HADMÉRNÖK

IX. Évfolyam 1. szám - 2014. március

Schüller Attila
schuller.a@gmail.com

ANALYSIS OF USER BEHAVIOUR FROM THE POINT OF VIEW OF INFORMATION SECURITY

Abstract

In information security, the human factor is the biggest threat as is true for the whole of safety technology. There are numerous regulations and recommendations that are intended to eliminate human errors and irresponsible behaviour. Some bad user behaviour is surveyed in this article, which points out that it has not been possible to reduce human errors to an acceptable level using current methods.

Ahogy a biztonságtechnika egészére igaz, úgy az információbiztonság részterületére is, hogy a legnagyobb veszélyt az emberi tényező jelenti. Számtalan szabályzás és ajánlás létezik, amely az emberi hibákat és felelőtlenségeket szándékozik kiküszöbölni. A cikk néhány rossz felhasználói viselkedést mér fel, ami arra hívja fel a figyelmet, hogy az emberi hibákat nem sikerült elfogadható szintre csökkenteni a jelenlegi módszerekkel.

Keywords: *információbiztonság, adatbiztonság, emberi tényező, felmérés ~ information security, data security, the human factor, survey*

INTRODUCTION

The discipline of information security has quite an old origin, as information security techniques were in use in the ancient world, such as cryptography (encryption) and steganography (data hiding). However, since its inception the problem has been in all systems and processes the people, that is, human frailty (e.g. corruptibility, carelessness, laziness, vulnerability to blackmail) can weaken the protection.

However, in many cases, the owners of information (companies, organizations, or individuals) do not pay enough attention to eliminating the negative effects of the human factor. Measures are often introduced for the sake of appearances but they are not able to protect against cybercrime.[1]

Cybercrime can cause damage of up to $600 billion a year worldwide according to the latest survey carried out by Symantec. [2] Although the number of reported security incidents has increased only marginally the amount of financial losses from intrusion appears to have been greatly reduced. However, because most companies do not use a common methodology when measuring these losses the data are only partially reliable.

In analysing the current situation, I examined the results of other research, before conducting my own survey of user habits. In addition, I analyzed people's actual behaviour using empirical methods, and I compared this with the answers that they gave in the survey.

ANALYSIS OF USERS' HABITS

The "Global State of Information Security Survey 2013" was carried out worldwide by CIO (Chief Information Officer News and Insight), CSO (Chief Security Officer Magazine) and PwC (PricewaterhouseCoopers). From their findings I would highlight the following. Most respondents believe their organizations have instilled effective information security behaviours into the organizational culture. The people carrying out the survey categorized respondents according to the way they describe their approaches to security. "Frontrunners (42%) say their organization has 'an effective strategy in place and is proactive in executing the plan.' These are key elements of true security leadership. Strategists (25%) say they are 'better at "getting the strategy right" than executing the plan,' while tacticians (16%) rate themselves 'better at "getting things done" than at defining an effective strategy.' Firefighters (16%) admit that they 'do not have an effective strategy in place and are typically in a reactive mode.' Based on these qualifications, the analysis reveals that only 8% of respondents rank as true leaders."[2] [3]

ISACA (Information Systems Audit and Control Association) is an international professional association that focuses on IT Governance. This organization also prepares an annual survey about information security.

According to the 2011 survey, 82% of companies with foreign shareholders have an information security strategy, this figure is only 59% for firms in 100% Hungarian ownership, while this figure is 61% for the respondents as a whole. However, only 18% of the respondent institutions aimed to develop a comprehensive information security strategy. Even worse is the case with the security awareness program, which is in place in 37% of the institutions, and only another 19% were planning its implementation. In terms of human factors, the worst situation was in the background checks as part of the admission procedure, only 17% of respondents carried out such checks. [4]

[1] By computer crime we mean crime committed for the purpose of profit or causing harm to IT systems to managed data confidentiality, authenticity, integrity, and availability, as well as the availability and functionality of system components or crimes committed using IT tools. [1]

[2] True leaders: „an elite group with the vision, determination, skills, and support to create the most effective security organizations." [3]

According to the 2012 survey, Hungarian companies have begun to realize the importance of an information security strategy, but we are still far from the cutting edge in terms of concrete steps. The use of administrative tools is more widespread than the use of technological tools. For example, nearly 50% of the companies surveyed have an overall information security strategy but only 14% of them have vulnerability analysis tools, as compared with the 46% internationally. [5] We should point out, however, that this result is worse than last year's, because 61% of the respondents had an overall information security strategy in 2011 [4], the rate has fallen, therefore, by 11%. The rate of application of vulnerability analysis tools was 25% [4], so this figure has also fallen by 11% in one year.

