IMPROVEMENT POSSIBILITIES REGARDING THE TRAINING OF ELECTRONIC INFORMATION SECURITY MANAGERS

Dr. Csaba KRASZNAY[1] – Zoltán SOM [2]

Abstract

How efficient are the governmental CISOs? Measurement of mandatory training after 2 years.

Upon the changes started by Act 50 of 2013 the students of the third class have begun their studies at the National University of Public Service as info-security managers during the fall of 2015. This seems to be a convenient time to reflect on the changes; as well as to take a look at the measurement results and provide some feedback. We do not aim to examine improvement options, but we do try to help certain areas with some recommendations. During our research, we placed special emphasis on areas that specifically hinder the realization of the government goals. We did not try to determine the success rate of the program itself, but tried to surface the hindering factors instead. We used questionnaires, word-usage tests, and personal interviews. We were interested how efficiently can people enrolled in the training program identify their own hindering factors, with special regard to those which hinder them in achieving their set goals once back in their own organizations. We included the lecturers in our research as well and asked them to fill out the same questionnaires. We presume that by improving the training program itself and by increasing the support of this area, the info-security managers who graduated already, will also have more support and a stabile professional background so that organizations that have the possibility and means, will improve the efficiency and methods of communication.

[1] National University of Public Service, Faculty of Political Sciences and Public Administration, Institute of E-Government, Budapest, Ménesi str. 5, krasznay.csaba@uni-nke.hu
[2] National University of Public Service, Faculty of Political Sciences and Public Administration, Institute of E-Government, Budapest, Ménesi str. 5, som.zoltan.kdi@office.uni-nke.hu

Keywords: Information security in public administration, Electronic Information Security Manager (Hungarian abbreviation: EIV), development possibilities, National University of Public Service (Official Hungarian abbreviation: NKE)

1. Introduction

Nowadays information is easy to create and access – to an extent never before to be seen in history. Which is all made possible by the fact that electronic and IT systems are widely spread and that the development of information technology as a whole is resulting in a "digital revolution". Information is power – according to the well-known proverb. As a result, unauthorized acquisition and possession of digital information currently being created as well as the vast amount of already existing digital information – by personnel, organizations, or even states poses as a legitimate threat. The primary target of such information acquisition attempts (by virtue of their size and extensiveness) is public administration, which makes it especially important to have information security managers possessing adequate level of both qualification and skill working for the public (on the field of public administration). According to international practice the information security manager should be a key figure in every company, someone who shall be the subject to the direct control of the top manager only.
The National Assembly of Hungary has also realized the importance of dangers posed by cyber attacks[3] threatening national safety and as a result, passed Act 50 of 2013 on the Electronic Information Security of Public and Municipal Bodies (official Hungarian abbreviation: Ibtv.) which – among other regulations – states that in the field of public administration special personnel should be appointed in charge of the protection and security of electronic information systems. In compliance with text of the Ibtv. the National University of Public Service (Official Hungarian abbreviation: NKE) has launched a vocational training programme in 2014 to train Electronic Information Security Managers (Hungarian abbreviation: EIV). Students enrolled in the program could begin the third year of their studies in the 2015-2016 study year. The first class started with 33 students but by the time this study has been prepared there were more than 100 professionals enrolled in the programme. In order to evaluate the training programme and to find possible means of improvement, a questionnaire has been prepared (to gain information effectively). At the moment these questionnaires have only been partially processed and have been filled and returned by 53 students so far. This study aims to process the data acquired through the aforementioned questionnaires and also to formulate recommendations based on such data and on personal observations in the same time.

1.1. Research Methods and Experiences

In the process of selecting the research methodology primary focus was placed on "measurability". Acquired information were thoroughly reviewed and categorized before being processed further. The input properties of the students enrolled in the programme were extremely diverse. A significant level of diversity can be observed in each of the more important aspects. Regarding the first class, the age of students varied from 35 to 61 with an average age of 44.7 years. The candidates in the second class were much younger, the average age in their case was 39.8 years with the youngest student being 29, and the eldest being 55 years old.
The questionnaire consisted of 37 questions. Based on the number of respondents, the survey should be considered representative, with the willingness to participate being above 97%. The course of this study is not limited to numerical data only, we also relied on observations of a rather

