Some Security Issues of the Governmental Cloud

ROUMEN TRIFONOV[1], RADOSLAV YOSHINOV[2]
[1] Faculty of Computer Systems and Control
Technical University – Sofia
8 St. Kliment Ohridski Bul., Sofia 1000
BULGARIA
e-mail: r_trifonov@tu-sofia.bg
[2] Telematics Laboratory
Bulgarian Academy of Sciences
8 Acad. G. Bonchev Str., 1113 Sofia
BULGARIA
e-mail: yoshinov@cc.bas.bg

Abstract: - The recent European studies testify that so far is no comprehensive analysis of the security frameworks of currently running or planned governmental Cloud deployments. Hence, there are no guidelines to define a generic security framework that allows to assess and benchmark Governmental Cloud security. In these circumstances, the present article aims to outline some key points for building Governmental Cloud Security Framework including Risk Assessment, Security Measures, Security Certification and Incident Reporting.

Key-Words: - Governmental cloud, risk assessment, security measures, security certification, incident reporting

1 Introduction

The idea of a central or local government leveraging the Cloud computing business model to increase the effectiveness and efficiencies of the ICT services is appealing, especially in a period of economic challenges for the European Union Member States. The concept of Governmental Cloud (Gov Cloud) proposes, among others, the following [1]: "…*Cloud computing service delivery model satisfies the most of the needs of public administrations, on the one hand, since it offers scalability, elasticity, high performance, resilience and security. However, many public bodies have not yet built a model for assessing their organizational risks related to security and resilience."*

A standard definition for the term Gov Cloud is currently lacking. However, we can adopt the Gov Cloud definition introduced by ENISA report [2], as:

"- *a Gov Cloud is an environment running services compliant with governmental and EU legislations on security, privacy and resilience (what);*

a Gov Cloud is a secure and trustworthy way (private Cloud or public Cloud) to run services under public body governance (how);

a Gov Cloud is a deployment model to build and deliver services to state agencies (internal delivery of services), to citizens and to enterprises (external delivery of services to society) (for who)."

The compelling business and financial benefits for adopting Cloud services require formalization of a security framework for governmental clouds. This security framework can be based on a collection and analysis of existing Cloud computing security literature, other relevant security best practices, and on the few existing real life case studies of Governmental Clouds in Europe.

In principle the security framework is as a conceptual structure intended to serve creation of a secure information system. In our case, the intention of the security framework is to serve as a comprehensive guideline for the creation, deployment, assessment and improvement of a secure Gov Cloud. It should be considered as the beginning of a continuous enhancement process by incorporating emerging elements, and by considering the lessons learned from its real-world application.

The European study of Governmental Cloud Security Framework [3] concluded that:

security and privacy issues are considered as key factors to take into account for migration, and at the same time are the main barriers for adoption. Protection of sensitive data is still an issue seeking solution, spanning from the Service Level Agreement (SLA) provisions to the actual technological mechanisms i.e. encryption etc.;

there is a clear need for Cloud pilots and prototypes in order to test the utility of the technology. There is also a need for best practices and success stories to be disseminated in the EU public administration community;

the main security challenges, requirements and barriers in the cloudification of governmental services are related to: data protection and compliance, interoperability and data portability, identity and access management, auditing, adaptability and availability, as well as risk management and detailed security SLA formalization;

there are no current studies that comprehensively analyse the security frameworks of currently running or planned governmental Cloud deployments. Hence, there are no guidelines to define a generic security framework that allows to assess and benchmark Gov Cloud security.

In these circumstances, the authors (who were members of the team that developed in 2007-2008 the National Information Security Policy) undertook a study of global and European best practices in order to offer to developers of the Governmental Cloud some key points for building Governmental Cloud Security Framework. The following areas, which in the opinion of the authors are crucial, were selected: Risk Assessment, Security Measures, Security Certification and Incident Reporting.

2 Risk Assessment for Cloud

It is necessary to find a pragmatic approach for assessing risks to Cloud applications (cloud SaaS applications) and applications hosted in Cloud environment (applications using cloud based IaaS and PaaS). This can be done by developing methods for assessing the impact level of breaches and then try to define a methodology for mapping the impact levels on required technical and organizational measures and certifications.