The situation has also deteriorated in respect of the IT risk assessment at an adequate depth. As shown in figure 1, the proportion of institutions where risk assessments are carried out regularly has decreased by 7% and the percentage of those which have no plans to introduce them has increased by 5%.

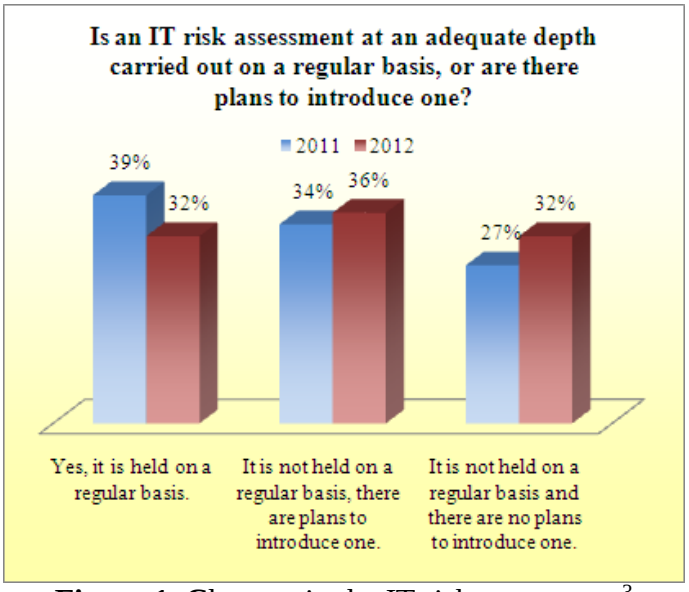

Figure 1. Changes in the IT risk assessment[3]

These surveys have been carried out at management level. They are, therefore, more likely to give information about what steps the company has taken to ensure information security and how strong it considers itself to be in this area. However, a bottom-up analysis of the organizations should be carried out to provide answers about how to ensure that the employees comply with the rules established. I have created a questionnaire to assess this and I examine the key indices for this.

I produced my questionnaire, which was in English and Hungarian, in such a way that people could fill it in online and their responses could be recorded directly in a database. Thus, after the data had been collected they could be easily evaluated using any spreadsheet software. These were two reasons for collecting data online: firstly I wanted to make use of modern technology as I have described above and secondly several of the questions were of a type that the majority of people either would not answer or would answer untruthfully if I had asked them personally. In [6] we learn that in China, for example, during the Cultural Revolution using traditional questionnaires it was almost impossible to gather valid and reliable data about the lives, opinions and attitudes of the Chinese with respect to the Communist regime.

I have previously investigated the attitude of the young with respect to information security (Hadmérnök 2/2011). During my present investigation I wanted to get as broad a picture as possible of the current situation. This is why I did not want to narrow it down by strictly defining

[3] This figure has been compiled by the author using sources [4] and [5].

the participants. I sent out the questionnaires not in a targeted, personalized way. Instead I asked the recipients to invite their friends to fill out the form, and I sent the Internet address of the questionnaire to on-line forums and a newsgroup too. Therefore is not possible to determine the exact number of respondents.

I received 139 responses after excluding those that contradicted themselves. They can be broken down into the following demographic groups. 87 women (63%) and 52 men (37%) replied. Among these 17 were under 15 years of age (12%), 33 were in the age group 16-20 (24%), 28 in the age group 21-25 (20%), 30 in the age group 26-30 (22%), 15 in the age group 31-40 (11%), 9 in the age group 41-50 (6%) and 7 were over 50 years of age (5%). 114 were born in Hungary (82%), 115 are at present living here (83%). 58 live in capital cities (42%), 22 live in other large cities (16%), 35 live in towns (25%) and 24 live in smaller locations (17%). It is also worthwhile to compare the distribution of persons of Hungarian origin and currently living in Hungary[4] with statistical data of the Hungarian population. I compare of these from different aspects. 36% (41) of the group of this respondents are male and 64% (72) of them female, while based on data from the population census 2011 [7], 47% of the Hungarian population are male and 53% of them are women. 43% (49) of Hungarian respondents live in Budapest, a further 10% (11) of them in other major cities, 27% (30) in small town, 20% of them in other settlements, by contrast, these rates were 17%, 20%, 32% and 31% respectively in the most recent census [8]. Other discrepancies can be seen in the field of educational qualifications. 40% (45) of the group containing members of Hungarian origin and currently living in Hungary completed primary school, 24% (27) of them completed high school and 36% (41) of them completed college or university, in contrast to the census statistics [9] in which the respective data were the following: 60%, 30% and 10%.

