SECURITY ISSUES IN CLOUD COMPUTING

PhD., Stefan IOVAN[1,2]
[1)] *West University, Computer Science Department, Timisoara, ROMANIA*
[2)] *Railway Informatics SA, Strategy Department, Bucharest, ROMANIA*
PhD. Candidate, Gheorghe DAIAN, *Railway Informatics SA, Cluj - Napoca, ROMANIA*

ABSTRACT: The cloud and virtualization alongside mobility has been dominating both the specialty press and the one related to strategy, implementation, analysis and economic impact for more than two years. New research supports the need for solutions that cover both traditional environments and the private externalised public cloud. Respondents indicated that 75% of business and operational managers plan to implement a hybrid delivery model. Meanwhile, 65% are worried about the limits imposed by the unique vendors and about security, while 72% said that portability between cloud models is important for the implementations they achieved in the cloud. This paper aims to explore a few of the vast range of security issues in cloud computing technology and to present some aspects about virtual machine viruses.

KEY WORDS: security, viruses, virtual machines, cloud computing, private cloud, public cloud.

1. INTRODUCTION

At this point, workloads are allowed at any input point and are run on the available resources (automatically moved where resources are available) according to the holder's rights and delivered in accordance with the holder's request, without the user being concerned about how this is achieved. No one is interested in what plant and how the electric current that powers the lamp in one's room was produced [1, 2].

The road travelled by any corporation towards the model of IT services usage defined by cloud computing is one of multiple phases. Each of these involves the gradual establishment of one or more of the elements that define the cloud computing model:

- usage on request ("*on-demand self service"*);
- geographically unrestricted access ("*broad network access*");
- organization of resources in groups ("*pooled resources*");
- scalability ("*rapid elasticity*");
- payment according to usage ("*measured service*").

The first step is the development of "*private clouds*" nuclei within the controlled environment of the corporation. These nuclei shall subsequently unite in an actually built "*private cloud*" controlled by the corporation. This way data are easier to manage, based on the flows that have already been known and appropriated by both managers and employees. In this phase, the main challenges relate to:

- *SLA* (***S**ervice **L**evel **A**greement*) – how quickly an application responds to the needs of the users spread over a wide geographic area and its degree of availability in the event of disasters;
- *Security* – the way in which equal secure access rights are ensured for users in various locations and potentially outside the corporation - "*mobile users*";
- *Control* – the way to access the applications provided, the applications that can be provided through this model, and the way in which access rights are divided.

The current IT services usage model at corporate level is certainly a hybrid one, and the challenge is real: how to ensure (secure) access to resources and how to present data to users in a consistent manner (a table or graph should look the same on a desktop computer and on a tablet) [3, 4, 7].

1.1. A few security issues

First of all, there are 7 security issues to be discussed with the vendor before resorting to cloud computing, problems that can be classified as:

1. *Privileged user access:* Who is at the base (root) of the sale chain of the services?
2. *Compliance with the regulations:* May the vendor be subject to periodic checks?
3. *Location:* Does the vendor allow some form of control over the data centre?
4. *Data segregation:* Is data encryption available at any level? Is it effective or tested by professionals?
5. *Data recovery:* What happens to the data in case of a disaster? Does the vendor provide a "*disaster recovery*" solution? How long until the resumption of the activity in case of disaster?
6. *Investigative support:* Does the vendor have the capacity to investigate any inappropriate or illegal activity?
7. *Long-term viability:* What happens to the data if the company goes out of business?

1.2. Applications for cloud security

IRIS is a mechanism that guarantees the correctness and availability of data migrated to the cloud. Companies using cloud computing to migrate data can verify if data is in the original format and if they have been modified or corrupted, using the IRIS system. The company has to maintain locally a short aggregate of all data collections, based on which one can verify the accuracy of the data in the cloud with a very efficient protocol.

HAIL is a technology that addresses the problem of availability of the resources migrated to the cloud. If the cloud service provider is not available, resources cannot be accessed, which can lead to significant losses for an organization that relies solely on IT services in the cloud. The solution proposed by HAIL consists in a system that distributes data to multiple cloud providers and adds redundancy using error-correcting codes. If a particular cloud provider is not available (is offline), the data is still accessible to the organization thanks to the cloud providers that are available (they are online).