A full risk analysis using classical methods can be very time consuming and might make sense for high-profile (expensive) applications. It is advisable to use simpler risk assessment and simple tools to identify the necessary protection measures and controls.

The threats related to the security of the cloud hosting environment and infrastructure layer can be covered by the certification of the underlying IaaS layer. Since the likelihood may depend on the implemented security controls and protection or redundancy mechanisms, it is important to document the assumptions under which this likelihood is valid. For Governmental Cloud applications the entire attacker community, including organized crime and state sponsored espionages, are important threat agents. In Cloud computing environment for applications with high value or high loss potential it is safe to assume that threat agent’s capabilities are very high.

That’s why, the methods which determine which measures and controls need to be implemented depend on the impact assessment of the elements of cloud technologies (SaaS, PaaS, IaaS). The applications and the way it use must be analysed in order to guarantee security and to avoid lock-in.

Over the last few years, many documents have been published containing risk exposure, guidance and control checklists for Cloud Computing. The risk profile for Cloud migration itself is also in a state of flux, as existing offerings are maturing and new offerings are emerging. We can see emergence of Cloud service brokers, who provide intermediation, monitoring, transformation/portability, governance, provisioning and integration services in addition to existing Cloud services.

In March 2010, the Cloud Security Alliance (CSA) published a document [4], which includes the top seven threats as identified by its members. More recently, in April 2011, the Open Web Application Security Project (OWASP) released a ‘pre-alpha list’ of its top 10 cloud security risks derived from a literature review of other publications and sources [5]. In May 2011, the National Institute of Standards and Technology (NIST) released new Special Publication [6], which provides a deep analysis of risk. In July 2011, ISACA released an issue [7], which provides a comprehensive guide to cloud controls taken from COBIT, Val IT and Risk IT. This publication highlights both the need for a consistent and broadly accepted risk assessment framework and the fact that its existence still remains elusive.

One of advisable methods for risk assessment in Govenmental Cloud applications can be so called “Risk-based Security Assessment and Testing Methologies” defined in the Guide EG 203 351 of European Telecommunication Standardization Institute (ETSI) [8]. This guide introduces test-based risk assessment, which is able to verify the assumption on risk factors with tangible measurement and test results.

In general, the testng activities (Fig. 1) can be divided into functional security testing, robustness testing, performance testing and penetration testing. While functional security testing, robustness testing and performance testing are used to chck the functionality, availability and efficient of the specified security functionality and systems (e.g. firewals, authentication and authorization subsystems access control), penetration testing (or security vulnerability testing) directly addresses the identification and discovery of so far undiscovered system vulnerabilities caused by security design flaws.

