Security Issues of Cloud Based Services - a Guide for Managers

Dragoş-Marian MANGIUC[1]

Abstract

The cloud is no longer the future, but the present for small and medium-sized computer-centric companies. Technologies in the Enterprise 2.0 area keep on gaining popularity, as the business cloud computing market flourishes. While the managers of all sizes companies start to evaluate the potential fit for cloud-based services, the security issues become more and more significant. In addition to the security provided by the cloud services providers and the security measures taken by customers themselves, a third "wave" of security sources arises: security provided as a service.

Based on both literature review and action research, the paper at hand is a synthesis for the results of a thorough review of the opinions and study attempts performed during the last years among Romanian and foreign companies' managers, in order to find and formulate a consistent, independent and impartial answer to the question: "Is the service-based security a valid option for the cloud-based services, or is it just a tempting promise made to attract customers?"

Keywords: *Enterprise 2.0, cloud-based security, security-as-a-service, cloud security provider, cloud computing, security services.*

JEL classification: M15.

Introduction

Any serious concern in the field of cloud computing technologies' management reaches, sooner or later, to deal with the issue of cloud-based data and services security. Most cloud service providers consider cloud security to be no longer an issue, and almost all state that the security "gaps" which used to concern the potential customers during the early years of cloud computing have been solved long ago, both at a theoretical and practical level. However, common sense leads to the conclusion that a cloud-based information system cannot be less exposed to security attacks than a "traditional" information system and, by consequence, the security issues cannot be solved entirely and for good for such systems, as no application type is immune to security risks. This is why, in the field of information systems audit (may them be cloud-based or not), the main concern is not to eliminate security risk (which is impossible), but to manage security risks and keep them at a reasonable level.

There is a high responsibility for the managers to assure reliable and secure information to the organization's stakeholders. Having a managerial position and a greater access than the employees to the organizational information, managers have

[1] **Dragoş-Marian MANGIUC,** University of Economic Studies in Bucharest
Email: **mangiuc@gmail.com,** Telephone: +40723 22 78 76

a holistic vision upon the company, being focused on the improvement of the performances and the increase of the organizational efficiency (Mandruleanu, 2012).

Most studies in the field of cloud-based information systems security are focusing either on the security mechanisms that cloud services providers offer, or on the security measures taken by their customers. In the author's opinion, there is a third significant source of security, which is the security provided as a cloud-based service, also known as security-as-a-service.

1. Research Methodology

This paper is one of the results of a larger research performed by the author in the field of cloud computing and Enterprise 2.0 technologies management, and also continues a previous doctoral research in the field of computer-assisted audit tools and techniques, whose final results were publicly defended in order to be validated by both the scientific and academic community. The main goal of the aforementioned research was the identification of some new areas of applicability for the modern knowledge-based information technologies in the field of computer-based audit.

Wherever possible, a direct identification of the practitioners' expectations was attempted by means of direct interviews and also by means of an empirical study questionnaire. The questions for the empirical study were carefully designed so as to get unbiased, objective answers. The members of the target group (mainly managers of computer-centric companies) were encouraged to add their own observations regarding the questionnaire. Validation of the research conclusions was performed by means of an informal discussion with some "real life practitioners", managers or executives of some companies which performed or are in the process of performing a migration to cloud-based services. Also, professionals from a cloud migration assistance and consulting company were interviewed.

In case some other author's opinion was enclosed in the paper, whether in exact quotation or synthetic form, a complete mention of the source identification information was made. Some of the data in the paper is based on the results of some previous scientific or market research studies that were credited accordingly.

The author has over ten years of previous experience in the research area, and also a series of previous research results (published articles, conference attendances and doctoral research). By publishing the research results in such a prominent journal, reviewed by both scholars and practitioners bearing some interest in the research area, the author attempts to get further validation of his opinions, both confirmation and rejection of the aforementioned opinions' scientific and practical importance being welcome.

