INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 4(26) • 2012
ISSN 1507-3858

Rafał Wojciechowski, Sergiusz Strykowski, Daniel Wilusz, Jan Świerzowicz
Poznań University of Economics

SECURITY CHALLENGES IN CLOUD COMPUTING FOR SMALL AND MEDIUM ENTERPRISES

Abstract: Cloud computing is a model of leveraging IT resources offered by providers via the Internet. In this model, small and medium-sized enterprises are able to transfer the costs of building and maintaining IT infrastructure to third parties. The IT resources are available on demand, and the consumers pay merely for the resources actually used. A key factor limiting the adoption of cloud computing are security concerns. However, these concerns should be collated with the security benefits possible to achieve thanks to the cloud's characteristics. This paper presents an analysis of the risks and benefits in the area of security related to cloud computing implementation in companies and an overview of initiatives aimed at increasing the awareness in this area.

Keywords: cloud computing, security, small and medium enterprises.

1. Introduction

Cloud computing is one of the most significant changes in IT technology observed in recent years [Gartner 2011]. The fundamental purpose of cloud computing is the scalable provision of IT-related capabilities as a service to customers using Internet technologies. Cloud computing allows companies to waive the responsibilities associated with maintaining the IT infrastructure and focus on their core competencies. In a cloud platform, resources can be provided to companies on demand, making it possible to quickly adapt the information technology to changing business strategies and needs at low capital investment.

Cloud computing is especially attractive for small and medium enterprises (SME) − due to the payment model based on charging only for the resources actually used, SMEs may get access to the best business applications and IT infrastructure at a price they can afford. Cloud service providers can in turn offer that price through economies of scale obtained in the cloud multi-tenancy environment. On the other hand, SMEs are full of concerns about the security threats in this new model; according to the research conducted by IDC, over 87% of IT executives recognize security as a key problem of cloud computing which prevents them from adopting the cloud service model [IDC 2009]. The security issues they list apply to the organizational, technical and legal aspects [*Cloud Computing*… 2009].

Real-world experience shows that security concerns should be collated with security benefits that arise from cloud characteristics. The fundamental advantages in this respect are high defense capabilities against ongoing and expected attacks which are possible to obtain thanks to massive concentrations of resources. Bearing in mind the security concerns of customers, the cloud providers take continuous actions to improve security measures, often making security as the main competitive differentiator.

The situation in the area of cloud security is not so clear. Cloud computing and its characteristics have both a positive and negative effect on security and the risks associated with it. Therefore in recent years several initiatives have been launched aimed at assessing risks, developing new security solutions and standards for the cloud, and specifying guidelines and best practices for current and future cloud consumers. The most active organizations in this area include the Cloud Security Alliance and the European Network and Information Security Agency.

The remainder of this paper is organized as follows. In Section 2, the main characteristics of cloud computing, deployment models, and service delivery models are described. In Section 3, security challenges in cloud computing are presented: first, three categories of security issues, namely organizational, technical and legal, are discussed, then security benefits, and finally a new trend in cloud computing – Security as a Service. In Section 4, an analysis of the most important current initiatives in cloud computing security is presented. The last section contains the conclusions.

2. Overview of cloud computing

The term *cloud computing* was introduced for the first time in its current meaning in 1997, but it started to gain more recognition around 2007. Gartner Research put cloud computing among the top 10 strategic technologies of 2011 [Gartner 2011].

With a variety of different cloud computing definitions [Geelan 2009], the National Institute of Standards and Technology composed a draft, where cloud computing was defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction” [Mell, Grance 2011]. In the draft, NIST also denoted five essential characteristics of cloud computing, three service models, and four deployment models.

A cloud provider delivers resources that are available over the network, and may be accessed from any standard platform. Cloud consumers can by themselves order and get resources, increase or decrease capacity at will, according to shifting changes in demand and are charged for what they actually consume (pay per use model). Usage is monitored and measured to ensure transparency both to provider and consumer. The cloud provider's resources are pooled in order to ensure optimal usage whilst no particular resource is assigned to any individual user.