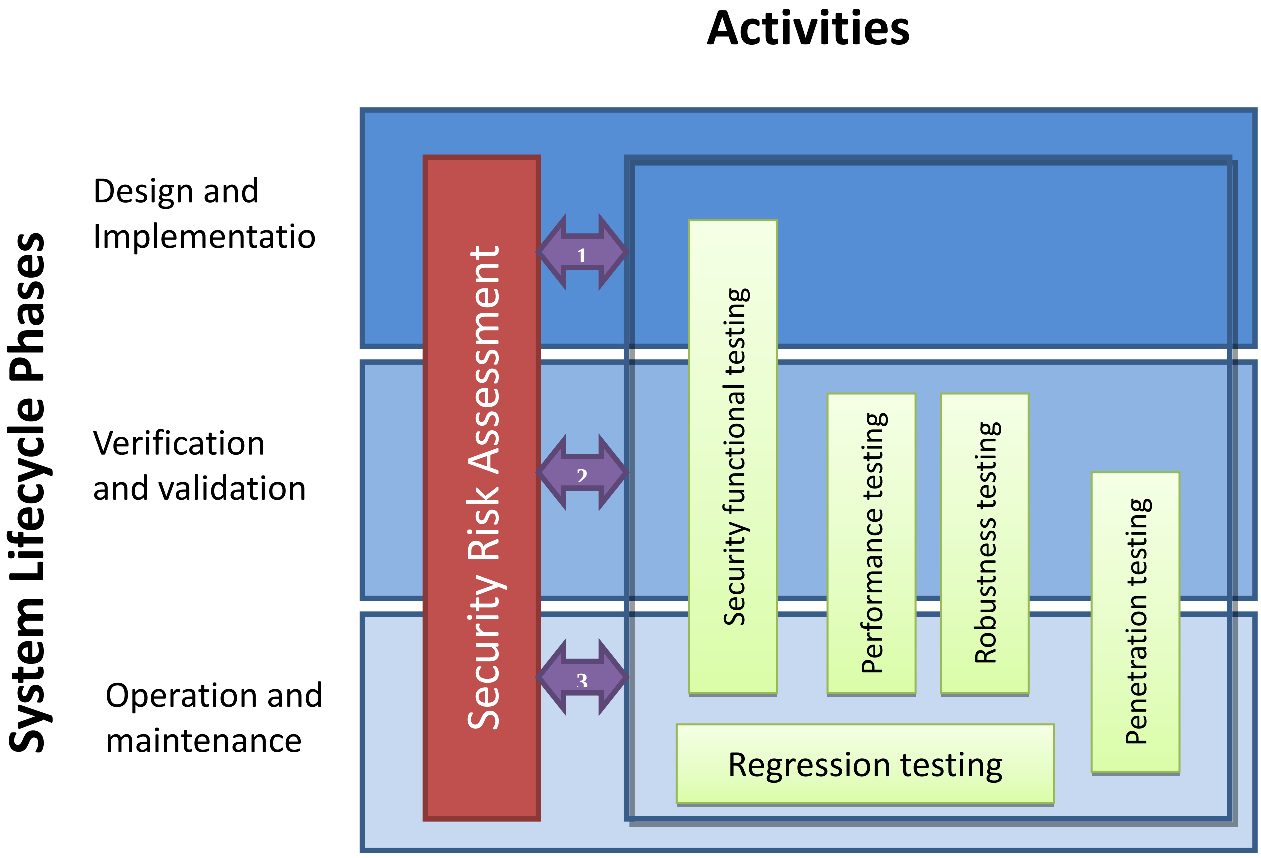

Fig. 1 The Testing Activities according to the Guide 203 351

3 Security Measures

As a result of study on European and global best practices in the application of Cloud technologies in the automation of administrative activities, the authors opted for the next measures that would like to advice for development of the National Cov Cloud Security Framework.

3.1. Loss of control of data and resources is one of the main barriers to Gov Cloud take-up. The "loss of control" issue is not only a matter of technologies but also of awareness, transparency, regulation, contractual agreements between providers and governmental customers. Another aspect of "loss of control" is the vendor lock-in problem i.e. what is the mitigation action for bankruptcy of the Cloud provider cases. Concerning vendor lock-in, from a technical point of view, without cost and time constraints, it should always be possible to migrate data and applications from one Cloud provider to another.

The competent authorities in cooperation with Cloud providers and government customers should closely work to mitigate "loss of control" addressing the issues of governance, monitoring and auditing, vendor lock-in and data handling. Required steps are:

- definition of a monitoring framework for Gov Cloud public service layers;
- definition of standard procedures for data handling;
- definition of standard procedures for data and service migration.

3.2. Cloud providers usually store data in their datacentres which can be located in many different places. The possibility to locate data and resources is often perceived as a barrier for Gov Cloud adoption rather than an advantage for data privacy issues. The definition of regulatory framework for data location can reduce the risks of objections from the governmental users, but the most critical concern for data protection is to ensure the security of data more than location of data.

To achieve this, it is necessary that the competent authorities in cooperation with Cloud providers and government customers could work closely on the following topics:

- definition of measures to improve the awareness of government agencies and Cloud service providers on existing EU legislation on the subject;
- foster the development of technological solutions compliant with the existing legislation;
- categorization of specific governmental institution requirements on data ownership and data privacy judged by the type of data handled;
- enhancement of the existing legislation on data and resource ownership with a focus outsourcing;
- enhancement of the existing legislation on data privacy with a focus on outsourcing.

