Interdisciplinary Description of Complex Systems 13(1), 9-14, 2015

MOVING TOWARDS CLOUD SECURITY

Edit Szilvia Rubóczki[1] and Zoltán Rajnai[2,] *

[1]c/o Obuda University
Budapest, Hungary

[2]Doctoral School on Safety and Security Sciences – Obuda University
Budapest, Hungary

DOI: 10.7906/indecs.13.1.2
Regular article

Received: 3 November 2014.
Accepted: 8 January 2015.

ABSTRACT

Cloud computing hosts and delivers many different services via Internet. There are a lot of reasons why people opt for using cloud resources. Cloud development is increasing fast while a lot of related services drop behind, for example the mass awareness of cloud security. However the new generation upload videos and pictures without reason to a cloud storage, but only few know about data privacy, data management and the proprietary of stored data in the cloud. In an enterprise environment the users have to know the rule of cloud usage, however they have little knowledge about traditional IT security. It is important to measure the level of their knowledge, and evolve the training system to develop the security awareness.

The article proves the importance of suggesting new metrics and algorithms for measuring security awareness of corporate users and employees to include the requirements of emerging cloud security.

KEY WORDS

cloud security, information technologies

CLASSIFICATION

ACM: C.1.2., C.2.1
JEL: O39

*Corresponding author, η: rajnai.zoltan@bgk.uni-obuda.hu; +36 30 445 1103;
Óbudai Egyetem, Biztonságtudományi Doktori Iskola, 1034 Budapest, Bécsi út 96/b, Hungary

INTRODUCTION

Computing is turning into a utility. Cloud is the most famous all of them, the new generation use cloud computing via their smartphones. Nowadays you can meet cloud computing everywhere. If you download an app on your smart phone, take a picture with that, storing your data – you choose cloud, because it is cheap, easy and accessible.

But what do you really know about the privacy and security? Who knows that? And who can say I know all the advantages and disadvantages of the cloud?

Unfortunately most of the cloud users do not know or do not care about it, and you can find a lot of frightening news about data integrity and confidentiality failed.

This article is focused onto what can we commence the measured results of security awareness, how can we improve it and providing a self-supporting for cloud users. All interested in the company's view, what can they do to keep their privacy and data security if they moving to the cloud, or if their employees use their mobile devices in the company's environment. How can the company create a security policy and how can they force their users to keep it up.

There is ongoing research to size up the security awareness in different companies. It includes usage of smartphones, downloading apps, using pendrives and CD-ROMs, how many different password they have, how many different business application they have to use, how often connecting to a Wi-Fi, how often sharing internet, or how often check their account on different community sites and how they can separate private and business life. On opinion is that the aforementioned features are useful, and optimize the cost, there are efficient and make everybody reachable anywhere anytime. But we need strict internet security rules, we need education to understand what can happen with us in cyberspace. It is possible to use these options – but there are a lot of situation what we need to handle using cloud computing.

CLOUD AND ENTERPRISE IT

IT is not a typical department. IT is an enterprise-shared service that is critical to the minute-to-minute functioning of the entire organization. The availability, the confidentiality and the integrity is the most important services and IT has to provide all of them to their customers. Enterprises have invested a lot in technology, hoping to improve their execution capability, drive productivity, improve profitability and attain sustained competitive advantage. Some have been more successful than others in getting the expected returns from their technology investments but few, if any, have been able to realize the full potential of their investments. In fact, with time many enterprise IT organizations have grown in complexity as well as in size and are proving to become quite unmanageable – a drain on their business margin structures and some are even viewed as inhibitors for supporting the ever changing needs of business.

Using enterprise cloud services the companies expect, that the availability, integrity and confidentiality are provided on a higher level and they can reduce the costs at the same time. Customers want particular concreate SLA-s to provide their paid services and their properties. CIOs have to answer several questions, for example which applications will be migrated to the cloud, which could give more savings, how can make a strategy to use cloud computing as part of the IT services mix. Generally, the level of computer security, data privacy practices and the expertise of major cloud service providers are likely to be greater than those provided by an in-house IT staff and systems. This makes the security concern less salient. Nevertheless, before moving data and applications to a cloud it is important to ensure the cloud provider has strong security and privacy policies in place.