2. Old vs. New In Cloud Services Security

In the area of security-as-a-service, two main categories of service providers aroused during the last years:

- The first category refers to the group of the traditional distributors for software security products, which are attempting to diversify their offer, in order to also include cloud-based services;
- The second category refers to emergent, freshly-founded companies activating in the field of information systems security which are looking forward to gain public recognition as cloud-based services distributors and, as a result, do not provide at all security services in their "traditional" approach (client-server systems security, network security, computer security or application-level security systems) (Zissis and Lekkas, 2012).

A recent market study (Wu, 2011) proves without a doubt that among the security services providers who are re-engineering their business models in order to include cloud-based technologies, the leading places are taken by the traditional distributors of anti-virus software products. However, a small group of other kind of companies has a more and more obvious presence, mostly in the niche markets, like the "cleaning" and filtering services for the huge number of e-mail messages received by the large organizations.

In the author's opinion, the idea of delivering security services through the cloud has its origins in a few main sources. The first and also the most "ancient" is already over a decade old and refers to spam, or, in other words, unsolicited e-mail. Since twelve or thirteen years ago, some software producing companies have enclosed in their software offer e-mail filtering applications, as e-mail was considered to be "the Internet's most precious resource" (Lederer, et al., 1997). Such companies were indirectly blaming the Internet services providers for not providing e-mail traffic filtering for their own subscribers and for allowing (for money) some aggressive marketing campaigns to treat each subscriber of the e-mail service as a potential customer. The market for e-mail traffic filtering services matured and diversified, including both companies who specialized in producing security software applications and Internet service providers who retail their own security solutions, or sell under their own brands security software developed by third parties (Song, et al., 2004).

The second development source for the advance of cloud-based security services is the market of externally achieved security services, usually called Managed Security Services (or MSS). The providers of such services allow the outsourcing (externalization) of the security system for the companies whose dimensions or resources do not allow an internal management of the security system. This business model implies that an external organization manages, based on a contract, the security systems and mechanisms of a company (like firewall equipment or intrusion detection systems – IDS). The customers' option for such systems is based on the same factors as the general option for the cloud: significantly lower costs when compared to the resources-intensive in-house solutions. The main difference between the cloud services providers and the managed security services providers is that the latter do not provide infrastructure services (as the security infrastructure belongs to the customer), but only personnel (security experts). For the small and mid-sized companies which do not have the possibility and the available resources to sustain a security department and to hire reasonably trained security experts, the alternative of services externalization looks like a passable choice (Benlian and Hess, 2011). This security assurance model has become an extremely important influence factor because it has broken the psychological barrier which traditionally had forbidden managers to publish or to hand over to a third party their own security policies and systems. The model evolved from providing the services exclusively at the customer's site to providing the services remotely, even from different countries or continents, as the jurisdiction issues were dealt with (Yara, et al., 2009). In the author's opinion, even if the security work as such is externalized, the responsibility to assure the security of the own information system is still in the duty of the customer organization's manager, and he still has the responsibility to directly or indirectly formulate the access and security policies, and also to continually monitor the security services providers in order to check whether the aforementioned policies were properly implemented and enforced. The security services provider manages equipment and data flows being the property of its customer. Thus, the recourse to such a business model has as a result the mere decrease of the operation expenses, without affecting the level of the capital expenses (equipment) which remain compulsory. As opposed to the aforementioned model, the option for cloud-based security services also allows a decrease of the capital expenses, as both equipment and management and monitoring tasks are the duty of the service provider.