3.3. The public users and providers should be free to choose the level of security provided and requested for the public services, with positive effects on the competition between providers and leaving the departments the possibility for implement the most effective and the best value for money solutions. A specific set of security measures focussed on Governmental Cloud deployment would be the way to improve trustworthiness in the Cloud supply chain. Suggested actions to enhance the security and protection of information for the Governmental Cloud services are:

- support pre-assessment process before procuring services;
- create a set of baseline security measures focussed on Governmental Clouds; for this reason the measures should include domains like security management, identity management, data redundancy, services availability etc;
- include risk impact levels in each domain in order to offer a sohpistication/maturity model;
- enable voluntary auditing (and/or certification) framework of information security measures;
- foster security labelling systems.

4 Cloud Security Certification Framework

In general, the Cloud Security Certification is a part of so called "Cloud Computing Certification Schemes (CCCS)", which include also certification procedures for Interoperability, Service Management, Reliable Access and Privacy/Data Protection.

Currently, there are 24 internationally recognized certification schemes in the field of information security. The classic scheme based on ISO/IEC 27001/27002 is hardly suitable for cloud application because of the orientation of these standards for needs of consolidated organization. In our opinion for information security certification of the Gov Cloud can be recommended so called "EuroCloud Star Audit (ECSA)" [9]. This is a certification scheme especially designed to assess "on-line" services. It evaluates an "on-line" Cloud service against the requirements of audit scheme and covers all participants of the specific supply chain of a service. The ESCA audit is a not-negotiable mandatory bandwidth of all important areas: provider's profile, contract and compliance including data privacy protection against local law, security, operations, environment and technical infrastructure, processes and relevant parts of the application and implementation up to interoperability and data portability.

5. Cloud Security Incident Reporting

The Governmental Cloud computing probably will become the backbone of e-Government applications. That's why certain Cloud security incidents could have a major impact in society and the incident reporting about Cloud security incidents could be implemented in an effective and efficient way.

The expert's perspective on the key issues of Cloud security incident reporting can be summarized as follows:

- it is difficult to assess the criticality of the Cloud services for a national regulator. There are many interdependencies, different layers of the cloud stack, different deployment models and different kind of data stored;
- Cloud services are often based on other Cloud services; they are distributed systems and built up in several layers. Incident reporting is different in these different layers;
- from the Cloud customer's point of view, most standard contracts do not commit providers to reporting about security incidents to customers. Even though, some Cloud providers do have dashboards where some incidents are published and explained;
- from the provider's side, it is up to the customer to include incident reporting obligations in contracts. For this reason, in many Cloud contracts incident reporting is not addressed;
- incident reporting is becoming more and more common in regulated sectors, like governmental administration where operators need to report incidents to regulators;
- incident reporting should be part of a bi-directional flow of information where providers report about security incidents to authorities and authorities' feedback common threats and common issues to the Cloud providers so they can improve security and resilience.

If the Cloud provider offers IaaS/ PaaS/ SaaS services to administrative bodies, he has signed a contract with the administrative institutions. When an incident happens, impacting the availability of the core systems of the customers, the provider will send, according to the contractual terms, a report with the technical specifications, the causes and remediation actions including impact analysis to the customer.

In the case of overruns certain threshold of impact (regulated by the national regulatory authority), the operator must report to this authority, since it is the one that collects more information on the scale of the impact (and is aware of the criticality of the services and data processed).

6. Conclusion

Having in mind the strong opinion about the prospects of Cloud applications as the basis for Electronic Governance in Europe and also, the documented intentions of the Bulgarian government to create National Governmental Cloud, this article aims to outline the problems related to the Governmental Cloud network and information security.

The article recommends possible approaches and solutions to these problems, based on the good European and international practices.

References:

[1] *Unleashing the Potential of Cloud Computing in Europe*, Communication from the European Commission (2012) 529 final, 2012

[2] *Good Practice Guide for securely deploying Governmental Clouds*, ENISA, 2013

[3] *Security Framework for Governmental Clouds*, ENISA, 2015

[4] *Top Threats to Cloud Computing* V1.0, Cloud Security Alliance, 2010, www.cloudsecurityalliance.org/Topthreats

[5] OWASP Cloud—10 Project, OWASP, 2011, www.owasp.org/index.php/Category:OWASP_ Cloud_ _10_Project

[6] *Cloud Computing Synopsis and Recommendations* Special Publication 800-146, NIST, 2012

[7] *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*, ISACA, 2011, www.isaca.org/cloud

[8] *Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies*, ETSI EG 203 251, 2015

[9] https://staraudit.org