There are three basic service delivery models of cloud computing*: Infrastructure as a Service* (Iaas), *Platform as a Service* (PaaS), and *Software as a Service* (Saas). In the IaaS model, a cloud provider offers a fundamental infrastructure (storage, networks etc.), on which consumers are able to deploy and run their software. The software deployed may include both operating systems and applications, and consumers retain control over storage and deployments, and possibly a limited control over selected networking components, e.g. firewalls. In the PaaS model, a cloud provider offers a computing platform and a platform-based solution stack enabling consumers to deploy custom-made applications. In this model, consumers have much less control over infrastructure than in the IaaS model. As an example of PaaS, Windows Azure and the Google App Engine are worth mentioning. In *the* SaaS model, consumers use software applications that are delivered within a cloud platform on a cloud infrastructure. The applications are accessed via a thin client (usually a web browser). In comparison to PaaS, in SaaS the consumers do not have control over the host environment configuration. It is quite typical that infrastructure (IaaS), platform (PaaS) and software (SaaS) are delivered by different providers. Many applications can be offered in a SaaS model, for example, web-based mail clients or CRM systems, e.g. Salesforce.com.

There are four main cloud deployment models: public, private, community, and hybrid. *Public cloud* is an infrastructure owned by an organization selling cloud services, e.g. Amazon EC2, which is open to the public, i.e. any individual or a company may have access to the cloud services offered. *Private cloud,* on the other hand, is an infrastructure that is open only to a selected organization. A data center for a private cloud may be located on-premises or provisioned by a third party. A cloud infrastructure shared by and open only to several organizations, which usually have similar information infrastructure requirements is called a *Community cloud*. Similarly to a private cloud, a data center of a community cloud may be located on-premises or provisioned by a third party. A *Hybrid cloud* is a composition of two or more clouds (private, community, or public) which are connected in a way enabling data and application portability between them.

3. Security challenges in cloud computing

3.1. Security risks

The research conducted by [*Cloud Computing*... 2009; Subashini, Kavitha 2011; Armbrust et al. 2009; CSA 2010] show that security risks fall into different categories and depend on the deployment and service models of cloud service. According to the ENISA's report, three security risk categories may be distinguished, namely: organizational, technical, and legal [*Cloud Computing*... 2009].

Organizational security risks

The decision on outsourcing the IT infrastructure maintenance means the loss of control over this infrastructure. The processes concerning IT infrastructure are carried out by the third party and the auditing of this processes is often limited or even impossible. There are numerous risk factors identified in the literature concerning organizational risk.

The human factor is deemed to be the weakest part of the IT system security. The employees of a cloud provider may pose a tremendous risk for cloud user data. If a company uses the cloud to store sensitive corporate data, malicious cloud administrators may copy the data, and remaining unnoticed, use it in a fraudulent way [Zissis, Lekkas 2012]. The lack of standards for tools, procedures, formats and interfaces means that the portability of data is hampered, or even made impossible, and consumers are often locked-in within one cloud service provider. Another problem resulting from cloud provider lock-in is the risk of consumer's business continuity in cases when the cloud provider goes bankrupt.

A company considering utilizing a public cloud has to be aware of the possible negative influence of co-sharing the cloud service on the business performance. One risk comes from the abuse of the cloud service by the cloud co-tenants. An example is the blacklisting of a co-shared IP address, caused by unsolicited e-mails sent by one of the cloud users. The source of other threats are external, malicious actions taken against one of the cloud co-tenants. For example, the DDoS (Distributed Denial of Service) attack on the service of one cloud consumer may affect the business processes of others [CSA 2010; *Cloud Computing*... 2009].

When using cloud services, a consumer cedes to a cloud provider the control of a number of issues that impact on security. This can result in the loss, or a significant reduction in, the consumer governance capabilities. On the other hand, a service level agreement may not contain a general obligation of a provider to deliver security services and shift the entire responsibility in this regard to the consumer, thus contributing to the emergence of serious gaps in security.

Technical security risks

The idea behind cloud computing is sharing computer resources among a number of cloud users. Companies planning to use cloud services must be aware of the risks concerning resource sharing, which comes from improper users' isolation and system security weaknesses.

In the IaaS service model, the virtual machines isolation and storage sharing is an issue of concern. The consumer's operating system has to be prevented from obtaining too high a level of control over the underlying platform [CSA 2010]. Otherwise, the data of other consumers may leak if security weaknesses are exploited. Moreover, the shared storage may also be the source of data leakage risk. If a cloud provider does not ensure the bleaching of the data when deleting, the other user may read the bits of assigned storage space and recover the deleted data of other users [Zissis, Lekkas 2012].

The cloud consumer, especially in the SaaS service model, is often forced to use the providers API in order to manage or interact with the cloud service. A discovery of API weaknesses is an attractive target for adversaries. The adversaries may use different attack techniques, such as cross-site scripting, SQL injections, field manipulation, etc. in order to access, change or destroy the data of a victim [Subashini, Kavitha 2011].

