да бъдат решени по друг начин. От друга страна, кардиналната промяна на ИТ в процеса на тяхното внедряване поставя много организационни и технологични въпроси – сигурността е най-важният сред тях. Както показват всички проучвания, именно опасенията във връзка с безопасността са основна пречка за разпространението на облачните технологии и услуги. Cloud Security Alliance [6] разпространява следните базови препоръки, формулирани в 7 категории рискове за информационната безопасност:

1. Неправомерно използване на облачни услуги

Рисковете от тази категория са свързани с несъвършенството на механизмите за регистрация и оторизация на потребителите, което дава възможност както за използването на съответни ресурси без заплащане на услугите, така и за използването има за незаконна дейност (например инсталиране на управляващи програми за зомби-мрежи, разпращане на спам или атаки, публикуване на вреден код и т.н.). Според експертите, най-уязвими са IaaS и PaaS услугите. Като мерки за противодействие те препоръчват въвеждането на строги правила за начална регистрация, използване на средства за мониторинг и анализ на мрежовия трафик, проследяване на черни списъци на IP адреси и информация за измами в областта на платежните системи.

2. Незащитени API

Уязвимостите във връзка с приложните програмни интерфейси (API) обикновено са свързани с тяхното дописване от страна на доставчиците на услуги. Това се прави с цел да бъдат предоставени допълнителни услуги, но като страничен ефект се увеличава сложността на API, а от там и различните рискове стават повече. Риск от тази категория съществува за всички типове облачни услуги - SaaS, IaaS и PaaS. Като мерки за противодействие Cloud Security Alliance препоръчва: анализ на подходите за осигуряване на безопасност на програмните интерфейси, осигуряване на строга оторизация и контрол на достъпа, прилагане на средства за шифриране на трафика, анализ на вериги от зависимости, свързани с API [2].

3. Действия на сътрудниците на компанията доставяща услугите

Тази категория риск е свързана с обстоятелството, че на едно място се съсредоточават много ИТ услуги, работещи под единно управление в интерес на различни клиенти, а в същото време процесите и процедурите на доставчика често не са прозрачни за клиентите. При това, персоналът има пълен достъп до данни и други ресурси - това създава риск от несанкциониран достъп, който може трудно да бъде установен. Този риск също се отнася за всички типове услуги, включително SaaS, IaaS и PaaS. Като контролни мерки се препоръчва: провеждане на детайлна оценка за нивото на сигурност в компанията доставчик в контекста на въпросите, свързани с персонала; отразяване на изисквания към персонала в договора за обслужване; условие към доставчика да предоставя пълна и актуална информация за подходите и практиките на управление и съответствията с изискванията.

4. Уязвимости на споделяната среда

Тези рискове са породени от това, че не винаги е възможно да се осигури надеждна изолация на средите, принадлежащи на различни клиенти. Уязвимостите от тази категория се отнасят за IaaS услугите. Като контролни мерки се препоръчва: инсталациите и конфигурирането да се осъществяват в съответствие с добрите практики; да бъдат внедрени средства за мониторинг, позволяващи откриването на несанкционирана активност; да се използват средства за строга оторизация и контрол на достъпа; в договора с доставчика да бъдат включени клаузи, регламентиращи своевременното обновяване и инсталиране на пачове на софтуера; да се провежда редовно сканиране за наличие на уязвимости и анализ на конфигурациите [1].

5. Загуба или кражба на данни

Загубата на данни може да бъде свързана с грешки на персонала (както на клиента, така и на доставчика), с използване на ненадеждни устройства и носители за съхранение на данни и медии, както и да се дължи на загуба на ключа за шифроване, на ненадеждно оборудване в центъра за данни или на липса на процедури за аварийно възстановяване и резервно копиране. Тези уязвимости са характерни за всички видове услуги. Препоръчителните мерки срещу тях са: да се контролира достъпът до API, данните да се криптират и да се контролира тяхната цялост при предаване, да се анализират средствата за защита на данните както на

етапа на проектиране, така и в процеса на тяхната експлоатация, да бъде установен реда за резервно копиране на данните [2].

6. Кражба на акаунти

Кражбата на акаунти може да се осъществи с измама, с използване на фишинг, компютърни вируси, уязвимости в оборудването и софтуера и т.н. За противодействие на този риск се препоръчва да не се ползват общи акаунти, да се ползват средства за многофакторна оторизация, да се провежда мониторинг за несанкционирана активност, да се анализират политиките за сигурност на доставчика [1,2].

7. Неизвестни и неидентифицирани рискове

Неизвестните рискове са свързани с това, че клиентът не разполага с пълна информация за облачната среда и следователно неговата информация за рисковете също не е пълна. За да се контролира тази категория рискове Cloud Security Alliance препоръчва от доставчика да се изисква информация за инфраструктурата, включително версии на софтуера, наличие на средства за защита, внедряване на средства за мониторинг на събития и управление на инциденти.

