HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Kovács Zoltán
zkovacs@nbsz.gov.hu

„ELECTRONIC WRITTEN TASKING ORDER SYSTEM" ACCOMPLISHED WITHIN THE PROJECT „SECURE ELECTRONIC COMMUNICATION" III.

Abstract

The main objective of the "Electronic Written Tasking Order System" is to convey the written tasking orders sent to SSNS via secure electronic communication lines decreasing the quantity of the paper based data carriers, which results rapid fulfilment of the requests of the tasking organizations, as well as it creates opportunities to carry out several related procedures in electronic form. This article series describe the designation of the Electronic Written Tasking Order System through the activities of SSNS proving that this system is a cloud system in terms of the tasking organizations. With reference to this it analyses the relevant security issues, the success of those issues and the classification for the critical information infrastructure.

A Szolgálati Jegy Rendszer fő célja a szolgálathoz beérkező megrendelések biztonságos elektronikus úton történő továbbítása, ezáltal a papír alapú adathordozók számának jelentős csökkentése és a megrendelői igények mihamarabbi kiszolgálása, valamint bizonyos kapcsolódó ügymenetek elektronikus alapokra helyezésének megteremtése. A cikksorozat a Nemzetbiztonsági Szakszolgálat feladatain keresztül bemutatja az elektronikus Szolgálati Jegy Rendszer rendeltetését, majd bizonyítja, hogy az a megrendelők szempontjából felhő alapú rendszernek tekinthető. Ennek kapcsán áttekinti a releváns biztonsági kérdéseket, azok érvényesülését, valamint a kritikus (létfontosságú) információs infrastruktúrává történő besorolás kérdéskörét.

Keywords: *elektronikus Szolgálati Jegy Rendszer, felhő alapú rendszerek, felhő alapú rendszerek biztonsága, kritikus információs infrastruktúra ~ electronic tasking order system, cloud computing, cloud security, critical information infrastructure*

INTRODUCTION

The following paragraph can be read in a study published in 2010, entitled: "Computer Network Operations: Threats and Possible Defence Solutions in Hungary"

"The "Comprehensive Programme for Integrated Governmental Functions" includes such important issues related to economy and national security that we cannot disregard. By means of the "Central Management System" the whole budget system of Hungary will become transparent, therefore misuse of data gained from this system might influence the whole economy of Hungary. Thus the protection of this system is a high priority. The "Taxpayer-centric data service model" sets up Data Warehouses, here the priority is to maintain tax secrecy. The "Secure Electronic Communication" affects the processes of the Special Service for National Security. Although this is one of the most interesting tasks, its technology is not known to the public. The budget of the whole programme is 13881 million Forints." [1]

If the author of this part of the study, Csaba Krasznay regarded the project named "Secure Electronic Communication" as one of the most interesting issues, it is worth examining what it means. Certainly, only those parts can be published which do not contain classified information, even though the principle of the above mentioned project can be known, with some other important pieces of information which can be necessary for the planning of other systems.

The first article of this series of articles reviews the designation of Electronic Written Tasking Order System (eWTOS) accomplished within the framework of the so-called "Secure Electronic Communication" project, and in accordance with the tasks of the Special Service for National Security (SSNS), the procedure of the orders, and then examines how the eWTOS can be applied in the IT strategy of the Ministry of Interior. The second article analyses a currently important issue proving that the eWTOS can be regarded as cloud computing in terms of the tasking organizations. Concerning this it groups the cloud computing along with their features and classifies the eWTOS in the appropriate category. The third article discusses the security issues of the cloud computing by analysing to what extent it concerns the eWTOS as well as how the security panels prevail during their accomplishment. Finally two conclusions are drawn. On the one hand, even though the eWTOS has not been qualified as a critical information infrastructure yet, as every condition is given it is only a question of time. On the other hand, thanks to the already evolved high level security panels, the system is protected properly, thus after the classification these do not have to be modified in merits.

The series of articles concentrate on – primarily security – solutions considered during the planning. These articles do not aim to analyse the technical or other problems which appeared during the implementation or to describe different mistakes and their handling. They will only be mentioned if it is necessary to explicate the previously mentioned issues.

Review:

The first part of these series describes the tasks of eWTOS. In order to clarify it the functions, the activities and the process of the tasking orders received from the tasking organisations are reviewed. After this, within the framework of a historical overview, it enumerates the events which have determined the current structure and operation. of eWTOS . After clarifying the bases, it describes the structure and principle of operation of eWTOS and presents the similarities and the differences between the paper-based and electronic processes. Finally it discusses how eWTOS, invented in 2005, suits to the IT strategy of the Ministry of Interior published in 2012. On the basis thereof it determines that the system utilizes such forward solutions and performs such functions today which were only drawn up as strategic purposes on the level of the Ministry of Interior in 2012.