Cloud provides significant opportunities for businesses of all size. Scaling is essential function of cloud, you can use the same service in a small business and use the same in large businesses as well. And cloud services have to handle the companies growing, for example a startup needs in the beginning and at the top of their up growth. While there is a clear evidence of upfront (capex) cost reduction, businesses embark on cloud for agility, elasticity, and mobility reasons.

Flexibility means how the service can conform to your company fluctuation. If you need more employee in the summertime – you want to pay only for that two or three summer months you use the cloud services. Monitoring these expected characteristics it could be not easy to provide a splendid service they want to subscribe for. Nowadays the cloud services are not so famous in Hungarian Enterprise environment. IT Management being afraid of cloud, try to bypass it, and solve IT problems in the traditional way. But on the other hand the employee uses cloud, they uses free cloud services – which have weaker SLA-s, if they have any Service Level Agreement. So companies have to solve the integrity of their IT infrastructure however their users not followed the IT policies.

Enterprises want to their IT environment less complex then it is supporting and serving the business needs. Cloud Computing can do it less complexity, and can provide a unified platform. This could be the second advantage after the first, cost.

ENTERPRISE SECURITY AWARENESS

Whether a company is deploying a private or hybrid cloud, security remains a major concern. Cloud security often refers to user authentication and data protection, typically through encryption. Among the many issues is the ability to authenticate employees to control the cloud services and data they have access to. In addition, managing cloud security so that policies and compliance standards enforced within an internal network are extended to the cloud remains a challenge for many organizations. Adding to the complexity is the virtualization layer that sits between the operating system and hardware in the infrastructure of cloud service providers. That layer also must be configured, managed and secured [1].

Cloud security is a complex issue influenced by many factors and choices including: solution architecture, service model, deployment model, and hosting environment. This not only requires a solid understanding of the cloud solution but also various security domains and an expert understanding of compliance and risk management. If you are a small or medium size organization, the chances are you will embark on a public, hybrid, or community cloud solution which will provide you with more security than you would have had otherwise. The main issue is to be aware of risks and utilize the security controls offered by the cloud vendor.

Based on a wide scale spectrum Hungarian research (National University of Public Service) [2] resumes the level of IT security awareness in Hungary. The research differentiate the small and mid-size businesses, the enterprise and the public sector as well. 25 % of the under 250 employee businesses, the employees need IT security trainings. Enterprise size companies have a strategy to create the IT security awareness, users have more IT security knowledge but have more IT expectations to make their work easier and efficient. Large enterprise employees take part in a training, and they can keep the rules in cyberspace. Large enterprises have resources and budget to manage these trainings and they have IT strategy to handle trainings and educate their employee's.

Some typically cloud security alliances at Enterprise IT Environment are shown in Figure 1. The proprietary information is at risk every day; and it's not just data which can be lost. Data breaches cost money, customers, and even market share. Unfortunately, many breaches result from a lack of employee awareness of the security risks inherent in their actions.