[3] HADARICS, Kálmán – LEITOLD, Ferenc, Detecting suspicious network activities and security related events with open-source software, Central and Eastern European eGov Days 2015, p.315-324

anthropological nature, as we personally attended the courses (together with the students) as supervisors. As a result, we were able to gather information that would be extremely hard (if even possible) to quantify, e.g. the general atmosphere or conversations among students during breaks between lectures. Since the diversity was worth mentioning regarding the level of knowledge previously acquired by the students enrolled, the biggest challenge was to find and reach "a common level of basic knowledge". Comparing the first and second classes the knowledge of the first class was more obsolete (most likely as a result of the higher average age value) than that of the second class. Taking the data found during the research into consideration we recommend setting up and using a training model capable of teaching some lacking basic skills as well – this model might need refining to suit the exact needs, or for it to be set up as an entirely new one.

The need to improve the basic IT knowledge of graduated lawyers or the need to improve the legal knowledge of technical graduates are both good examples. This would also contribute to national security, as this way (at least some) organizations would be able to be up-to-date about IT systems and different means to abuse them along with appropriate counter-measures.[4]

Our hypothesis was that a heterogeneous spatial distribution will be experienced regarding the base of operation of employers of the students enrolled. Even though people in charge of the protection and security of electronic information systems working for public or municipal bodies are legally bound to be enrolled in professional training programmes, the students were mostly from Budapest or from settlements near Budapest, thus our hypothesis was rejected. In respect of the first two classes the ratio of students from Pest county (or even from settlements near the capital) and of those who were from elsewhere were 24:9 and 21:9 respectively. This might lead to the conclusion that the knowledge and understanding of the contents of the Ibtv. is recognized primarily by central bodies of public administration, whereas in the cases of country offices and local governments the challenges regarding information security have not yet reached the appropriate level of consciousness or that these bodies lack the capacity to act or simply do not recognize the question as a priority. These organizations are most likely planning to use the 5 year deadline posed by the Ibtv. to its full extent but this might result in hardships for the NKE as nowadays the classes only have few dozens of students but as the end of the deadline approaches, hundreds of students will be legally bound to enrol. Numerous researches conducted during the previous years have shown that organizations are characterized by a so-called "imaginary" level of security which unfortunately rarely matches that of their level of security in reality.[5]

"It is impossible be convince anyone of anything, it is only possible to show something new that shall result in the person arriving to an alternate, better decision."[6]

Upon analyzing the vocabulary of the theses submitted at the end of the vocational training programmes, a notable improvement can be observed regarding legal, IT, technical and information security matters. In some of the submitted works of students the question of information security improvements was addressed on an organizational level paired with professional level recommendations.

Graduated professionals are able to surpass the possibilities offered by legal regulations, they are also able to realize the opportunities hidden in serving as an example within the organization as well as those reachable by development of organizational culture and furthermore are able to set and

---

[4] LENTE, Csaba, ITBN, http://miszk.hu/hir/merlegen-az-informatikai-biztonsag.html, downloaded: 12.11.2015.

[5] ILLÉSY, Miklós – NEMESLAKI, András – SOM, Zoltán: Electronic Information Security Consciousness in Public Administration in Hungary. Information Society [in Hungarian] (Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. Információs Társadalom 2014. (XIV.)/1., p. 52-73

[6] KRASZNAY-SOM: Creating Parental Consciousness with the Help of Information Security Trainings in Public Administration [in Hungarian] (A szülői tudatosság megteremtése a közigazgatási információbiztonsági képzések segítségével), VIII. Nemzetközi Médiakonferencia

achieve goals on their own.[7] [8] [9] In order to be able to comply with the regulations, one must possess not only professional knowledge on the subject, but also a full and thorough understanding of the needs of the given organization.[10]

One set of questions primarily focused on the change of knowledge maps and situation assessment of the students during the course of the programme. The following question was asked: "To what extent did your knowledge regarding the question of information security change since the beginning of the programme?"

"Please indicate your answer on a scale from 1 to 7, 7 being the most." (2nd year, during the middle of the 1st semester).

The average value of the answers submitted (rounded up to the second decimal) was: 4.46. This means that even during the course of just one quarter of a year, the participants feel that they gained significant knowledge on the subject. The average value of the answers for the same question was 5.21 in the 1st year, in the 2nd semester.