The third development source for the expansion of cloud-based security services is the constantly decreasing efficiency of the security assurance process, when the security assurance is performed at the final nodes of the network (which may be desktop computers, laptops, servers, mobile devices or some other type of equipment). The causes of the decrease are the enormous raise in the number of terminals of all kinds, as well as the huge variability of the configurations (hardware, operating system, platform, application software etc.), the final result being the impossibility of an efficient management of the owned resources (Desmet, et al., 2012). Moreover, as a lot of these terminals are new generation mobile devices, solving configuration conflicts and repetitively update security applications become resource-intensive tasks. And it is a common issue that because of the mobility requests or the old age, most of the existing terminals do not have the necessary resources (computing power, memory, storage space or Internet bandwidth) to execute complex security applications. Because of such issues, along with the enormous increase of the malware applications, securing the terminal nodes of a network has become a major issue. A few millions malicious new code sequences are discovered each year (Ding, et al., 2011). All the aforementioned phenomena led to a change in the way terminal nodes security is thought of and designed: instead of protecting the terminals by executing security applications on them, couldn't the terminals be protected directly from the cloud? This means traffic filtering and the identification of the potential threats are not accomplished directly on the terminals, but are performed by specialized equipment directly from the cloud. Even if in the beginning the idea looked more like a fantasy, the concept got through significant development, especially since a recent study (Oberheide, et al., 2008) proved that by comparison with the terminal-based security applications, the cloud-based security applications offer 35% better detection of the security threats, having an overall detection rate around 98%. Such a detection rate significantly surpasses the detection performance of an independent detection system running on a terminal node of a network (as previously stated, most of the terminals are seriously constrained by their own resources and existing incompatibilities to run a single version of a single security application).

The actual offer in the field of security delivered as a service in the cloud may be synthesized by enumerating the main services created in order to improve information security:

- E-mail messages filtering and "cleaning" (including back-up, archiving and e-discovery);
- Web content filtering;
- Vulnerabilities management;
- Identity-as-a-service (IDaaS).

3. E-Mail Traffic Filtering and Cleaning

Providing security services for e-mail basically means eliminating spam messages, phishing attacks-containing messages, as well as malicious applications included in different e-mail messages. Such operations are performed over the e-mail message flow entering an organization, so as the messages effectively entering the organizational network are clean and unpolluted by malicious agents. In the author's opinion, this approach has significant advantages, as it is possible to use multiple search engines, along with an indirect increase in the terminals' performance, which are no longer configured to allocate their own resources in order to execute security applications (Mangiuc, 2011). It is quite obvious that such "centralization" allows for a better and easier management of the systems and security policies. Moreover, as the platforms executing the security applications are not directly connected with the network terminals, the issue of different configurations management and the issue of compatibility are no longer real concerns. This way, the process of managing a large number of security applications' versions, acquisitioned from different software producers, is replaced by the much simpler process of managing a single security system, provided by a single software producer. The following may also be mentioned as side benefits:

- The decrease of the bandwidth used inside the organizational network for the e-mail traffic (as the unwanted messages have been eliminated before entering the organization's data flow);

- The decrease in the organization's e-mail servers load (as the servers no longer need resources to manage and deliver the unwanted messages);
- An increase in the organization's efforts to eliminate unwanted e-mail.

Even if, in a traditional way, the e-mail messages filtering process pays the highest attention to the received e-mail messages, the outgoing e-mail messages also have to be taken care of (Andrade Gonzalez, et al., 2009). A large number of organizations would suffer from serious image issues if they have sent their customers or business partners e-mail messages containing malicious code sequences and, as a consequence, are trying as much as possible to avoid such an accident. In the author's opinion, the systems employed for e-mail traffic filtering and cleaning may also be used for the organization-level encryption of the e-mail messages sent to customers and business partners, so as to avoid the need that each e-mail message is encrypted by its sender (which may or may not have knowledge in the field of encryption techniques). After the encryption process, communication with the customers' and business partners' servers may be realized by means of a specialized protocol, such as SSL (Secure Socket Layer) or TLS (Transport Layer Security).

Another obvious advantage of the aforementioned approach is the gain of knowledge at an organizational level, happening when all the discovered threats are visible for all the network terminal nodes, no matter their type, configuration and platform. The fact that each terminal is able to access "the big picture" becomes a significant help for the organization's managers and security experts.

Delivering security as a service in the field of electronic mail may be rapidly extended to a set of back-up and archiving services (Tauber, 2011). Such services usually imply storing and indexing the e-mail messages received and sent by an organization (and also their attachments) in a single catalog. This centralized catalog allows the organization to index and search the e-mail database using different criteria such as a time interval, the sender, the receiver, the subject or the content. Features of this kind are extremely useful for the e-discovery process, which would prove to be extremely expensive in their absence (Grensing-Pophal, 2011).

