HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Kovács Zoltán
zkovacs@nbsz.gov.hu

CLOUD SECURITY IN TERMS OF THE LAW ENFORCEMENT AGENCIES

Absztrakt/Abstract

A felhő alapú rendszerek költségcsökkentő és hatékonyságnövelő tulajdonságaik miatt egyre jobban elterjednek. Ez a tény több szempontból is új kihívások elé állítja a rendvédelmi szerveket. Egyrészről a felhő alapú rendszerek használata elkerülhetetlennek tűnik a rendvédelmi szervek számára, ezért mint (leendő) felhasználóknak tisztában kell lenniük azok biztonsági kockázataival, kihívásaival. Másrészről ezeknél a rendszereknél is biztosítani kell a törvényes ellenőrzést, amely szintén új fajta gondolkodásmódot és megoldásokat igényel a rendvédelmi szervektől és a szolgáltatóktól egyaránt. A cikk a rendvédelmi szervek sajátos – és a fent említett kettős szerepe – szempontjából csoportosítja a felhő alapú rendszerek biztonsági kérdéseit.

Due to its cost reducing and efficiency increasing features cloud computing is becoming more and more widespread. This fact poses new challenges to the law enforcement agencies in several aspects. On the one hand, application of cloud computing seems inevitable for the law enforcement agencies, thus as (future) users should be aware of their security risks and challenges. On the other hand, it is imperative to ensure lawful monitoring, which requires new approaches and solutions from both the law enforcement agencies and the service providers. This article describes the challenges of cloud computing security issues, grouping them in terms of the special – and the aforementioned dual role – of the law enforcement agencies.

Kulcsszavak/Keywords: *felhő alapú informatika, felhő alapú rendszerek biztonsága, törvényes ellenőrzés ~ cloud computing, cloud security, lawful monitoring*

1. INTRODUCTION

The law enforcement agencies have to face new challenges by the spread of cloud computing systems. Due to the efficiency and the lower expenditure, reserving their high safety requirements these organizations will sooner or later apply systems like these [1]. However, the greatest challenge of cloud computing, as a recently appeared, rapidly and continuously developing, altering technology is establishing complete security. The traditional IT safety solutions cannot entirely be applied in the cloud, what is more, there are new security risks which require new solutions. In addition, the interests of the users and the cloud providers – due to the expenditures and the responsibility to provide security – might be contrary.

The law enforcement agencies have to be concerned with cloud not only as users, but also as an organisation doing lawful monitoring as well. In this role, besides the technical challenges given by the new technology, the other accentuated problem is that the traditional (communication) provider model is being replaced by a new model, thus the creation of the lawful monitoring requires not only technical, but also new legal solutions and lateral thinking.

What security issues should be considered with in the cloud? What aspects should be examined concerning security? Can the issues which have to be considered during the contracting be defined so that the system used will meet – the sometimes really high - requirements of the law enforcement agencies? This article is searching the answers for these questions, collecting viewpoints published on cloud, complementing and organizing the reasons in a specific way.

2. SECURITY ISSUES – BASICS

The studies, blogs on cloud computing published on the INTERNET, search for answers or try to give definitions, advice in a plenty of ways, sometimes aspiring to completeness, sometimes riving off a very focussed topic related to the security of cloud computing. Like in the definition and categorization of cloud computing the study published by the Information Technology Laboratory of NIST (National Institute of Standards and Technology) under the title „The NIST Definition of Cloud Computing” is regarded widely accepted and quasi-standard, as far as security concerned the same could be written about the ›‚SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING” [3] by Cloud Security Alliance. Accepting the content of this study, in this article the major issues of the security of cloud computing will be reviewed on the basis of this categorisation hereinafter.