An alternate group of questions aimed to find out more about the attitude of the organization towards the training programme. Answers for the question *"How were You chosen to participate in the training programme?"* showed a significant diversity – between the 1st and 2nd year students of the EIV. Taking answers that were given in the students own words into consideration as well, it can be observed that among 2nd year students more people have chosen to participate in the programme of their own free will, rather than being chosen and delegated to participate in a mandatory manner by their organization. A triple-blind review method was used to determine what answers fall under which category. 1) being "Did you have your own reasons to volunteer?" or rather 2), which was: "Are you participating in the training due to some form of external duress?". All three reviewers had to decide on the same category for the data to be considered legitimate.

Upon reviewing the time spent being employed by the organization that have selected and sent their employees to participate in the programme, it can be seen that in one third of the cases, those employees were chosen who have only been employed for two years or less. The remaining nearly two thirds are expected to possess a significant level of organizational experience. The fact that these employees are – most likely – to be accepted more widely in the organizational structure, can immensely boost the acceptance of information security into the given organization.

2. Recommendations for the Improvement of the Training

2.1.Geographical Decentralization

Professional events are in most cases organized and held in Budapest which makes it harder for students not living in the capital to participate and as such they are most likely to face hardships when attempting to further their professional career. A possible model would be to set up knowledge-centres where the training courses could be hosted in a rotational manner. As a result, a

[7] Susan M. Weinschenk: The Science of Convincing [in Hungarian] (A meggyőzés tudomány), HVG könyvek, 2015, p. 300

[8] Tipton, Harold F., Micki Krause. "Chapter 46 - Beyond Information Security Awareness Training—It Is Time To Change the Culture". Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications, 2007

[9] SOM, Zoltán: Educational Questions Regarding Information Security: Demands and Possibilities [in Hungarian] (Az információbiztonság oktatási kérdései: igények és lehetőségek), NKE KDI Kutatási Fórum, 2014.

[10] SZÁDECZKY, Tamás: The Conflict of the Regulation of IT Security, Info-Communication and Law [in Hungarian] (Az IT biztonság szabályozásának konfliktusa, Infokommunikáció és jog) 2013.3

knowledgebase could be set up that geographically speaking, might be diverse, but viewing the question professionally, something extraordinary could be achieved on national- or even international level.
Activities that take most of the students' time is either preparation for classes, preparing essays to be submitted, or practicing in general. The "aging" of knowledge gained poses a special threat once the training program is over. This is to be countered by the regulations of the Ibtv., which state that follow-up trainings shall be attended by professionals annually. This is mostly done trough e-learning instruments but experience shows that apart from the e-learning framework, personal meetings and discussions can also help keeping professional knowledge up-to-date. Personal meetings are also good ways to share good and best practices among professionals.
We recommend setting up an organizational structure or professional association that allows EIV graduates to meet on a regular basis and share their professional experiences with each other. Such associations should consider setting up bases outside the capital as well. Although social media seems to serve as a perfect platform for this, the possible sensitivity of the information to be shared might still require a form of personal meeting. Apart from "knowledge maintenance", setting up and operating such association(s) have some additional benefits as well:

- The professionalism and state of such a professional association could make wide-range professional discussions possible, which might lead to agreements or proposals that might help the development and better (common) understanding of the regulations of the Ibtv. in practice.
- Meeting on a regular basis would serve as an opportunity to exchange success stories, discuss ideas and suggestions as well as informal consultations.
- Undergraduate students might also attend such meetings, which would serve as an opportunity for them to get involved with the practical side of their expertise, as well as access professional information, which would all contribute to making good and best practices into "daily routine".
- It would be highly important to have a forum to share methods and outcomes of communication and "consciousness trainings" organized and held within the organization with one another.
- By being able to support both formal and informal forms of communication between organizations regulated by the Ibtv., these forums could contribute to a much faster professional reaction on this field.

It would also be important to discontinue the seemingly closed setting of the training. This would create an opportunity for professionals not working on the field of public administration to join the professional community of the EIV graduates, through which information security managers could get to know various types of good and best practices unique to different kinds of organizations. Although numerous organizations operate that would be suitable to gather and unite all professionals on the field, but all of them are based in Budapest and as a result, professionals not living and/or working near the capital could be easily left out. In the current state, hardships arise regarding logistics, financial matters and time management even if they *were* still willing to participate in such events.