The cloud consumer is exposed to both the Distributed Denial of Service (DDoS) as well as Economic Denial of Service (EDoS) attacks. The DDoS aims at making the web service unavailable by the mass service requests performed by a large number of computers. The EDoS is carried out in order to cause financial damage to the cloud consumer by exploiting the cloud resources (storage, bandwidth, computation power) [*Cloud Computing*... 2009]. The use of a cloud service which does not prevent these types of attack may be a serious threat to the business performance (DDoS) and reputation (EDoS) of the cloud consumer.

Legal security risks

The cloud consumers have to be aware of the legal implications of using cloud services. The main issues of concern are: personal data protection, civil responsibility, multiple jurisdictions, and software license agreements.

Cloud consumers who collect and store personal data remain responsible for establishing appropriate security measures to protect it. According to the legislation of many countries, the use of an external service to handle the data does not necessarily waive the responsibility of the data collector for its protection. Therefore, the cloud consumer may be still sued in a civil or criminal trial. Moreover, in some jurisdictions it is forbidden to store personal data abroad − as the cloud model is based on internationally distributed datacenters this may be an issue of concern [*Cloud Computing*... 2009].

The jurisdiction also influences the data security. In some countries, the cloud provider may be forced by the court to make the user's data available (US PATRIOT Act) [Armbrust et al. 2009]. Furthermore, there are jurisdictions where the user is obliged to decrypt encrypted data and may be prosecuted if he/she refuses the decryption (UK RIPA).

3.2. Security benefits

The characteristics of cloud computing can also influence security and the resilience of IT systems in a positive way and even stimulate improvements in this area [*Cloud Computing*... 2009]. The key security benefits of cloud computing are discussed below.

According to the results of the survey conducted among small and medium enterprises [Catteddu, Hogben 2010], security is one of the key concerns for cloud consumers and many of them make a decision on the cloud provider based on the level of security measures offered. It is therefore a strong argument for cloud providers to continuously improve the security practices and even make them the essential competitive differentiator.

In case of a security breach it is necessary to conduct an investigation and examine the evidence. Virtualization provides the ability to quickly clone virtual machines covered by the investigation and conduct forensic analysis over the clone, contributing in this way to the short down-time of a system, which would have been an issue with traditional computing.

One of the characteristics of cloud computing is the ability of providers to scale resources on demand, i.e. allocating them in those areas where they are currently required. Cloud providers may therefore increase the level of support for defensive measures in cases of an ongoing or expected attack, such as a DDoS attack. This ability would have contributed positively to the resilience of government web systems during the attacks of the Anonymous hacker group in January 2012.

The service level agreement signed between a cloud provider and consumer often records the set of provisions, including financial compensations and liabilities, for the consequences of security breaches. Such provisions motivate cloud providers to more frequent and stricter internal audits, which has a positive impact on increasing the level of security.

The concentration of resources typical for a cloud infrastructure has a beneficial effect on reducing the unit price of the overall security procedures for controlling physical access, managing data, installing patches, incident management and maintenance processes.

3.3. Security as a Service

One of the current trends in cloud computing is to detach security measures and procedures and offer them as a separate cloud service. This approach is referred to as *Security as a Service* (SecaaS) [SecaaS 2010]. The service-based approach allows companies to utilize security measures in new ways, or in ways that would not be economically viable if those measures were provided locally. Unfortunately, the existence of many different forms of security services on the market led to customer confusion, which made the choice of proper security solutions difficult and consequently has resulted in the current limited use of this approach.

In order to increase transparency in the area of Security as a Service, the Computer Security Alliance established a new project to categorize the different security services offered via the cloud [SecaaS 2011]. The project aims at helping customers understand the nature of the security solutions offered via the cloud in order to enable them to evaluate these solutions and determine whether they are appropriate to their needs. The security services have been divided into ten categories: Identity and Access Management (IAM), Data Loss Prevention (DLP), Web Security, Email

Security, Security Assessments, Intrusion Management, Security Information and Event Management (SIEM), Encryption, Business Continuity and Disaster Recovery, and Network Security. For each category, the following elements were determined: core functionalities, optional features, challenges, included services, related services, related technologies and standards, threats addressed, and examples of services available on the market.

4. Analysis of initiatives for cloud computing security

Due to consumers' concerns about cloud computing security, a number of initiatives has emerged to develop security solutions and standards aimed at improvements in this area.

