Local Governments and Cloud Computing Security

Inita Kindzule[1], Edzus Zeiris[2] and Maris Ziema[3]
[1]*Project Development Division, Information Technology Centre of the Riga City Council, Brivibas 49/53, Riga, Latvia*
[2]*ZZ Dats Ltd., Elizabetes 41/43, Riga, Latvia*
[3]*Faculty of Computer Science and Information Technology, Riga Technical University, Meza 1/3, Riga, Latvia*

Keywords: Local Governments, Enterprise Architecture, Cloud Computing Security, Risks Assessment, SOA, Systems Architecture.

Abstract: The Cloud computing solution has enormous potential to provide companies, industries and economy in general with remarkable benefits but there are certain challenges that have to be taken into account when choosing this solution. The purpose of this paper is to provide results of research about local governments' Cloud computing security, assisting them in making appropriate risk-based security decisions about how to securely embrace Cloud computing. To ensure that managing information of system-related security risks is consistent with the organization's mission/business objectives, and that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes.

1 INTRODUCTION

One of the most topical and relevant innovations of recent years in Information and communication technologies (ICT) across the globe is recognized to be Cloud computing solutions. The application of these solutions provide both the companies and citizens as well as economy in general with important benefits because of them allowing different institutions, employees and users to achieve immediate results while at the same time ensuring substantial long-term gains (World Economic Forum, 2010). At the same moment the readiness of users to use and the reaction to the innovations at all must be considered. Ever the Cloud computing solution is good innovation with significant benefits for municipality, employees and other users, the reaction of user may be as resistance and disagreement with new solution. The users at the initial implementation stage may be doubt in the solution. In this case additional training for users must be considered.

The application of Cloud technologies reduces costs of operation and capital that's associated with servers, software licenses, maintenance fees, data center space and the employment of IT personnel. Owing to Cloud solutions, the local governments will not have to stick with dated legacy systems and hardware that requires expensive maintenance procedures. It is especially important taking into account the limited resources of municipalities which in their turn are planned in good time (Chandrasekaran and Kapoor, 2010). Comparing to many other technological accomplishments the Cloud computing is able to provide with rapid and considerable return with limited investment (Eggers, 2011).

The development speed of contemporary IT solutions also determines safety requirements and solutions. The conditions that were viable two or three years ago are not suited to requirements of Cloud computing and system threats. Security measures have to be modular and capable of further development. It also has to be taken into consideration that by increasing the level of security in Cloud computing solutions it could limit the usability of solutions as well as affect their efficiency (ISO/IEC 9126) due to the possibility of these system quality indices to be mutually contradictive. Therefore upon implementing the needed security measures in Cloud computing solutions it is necessary to find a trade-off between different system quality indices.

A security in its nature is a protection against different kinds of threats, losses and criminal activities. The security of computer systems is a considerably broad conception. According to

Kindzule I., Zeiris E. and Ziema M..
Local Governments and Cloud Computing Security.
DOI: 10.5220/0004129102840288
In *Proceedings of the International Conference on Data Communication Networking, e-Business and Optical Communication Systems* (ICE-B-2012), pages 284-288
ISBN: 978-989-8565-23-5

definition computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information / data, and telecommunications) (NIST, 1996).

2 SECURITY ASSESTMENT

The security is one of the most significant challenges to local governments (Hodgkinson, 2012; Chandrasekaran and Kapoor, 2010; Eggers, 2011), that's why it is necessary to evaluate whether the existing system architecture is appropriate and suitable for the implementation of Cloud computing solutions. In order to carry out such evaluation all risks have to be assessed. The planning of computer system security can be based on the model of risk analysis. For any computer system it is necessary to analyze all possible risks related to the system in development as well as the security of the computer system. In development of security of computer systems it is possible to use the simulation process of possible risks offered by Common Vulnerability Scoring System (CVSS) which is sufficiently simple and easy to adopt as well as other analogical methods (Mell et al., 2007). For instance, Threat Risk Modelling using the Microsoft Threat Modelling Process (OWASP, 2005). There are five steps in the threat modelling process that are displayed in Figure 1.