2.2 Improving Technical Conditions and Support

Regarding the question of courses taught and areas touched upon, the students insist on an even more practice-oriented training programme. Unfortunately the required infrastructure for this to be realized is currently not available. In accordance with the development plans of the NKE, there

would be need for a cyber-security laboratory to be set up that could serve the educational needs of the EIV training programme as well, apart from those of the military, police and public administration programmes. Since the Ibtv. states that the NKE shall participate in information security-, cyber-security-, and vital information systems related defence exercises, the educational needs of students enrolled in the EIV training programme and those of the regular training programmes could be easily synchronized.

During cyber-security related exercises, it is essential to improve communicational skills. Most EIV students seem to have major inadequacies regarding this skill, whether it was about contacting cyber-security authorities or a simple conversation within the organization. It would be advised to add some form of a communications training to the EIV training programme.
Materials that graduates could easily use during their everyday work are also lacking. Although the university lecture notes offered during the training programmes do help, it would be an even bigger help to have a form of "tuition assistance" prepared with assistance from the National Institute on Cyber-Security, which would feature an "information security schedule" for the next year (or maybe next 6 months).[11] This could also include pre-conceived templates, which (after some customization) could be used to start the process of information security within the organization. We recommend the development of a knowledgebase of best-practices and know-how based on real life experiences that features easily applicable solutions for problems that are likely to occur. Should the abovementioned professional community exist, dissemination and discussion of such materials could be carried out easily.

3. Risks

3.1 Career Abandonment

According to numerous governmental analyses conducted in the past years, there seems to be an immense shortage of professionals in the IT sector of public administration. The "suction effect" of the private sector will most likely to become considerably stronger in the near future regarding electronic information security managers. Since the difference in wages between the private and governmental sectors are even more significant than in different IT areas, this risk should be kept in mind. We would recommend the development of a career model for EIV graduates. To have the manpower required to be able to sustain our cyber capability is of national interest.[12] In the same time , upon reviewing the reports of ENISA[13], it can be seen that the TOP 15 threat – abuse types are constantly increasing.

---

[11] The National Institute for Cyber-Protection (Nemzeti Kibervédelmi Intézet) has been established, http://www.kormany.hu/hu/belugyminiszterium/rendeszeti-allamtitkarsag/hirek/megalakul-a-nemzeti-kibervedelmi-intezet, downloaded: 01.11.2015.

[12] KRASZNAY, Csaba: Protection of Citizens During a Cyber-Conflict [in Hungarian] (A polgárok védelme egy kiberkonfliktusban), Hadmérnök, VII. Évfolyam 4. szám - 2012. december, http://hadmernok.hu/2012_4_krasznay.pdf, downloaded: 01.11.2015.

[13] ENISA, European Union Agency for Network and Information Security, https://www.enisa.europa.eu

3.2 Lacking Synergy

If there will not be at least a loose network set up between the graduates following their graduation, e.g. the abovementioned professional associations will not be organized and set up, there is a serious risk that there will be no chance to utilize aforementioned synergies. We find it crucial to set up at least a framework of an association before the 3rd year of the first class enrolled in the programme ends (by the fall of 2016), by providing the necessary financial and infrastructural conditions for it to operate. The following benefits could be achieved considering the different classes:

- 1st year students could get a feedback about the training going according to plan, since 3rd year students are almost graduating. Through the establishment of the association framework an adequate level of transparency could be added to communicate this.
- 2nd year students would get positive feedback (similar to 1st year students), but in addition a direct connection could be set up between the two classes.
- The 3rd (senior) year class could see what factors are directly influencing and affecting this career at the moment. Professional and personal relations could be established even before graduation.
- Patterns and models could be developed that could support the development of professional – human relations by creating opportunities to meet on a regular basis.

This way graduates can get information on the development of various good and best practices; which methods/ strategies were operational (what conclusions were drawn, what initiatives failed; sharing such information is highly important as such exchange of experiences and getting to know different scenarios could save the organization from "years of trying" during the process of information security development) all within the public sector but regarding different workplaces. As useful the annual online follow-up training may be, it cannot provide EIV students and graduates the opportunity to share their practical experiences. All risk factors should be considered seriously as some models exist that might not have worked or that were not able to produce adequate results.[14]

Our current research shows that there are recommendations that are several years old (e.g. ENISA), yet they have still not widely known in Hungarian public administration. The essence of our recommendation is that education and training would be provided by outstanding knowledge-centres in some areas. International models as well as good and best practices of other professional workshops could be integrated into domestic knowledge bases in a cost effective manner.