4. Web Content Filtering

The process assumes that the whole Web traffic generated by the terminal nodes of an organizational network (no matter if they reside physically inside the organization's area, are taken home by the employees or are moving as mobile devices) to be diverted to a cloud-based security services provider, which is able to scan the data flow in order to isolate the possible malicious applications or code sequences, delivering to the final users (terminal nodes of the network) only safe Web content. In this manner, an organization will be able to implement its own Web content-related policies, for example:

- Partially or totally forbidding the access to certain websites;
- Totally forbidding or bandwidth limiting for certain protocols (like audio or video streaming);
- A list of sites having priority access or whose users benefit from higher priority when using the available bandwidth of the communication channel.

Such policies are commonly used nowadays in order to limit employees' access to the social networks and to the entertainment sites delivering high quality multimedia content, consuming or overloading the bandwidth of the organization's Internet connection (Gao, 2012). It is obvious that exactly like e-mail messages filtering the process results in a decrease of the organizational network load, as access is granted only for the content which is compliant with the security policies.

Because of the very high number of websites accessible today, the older filtering solutions, traditionally implemented at the level of each terminal of the organizational network, are less and less effective each day. The acquisition of cloud-based security services in this area brings an additional level of security, and its importance is continually increasing. Specialized servers in the cloud may perform processing which would "clog" the resources of a single terminal, rendering it unusable for its main tasks. Among the most common processing in this area may be mentioned:

- The detailed examination of the data in the header that the HTTP (Hypertext Transfer Protocol) protocol attaches to each data packet;
- The semantic examination of the content of each requested or published page;
- The examination of the hyperlinks in the content of each page;
- The creation or access of a global service which grants reputation scores to websites, web pages and web resources. The appeal to the enormous databases of such a service (also based on the cloud) may significantly improve the efficiency of the filtering and search engines attempting to "clean" the Web traffic of an organization.

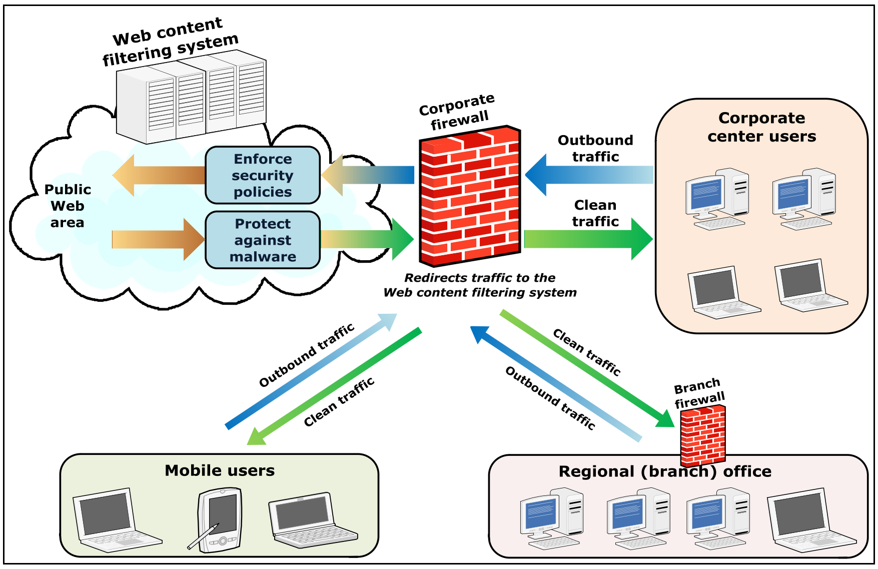

Figure 1. The Web Content Filtering Process

For the organizations which process confidential data (and this includes most of them), the Web content filtering also implies the analysis of the traffic flowing from inside the organization to the outside. Users from inside the organization may intentionally or accidentally send to the exterior data elements whose broadcast is forbidden by the legal framework or the internal policy of the organization (personal numeric codes, social security numbers, information regarding bank accounts or credit cards, information protected by the intellectual property laws etc.). Preventing data leaks may be improved by analyzing the content of the files, the file types, some authors even proposing some pattern-matching techniques. The Web content filtering process is synthetically explained in Figure 1.