In the document, the security aspects are divided into 13 domains, further classified into 2 main parts: governance and operation. The governance part includes mostly strategic, while the operational part discusses tactical security questions. The domains defined by the CSA and their short description can be found in the chart below:

DOMAIN	GUIDANCE DEALING WITH...
Governance and Enterprise Risk Management	The ability of an organization to govern and measure enterprise risk introduced by cloud computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues.
Legal Issues: Contracts and Electronic Discovery	Potential legal issues when using cloud computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.
Compliance and Audit	Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.
Information Management and Data Security	Managing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.
Portability and Interoperability	The ability to move data/services from one provider to another, or bring it entirely back in-house. Together with issues surrounding interoperability between providers.

1/a. table. Governance Domains [3]
Source: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; (05/01/12)

DOMAIN	GUIDANCE DEALING WITH...
Traditional Security, Business Continuity and Disaster Recovery	How cloud computing affects the operational processes and procedures currently used to implement security, business continuity, and disaster recovery. The focus is to discuss and examine possible risks of cloud computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models. Further, the section touches on helping people to identify where cloud computing may assist in diminishing certain security risks, or entails increases in other areas.
Data Center Operations	How to evaluate a provider's data center architecture and operations. This is primarily focused on helping users identify common data center characteristics that could be detrimental to on-going services, as well as characteristics that are fundamental to long-term stability.
Incident Response, Notification and Remediation	Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident-handling program.
Application Security	Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).
Encryption and Key Management	Identifying proper encryption usage and scalable key management. This section is not prescriptive, but is more informational in discussing why they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.
Identity and Access Management	Managing identities and leveraging directory services to provide access control.

DOMAIN	GUIDANCE DEALING WITH...
	The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity, Entitlement, and Access Management (IdEA).
Virtualization	The use of virtualization technology in cloud computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.
Security as a Service	Providing third party facilitated security assurance, incident management, compliance attestation, and identity and access oversight. Security as a service is the delegation of detection, remediation, and governance of security infrastructure to a trusted third party with the proper tools and expertise. Users of this service gain the benefit of dedicated expertise and cutting edge technology in the fight to secure and harden sensitive business operations.

1/b. table. Operational Domains [3]
Source: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; , (05/01/12)

The Cloud Security Alliance^{SM} (CSA) first published the study mentioned above in April 2009, the V3.0 version of which was published in 2011. In the latter one, the concept of Security as a Service (SecaaS) (Chart1, last domain) appeared first. About the purpose of its introduction the authors wrote the followings:

„SecaaS is looking at Enterprise security from the cloud – this is what differentiates it from most of the other work / research on cloud security. Predominantly cloud security discussions have focused on how to migrate to the Cloud and how to ensure Confidentiality, Integrity, Availability and Location are maintained when using the Cloud. SecaaS looks from the other side to secure systems and data in the cloud as well as hybrid and traditional enterprise networks via cloud-based services. These systems may be in the cloud or more traditionally hosted within the customer's premises. An example of this might be the hosted spam and AV filtering. "

In 2011 Security as a Service Working Group of Cloud Security Alliance^{SM} published a study under the title „Defined Categories of Service 2011"[4], which discusses the above-mentioned topics in detail. In accordance with the content of the basic document, the authors differentiate 10 categories within the topic "Security as a Service" as follows:

- Category 1: Identity, (Entitlement,) and Access Management: *„Identity and Access Management (IAM) should provide controls for assured identities and access management."*
- Category 2: Data Loss Prevention: *„Data Loss Prevention is the monitoring, protecting, and verifying the security of data at rest, in motion and in use both in the cloud and on-premises."*
- Category 3: Web Security: *„Web Security is real-time protection offered either on-premise through software/appliance installation or via the cloud by proxying or redirecting web traffic to the cloud provider."*
- Category 4: Email Security: *„Email Security should provide control over inbound and outbound email, thereby protecting the organization from phishing, malicious attachments, enforcing corporate polices such as acceptable use and spam, and providing business continuity options."*
- Category 5: Security Assessments: *„Security assessments are third-party audits of cloud services or assessments of on- premises systems via cloud-provided solutions based on industry standards."*