HomeAlone. For confidential applications, there is a model called "private cloud", in which the cloud service provider reserves resources for a particular organization. These resources are not shared with other companies using the same cloud. But how can an organization be sure that cloud resources are allocated exclusively for its own use? HomeAlone is a system that solves this problem by making sure that certain cloud resources (virtual machines) have been reserved for a specific organization. The protocol is carried out without even involving the cloud service supplier: the organization that wants to check resource isolation carries out a protocol between the virtual machines running on the same actual machine. Interestingly, the protocol is based on the same techniques that hackers use to spy on other users' virtual machines in the cloud.

2. VIRTUAL ENVIRONMENTS SECURITY

Companies fail to ensure security of the virtual environments. A third of the companies admit that they did not invest in the security of virtual cloud computing environments [5]. This means that many companies risk exposure to serious and costly breach, concluded the security company that commissioned the study.

The study conducted globally among companies with 100 or more IT stations, also found out that 42% of companies consider that their virtual servers are more secure than the physical ones, despite the fact that one in three companies said that their knowledge about virtualization is "*basic*".

There is a common perception that virtual machines are safer than physical ones, but this is just a myth. In reality, virtual systems are just as vulnerable to "*malware*" in the form of "*e-mail attachments*", "*drive-by-downloads*", "*Trojan botnet*" and to "*spear-fishing*" attacks.

Despite the limited knowledge about virtualization, the study found out that 81% of the services launched in virtual environments are critical to companies. Around half of the companies that run applications on virtual services admitted to not fully understand virtualization and environment security. All this combined with a serious lack of knowledge among IT professionals could put at risk the benefits of virtualization.

There is no doubt that the benefits of virtualisation are huge - in terms of cost and accessibility. But underestimating risks puts businesses of all sizes in a dangerous position. Lack of knowledge among IT professionals is the main cause, so companies need to invest in understanding the concept of virtualization.

Another common problem is that companies are so much focused on performance and cost that they often overlook security or address it only towards the end.

According to Forrester, many IT professionals believe that a virtual server is as vulnerable as a physical one. But this is not true. The risks are different. It should be noted that basic knowledge is not sufficient when a company's security is at stake. Industry must invest in appropriate solutions, with a comprehensive education programme for professionals (system administrators).

To help companies achieve productivity benefits and efficiency in the virtual IT without running security risks, companies have developed some virtualization products that integrate with the "*corporate*" security suite.

It is considered important to have visibility onto the physical and virtual machines on a single screen and to be able to report them together. It is also important that the physical assets be managed by a system able to implement appropriate security policies. Virtualization can help improve security, but only if companies invest in security controls and management systems to track virtual machines and enforce security policies.

2.1. Viruses of the virtual machines

Viruses which target virtual machines are growing in number and soon they will become a dominant force in the world of cyber crime. Many alerts on the increase of the incidence and on the problems caused by this type of viruses have been released.

A lot of the present-day viruses target virtual machines, which means that they do their work if they are run on a virtual machine. Anyone who finds a piece of malware and wishes to examine it must first run the "*malware piece*" on a virtual machine to see what it does. At that time the virus will detect that it is being run on a virtual machine and will not start to do what was programmed to do, preventing us to see its behaviour.

There is also the possibility that a virtual machine running a particular operating system is attacked and details be copied directly by the host, putting companies at an even higher risk.

Numerous studies have shown that most security breaches are caused by human error, such as using an unencrypted USB stick or by an employee downloading malicious soft-ware. This new issue comes to complete the list.

When it comes to virtual desktops, these present yet another risk factor, because they involve the users clicking and downloading programmes. It presupposes more than just an administrator running an Exchange server or a SharePoint server; it presupposes people who use their desktops to run cloud environments [6]. This leads to advanced persistent threats, which are directed towards users.