5. Vulnerability Management and Identity Management-as-a-Service (IDaaS)

As the presence of the organizations in the virtual environment (on the Internet) is stronger and stronger, growing in both dimensions and complexity, and the weight of the Web-based transactions in the total business turnover is increasing; providing the security of the information systems configuration and operation process has become more and more difficult and, at the same time, more and more important. As a consequence, many of the security-as-a-service providers are attempting to discover, identify in detail and sort (based on priority) the vulnerabilities of such systems. Subsequently, they report the identified vulnerabilities, attempt to fix them and sample the security of the systems operating in the new set of conditions. The information in this category may be used afterwards to monitor and report the compliance with certain industrial standards like ITIL (Information Technology Infrastructure Library) or PCIDSS (Payment card Industry's Data Security Standard).

Identity management-as-a-service (IDaaS) is the latest trend in the security-as-a-service delivery techniques package, extremely new when compared to e-mail filtering, Web content filtering or vulnerabilities management, which may be already considered mature products in the area (Sanchez Garcia, et al., 2011). Among the components of the IAM (Identity and Access Management) system, most of the service providers offer support in the field of authentication management, as this aspect is of main importance for the customers of a company (Gomi, 2012). However, the main issue that the cloud-based security services providers have to solve is the need for a collaborative meta-system, a system of virtual directories able to facilitate both the corporate customers' authorization process and the subsequent auditing of the corporate security system. The domain of IDaaS is extremely comprehensive, as the area is still at an early stage, and the actual state of the services still suffers from significant deficiencies. A synthetic image of the IDaaS working model is presented in Figure 2.

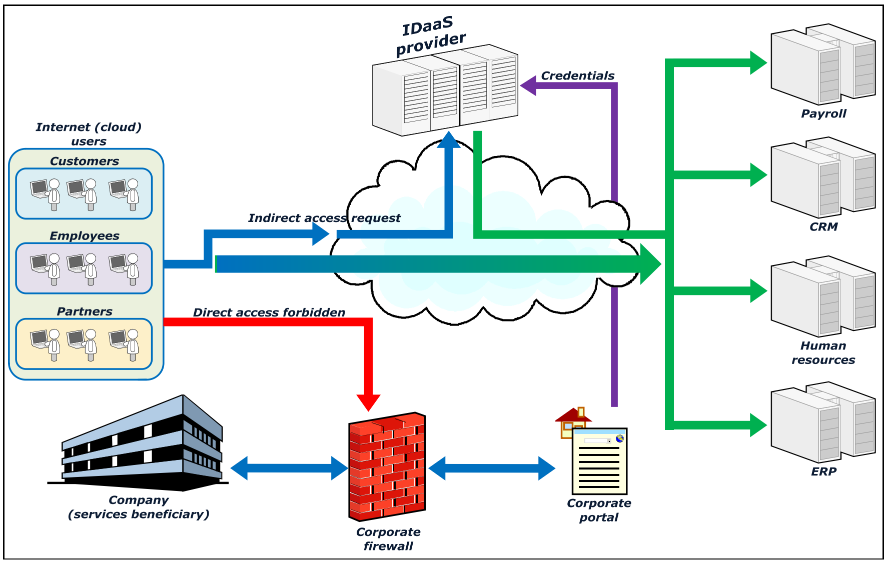

Figure 2. A View of the IDaaS Model

Conclusions

In the author's opinion, the offer for cloud-based security services has the defining characteristics of any emergent domain in the IT industry: intentions are remarkable, the future projections are extremely interesting for managers, but the actual implementation level still suffers from the lack of previous experience and the lack of standardization (which is at a very early stage). Some of the elements in this offer are not only viable, but are quickly approaching a certain degree of maturity. It can be considered that the Web content filtering services and the e-mail traffic filtering services are already a few years old, and the models and methods behind them are developed to an acceptable level (when compared against the requests of the current main IT security industry standards). As opposed to the aforementioned services, some other components are extremely new, still suffering from some deficiencies inherent to the maturation process. Even if such services are currently offered by multiple companies, and the providers are using their own specialized cloud-based systems, the analysis of the existing offers still does not reveal the existence of a complete and integrated cloud-based security solution, mature enough to directly compete with its more "traditional" counterparts.