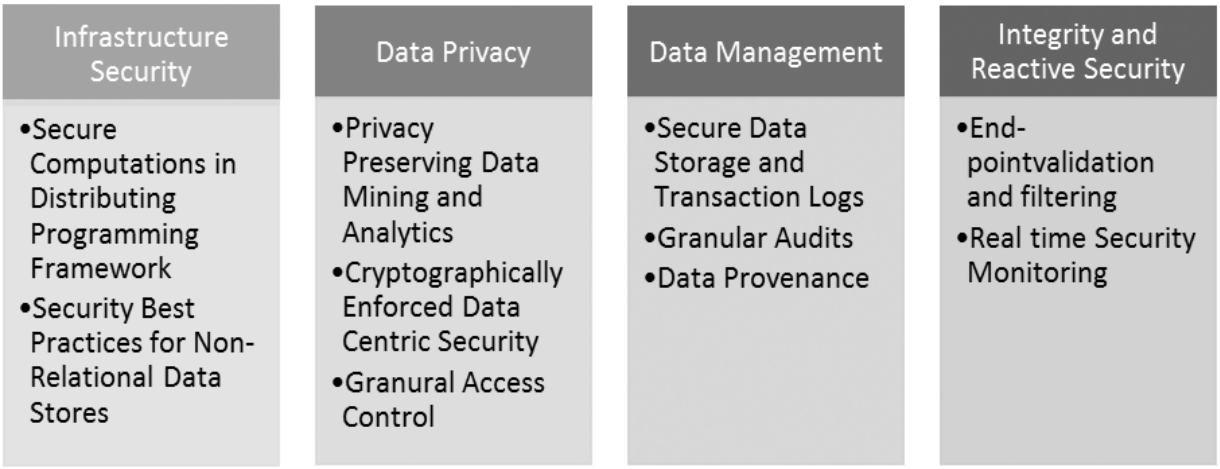

Figure 1. Some typically cloud security alliance at Enterprise IT Environment.

BYOD

Developing of mobile devices the demand has been growing. The users want to use their high-tech smartphones or tablets all the time. It used during travelling – *even in a plane now* – they bring inside to the company, and try to download the company mailbox to this devices or try to connect to the company's server. More and more company have a new policy – *every employee can bring not more than 3 own different devices into the company, typically a smartphone, a laptop and a tablet* – and get access to use it in work time too.

But, on the company side has to solve the different mobile management. By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime. With mobile devices becoming ubiquitous and applications flooding the market, mobile monitoring is growing in importance.

PRIVACY AND DATA SECURITY IN THE CLOUD

The economic case for cloud computing has gained widespread acceptance. Cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources. The economies of scale increase revenue for cloud providers and lower costs for cloud users. The resulting on-demand model of computing allows providers to achieve better resource utilization through statistical multiplexing, and enables users to avoid the costs of resource over-provisioning through dynamic scaling [3, 4].

At the same time, security has emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing. This view originates from perspectives as diverse as academia researchers, industry decision makers [5], and government organizations. For many business-critical computations, today's cloud computing appears inadvisable due to issues such as service availability, data confidentiality, reputation fate sharing, and others.

HOW TO TEACH CLOUD SECURITY FOR CONSUMER?

First of all teaching cloud security is the most important task we have to manage. Security questions are here, the treatment of the cyberspace are frightened us. Any IT devices, software, hardware are reachable for everybody, and you cannot mention any kind of job not using an IT application via Internet. IT became an essential service, and all of part of business

and private life to use IT and cannot manage a lot of action without IT service. Cloud computing brings new training and learning tools to education. Teachers or trainers reach their students in an easy way in different platforms, for example the web conference, social community sites, common sites, hosting sites or they can evolve closed user group for a training teams.

Cloud computing advantages bring new possibilities in studying for students as well. They have anywhere and anytime access, the students can apply for different universities, or listen in a foreign course. The borders disappear, there is no physical barrier, and there is no distance between students in different universities, different countries. Students can use any device they have and connect easily to the university cloud. Studying can be supported a sort of interactive or online elements, they can solve problems commonly or work together on a same project using co-working apps. I like to mention and other advantages of using cloud at the university, student can get several cloud skills which are good experience – and usable for a job application. Students take part in foreign scholarships or foreign project without traveling abroad.

In Hungary some university have started to use advantages of the cloud. For example the Óbuda University started a course in 2014, which is available for students at partner universities. The Informatics Faculty of ELTE was the first in Hungary moved to the cloud, providing several features to its students. The Miskolci University and the Debreceni University had moved to the cloud and provide their students mailbox, SharePoint sites, OneDrive cloud storage with 1 TB, and professional web conference with presence and chat functions. The underlying research asks how the IT security awareness could be extend, what different didactics we have and what are of them effectiveness for users. It is tempted to size up the average knowledge, and to try different learning tools and follow up the effectiveness of the different tools [6].