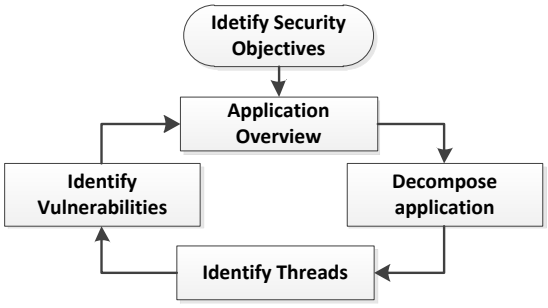

Figure 1: Threat Model Flow.

2.1 Security Risks Assessment Dimensions

In order to provide a prospective IT service the agencies are responsible for ensuring that a safe and secure Cloud solution is available and they should carefully examine agency security needs across several dimensions, including but not limited to:

- Statutory compliance with laws, regulations, and agency requirements;
- Data characteristics to assess which fundamental protections an application's data set requires;
- Data privacy and confidentiality to protect against unintentional and nefarious access to information;
- Integrity to ensure data is authorized, complete, and accurate;
- Data control and access policies that define where data can be stored and who can access the physical locations;
- Management that ensures that Cloud computing service providers are sufficiently transparent, have appropriate security and management controls, and are able to provide the information necessary for the agency to properly and independently assess and monitor the effect of those controls (Kundra, 2011).

Cloud computing ensures dynamic provisioning of resources which is the integral function of Cloud computing architecture. All available resources are dynamically distributed to other points in the Cloud as needed ensuring that there is practically no downtime. Therefore, one event or anomaly will not incapacitate the entire system. Cloud providers use reliable IP networks to connect parts of a Cloud and to connect end users to Cloud services. Owing to this most government networks are able to leverage network embedded technologies already in place, including security. Many Cloud applications are designed to start working immediately. Additional components of the application are only transferred, in modular format, when necessary. Cloud systems can also provide means for information assurance. Information can be backed up automatically by the main system. Cloud systems can be reached from multiple locations, and data can be stored centrally. So there is no doubt about availability part of security. By utilizing Cloud computing solutions an increased attention has to be paid directly to the side of confidentiality and partially to the integrity which can cause problems in distributed computing architecture, like Service Oriented Architecture (SOA).

3 RIGA CITY COUNCIL ENTERPRISE ARCHITECTURE

The mission of Riga local government concerning

the ICT is to develop and support common ICT solutions for employees so that they can provide fast and effective high quality services to residents. To support this mission Riga city council has set two main objectives to be achieved in ICT field for the years 2012 to 2015: to provide means for governments' internal information and documents to be handled electronically and ensure that services to customers (both internal (employees) and external (citizens)) are delivered as fast as possible while remaining effective and of high quality (Riga city council ITC, 2012). According to needs of Riga city council to fulfil this mission it was found out that it is necessary to build the system architecture towards Cloud principle thus satisfying the requirements for an acceptable quality and volume. In order to support Cloud computing the applicable architecture of local governments has to correspond with the following requirements: an integrated platform among various local government business function support systems, application independence, support of Legacy systems, integration of inter municipal application data, application access from any web site and e-services for citizens.

To ensure the criteria set for the architecture including security requirements and the mission of ICT in Riga city council, a modular system architecture that is based on the central data base (CDB) and supports Cloud computing has been selected. It allows creating new modules in web environment and integration of Legacy applications – either virtualizing them or using Microsoft ClickOnce technologies to access the Cloud (See Figure 2).

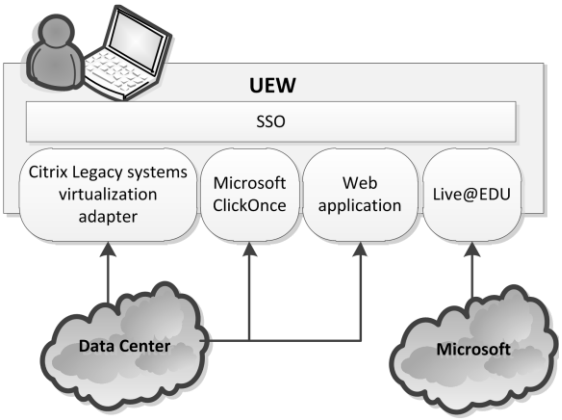

Figure 2: Local Governments Enterprise Architecture.