The second article of the article series demonstrates that eWTOS is a cloud computing system in terms of the tasking organizations sending written tasking orders to the SSNS. In order to demonstrate that, first, the article reviews the features and characteristics of cloud computing systems. After that, it declares that eWTOS is a Community cloud (in the Deployment model category), and a Software as a Service (in the Service models category). It establishes that eWTOS is very important because today there are rather few cloud computing systems used by national security services and law enforcement agencies, so it is subservient to analyse carefully the experiences of it.

SECURITY ISSUES OF EWTOS

Risks and Security Issues of Cloud Systems

The greatest challenge of cloud systems, as a recently appeared, rapidly and continuously developing, altering technology is to establish 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. [2] These are the problems that had to be faced with during the development of eWTOS, and it was compounded by the fact that increased security requirements have to be fulfilled, since in eWTOS classified information must be transferred and handled.

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” [3] is regarded as 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” [4] by Cloud Security Alliance. 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 issues.

The Cloud Security Alliance^{SM} (CSA) first published the study mentioned above in April 2009, whose V3.0 version was published in 2011. In the latter one, the concept of Security as a Service (SecaaS) appeared first. In 2011 Security as a Service Working Group of Cloud Security Alliance^{SM} published a study under the title „Defined Categories of Service 2011”[5], which discusses the above-mentioned topics in detail.

In the aforesaid documents the CSA discusses the security issues of cloud computing focussing on business organizations. In terms of eWTOS these issues should be analysed differently, according to the method which was recommended to law enforcement agencies. [6] In this case, using the above mentioned documents of CSA (yet classifying the security issues differently, sometimes complementing and modifying the content) the analysis should be carried out along the four dimensions below:

1. The role of the law enforcement agencies:
   - user,
   - executor of lawful monitoring.
2. Deployment Models:
   - Private cloud,
   - Community cloud,
   - Public cloud,
   - Hybrid cloud.

3. Service models:
   - Cloud Software as a Service (SaaS),
   - Cloud Platform as a Service (PaaS),
   - Cloud Infrastructure as a Service (IaaS).
4. Security issues to examine:
   - operational reliability, operational safety,
   - data security,
   - other (legal, physical, etc.) security,
   - lawful monitoring.

In terms of eWTOS, the dimensions 1 to 3 were discussed in the previous article, so the security issues should be examined within the following frame:

1. The role: user,
2. Deployment Model: community cloud,
3. Service Model: Software as a Service.

During the analysis of the security issues of the four dimensions (operational reliability, operational safety, data security, other (legal, physical, etc.) security) the correspondence or diversions of the interests of the provider and the user should also be examined. [6] In terms of eWTOS a special situation occurred. On the one hand, the provider is one of the users, on the other hand, in certain security issues (e.g. data security) legal requirements must be satisfied. In the light of the foregoing it is considered that the interests of the user and the provider correspond in all the three issues, moreover the SSNS, which is also a provider, demands higher level security requirements than the users (tasking organizations) would do (e.g. access privileges). So, the correspondence or the diversion of the interests of the provider and user should not be examined anymore.

Operational reliability, operational safety

The issues of operational reliability, operational safety (hereafter operational reliability) concerning cloud computing (and also eWTOS) are remarkably similar to that of the traditional IT systems. Accordingly, the accepted and used security standards of traditional IT systems are perfect basic to analyse these questions. This category concludes the features relating to the reliable functionality and operation in normal circumstances.

Regarding the operational reliability field, two issues are worth discussing: administrative and technical. While the latter is evident for everyone, the former is not, or not as much as that concerning the data security topic. However, this is of great importance to evolve complete operational reliability.

The administrative issues involve practically each factor that is not technical, but supports operational reliability. Regarding eWTOS, complete system plan-, developing-, implementation-, test-, and operational documentations, as well as regulations, rules of orders for operation, a disaster recovery plan are done. Users and repairmen are trained in different levels, and custom service is evolved. During the operation of eWTOS, updating the above mentioned documents, repetitive trainings, and non-stop running of custom service are very important tasks.