4.1. Cloud Security Alliance

The most notable example of an initiative dealing with cloud security is the Cloud Security Alliance (CSA), which gathers around 120 cloud vendors and other stakeholders. The mission of CSA is to develop guidelines and promote best practice aimed at ensuring the security of cloud computing.

The Cloud Security Alliance has become an incubator for developing global standards for cloud security through analyzing and aligning the various security policies established by the standardization bodies of different countries, and proposing cloud security standards to international standardization organizations for approval. CSA leads many research projects which aim to increase the security of cloud computing and reduce the fears of potential customers. The major initiative of CSA is *Security Guidance for Critical Areas of Focus in Cloud Computing* [CSA 2011]. This work serves as a high-level textbook for business executives and IT engineers who are interested in leveraging cloud services as an alternative or supplement to the traditional IT infrastructure. In particular, the document provides a road map for IT managers who would like to apply the paradigm of cloud computing in their companies.

Security mechanisms in the cloud are not essentially different from the security mechanisms in other IT environments. However, the cloud computing model may cause different threats to organizations than in traditional IT technologies. There are three areas within which issues related to the cloud security should be considered: cloud architecture, governing in the cloud, and operating in the cloud. These areas were identified to emphasize security, stability, privacy and confidentiality in a multi-tenant environment. The main point of interest focuses on maintaining the integrity of users' data whilst keeping the concept of shared infrastructure.

Each of these areas raises different security issues of cloud computing. The cloud architecture area deals with security aspects that are inherent in the main characteristics of cloud computing, various delivery models, and deployment models. The governing area consists of the security domains concerning the management level of enterprises, such as governance and enterprise risk management, legal issues, compliance and audit management, information management and data security, interoperability and portability. In turn, the operating area includes the security domains related to the operational level of enterprises, such as human resources and physical security, business continuity and disaster recovery, security of data centers, incident response, application security, virtualization, identity, and access management.

The security of an organization is determined by the maturity, effectiveness, and the completeness of the security mechanisms tailored to the potential threats. These security mechanisms are applied at one or several layers, starting from the physical security equipment, through the network security infrastructure, the security of IT systems, the security of applications, up to the security procedures for people and processes.

In the SaaS model, security mechanisms and their scope are negotiated under a contract for the provision of services. Service levels, compliance, and privacy are subject to detailed legal arrangements included in the contract. In the IaaS model, the cloud provider is responsible for the security of IT infrastructure and abstraction layers, whereas the higher layers of the stack are the responsibility of the consumer. The PaaS model provides the intermediate solution in which the platform security is the duty of the provider, but the security of applications running on that platform is the responsibility of the consumer. Awareness of the differences between the service delivery models is essential for the proper and conscious risk management in an organization.

4.2. European Network and Information Security Agency

The European Network and Information Security Agency (ENISA) is an agency of the European Union, serving as a center of excellence for EU member states and European institutions in the field of information security in IT systems and computer networks, in particular the Internet. The agency's activities are focused on providing advice and recommendations, developing standards and guidelines as well as being a European center for information on best practice in the field of computer security. In the area of cloud computing, ENISA has developed a report entitled *Cloud Computing Report: Benefits, Risks and Recommendations for Information Security* [*Cloud Computing…* 2009].

The report contains a detailed analysis of issues related to information security in cloud computing: analysis of the security benefits, security risk assessment, analysis of risk sources, analysis of vulnerable organization activities and assets and a list of recommended actions for consumers and providers in order to counter security risks.

Cloud computing risk assessment was carried out by analyzing three scenarios: cloud computing opportunities and threats for small and medium-sized enterprises, the impact of cloud computing on service resilience, and cloud computing opportunities and threats in e-government.

The selection of SMEs as a survey object was dictated by the fact that 99% of companies in the EU belong to this market segment. The survey included companies from 16 European countries, the USA, Canada, and India. The survey results showed that due to cost reduction and flexibility in the access and utilization of IT resources, the migration to cloud computing is very attractive to many SMEs. The main problems recognized were concerns about data confidentiality and the fears of cloud providers being able to deliver reliable technical infrastructure. Nevertheless, SMEs must face the fact that many of their employees will use the cloud services, regardless if it is officially recognized as acceptable or not.