The result is a more flexible and efficient system that can swiftly respond to changing conditions and requirements. The selected Cloud computing solution provides local governments with possibility to collaborate with employees and other institutions or generate new categories of collaborators, so it also helps local governments to adopt new innovations in ICT.

3.1 Security Solution

To support a special attention to confidentiality as a part of security, custom security solution was chosen that is based on Microsoft Identity framework principles and adopted for Riga city council needs. The solution uses Security Assertion Markup Language (SAML) 2.0 security tokens to secure web services in SOA that is in the background of entry solution. This solution is enhancements on patented Web Services Security System (Zeiris et al., 2008).

The chosen solution is approbated at Riga city council by creating universal environment for employee (Universal Employee Workplace - UEW) which at this moment is integrated with Microsoft Live@edu Cloud solution, one legacy system using Microsoft ClickOnce solution that is a Microsoft technology enabling the user to install and run a Windows application by clicking a link in a web page, one legacy system using Citrix virtualization platform, that is one of the virtualization platforms enabled by Cloud computing, as well as created more than ten new application modules and developed digital signature solution that is working with cryptographic devices using Java Applets. For applications interoperability inside UEW environment the Single Sign On (SSO) solution is developed and used. To support data integration with external resources, notably other municipalities, a Master Index solution has been integrated that allows finding and using the necessary data from other local databases (Stipravietis et al., 2011). All these solutions are very important because Riga city council ICT (including other Latvian municipalities) has been in development since 1997 and there are so many Legacy systems and solutions to integrate and to make them available in municipality Cloud UEW solution.

To provide e-services to residents in Cloud, Riga city council has developed e-service portal www.eriga.lv and Local government interoperability framework (Pruse and Zeiris, 2010), that is integrated in common security model.

4 ENSURING SECURE ENVIRONMENT

The Center for Digital Government (2009) points

out that public sector is a unique environment which with its particular characteristics is considered to be an ideal area for application of Cloud computing, however, it accordingly creates particular challenges (The Center for Digital Government, 2009). In order to achieve the projected targets it is also important to comprehend the risks involved as well as develop appropriate plans that will help to reduce their possibility. It is crucial for increased success and appropriate return of investment (CISCO, 2010).

Risk management involves identifying and assessing risks, and taking the necessary steps to reduce them to an acceptable level. Throughout the system lifecycle, all identified risks that are identified must be carefully balanced against the security and privacy controls available and the expected benefits (See Table 1).

Table 1: Security controls and expected benefits.

Security controls available	Expected benefits
• **The characteristic system complexity** of a Cloud computing environment, and the dependency on the correctness of these components and the interactions among them; • **The dependency on the service provider to retain logical separation in a multi-tenant environment** (n.b., not unique to the Cloud computing model); • **The necessity to ensure that the organization will retain an appropriate level of control** to achieve situational awareness, consider alternatives, set priorities, and implement changes in security and privacy that are in the best interest of the organization.	• **The ability to concentrate resources** on areas of high significance as more general security services are assumed by the Cloud provider; • **Potential platform strength** achieved by having greater uniformity and homogeneity, and resulting improved information assurance, security response, system management, reliability, and maintainability; • **Improved resource availability** through scalability, redundancy and disaster recovery capabilities; improved resilience to unexpected level of service demand; • **Improved backup and recovery** capabilities, policies, procedures and consistency; • **Ability to leverage alternate Cloud services** to improve the overall security condition, including that of traditional data centers.

The privacy of data is the most significant and important prerequisite. Although challenges in public sector do not differ from private sector yet the matters of supply and security in this field are more pronounced. Government institutions are responsible for the safety of personal information of citizens and they must ensure high level of availability of critical public infrastructure (Chandrasekaran and Kapoor, 2010). Eggers (2011) also points out that the greatest limitation to extensive use of Cloud in local governments is exactly security because the information that contains personal data available to the government has to be confidential (Eggers, 2011).

National and economic security of the country is dependent on the strict and consequent approach to IT security and data confidentiality. Political matters and domestic conditions are additional factors that present a question associated with actual physical location of cloud-based resources (CISCO, 2010).