- Category 6: Intrusion Management: *„Intrusion Management is the process of using pattern recognition to detect and react to statistically unusual events. This may include reconfiguring system components in real time to stop / prevent an intrusion.”*
- Category 7: Security Information and Event Management (SIEM): *„Security Information and Event Management (SIEM) systems accept (via push or pull mechanisms) log and event information. This information is then correlated and analyzed to provide real-time reporting and alerting on incidents / events that may require intervention. The logs are likely to be kept in a manner that prevents tampering to enable their use as evidence in any investigations.”*
- Category 8: Encryption: *„Encryption is the process of obfuscating/encoding data (usually referred to as plain text) using cryptographic algorithms the product of which is encrypted data (usually referred to as ciphertext).”*
- Category 9: Business Continuity and Disaster Recovery: *„Business Continuity and Disaster Recovery are the measures designed and implemented to ensure operational resiliency in the event of any service interruptions.”*
- Category 10: Network Security.: *„Network Security consists of security services that allocate access, distribute, monitor, and protect the underlying resource services. Architecturally, network security provides services that address security controls at the network in aggregate or specifically addressed at the individual network of each underlying resource.”*

Besides the short description, all the categories are classified according to their nature (preventative, protective, detective, reactive) and the most relevant pieces of information is described list-like, in a chart form, as follows:

- core functionalities
- optional features
- challenges
- services
- threats addressed
- reference examples
- references / additional resources.

In these two documents, some overlaps can be observed between the given domains in the basic document and in the categories of the domain “Security as a Service” (e.g.: Identity and Access Management, Encryption etc.). These overlaps indicate how novel the security problems of cloud computing are, and there are not completely accurate circumscriptions, definitions and standards. The participants and stakeholders of this industry – including CSA, ETSI and ITU – are working on it.

3. SECURITY ISSUES – IN TERMS OF THE LAW ENFORCEMENT AGENCIES

In the aforesaid documents the CSA discusses the security issues of cloud computing focussing on business organizations. For the law enforcement agencies – owing to their special status – these documents are worth applying for analysis, but classifying differently, sometimes complementing and modifying the content. The analysis should be carried out along the four dimensions below:

- The role of the law enforcement agencies:
  - user,
  - executor of lawful monitoring.

- Deployment Models:
  - Private cloud,
  - Community cloud,
  - Public cloud,
  - Hybrid cloud.
- Service models:
  - Cloud Software as a Service (SaaS),
  - Cloud Platform as a Service (PaaS),
  - Cloud Infrastructure as a Service (IaaS).
- Security questions for analysing:
  - operational reliability, operational safety,
  - data security,
  - other (legal, physical, etc.) security,
  - lawful monitoring.

3.1. The role of the law enforcement agnecies:

The role of law enforcement agencies can be twofold. On the one hand as a user, they can satisfy their own demands according to their – sometimes really high – security requirements, on the other hand they have to execute the tasks of lawful monitoring, according to acts and laws.

Because of the double role, the security issues should be analysed from a dual perspective. For instance, the availability and the interoperability are very important for the users, but not so relevant for the executors of lawful monitoring. On the other hand, retaining the users activity logs might be more significant for the law enforcement agencies being in the role of executor of lawful monitoring, than as users.

During the analysis it must be considered that in certain cases the enforcement of the lawful monitoring's requirements is contrary to the interests of both the provider and the user (it is the providers' responsibility to cover the costs of installing and maintaining it, while the reason why the users decide to use the cloud is to avoid lawful monitoring).

3.2. Deployment models:

The definition of deployment models can be found in several articles (e.g.: in [1], [2]), thus this article does not discuss it. For reasons of simplification it can be assumed that the law enforcement agencies as users will use a private cloud, while they will focus on public clouds regarding the lawful monitoring. In this case the analysis will be simplified to two dimensions, thus it is worth working out templates which could be applied by many law enforcement agencies. (Certainly, in other cases considering the peculiarities of the given role and the deployment model, the content of the template has to be reconsidered and the questions of security must be re-analysed.)