It can be seen from the data that the survey is not representative. Nevertheless, dividing the data to take into account differences with respect to age and gender may provide an opportunity to study and analyse the characteristic behaviour of the different groups. However, during my present investigation my aim was to measure the general risk to information security posed by the human factor, so I did not do this.

38% (57) of the respondents believe that their home PC or work computer cannot be attacked. This is the illusion of invulnerability: people believe – wrongly – that bad things can only happen to others. This unrealistic optimism has been shown in connection with several beliefs: people expect fewer health problems, fewer and less severe accidents, fewer failures etc. in their own future than what they might expect to happen to an average person similar to themselves. This behaviour is a natural defence against stress. [10] In the same way that people see themselves as better drivers and more cautious than they are in reality, this is also true for information security: if an antivirus and a personal firewall are installed on their computers, they think that this will protect them against all dangers. The illusion of invulnerability is also present at management level, when, after introducing robust information security rules, the managers sit back and relax, neglecting the considerable risk posed by the employees' non-compliance with these rules.

According to the Norton Cybercrime Report 2012, 14 adults become victims of cybercrime every second somewhere in the world. This means everyday more than a million people, which is twice as many as the number of newborn babies. 69% of adults surveyed had experienced cybercrime at some point in their lives. Compared with the 2010 survey overall, cybercrime increased by 3%. Over the 12 months examined, 15% of adults surveyed suffered a crime in the real world and 44% of respondents experienced cybercrime. [2] These data show that we are slow to respond to the challenge posed by the rapid increase in cybercrime. This lack of suspicion and preparedness are part of the reason why cybercrime is so effective.

[4] This figure is 113.

It is interesting to note that according to my survey, 17% (24) of respondents do not believe that the computers at their workplace are targets for hackers. They think, however, that their home PC is in danger. A workplace computer contains more important and (from the economic point of view) more valuable data, therefore, respondents presumably have concluded that their company computers are equipped with some serious protection, and are therefore much harder to access electronically.

41% (56) of users do not comply with the security measures. 4% (5) of them because they regard them as excessive, 37% (51) of them understand the need for regulations, but despite this, they do not pay attention to them. This very high ratio shows that with regulations alone, only a false sense of security can be achieved. In addition to the regulations, methods need to be developed and implemented that take away from the users the option to transfer their rights to another person, whether deliberately or through careless behaviour. Results were poor for those who declared in the questionnaire that they respect the information security measures. 29% (24) of these users use the same password everywhere, 20% (17) of them choose simple passwords, and 4% (3) of them leave their passwords in a place that is easily accessible. The above careless behaviour demonstrates that some people have a false sense of security and think that they are behaving in a responsible manner with regard to information security, while in reality they are making fundamental errors.

8% (11) is the number of those who – with or without permission – take home data from their workplace, although they do not comply with the security measures as they admitted in their response to a further question. One way for companies to protect themselves is if they do not allow corporate documents to leave the premises physically or electronically. According to the Kaspersky Lab survey, 29% of the companies surveyed prohibit, and a further 19% of them restrict the use of removable media (flash drives, external hard drives etc.) in one way or another. In 49% of the companies the FTP (File Transfer Protocol) connection, in 50% of them the cloud storage solutions, in 52% of them personal e-mail are prohibited or restricted. [11]

Biometric authentication within the enterprise could enhance information security in several ways. Thereby the access to data and the verification of the documents issued and updated by the user can be done easily and securely, however, partly due to legal regulations, and partly because of the users' aversion to such a method, in practice it is not used widely. The survey I conducted shows that 49% (68) of users would not be disturbed if biometric identification were employed at their workplaces, 16% (22) of them would be disturbed and 29% (41) of them would react positively or negatively depending on the method of identification. 6% (8) of the respondents did not answer this question.