State authorities and local governments are at times being reserved concerning Cloud strategy by basing their concerns on requirements of security, legal and regulative compliances (Hodgkinson, 2012).

Security has always been topical, however, the security requirements and solutions have changed with time, and they have to suit the requirements of Cloud computing and system threats. Appropriate security is crucial to success of Cloud application or other solution on the operation of any government.

5 CONCLUSIONS

In conclusion it is important to point out that there is no common solution that can be applied to all local governments and state institutions, however, all those that have implemented this solution early on, have achieved significant and fortunate results.

Key security considerations include the need for local governments to:

1. Be educated about the issues associated with Cloud computing, specifically the opportunities, risks and current best practice;
2. Accurately determine security requirements during the initial planning stage at the start of the systems development life cycle;
3. Determine the degree to which negotiated service agreements are required to satisfy security requirements; and the alternatives of using negotiated service agreements or cloud computing deployment models which offer greater cleamess and control over security;
4. Assess the extent to which the server and computing environment of business users and consumers meets organizational security requirements;
5. Continue to maintain security management practices, controls, and accountability over the security of data and applications; and to improve data security for the infrastructure services and users documents and improve

service availability.

ACKNOWLEDGEMENTS

This work has been supported by the Riga City Council Information Technology Centre.

REFERENCES

Chandrasekaran, A., Kapoor, M. (2010). State of Cloud Computing in the Public Sector – A Strategic analysis of the business case and overview of initiatives across Asia Pacific, Frost & Sullivan 2011 – *Market Insight, Frost & Sullivan Ltd.*, Available on: http://www.frost.com/prod/servlet/cio/232651119;

Eggers, B. (2011). Cloud computing in government explodes, Deloitte, February 02. Available on: http://globalblogs.deloitte.com/deloitteperspectives/2011/02/cloud-computing-in-government-explodes.html;

World Economic Forum in partnership with Accenture (2010). Exploring the Future of Cloud Computing: riding the next Wave of technology-driven transformation, p.21. Available on: https://members.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf;

Hodgkinson, S. (2012). Why Government Agencies need the Cloud, Ovum, February, p.19. Available on: http://www.telstra.com.au/business-enterprise/download/document/business-ovum-government-cloud-white paper-17-feb-2012-aus.pdf;

Kundra, V. (2011). Federal Cloud Computing Strategy, February 8, p.39. Available on: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf;

Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standarts and Technology, *National Institute of Standards and Technology U.S Department of Commerce*. Gaithesburg, September, pp.800-145.;

Mell, P., Scarfone, K., Romanosky, S. (2007). Common Vulnerability Scoring System (v2). - CVSS;

OWASP (2005). The Open Web Application Security Project: A Guide to Building Secure Web Applications and Web Services 2nd ed.;

National Institute of Standards and Technology (1996). An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, *Technology Administration U.S. Department of Commerce*, p.278.;

Pruse, I., Zeiris, E. (2010). eRiga.lv: Local Government Interoperability Framework// MeTTeG10 *Proceedings of the 4th International Conference on Methodologies, Technologies and Tools enabling e-Government*, Olten, Switzerland, 1-2 July, p.11-20.;

CISCO (2010). Realizing the Potential of the Cloud in Government - Maximizing Return on Investment with Cloud Services, p.14 Available on: http://www.cisco.com/en/US/services/ps10658/ps11786/services_realizing_the_potential_cloud_in_government_wp.pdf;

Riga City Council Information Technology Center (2012). Riga municipality goals in ICT for years 2012 - 2015.;

Stipravietis, P., Kindzule, I., Pruse, I., Zeiris, E. (2011). Design of Horizontal Data Integration// eChallenges *e2011 Conference Proceedings*, Italy, Florence, 26-28 October, p. 11.;

The Center for Digital Government (2009). Clouds Rolling In: The Calls for Increased Agility, Stability and Performance a Cloud Computing Comes to State and Local Government: a strategy paper, California, p 12. Available on: http://media.govtech.net/Digital_Communities/CDG/CDG09_STRATEGY_Microsoft_V.pdf;

Zeiris, E., Ziema, M., Amanis, I. (2008). Web Services Security System / Patent No. LV 13720 - Latvia, published on 20th of August.