3.3. Service models:

The definition of service models can be found in many articles (e.g.: in [1], [2]), thus this article does not deal with it.

3.4. Security questions for analysing:

As was mentioned at the beginning of this article, the studies, blogs on cloud computing published on the Internet, search for answers or try to give definitions, advice in a plenty of ways, sometimes aspiring to completeness, sometimes riving off a very focussed topic related to the security of cloud computing, or draw attention to a less known security issue.[5-15][21-22] The more significant participants of this market publish different studies focussing on specific security issues with the unconcealed aim to offer solutions for these issues with their own products.[16-20]

Based on the CSA documents outlined in the previous chapter, and applying the aforementioned articles and blogs – in a different way, however, - it is advisable to classify the security issues to be considered into four main groups:

- 3.4.1. operational reliability, operational safety
- 3.4.2. data security
- 3.4.3. other (legal, physical, etc.) security
- 3.4.4 lawful monitoring.

3.4.1. Operational reliability, operational safety

The questions of operational reliability as far as cloud computing concerned are considerably analogous with that of the traditional IT systems. It concludes the features relating to the reliable functionality and operation in normal circumstances. For instance accessing the service with the devices defined in the contract (e.g. tablet PCs with Android operational system), from a particular place (anywhere where the Internet connection is available) with defined availability (e.g. 95%, with the loss of service is not longer than 30 minutes), in addition the operational reliability includes the backup of our data, redundant storage and disaster recovery as well.

The questions of operational reliability can be managed purely in a technical way, where the interests of the providers and the users concur (the providers intend to provide, while the users intend to receive a reliable service). The extent of the safe service is merely a matter of money and agreement. (About the possibilities of the users concerning the contract see the chapter on “Other (Legal, Physical, etc.) Security”.)

Regarding the operational reliability field, the separation of responsibilities seems to be obvious, basically it is the providers that take all responsibilities, regardless of the service models (SaaS, PaaS, Iaas).

The applied standards and solutions concerning the traditional IT provide a perfect starting point for the analysis of the operational reliability issues of cloud computing. Here the undermentioned questions are to be examined:

- From CSA's governance domains [3]:
  - Portability and Interoperability
  - Compliance
- From CSA's operational domains:
  - Business continuity [3][4]
  - Disaster recovery [3][4] [7]
  - Data Center Operations [3]
- Others:
  - Availability [5][12] or Reliability and liability [22]: availability of your data in the cloud in normal way or in a redundant and highly available way, expect the cloud to be a reliable resources.
  - Redundancy (include: redundant storage) [23]: redundancy supports high availability for the application layer, and must be built-in across the infrastructure and associated tools.
  - Access and usage restrictions [22]: access and use the cloud where and when you wish.
  - Risk Mitigation Plan [21]: This plan should include documentation of risk, responses to those risks, and education and training.
  - Data format [10]: In which kind of format of data have to transfer your data into the cloud (provider) and can you get back your data from the provider.

3.4.2. Information Management and Data Security

All the factors emerging with reference to the safe access to the users' data (management, application etc.), and the prevention of unauthorized access can be regarded as a question of information management and data security (hereafter data security), for instance the identity and access management, the use of encryption and the protecting against phising. Some of them are already available in connection with the traditional IT systems, or can easily be implemented to the cloud (e.g. antivirus protection), the others require completely new solutions (e.g. data segregation, protection against cross-VM side-channel attacks [11]). Some of the data security issues can easily be solved (e.g. shutting down unnecessary and vulnerable applications) others require technically complex, or even legal solutions (so that the providers – including their system administrators – can not have access to our data [10][22].