Concerning the tasks belonging to technical issues of operational reliability – including but are not limited to – the following things have been evolved by the developers of SSNS. Criteria of reliable basic components are satisfied with high quality hardware and software elements During the selection the following criteria were defined: long term manufacturer support, quality assured manufacturing and quality control processes, which increase the possibility of long term, fail-safe operation of the system Besides the fact that these are also the basic requirements in case of unique software, at eWTOS the control of the source code is another possibility. The eWTOS includes redundant elements, which means geographical redundancy in most cases, in other cases at least the possibility of evolving the geographical redundancy. In order to ensure high availability, redundancy is evolved by two physically same-way build up configurations which logically seems only one, so in case of malfunction of any equipment, the other configuration can take over all the tasks without loss of data packets. The RAID storage and fully comprehensive backup and data recovery system ensures the high level of data access. For interoperability eWTOS has well defined interfaces and uses standard data formats. It has a fully regulated version of control subsystems, which is connected to a pilot system, where new versions of software and hardware equipment can be tested before they are used in a hot system. The eWTOS includes a log and event analysis subsystem which can analyse all kinds of activities and states even automatically, and this can help not only the information management and data security, but also the operational reliability as well.

Regarding the operational reliability issues, the separation of responsibilities seems to be obvious; basically it is the SSNS that takes all responsibilities.

Information Management and Data Security

All the factors emerging with reference to the safe access to the user data (management, application, 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 vulnerability of the software used. In the eWTOS the data security issues have been solved in two different ways. On the one hand, well known solutions can be used, which are already available in connection with the traditional IT systems, or can easily be implemented to that system (e.g. antivirus software).On the other hand in order to solve new problems, completely new solutions must be implemented (e.g. data segregation).

Some of the data security issues could easily be solved in a technical way. For example on the online subsystem only the most necessary software was enabled to install because of the security risk of software vulnerabilities. However, on the offline terminals which are used for other tasks by the owner, SSNS could give only recommendations. But in this case, increased security requirements have to be fulfilled too, because of handling classified information on them.

The data security issues can be solved completely in technical, legal and administrative ways, however, some of the elements cannot be solved only in a technical way, or can be solved with unrealistically large expenditure. Some of them are ensured by law, others can be ensured by internal regime rules.

Due to the limitations of space and the information which is allowed to be published, without being exhaustive, the identity and access management of eWTOS should be reviewed:

- the whole system, the facilities of eWTOS, and the encryption devices correspond to legal requirements and authorised by law;
- application of multi-level, high level encryption methods (e.g. IPSec, which is mentioned in the IT strategy of the Ministry of Interior;
- encryption of the whole data communication;
- users management:
    a) create,
    b) inhibit,
    c) delete;
- multilevel authentication with biometric user identification;
- access management and control;
- full logging user activity;
- verifying user activity
- concerning the whole organization,

- concerning only one case;
- application, handling and verification of digital signatures, timestamp, certificates;
- matrix of signature management (determining the person that can sign a particular document)
- the whole lifecycle of a document can be tracked (even in case of an offline workstation;
- the content of the written tasking order cannot be modified after the application of (digital) signature;
- the documents can be:
  a) opened to read or edit,
  b) printed

only by special applications developed by SSNS.

The responsibilities are distributed between the user and the provider (SSNS), who is a user at the same time. The questions of data security should be analysed through the life cycle of the data [6] illustrated by Figure 1.

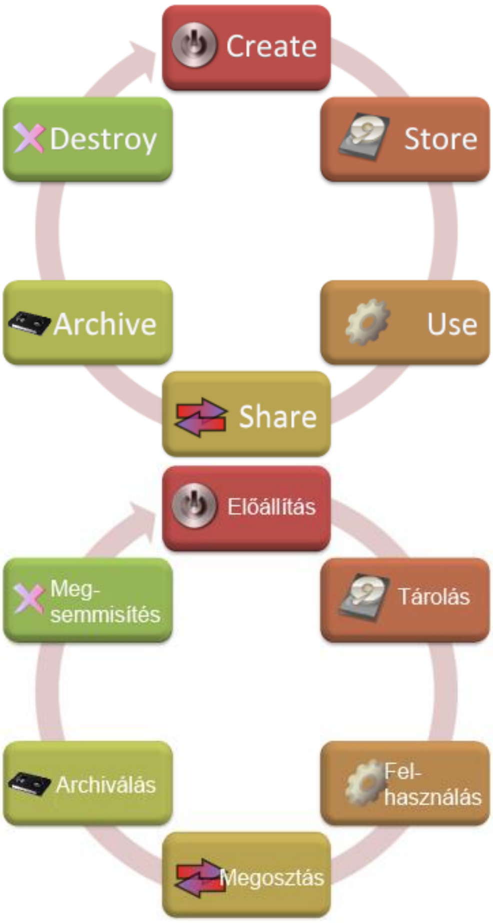

Figure 1. Data Lifecycle [1]

Regarding a traditional cloud system (i.e.: established and run by business organizations) in terms of security the six phases of the data lifecycle can be divided into two main groups concerning security: phases with and without data movement.