3.3 The Disintegration of Educational Background

Keeping the integration of the teaching staff shall also be kept in mind. Currently the best Hungarian professionals of information security are holding lectures in the EIV training programme, losing them would mean a major drawback. Intellectual infrastructure in general is something that is worth spending money and time on, but in this case, if the lecturers of regular training programmes of the NKE would be included in the EIV programme, such a knowledge

[14] Why Germany's Cybersecurity Law Isn't Working, http://www.defenseone.com/ideas/2015/08/why-germanys-cybersecurity-law-isnt-working/119208/, Downloaded:: 01.11.2015.

workshop could be established that would surely stand its ground even considering European standards.

4. Possible Benefits

4.2 Development of IT in Public Administration

In accordance with the National Info-Communication Strategy, large-scale government-funded IT developments can be expected in the following years.15 In order to guarantee the possibility of the development of the Good State, one of the most important elements is rapid IT development within public administration. Such development however shall be realized on structural level (in the planning process) by placing focus on interoperability between different systems as well as on transparency. This however means that there is a similar need for professionals on this field as the one regulated by the Ibtv. and which were solved by introducing the EIV training programme. This means that there is a great need for professionals aware of international trends as well as (EU and further) recommendations, who work in public administration as IT managers, operators, developers who would become members of the management.
It has been true till this point and it seems even more so regarding the future that IT systems are essential in the process of creating a good and modern state. It is a "fact that the organization of public administration in the present world would be impossible without IT instruments" but this also means some threats which should be addressed.[16] Employees in public administration are not yet prepared for the introduction of IT on large scale. The educational-training background is only just being developed. Most IT managers and lead developers in public administration do not possess international experience or evaluations on their field of expertise, which raises the question about how development can be expected in the future. The EIV training programme is the first training to serve as a good example on how to begin tackling the issue of chronic lack of IT professionals. Should the EIV become a complete success, it could serve as a good example for launching e.g. an IT manager training in public administration.
A further benefit is that professionals graduating on EIV gain a wide range of multidisciplinary knowledge and as a result can effectively support the managers in charge of IT at their organization too. Such question include planning, development, operation, etc. in different life-cycles and areas.
At least partially including ITIL, it will contribute to help the students develop a process-oriented way of thinking. In order to keep the prestige and seriousness of the training programme, it is advised for the required performance terms and percentages to be complied with strictly.

---

[15] National Info-Comunication Strategy 2014-2020. The strategy of developing the info-communication sector (2014-2020) v7.0. http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunikacios20Strategia 2014-2020.pdf

[16] BUKOVICS, István: Sustainable Public Administration, the Theory of Sustainable Security [in Hungarian] (A fenntartható közigazgatás, fenntartható biztonság elmélete). Polgári Szemle, Gazdasági és társadalmi folyóirat, 9: (3-6) pp. 211-225. 2013

4.3 Development of Data Assets in the Field of Public Administration

Both the Magyary plan and the concept of Good State assume that all necessary information, automatic data structures, required to come up with the most suitable decision are available. Based on which, the best possible decision will be made. Unfortunately this cannot always be realized due to the segmented system and the practice of supplying data through manual means.
The representation of data is information, and a set of data is called a data asset. The preparation of a data asset-inventory of an organization is an important subsidiary result of the information security process regulated by the Ibtv. Public administration professionals to be enrolled in training programmes offered by the NKE would be able to get familiar with not only the actual state of data assets and software inventory but also with plans regarding possible changes or exchange in the future, improvement plans even during their study years.[17]

5. Summary and Recommendations

The study showed how important it is to train and monitor the professional career of people in charge of information security. Should these be successfully realized, the "only" thing left would be to bring a culture that is based on the willingness to change to organizations in public administration. Change is most likely to be opposed. This is like a principle of human nature. Why would this be any different regarding the question of electronic information security? Taking the direct and indirect benefits stemming from an adequately constructed cyber-security system in public administration into consideration, any opposition should be addressed accordingly. There should be ways for users to give feedback and support should be offered to all users. The most important element of this might be the willingness to communicate. The manager who is also an information security professional must possess the following skill set: leadership skills, presentation and communication skills, which means delivering the right information to the right persons in a manner that is easy to understand and shall serve as a good example for the entire organization. Through the Ibtv. the government – either consciously or by following the pattern set overseas – placed emphasis on supportability and improvability regarding organizational and work culture in public administration. Without the realization of such cultures, change can only be achieved by utilizing much more significant (re)sources. It is clearly visible that we have arrived to a tipping point regarding the question of information security, some results can be seen even on short term, but to be able to advance further. the development of the abovementioned key areas are advised. It might be necessary to consult knowledge workshops abroad or even invite visiting professors in order to grasp foreign professional experience and expertise. In order to truly reform public administration and achieve value creation, similar steps would be required to the ones taken on the field of information security, on the levels of both development and operation. Maintaining and developing information security is considered a priority on EU level among the member states on a more global scale but should also be considered one on national level as well.