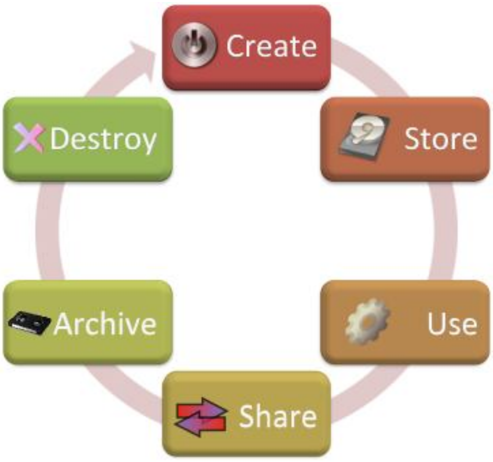
The data security issues can be solved in technical, legal and administrative ways, however, some of the elements can not be solved only in a technical way, or can be solved with unreal large expenditure (for example the questions of prevention of the cloud provider espionage [12] or insecure or incomplete data deletion [14].)

Concerning the data security issues, the providers and the users might have diverse interests. The primary interest of the providers is a reliable service, the defence of the users' data is subsidiary. Due to the permanent urge of development it means extra and considerably high expenses which are hard to devolve entirely to the user, at the same time the data security is definitely in the users' own interest.

The responsibilities are distributed between the users and the providers and the degree of distribution significantly depends on the service model. The responsibilities of the users are minor in the SaaS model, but they are considerable in the IaaS model. The issues to be examined are as follows.

- From CSA's governance domains [3]:
  - Information Management and Data Security (ezen belül főleg Data Security).
- From CSA's operational domains:
  - Incident Response, Notification and Remediation [3]
  - Application Security [3]
  - Encryption and Key Management [3] [4]
  - Identity and Access Management [3] [4]
  - Virtualization [3]
  - Security as a Service [3] [4]
  - Data Loss Prevention
  - Web Security
  - Email Security
  - Intrusion Management [3] [4] [6]
  - Security Information and Event Management (SIEM)
  - Network Security
- Others:
  - The documents of CSA entirely cover the data security issues.

The questions of data security should be analysed through the life cycle of the data, which is illustrated by Figure 1.



1. figure. Data lifecycle
Source: https://securosis.com/blog/data-security-lifecycle-2.0; (05/01/12)

In terms of security the 6 phases of the data lifecycle can be divided into 2 main groups concerning security: phases with and without data movement.

Phases with data movement:

- create
- use
- share
- destroy

Phases without data movement:

- store
- archive

(Note that in the case of cloud computing, any kind of active operation done by the users will be associated with data movement.)

This classification is to be done to separate the responsibilities of the users and the providers in the different service models, (within a model the users have greater responsibilities in operations including data movement than in operations without data movement), which can help make templates mentioned in the deployment models.

3.4.3. Other (legal, physical, etc.) security

This category includes all the security issues which can not be managed in a technical way, or even a third party can be involved (e.g. audit). The legal guarantees (primarily contractual, or regulated by the law) which can solve the particular issues in an unambiguous way, including the questions emerging about reliability and data security issues, as well as the physical defence of data centres are classified here.

The questions belonging to this category can be solved only in legal ways (the legal issues are given, but the physical security or the audit, which require involving a third party, can be influenced by the users only through legal ways).

In this category, the interests of the providers and the users differ in each case. The influence of the users on the questions belonging to this category, e.g. the content of the contract, can vary between the extremes (e.g. while in (a public) SaaS model this can be the approval or disapproval of a contract (including all conditions) written by the providers, in a (private) IaaS solution the content of the contract and the other conditions can be defined in a negotiation directly between the providers and the users).

It is where the separation of responsibilities is probably the most unambiguous, the responsibilities of the users extend to ascertain each relevant question in the contract, including the supervision of the written requirements as well. The physical, technical implementation written in the contract belongs to the responsibilities of the providers. The questions to be analysed are as follows:

- From CSA's governance domains [3]:
  - Governance and Enterprise Risk Management
  - Legal Issues: Contracts and Electronic Discovery
  - Audit
- From CSA's operational domains:
  - Traditional Security [3]
  - Security Assessments [4]
- Others:
  - Long-term viability [7]: you must be sure your data will remain available even after your cloud computing provider go bankrupt or get acquired and swallowed up by a larger company.
  - Access logs and other statistics ownership [10]: in the contract it has to be regularized, what the providers are allowed to do with the logs and other statistical information – collected by themselves – because sensitive information can be extracted from this logs.
  - Cloud provider espionage [12]: in the contract, the access to the user's data by the provider (including its administrators and other professionals) has to be regularized so that it will extend over not only the random and (sometimes inevitable) normal access cases (which may be necessary for the providers' work), but also the theft of company proprietary information by the cloud provider.
  - Transitive nature [12]: the cloud provider might use subcontractors, the cloud user has not contract with them. These issues should also be regularized.
  - Insecure or incomplete data deletion [14]: the user's data should really be deleted (if it is the users' request), so that they can not be recovered, even from back-up.

3.4.4. Lawful Monitoring

While the previously examined security issues are more relevant for the law enforcement agencies as users, and less relevant as the executors of lawful monitoring, in this issue, it is just the opposite. This group includes those forms of monitoring which have already been developed and accepted in the traditional communication networks (e.g. lawful interception), and those that have been developed specifically for IT systems (e.g. computer forensics).

The issues belonging to lawful monitoring can be resolved in technical and legal ways, but at the moment these are the most complicated questions. On the one hand, the legal relationship has been set up between the providers and the executors of lawful monitoring (not between the providers and the users, as in the cases of other security issues), and this relationship is usually based on legal obligations. While concerning the communication networks there is an evolvelved, widely accepted lawful monitoring based on similar laws in democratic states, as regards cloud computing it is different. The lack of currently existing legal regulation might cause problems concerning lawful monitoring, or even it might prohibit it. For this reason, you can not talk about such sophisticated monitoring systems, like the ones that are available as concerns telephone systems.

In this category, the interests of the providers and the users are almost the same, but contrary to that of law the enforcement agency which executes the tasks of lawful monitoring, as it was mentioned concerning the roles of the law enforcement agencies. There are only a few exceptions (e.g. applying devices which can be suitable to confirm or exclude whether the data stored in the cloud was generated originally by a specific user or they were manipulated).

The responsibilities are clear, as long as there are statutory requirements, or can be made clear, if in the lack of regulation, the law enforcement agency and the provider do a contract.

As concerns lawful monitoring the issues to be analysed are as follows:

- data retention
- lawful interception
- forensics tools.

As the concept of Security as a Service was introduced in the above-mentioned documents of CSA, the concept of Lawful Monitoring as a Service (LMaaS) (or something like that) might be introduced. If this concept – like the other issues – can be standardised, the providers can provide the required information to the law enforcement agencies as a service, regardless of the nationalities of the participants, the physical location of the data centres and other technical devices, and the questions, when and which country's legal system should be followed.

4. CONCLUSIONS

This article has reviewed the security *issues* of cloud computing, and then established a unique, essential classification in terms of the law enforcement agencies. From the „Service models – Deployment models – The role of law enforcement agencies – Security questions for analysing" four-dimensional space the latter two have been examined in detail. The chapter "Security issues to be analysed" sets up a new classification where it introduces what is meant by operational reliability/operational safety, data security, other (legal, physical, etc.) security and lawful monitoring, the way they can be solved (technically, legally), how the previously mentioned questions can be classified into the newly set up category, as well as how the interests of the parties relate to each other.

As a conclusion, the law enforcement agencies are able to set up strong security requirements for cloud as a result of the more and more clear security standards, with the proviso that the continuous monitoring and upgrade of the security requirements and solutions are crucial due to the technical development and the recently appearing threats. It is not so easy for the executors of lawful monitoring, in these cases further legal and technical solutions should be searched and found, during a corresponding standardising process, which all the questions (thus security questions) of cloud computing go through.

Conclusions drawn from this article:

- Concerning lawful monitoring the concept of Lawful Monitoring as a Service (LMaaS) (or something like that) should be introduced and standardised.
- Templates are to be worked out based on the most frequently used cases (law enforcement agencies as users use private cloud, as executors of lawful monitoring focus on public cloud), and can be applied by law enforcement agencies freely, so that the agencies will not have to work out comprehensive requirements.