Based on the survey data, 36% (50) of people do not give their passwords to anyone. This means the remaining 64% (89) of them are willing to reveal their passwords: 1% (2) to anyone, 39% (54) only to a trustworthy person, and 24% (33) only if after using it they change it immediately (figure 2). In my daily work, I experience worse rates: a significantly lower proportion of the people I come in contact with are unwilling to provide their access data, and at least 6-8% of them reveal their password without justification (in even worse cases, they add that they use the same password everywhere).

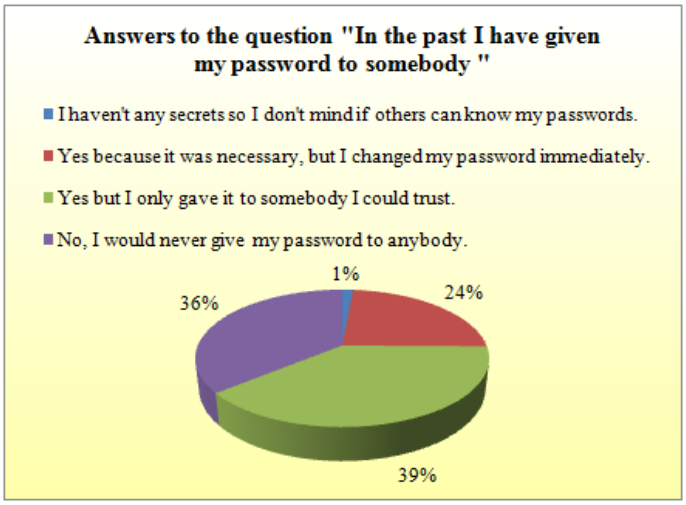

Figure 2. Willingness to reveal passwords

I got the following answers for the way people treat their passwords (figure 3). 4% (6) of the users write down their passwords in a place that is easily accessible. This can be very dangerous because it could easily fall into the wrong hands, allowing unauthorized access to the system. A better solution would be if the user wrote down their passwords in a way that nobody else could make sense of (e.g. the last 4 letters are the true password in a 7 character word). 6% (9) of the respondents said they use this method. 29% (40) of the respondents use the same password everywhere, so if access data for a system are obtained by unauthorised people they could easily penetrate the rest of the system too. 20% (28) of the survey participants choose simple passwords that are easy to figure out/decrypt/remember by somebody observing them. Only 5% (7) of users change their passwords regularly, but if more users did so, this would increase security significantly.

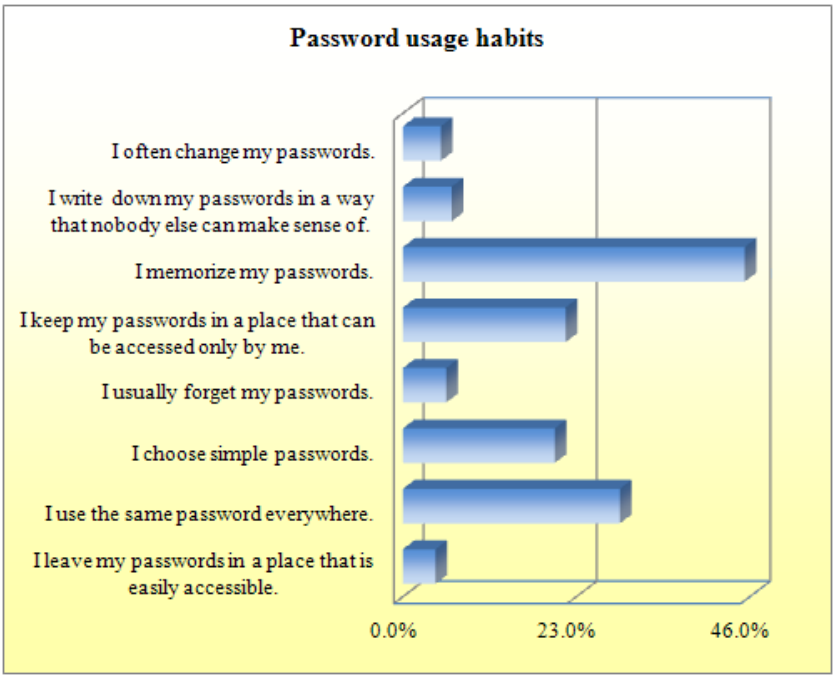

Figure 3. Password usage habits

I used an anonymous online questionnaire to collect data, because with it I was more likely to get true answers than if I had asked people personally. Nevertheless, the replies were often over-optimistic, which is also clearly visible in responses given about social networking sites. 6% (8) of respondents accept the fact that everybody can see their personal data, 27% (38) of