[17] ORBÁN, Anna: Some Aspects of Teaching Public Administration IT [in Hungarian] (A közigazgatási informatika oktatásának egyes aspektusai), PRO PUBLICO BONO: Magyar Közigazgatás; 2013:(3) p. 111-120. 2013.

6. Bibliography

[1] BUKOVICS, István: Sustainable Public Administration, the Theory of Sustainable Security [in Hungarian] (A fenntartható közigazgatás, fenntartható biztonság elmélete). Polgári Szemle, Gazdasági és társadalmi folyóirat, 9: (3-6) pp. 211-225. 2013.
[2] ENISA, European Union Agency for Network and Information Security, https://www.enisa.europa.eu
[3] HADARICS, Kálmán – LEITOLD, Ferenc, Detecting suspicious network activities and security related events with open-source software, Central and Eastern European eGov Days 2015, p.315-
[4] ILLÉSY, Miklós – NEMESLAKI, András – SOM, Zoltán: Electronic Information Security Consciousness in Public Administration in Hungary. Information Society [in Hungarian] (Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. Információs Társadalom 2014. (XIV.)/1., p. 52-73
[5] KRASZNAY-SOM: Creating Parental Consciousness with the Help of Information Security Trainings in Public Administration [in Hungarian] (A szülői tudatosság megteremtése a közigazgatási információbiztonsági képzések segítségével), VIII. Nemzetközi Médiakonferencia
[6] KRASZNAY, Csaba: Protection of Citizens During a Cyber-Conflict [in Hungarian] (A polgárok védelme egy kiberkonfliktusban), Hadmérnök, VII. Évfolyam 4. szám - 2012. december, http://hadmernok.hu/2012_4_krasznay.pdf, downloaded: 01.11.2015.
[7] LENTE, Csaba, ITBN, http://miszk.hu/hir/merlegen-az-informatikai-biztonsag.html, downloaded: 12.11.2015.
[8] National Info-Comunication Strategy 2014-2020. The strategy of developing the info-communication sector (2014-2020) v7.0. http://2010-2014.kormany.hu/download/b/fd/21000/Nemzeti%20Infokommunikacios20Strategia 2014-2020.pdf
[9] ORBÁN, Anna: Some Aspects of Teaching Public Administration IT [in Hungarian] (A közigazgatási informatika oktatásának egyes aspektusai), PRO PUBLICO BONO: Magyar Közigazgatás; 2013:(3) p. 111-120. 2013.
[10] SOM, Zoltán: Educational Questions Regarding Information Security: Demands and Possibilities [in Hungarian] (Az információbiztonság oktatási kérdései: igények és lehetőségek), NKE KDI Kutatási Fórum, 2014.
[11] Susan M. Weinschenk: The Science of Convincing [in Hungarian] (A meggyőzés tudomány), HVG könyvek, 2015, p. 300
[12] SZÁDECZKY, Tamás: The Conflict of the Regulation of IT Security, Info-Communication and Law [in Hungarian] (Az IT biztonság szabályozásának konfliktusa, Infokommunikáció és jog) 2013.3
[13] Tipton, Harold F., Micki Krause. "Chapter 46 - Beyond Information Security Awareness Training—It Is Time To Change the Culture". Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications, 2007.
[14] The National Institute for Cyber-Protection (Nemzeti Kibervédelmi Intézet) has been established, http://www.kormany.hu/hu/belugyminiszterium/rendeszeti-allamtitkarsag/hirek/megalakul-a-nemzeti-kibervedelmi-intezet, downloaded: 01.11.2015.
[15] Why Germany's Cybersecurity Law Isn't Working, http://www.defenseone.com/ideas/2015/08/why-germanys-cybersecurity-law-isnt-working/119208/, Downloaded:: 01.11.2015.