References

[1] Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél – Hadmérnök VI. Évfolyam 4. szám - 2011. december

[2] Peter Mell and Tim Grance: The NIST Definition of Cloud Computing Version 15, 10-7-09;
http://www.nist.gov/itl/cloud/index.cfm; (2011. 10. 21.)

[3] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; (2012. 01. 05.)

[4] Defined Categories of Service 2011 https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf; (2012. 01. 05)

[5] Ariel Silverstone: Clear Metrics for Cloud Security? Yes, Seriously http://www.csoonline.com/article/507823/clear-metrics-for-cloud-security-yes-seriously?page=1; (2012. 01. 02.)

[6] [6] Phil Cox: Intrusion detection in a cloud computing environment http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment; (2012. 01. 02.)

[7] Jon Brodkin: Gartner: Seven cloud-computing security risks http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0; (2012. 01. 02.)

[8] Phil Cox: Securing data in the cloud http://searchcloudcomputing.techtarget.com/tip/Securing-data-in-the-cloud; (2012. 01. 02.)

[9] Francoise Gilbert: Ten key provisions in cloud computing contracts http://searchcloudsecurity.techtarget.com/tip/Ten-key-provisions-in-cloud-computing-contracts; (2012. 01. 02.)

[10] Joseph Foran: Ten questions to ask when storing data in the cloud http://searchcloudcomputing.techtarget.com/tip/Ten-questions-to-ask-when-storing-data-in-the-cloud; (2012. 01. 02.)

[11] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage: Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf ; (2011. 11. 05.)

[12] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon , Ryusuke Masuoka, Jesus Molina : Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control http://www.parc.com/publication/2335/controlling-data-in-the-cloud.html; (2011. 11. 05.)

[13] Yanpei Chen, Vern Paxson, Randy H. Katz: What's New About Cloud Computing Security? www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf; (2011. 11. 05.)

[14] DANISH JAMIL, HASSAN ZAKI: CLOUD COMPUTING SECURITY www.ijest.info/docs/IJEST11-03-04-129.pdf; (2011. 11. 05.)

[15] http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html; (2011. 10. 23.)

[16] Virtualization and Cloud Computing: Security Threats To Evolving Data Centers (Trend Micro) http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/final_cloud_virt_report.pdf; (2011. 11. 05.)

[17] Securing Microsoft's Cloud Infrastructure
http://www.globalfoundationservices.com/security/; (2011. 11. 05.)

[18] Intel's Vision of the Ongoing Shift to Cloud Computing
http://charltonb.typepad.com/papers/Cloud Vision.pdf; (2011. 12. 03.)

[19] Virtualization and Cloud Computing: Security Best Practice (Trend Micro)
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/final_cloud_virt_best_practice.pdf; (2011. 11. 05.)

[20] Axel Buecker , Koos Lodewijkx , Harold Moss , Kevin Skapinetz , Michael Waidner : Cloud Security Guidance (IBM Recommendations for the Implementation of Cloud Security) Redpaper
http://www.redbooks.ibm.com/redpieces/abstracts/redp4614.html?Open&pdfbookmark; (2012. 01. 02.)

[21] Chris Preimesberger: Cloud Computing: Cloud Computing Security: 10 Ways to Enforce It
http://www.eweek.com/c/a/Cloud-Computing/Cloud-Computing-Security-10-Ways-to-Enforce-It-292589/; (2011. 11. 05.)

[22] Paul T. Jaeger, Jimmy Lin, Justin M. Grimes: Cloud Computing and Information Policy: Computing in a Policy Cloud?
http://www.tandfonline.com/doi/abs/10.1080/19331680802425479; (2011. 11. 05.)

[23] http://blogs.sungard.com/as_cloud/tag/cloud-computing-redundancy/; (2012.01.24.)

[24] https://securosis.com/blog/data-security-lifecycle-2.0; (2012. 01. 05.)