The report lists and describes in detail 35 key risks associated with cloud computing. The risks are classified into three main categories: policy and management, technical issues, and legal issues. For each risk the following factors were determined: probability of occurrence, the level of impact on organization activities, the risk sources, the potential losses, and the risk level. Additionally, if the risk was evaluated as significant, the probability of occurrence and level of impact for standard IT technology were added for comparison.

The report specifies three main recommendations referring to risk management in cloud computing: information assurance framework, legal recommendations, and research recommendations. The information assurance framework includes a list of questions to be asked by a cloud consumer, and a list of points to be checked by a cloud provider to ensure that cloud infrastructure and management policy meet the requirements of information security. The list includes the security requirements related to legal issues, physical security, policy and technical issues. The list is intended to serve as a tool for cloud consumers to assess the risk of adapting cloud computing and compare the services offered by various cloud providers. The report also presents the recommended division of liabilities and responsibilities between a consumer and a provider.

In terms of legal recommendations, the report lists the areas in which consumers should pay attention when reviewing SLAs and other cloud service agreements. In terms of research recommendations, the report points out the following issues as priority research areas for improving cloud computing security: building trust in the cloud, protection of data in large systems that contain data of many organizations, and design of large-scale computer systems.

4.3. National Institute of Standards and Technology

Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) is an initiative led by the National Institute of Standards and Technology with the goal of developing high-quality standards for cloud computing systems, and increasing the level of technical confidence before standards are adopted [SAJACC 2011].

Within SAJACC, there has been developed a web portal with a repository of documented use cases addressing issues that can be encountered during cloud adoption. There are 25 use cases to date (January 2012) divided into three groups that reflect the requirements put on cloud systems: interoperability, portability, and security. Government agencies, academia and industry are engaged in the development process of the use cases and the cloud specification documents. The SAJACC's goal is to engage industry, government agencies, and academia to provide input into the discussion over cloud computing requirements and specifications that will lead to the creation of international cloud computing standards.

A web portal with tools to e-collaboration eases the exchange of information between parties involved in the development of the standards. After a use case is developed, SAJACC conducts tests to examine to what extent the use case can be supported by a cloud system. Afterwards, the results of the tests are published on the SAJACC web portal and may be discussed .

4.4. Risk assessment guidelines for companies

The IT managers of enterprises should make a careful assessment of the risk tolerance of their assets, meaning data and functions. This assessment should be performed for various possible deployment models. It is important for managers to realize that the decision on the adoption of cloud computing is not an "all or nothing" issue. In the cloud computing model, assets need not to be at the same location and it is possible to select only part of the data and functions that should be moved to the cloud.

In the initial stage of the risk evaluation, the data and functions considered for transfer to the cloud should be determined. During this evaluation the potential use of the assets after moving to the cloud environment should be considered to take into account scope creep, because often the amount of data and functions turns out to be greater than originally anticipated. It is possible that some information may be too sensitive for migrating to the cloud, e.g. intellectual property, financial information, health data.

For each of the identified assets, the importance for a company and the consequences in cases of potential security breaches should be determined. For example, the IT managers need to answer questions about the negative consequences of disclosure of an asset to the public, access data by cloud provider employees, manipulation of a function, etc. The evaluation should encompass the requirements for confidentiality, integrity, and availability of the assets, and the changes in the risk of security breaches if they are moved to the cloud.

When a potential cloud consumer has knowledge about the importance of their assets, the next stage is to determine acceptable cloud deployment models. Prior to the analysis of potential service providers, it is necessary to investigate whether it is possible to accept the risks specific to the different deployment models and their variations regarding the cloud location. The basic cloud options are as follows: public, private located on-premises, private located off-premises, community, and hybrid.

Finally, a review and analysis of the cloud computing solutions offered by different cloud providers should be carried out. Each of the potential solutions should be examined in terms of the scope of control for implementing the required risk management at each of the cloud architecture layers, i.e. software, platform, and infrastructure. For each of the considered deployment models the data flow between the enterprise, cloud services, and other nodes representing business partners should be outlined. Before making a final decision, IT managers should understand whether and how the data can be transferred to and from the cloud for the various deployment models in order to identify points which are particularly exposed to risks. This allows them to gain knowledge about the importance and risk tolerance for the assets considered for transfer to the cloud within the acceptable deployment models.