Advanced persistent menace often comes in the form of an email and seems to be a real message from companies or even colleagues that requires downloading the attached file. This causes problems on an isolated PC, but when it is attached to the entire virtual network, the consequences are more serious.

Social engineering causes the persistent

threats to assault users. It is possible that in the end we click on something that could turn into a cyber attack. The only way to protect from these threats is to adopt the same attitude towards security to virtual machines as in the real world.

There is no significant difference between the virtual world and the real world. If an object (thing) needs protection, if it is moved to the cloud or in a virtual environment, it still needs protection, but people forget this when jumping from the real world into the virtual one.

All attacks currently noted are specific to virtual machines, and given that even small companies adopt virtual strategies due to their lower cost, it's likely they become the next frontier [6, 7].

3. ESSENTIAL ELEMENTS FOR SECURITY IN CLOUD

Today everything is mobile, connected, interactive, immediate and fluid. As business expectations grow, they put pressure on service delivery. IT organizations must ensure appropriate technological services to the users and business customers anytime and anywhere they are needed – at low-cost, and in a secure and fast manner. These are essential elements for the continued development of operating in the cloud.

Most analysts and industry surveys mention data security and privacy among the main concerns of managers. While operational resources and corporate data in the cloud are attractive targets for attackers, the characteristics of operation in the cloud and the focus on the related virtualization technology cause a significant change in the domain of security development.

In our view, cloud security must be centred on information, must be integrated, adaptive and proactive. For this reason, efforts should focus on providing solutions that are appropriate to these threats and to respond effectively to the new security dynamics.

For the transfer to the cloud to be successful, it is necessary to assess risks and manage them in time. These risks are related to:

1. Security of devices that provide access in the cloud environment. Users access the cloud environment, the data resources and its applications on a wide variety of devices including computers, laptops, PDA's, mobile phones, smart-phones and PC tablets. An ever growing trend blurs the boundaries between the personal and business operating devices, making it more difficult for the company to control the security of the devices that provide customer access.

There are two prerequisites for access to the cloud:

- User's authentication based on a combination of user name / password, user name / security token or username / PKI type credentials (***P**ublic **K**ey **I**nfrastructure*), before establishing an internet connection to the cloud;
- Internet connection through a secure solution for remote access.

It is also necessary that the access devices be equipped with enough anti-malware programmes and data protection measures for booth host and data, as well as IDS/ IPS software (***I**ntrusion **D**etection **S**ystem / **I**ntrusion **P**revention **S**ystem*) of the "*host-based*" type and personal firewalls.

2. Security and availability of cloud platforms. The majority of cloud environments in the organizations are hybrid, consisting of both virtualized and non-virtualized IT resources. All IT resources are to be equipped by the cloud service provider with data protection measures against malware, as well as with network and host security solutions. In addition, when virtualized resources are used, the cloud service provider needs a set of security solutions specially designed to protect this type of resources. If a cloud service provider offers services to different "*tenants*" the cloud platform must also meet the requirements of isolation of the latter.

When PaaS type ("*Platform as a Service*") or SaaS type ("*Software as a Service*") services are provided it is necessary to implement additional security solutions that respond to specific threats at the level of the applications and data.

3. Management of Identity and access to the cloud. Provisioning, governance and security management in the cloud are provided by a set of services for identity and access management and security. In many organizations these services not only deliver security solutions for the cloud environment, but also to the traditional IT infrastructure. In most cases, this is achieved by providing a link to the cloud, or by creating an extension of the already existing identity, access and safety management.

4. Management of cloud security and compliance. These processes require more than security products involving personnel, processes, policies, procedures and evidence certifying that the environment operates to a certain level of security. In general, security management and compliance is confronted to the 5P model:

- *P1—Personal:* The appropriate roles are performed by the appropriate employees that possess knowledge necessary to monitor cloud operation safety.
- *P2—Policies:* An appropriate set of policies and procedures is available and used to govern security and continuity in the cloud.
- *P3—Processes:* Appropriate security and continuity models of the business processes are prepared to ensure data transfer between the beneficiaries and the private cloud provider. Proper and safe operation of cloud services is ensured.
- *P4—Products:* The appropriate defence technology and strategies are prepared to manage and reduce security risks.
- *P5—Samples:* Validation methods and measurements and performance indicators are ensured to determine the effectiveness of cloud security control.