References

1. Andrade Gonzalez, E.A., Reyes Ayala, M. & Tirado Mendez, J.A., 2009. *Security System for Mobile Users*. Aic '09: Proceedings Of The 9th WSEAS International Conference on Applied Informatics and Communications Book Series: Recent Advances in Computer Engineering, pp.31-33.

2. Benlian, A. & Hess, T., 2011. *Opportunities and Risks of Software-As-A-Service: Findings from a Survey of IT Executives*. Decision Support Systems, 52(1), pp.232-246.
3. Desmet, S., Volckaert, B. & De Turck, F., 2012. *Design of a Service Oriented Architecture for Efficient Resource Allocation in Media Environments*. Future Generation Computer Systems-The International Journal of Grid Computing and Escience, 28(3), pp.527-532.
4. Ding, Y., et al., 2011. *Feature Representation And Selection In Malicious Code Detection Methods Based On Static System Calls*. Computers & Security, 30 (6-7), pp.514-524.
5. Gao, X. & Guan, J., 2012. *Network Model of Knowledge Diffusion*, Scientometrics, 90(3), pp.749-762.
6. Gomi, H., 2012. *Authentication Trust Metric and Assessment for Federated Identity Management Systems*. IEICE Transactions on Information and Systems, E95D(1), pp.29-37.
7. Grensing-Pophal, L., 2011. *A Whole New World: Best Practices for Navigating E-Discovery*. E-Content Magazine, 34(4), pp.16-21.
8. Lederer, Al., Mirchandani, Da. & Sims, K., 1997. *Marketing on the Web: A resource-based perspective*. Association for Information Systems Proceeding of the Americas Conference on Information Systems, pp.197-199.
9. Mandruleanu, A. (2012), *The Impact Of Integrators On The Organisational Intellectual Capital*, Management Marketing, no 3/2012, pp. 434-435
10. Mangiuc, D., 2011. *Enterprise 2.0 – Is the Market Ready?*. Journal of Accounting and Management Information Systems, 10(4), pp.516-534.
11. Oberheide, J., Cooke, E. & Jahanian, F., 2008. *CloudAV: N-Version Antivirus in the Network Cloud* [Online]. Presented at the USENIX Conference, San Jose, California, July 2008, Available at: http://www.eecs.umich.edu /fjgroup/pubs/ cloudav-usenix08.pdf [Accessed 10 August 2012].
12. Sanchez Garcia, S., Gomez Oliva, A., Perez Belleboni, E. & Pau de la Cruz, I., 2011. *Solving Identity Delegation Problem in the E-Government Environment*. International Journal of Information Security, 10(6), pp.351-372.
13. Song, W., Chen, Dr. & Chung, Jy., 2004. *An Investigation on Using Web Services for Micro-Payment*. Web Services, Proceedings Book Series: Lecture Notes in Computer Science, 3250, pp.213-226.
14. Tauber, A., 2011. *A Survey of Certified Mail Systems Provided on the Internet*. Computers & Security, 30(6-7), pp.464-485.
15. Wu, W.W., 2011. *Developing an explorative model for SaaS adoption*. Expert Systems with Applications, 38(12), pp.57-64.
16. Yara, P., et al., 2009. *Global Software Development with Cloud Platforms*. Software Engineering Approaches for Offshore and Outsourced Development Book Series: Lecture Notes in Business Information Processing, 35, pp.81-95.
17. Zissis, D. & Lekkas, D., 2012. *Addressing cloud computing security issues*. Future Generation Computer Systems-The International Journal of Grid Computing and Escience, 28(3), pp.583-592.