Phases with data movement:

- create
- use
- share
- destroy

Phases without data movement:

- store
- archive

This should be done because, in case of cloud computing, any kind of active operation accomplished by the user will be associated with data movement.

With respect to eWTOS, the lifecycle of data should be analysed in another way, since the security elements for data transferring are built into the system by SSNS. Every user (including the SSNS) has to analyse the following questions: in which stage of the processes are they concerned? in which stage are they concerned entirely or partly? , what are the security elements ensured by eWTOS, as well as, what are the ones that are their responsibilities to ensure? (e.g.: the storage of data of a document created in an offline workstation is the responsibility of the maker, but after transmission to the SSNS it is the responsibility of the SSNS. However, the protection of a transferred document is not the responsibility of the user even when it is addressed to the authorization organization and not to the SSNS, because the protection of the documents is guaranteed by eWTOS.)

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.

Regarding eWTOS this security issue is limited. The other (legal, physical, etc.) security issues which are significant when the provider is a business organization, in this case it is not necessary to analyse, because on the one hand the interests of user and the SSNS (who is provider and user at the same time) concur, and on the other hand this field is strongly regulated by law. In the traditional cloud computing case, this security issue includes things like content of contract, long-term viability (meaning accessing data in case the provider go bankrupt or get acquired and swallowed up by a larger company), access logs and other statistics ownership, provider espionage, transitive nature, or insecure or incomplete data deletion. In regards to eWTOS, some of these problems a priori are not interpreted, others are regulated by law in a sufficient way.

The physical security is guaranteed by two reasons. One of them is that the physical security of the datacentre, the online (and offline) terminals have to be established according to Act No. CLV of 2009 on the protection of classified information (PoCI). The other is that the premises, where the equipment of eWTOS is installed owned by national security services and law enforcement agencies, so for others reasons (e.g.: to observe regime about internal security), there are high level manpower and technics of security. This is especially true for the datacentre which is located at SSNS.

A third party can be involved when the contractor or maintainer of eWTOS carry out any kind of work on the system, but this is regulated in extremely precise and detailed contract, between SSNS and the contractor. This contract includes the same guarantee elements as any other contract signed by SSNS, including Nondisclosure agreement and security checks. On the other hand, audit is only made by National Security Authority, only according to classified information protection, edge along regulations of law, and can access only data which belong to its circle of competence, so unauthorized data access cannot occur regarding to audit.

The responsibilities are definite in this issue, the legal guarantee is provided by law and the SSNS, physical security are provided by the owner of the premises where demarcations are unequivocal.

In conclusion it can be ascertained that eWTOS fulfils all security criteria (confidentiality, availability, integrity, authenticity and non-repudiation) [7], therefore all data created, stored, transferred, etc., in this system are protected properly.

EWTOS, as a critical information infrastructure, and the effects of classification on the security solutions

As a final step, it is appropriate to examine whether eWTOS can be classified as a critical information infrastructure, if yes, how it affects the security solutions.

According to the highly accurate definition of Dr. Ferenc Kovács: *„The critical infrastructures are the critical elements of the national, federal and EU infrastructure, whose significant damage, failure or loss would have a serious impact on the security, economy of the nation or nations, on the environment, the public health, and the efficient operation of governments or the state.”* [8]

Act No. CLXVI of 2012 on the identification, designation and protection of critical systems and facilities [9] uses the phrases *essential* instead of *critical infrastructure*. It can be found on the part of the interpretative provisions of the Act:

„f) essential constituent: such constituent of a device, premises, or system of a sector defined in supplement 1–3, which is crucial to supply essential social services, particularly to ensure health, security of a person and property, economic and social public services, and due to the lack of continuous supply of these processes, the failure of them would have significant consequences,

g) national essential constituent: essential constituent designated by this law, which because of the lack of continuous supply of essential social processes, the failure of them would have significant consequences for Hungary,”

It is said by the designation of national essential constituent part of his Act:

„2. § (1) Designation or withdrawal of designation on national essential constituent can be initiated by:

a) the operator or

b) any organizations defined by Government Decree (hereinafter: proposing authority)

from belonging to sectors defined in supplement 1–3, to designated organization defined by Government Decree (hereinafter: sectoral designation authority) with presentation of identification report prepared after the identification process.”