5. Conclusions

On the one hand, a cloud provider must offer services in a manner flexible enough to handle the largest number of consumers in order to achieve cost efficiency resulting from economies of scale, reuse, and standardization of IT resources. On the other hand, the cloud should be fitted with proper security mechanisms which are often perceived as imposing restrictions and rigidity. The initiatives in the area of cloud computing security are evidence that the vendors are aware of the concerns of small and medium enterprises about the transfer of their data and functions to the cloud. The initiatives aim to increase knowledge and the awareness of potential customers of the security threats and mechanisms to prevent and deal with such issues. In consequence, this should lead to the increased adoption of the new model of leveraging IT systems in enterprises.

The available studies on cloud security contain a large number of various guidelines and recommendations related to security mechanisms that can be taken into consideration in the cloud environment. However, not all cloud solutions require all possible security mechanisms. The assets which are not of critical importance, do not require as high a level of security control as those which are extremely sensitive. Therefore, a decision on the adoption of cloud-based solutions should be preceded by a thorough evaluation of risk tolerance and potential threats to company data and functions. The results of this evaluation ensure the appropriate context which is essential to choose the most suitable cloud computing solution for the company.

IT managers should investigate different combinations of cloud deployment and service delivery models which are acceptable for the different data and functions of their businesses. This will enable them to evaluate properly the available cloud computing solutions, taking into consideration the various security aspects.

References

Armbrust M. et al., *Above the clouds: A Berkeley view of cloud computing*, Technical Report No. UCB/EECS-2009-28, EECS Department, U.C. Berkeley 2009.

Catteddu D., Hogben G., *An SME perspective on Cloud Computing*, European Network and Information Security Agency, 2010, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey [accessed 19.01.2012].

Cloud Computing: Benefits, risks and recommendations for information security, eds. D. Catteddu, G. Hogben, European Network and Information Security Agency, 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport [accessed 19.01.2012].

CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*, Cloud Security Alliance, 2011, https://cloudsecurityalliance.org/research/security-guidance/ [accessed 19.01.2012].

CSA, *Top Threats to Cloud Computing V1.0*, Cloud Security Alliance, 2010, https://cloudsecurityalliance.org/research/top-threats/[accessed 19.01.2012].

Gartner, *Gartner Identifies the Top 10 Strategic Technologies for 2011*, Gartner Research, 2011, http://www.gartner.com/it/page.jsp?id=1454221 [accessed 19.01.2012].

Geelan J. (2009), *Twenty-One Experts Define Cloud Computing*, "Cloud Computing Journal", http://cloudcomputing.sys-con.com/node/612375 [accessed 19.01.2012].

IDC, *IDC IT Cloud Services Survey: Top Benefits and Challenges*, IDC, 2009, http://blogs.idc.com/ie /?p=730 [accessed 20.01.2012].

Mell P., Grance T., *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [accessed 19.01.2012].

SAJACC, *Standards Acceleration to Jumpstart Adoption of Cloud Computing*, National Institute of Standards and Technology, 2011, http://www.nist.gov/itl/cloud/sajacc.cfm [accessed 19.01.2012].

SecaaS, *Defined Categories of Service 2011*, Cloud Security Alliance, 2011, https://cloudsecurityalliance.org/research/secaas/ [accessed 19.01.2012].

Subashini S., Kavitha V., *A survey on security issues in service delivery models of cloud computing*, "Journal of Network and Computer Applications" 2011, vol. 34, no. 1.

Zissis D., Lekkas D., *Addressing cloud computing security issues*, "Future Generation Computer System" 2012, vol. 28, no. 3.

WYZWANIA DLA BEZPIECZEŃSTWA PRZETWARZANIA W CHMURZE DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

Streszczenie: Przetwarzanie w chmurze jest modelem korzystania z zasobów informatycznych udostępnianych przez dostawców chmury za pomocą Internetu. W tym modelu małe i średnie przedsiębiorstwa mogą przenieść koszty budowy i utrzymania infrastruktury informatycznej na podmioty trzecie. Kluczowym czynnikiem ograniczającym rozpowszechnienie przetwarzania w chmurze są obawy związane z bezpieczeństwem. Te obawy powinny być jednak zestawione z korzyściami w zakresie bezpieczeństwa możliwymi do uzyskania dzięki cechom charakterystycznym chmury. W artykule przedstawiono analizę zagrożeń i korzyści w obszarze bezpieczeństwa związanych z wdrożeniem przetwarzania w chmurze w przedsiębiorstwach oraz przegląd inicjatyw ukierunkowanych na zwiększenie świadomości przedsiębiorstw w tym obszarze.

Słowa kluczowe: przetwarzanie w chmurze, bezpieczeństwo, małe i średnie przedsiębiorstwa.