ONLINE TRAININGS VS. PERSONAL TRAININGS

Online trainings can produce great results by decreasing costs and improving performance. Also, unlike a onetime classroom session, the e-learning course is available for others. Online or E-learning trainings improve training costs, each time the course is accessed your return on investment improves because you are dividing the fixed production costs by number of uses. You also have savings through decreased travel, reduced material, and hopefully improved (and more efficient) performance [7].

E-learning is not bound by geography or time, you can control training's impact on production by training people during down times. In addition, with the current economy, you're asking people to do more with less. So e-learning is a great way to give them the tools and skills needed to enhance their performance. E-learning allows you to create a standardized process and consistency in the delivery of content. It also compresses delivery time. We have combined e-learning courses with facilitated sessions. E-learning delivered consistent content. Live sessions were interactive case studies that applied the information.

Personal training has different advantages, you can get a real-time feedback, and you can check the level of the students and shape the content to the students need. You can give a soul to the content or emphasis the logical skeleton. You can answer their question and realize the trammels and you can help them to overtake that trammels. Yes, it is cost a lot, it has personal limit, and you can find a suitable place and a suitable time for all of the participants.

One opinion is that the aforementioned didactic elements, to be mixed together, need a smart selection of the content, and alternate the tools, to create a balance in the education.

REFERENCES

[1] CRN Staff: *The 20 Coolest Cloud Security Vendors*.
http://www.crn.com/slide-shows/cloud/232602538/the-20-coolest-cloud-security-vendors.htm?pgno=1, 2012,

[2] Sasvári, P and Som, Z: *Examination of the information security awareness of the Hungarian business and public sector*. In Hungarian.
Lecture, National IT Security Day – ITBN 2014, 2014,

[3] –: *Amazon web services economics center*.
http://aws.amazon.com/economics,

[4] Armbrust, M. et al.: *Above the Clouds: A Berkeley View of Cloud Computing*.
Technical report EECS-2009-28, UC Berkeley, 2009,
http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html,

[5] Shankland, S.: *HP's Hurd dings cloud computing*.
CNET News. IBM, 2009,

[6] Mester, G.: *Introduction to Cloud Robotics*.
Proceedings of the SIP 2014, 32nd International Conference Science in Practice, pp.1-4, Osijek, 2014,

[7] Kuhlmann, T.: *Why E-Learning is so Effective*?
http://www.articulate.com/rapid-elearning/why-e-learning-is-so-effective, 2010.

KRETANJE PREMA SIGURNOSTI OBLAKA

S.E. Rubóczki i Z. Rajnai

Sveučilište Obuda
Budimpešta, Madžarska

SAŽETAK

Računalni oblaci sadrže i isporučuju više različitih internetskih usluga. Više je razloga zbog kojih se odlučuju koristiti resurse računalnih oblaka. Razvoj oblaka se ubrzava i za njime kasni mnoštvo pridruženih usluga poput svjesnosti mase i sigurnosti oblaka. Nove generacije, npr. bez razloga pohranjuju video snimke i fotografije u resursima oblaka, dok ih je samo neznatan broj upoznat s pojmovima privatnost podataka, upravljanje podacima i vlasništvo podataka pohranjenih u računalnom oblaku. U poduzetničkom okruženju korisnici moraju biti upoznati s pravilima korištenja računalnih oblaka ali su oskudnog znanja o tradicionalnoj sigurnosti informacijskih tehnologija. Bitno je mjeriti razinu njihovog znanja i razvijati sustav učenja kako bi povećavao svjesnost o sigurnosti.

Rad dokazuje značajnost predlaganja novih metrika i algoritama mjerenja svjesnosti o sigurnosti za korporativne korisnike i zaposlenike kako bi se odgovarajući zahtjevi uključili u razvijajuću sigurnost računalnih oblaka.

KLJUČNE RIJEČI

sigurnost oblaka, informatičke tehnologije