The infrastructures of law enforcement agencies are listed into Public Safety – Protection sector in supplement 3 line 41.

As it is said in „Green Paper on a European Programme for Critical Infrastructure Protection: *„ICT*[1] *systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).”* [10]

In view of the above, everything is given for eWTOS to be a critical (essential) information infrastructure. The initiation of designation, so the classification, has not been accomplished yet, and thus eWTOS is not a critical information infrastructure. The system was established to replace certain paper based processes, so there would not be any alternatives working parallel. After the initial period when electronic and paper based written orders with the same content

[1] ICT: Information and Communications Technologies

are handled parallel in the system; most of the written orders will be handled only in electronic form, so the failure or damage of eWTOS could set back the national security and law enforcement work, so *"influences serious consequences to the security ... of nation ... to efficient operation of ... or state."* [8] The improvement of eWTOS is planning with installation of more online workstations and subsystems which will be able to handle TOP SECRET! classified documents, so the dependency upon eWTOS will increase. Based on these, it can be declared that the classification of eWTOS as a critical information infrastructure is only a matter of time.

It is clear that eWTOS is suitable for excessively high level requirements in all the three security issues (operational reliability, data security, and other (legal, physical, etc.)). The security elements of eWTOS do not have to be changed even after the system is classified as a critical information infrastructure, because they have been evolved to meet these requirements. However, the security elements must be reviewed and upgraded time to time, because new vulnerabilities might be discovered, new attack methods might be evolved, and these could be a threat for eWTOS as well.

CONCLUSIONS

The second article verified that eWTOS can be regarded as cloud computing in terms of the tasking organizations. The security issues of any info-communication systems, including the cloud computing systems, used by the national security services and law enforcement agencies have high priority for them. This article has analysed the security issues of eWTOS by the syllabus connected with cloud computing system recommended by the author. [6]

In conclusion the planned and installed security elements covers the issues of cloud security published in the professional literature. Moreover, eWTOS, as a system handling classified data must meet significantly higher level requirements. From this perspective eWTOS can serve as a model for planning other systems.

On the other hand, we must add that we are only talking about the issues considered in the planning stage; the practical experience is rather limited yet. It is practical to review and analyse the security issues periodically whether they have lived up to the expectations in every aspect. (On the basis of test run and the four month operation it is stated, that problems occurred basically in the operational reliability field. These problems were not caused by lack of planning, but lack of realization of some hardware and software components.)

Today, it is very rare, that a cloud computing system is used by a national security service or a law enforcement agency. It is expected that the need of using cloud systems will grow by organizations mentioned above. At present there is no "security analysis template" available by a national security service or a law enforcement agency, which could help them to prepare the detailed requirements, including significantly detailed security requirements. In order to avoid that every organization must work out an overall, comprehensive requirement independently, it is subservient to create a template like this.

This work can be helped by analyses and developing of industry standards and best practices of developed countries and international organizations and moreover the analysis of eWTOS, as a „cloud model project". Moreover, it is more fitting to use the security requirements of a cloud computing system as a basic of template mentioned above, which was created especially for Hungarian national security services and law enforcement agencies, fit to the Hungarian law, and the security requirements of it are upgraded by growing experience, and then complete that with recommendations of international organizations which were evolved by primarily taking account only business organizations, not the other way around.

References

[1] Kovács László (szerk.): SZÁMÍTÓGÉP-HÁLÓZATI HADVISELÉS: VESZÉLYEK ÉS A VÉDELEM LEHETSÉGES MEGOLDÁSAI MAGYARORSZÁGON. Tanulmány. Budapest, 2010 ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM p. 56.

[2] 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.)*

[3] 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.)

[4] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf – (2012.01.05.)

[5] Defined Categories of Service 2011 https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf – (2012.01.05)

[6] Kovács Zoltán: Cloud security in terms of the law enforcement agencies – Hadmérnök VII. Évfolyam 1. szám - 2012. március

[7] Útmutató az IT biztonsági szintek meghatározásához. www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.pdf – (2013.04.04.)

[8] Kovács Ferenc: Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása. Tanulmány. GKM, 2005. p. 7.

[9] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyar Közlöny 154. szám 2012. november 22. p. 26099 - 26107 http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/mk12154.pdf - (2013.04.04.)

[10] Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final. http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf - (2013.04.04.)

Figures

[1]Figure 1. Data Lifecycle https://securosis.com/blog/data-security-lifecycle-2.0, (2012.01.05.)