5. Impact of security on the participants to the cloud environment. Consumers have a set of credentials (user name and authentication mode), a role at the level of the cloud (which defines the privileges and access rights to the cloud) and a security domain (which defines the type of access to one or several sub-sequences of the cloud).

Service delivery staff (a category that includes administrators, developers, architects and security administrators) ensure proper setup and operation of security in the cloud [8, 9].

Those charged with governance of the security services set the general security levels and directions in the cloud and make sure that cloud security is aligned with the organizational, industrial or government provisions (Audit and Compliance). This category includes: IT manager, business manager, security manager and security auditor.

4. CONCLUSIONS

Although we are going through a crisis, cloud computing technology is making permanent progress and is becoming more popular, so it is possible that in a few years IT technology as we know it today should change fundamentally: All data and applications are in the cloud, we can access them from anywhere, from the PC, phone or tablet [7-9].

To deal with security challenges, it is necessary to understand and to perform a complete risk analysis. It is also necessary to develop architecture with a high level of security for cloud-based services. Companies need to define additional security measures needed to protect the most important information in different types of cloud environments.

We believe that we are just getting started with these analyzes. There are many case studies and many questions. There are issues related to human resources and new jobs in IT, but also profound changes in business models and in the economic approach.

5. REFERENCES

[1] **Iovan, St. and Ionescu, P.-V.** (2011) *Cloud Computing: A Short Introduction*, Bucharest: Proc. of 12th European Conference

(***E_COMM_LINE 2011***), România, ISBN-10: 973-1704-20-5;

[2] **Iovan, St. and Ionescu, P.-V.** (2012) *Security Issues in Cloud Computing Technology*, Bucharest: Proc. of 13th European Conference (***E_COMM_LINE 2012***), România, ISBN-10: 973-1704-22-1;

[3] **Daian, Gh.I. and Iovan, St.** (2012) *Cloud Computing in Romania and on Emerging Markets*, Targu Jiu: Annals of the "Constantin Brancusi" University, (***CONFERENG 2012***), Romania, Engineering Series, **Issue 3/2012**, pag. 112 - 124;

[4] **Ionescu, P.-V. and Iovan, St.** (2012) *The Adoption of Cloud Computing at the Governmental Level and the Problem of Interoperability*, Bucharest: Proc. of 13th European Conference (***E_COMM_LINE 2012***), România, ISBN-10: 973-1704-22-1;

[5] **Iovan, St. and Ionita, Pr.** (2011) *Breaking into the Clouds*, Bucharest: Proc. of 12th Europeam Conference (***E_COMM_LINE 2011***), Romania, ISBN-10: 973-1704-20-5;

[6] **Iovan, St. and Daian, Gh.I.** (2012) *Enterprise Services Architecture in the World of Information Technology*, Targu Jiu: Annals of the "Constantin Brancusi" University, (***SYMECH 2012***), Romania, Fiability & Durability Series, Supplement **No. 1/2012**, pag. 375 – 381;

[7] **Iovan, St. and Daian, Gh.I.** (2013) *Impact of Cloud Computing on Electronic Government*, Ranca-Gorj: Annals of the "Constantin Brancusi" University, (***SYMECH 2013***), Romania, Fiability & Durability Series, Supplement **No. 1/2012**, pag. 71 – 77;

[8] **Ivanus, Cr. and Iovan, St.** (2013) *Providing Products and Services in Cloud Computing Technology*, Bucharest: Proc. of 14th European Conference (***E_COMM_LINE 2013***), România, ISBN-10: 973-1704-22-1;

[9] **Iovan, St. and Ivanus, Cr.** (2013) *Cloud Computing Essential Element – Data Center*, Bucharest: Proc. of 14th European Conference (***E_COMM_LINE 2013***), România, ISBN-10: 973-1704-22-1;