НЕДОСТАТЪЦИ НА CLOUD COMPUTING

При прехода към облачни услуги виртуализацията и синхронизацията на данните размиват периметъра на ИТ инфраструктурата, изчислителните ресурси на доставчика се разделят между всички негови клиенти. В резултат възникват редица въпроси – кой има достъп до данните, как се осигурява работоспособността на ИТ системите, как се съхраняват данните и т.н. Основният проблем е, че при предаването на част от собствената си инфраструктура към доставчик на облачни услуги потребителите губят контрол (фиг. 3)[4].

Фигура 3. Степени в загубата на контрол при преход към облак

И все пак, някои организации вече са пренесли част от своите ИТ активи в облачна среда, други са далеч от такава стъпка. Според експертите, повечето организации разполагат с ИТ ресурси, които могат да пренесат в облака безопасно и изгодно [3]. На въпроса за каква част от ИТ ресурсите миграцията в облака има смисъл, всяка организация трябва да си отговори самостоятелно, като оцени съотношението между възможните предимства и рискове.

ЗАКЛЮЧЕНИЕ

Cloud computing не е просто нова технология, а фундаментално нов бизнес - модел. Услуга, която позволява сами да конфигурираме това, което ни е необходимо, веднага да получим услугата и да платим само за това, което наистина използваме. Получават се услугите, които са необходими за всеки ВУЗ, когато са необходими като те са достъпни на момента и се заплаща само за това, което се използва. През следващите 5-10 години се предполага, че няма да става въпрос само за доставяне на тези услуги чрез технологии в облака. В момента виждаме различните устройствата, като смартфони, таблети да се използват за стартиране

на приложения. Това не само променя достъпа до приложенията и услугите, а променя начина, по който се правят нещата. Вече имаме технология, която позволява това което виждаме на нашия десктоп в къщи или в офиса да го виждаме на Windows, Mac или Linux машина, на Ipad, Android или друго устройства. Другото, което виждаме е фундаменталното изместване от десктоп компютъра като място, от което се стартират различни приложения. Информационните технологии ще увеличават иновативността си и нивата на промяна. Ще има голяма мобилност, големи възможности на нови типове и класове приложения.

Една успешна реализация при въвеждането на облачна технология при обработка на документацията в университетските администрации е чрез множество контроли, при които първичната проверка на данните напълно се автоматизира. Това от своя страна повишава ефективността на извършвания контрол. Единственото техническо изискване за потребителите е наличието на Интернет свързаност. Възможно е и внедряването на цялостна финансово-счетоводна система в облака и включването на мобилни приложения в помощ на финансовите структури. Удобството за потребителите, е че не съществува ограничение за "работни места", а само за ключ към базата данни. Това позволява достъп дори от личния лаптоп или смартфон, където и да се намираме.

ЛИТЕРАТУРА

[1] Желева Б., К. Иванов Анализ на съществуващите системи клиент-сървър с оглед обслужване на обучаващи среди от тип виртуални университети, Национална конференция по електронно обучение във висшето образование с. 27-31., Китен, 2004.

[2] Иванов К., Б. Желева. Приложимост на съвременни средства за гарантиране сигурността и защитата на информацията в e–learning системи, Шести международен симпозиум ТЕХНОМАТ & ИНФОТЕЛ'2004, публикуван на CD носител с ISBN 954 9368 05 X, том 1, Сл. бряг, 2004 .

[3] Иванов К., Т. Христова. Изисквания към структурата и функциите на информационното обслужване на студентите в МГУ "Св. Иван Рилски", Годишник на МГУ "Св. Иван Рилски", ISSN 1312-1820, том 51, св. IV, стр. 61 – 64, София 2008 .

[4] Списание CIO, бр.7, 13.7.2012.

[5] Borko F., A. Escalante. Handbook of Cloud Computing, 2010.

[6] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3.0, 2011, https://cloudsecurityalliance.org.; достъпен на 21.08.2012 .

[7] Internal Cloud http://www.techopedia.com; достъпен на 21.08.2012.

[8] Ivanov K., K. Tcholakov, B. Stoinova. Possibilities for implementing contemporary IT achievements in e-learning systems, TEL /Technology enhanced learning/Enlargement Workshop, Sofia, 2005.

[9] Sultan N. Cloud computing for education: A new dawn?. International Journal of Information Management, 2010.

[10] Tuncay E. Effective use of cloud computing in educational institutions,2010, WCES-2010.

[11] Winkler Vic (J.R.). Cloud Computer Security Techniques and Tactics. Securing the Cloud ISBN: 978-1-59749-592-9, 2011.

За контакти:

Доц. д-р Кънчо Иванов, Катедра "Информатика", МГУ "Св. Иван Рилски", гр.София, тел 02 8060564, e-mail:kantcho.ivanov@gmail.com

Ас. Биляна Стойнова, Катедра "Математика", Технически университет – гр. Габрово, e-mail: bilyana_zheleva@abv.bg

Докладът е рецензиран.