them say they have not given personal data, and 59% (82) of them have made them available only for their friends. 65% (90) of the survey participants claim that they only accept somebody as a friend if they actually know them and only 4% (5) responded that they accept everybody, even if they do not know them. I chose an empirical method to test this information. I created a fictitious person on one of the most popular social networks and I requested to be the friend of 60 people chosen at random. The first acceptance arrived within 4 minutes. I had 7 friends in 2 hours, and in the end I made 33 friends, so 55% of the people I chose accepted my request to be their friend, although we were complete strangers. Two other people accepted me as a friend without my request. On analyzing the data, I found that of these people, more than 60% (21) of them made available to strangers their place of residence, workplace and qualifications, 57% (20) of them revealed their marital status and birth place and 6% (2) of them their birthdays. Of course, this figure is higher for their friends, for example 89% (31) of them allowed their friends to read their birthday data. According to my survey on Facebook 71% (25) of users publish their e-mail addresses and/or telephone numbers, but only 3% (1) of people who make these data visible to anyone. 94% (33) of people upload photos of themselves and 89% (31) of them so that anybody can see them. In figure 4 I compared the answers of persons filling out the questionnaire with data experienced in reality. There were significant differences between the two groups. This does not mean that the respondents wanted to falsify the results, but they are not aware of the concept of personal data, so they believe that they have not given such information.[5]

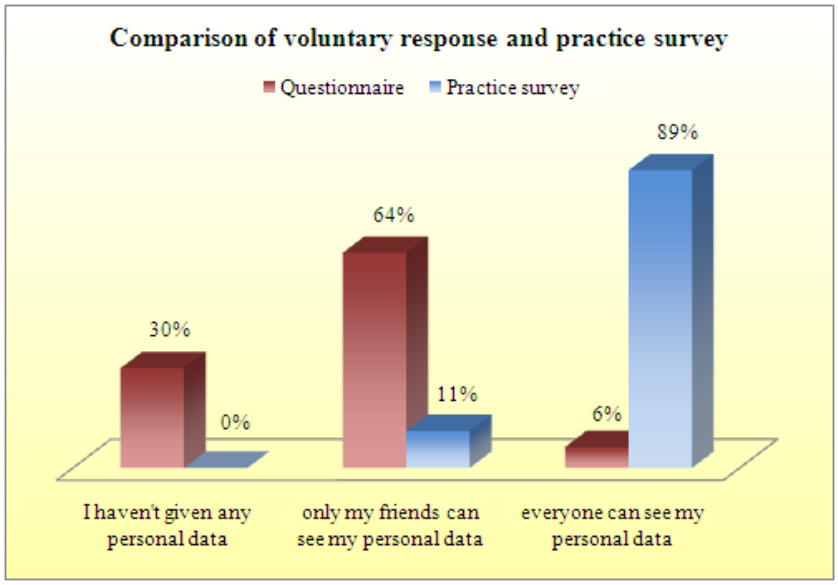

Figure 4. Indications of the human factor in the responses

The Hungarian Data Protection Act defines personal data as follows: data relating to the data subject, in particular the name and identification number of the data subject, as well as one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject. [12] It would be difficult to provide any data on this basis that is not considered personal data. People ought to be aware of the personal nature of same of their data (e.g. date of birth, marital status), however, the responses show that the majority of people do not consider such data personal, which they publish without any particular reservations.

[5] Of course I did not take into account the name in the survey because this piece of data is displayed in all cases. Users can register with a fake name, but I could not check up on this. However, they did not use a fake ID (e.g. the name of a film character) and I ignored other potentially dubious data (e.g. university studies in Bogota).

People give positive answers to some extent instinctively. The following factors can influence their judgement.

The *availability heuristic* can cause inaccuracies in the probability estimation: when applying it, the judgment of the frequency of an event depends on how imaginable the event is, how easy it is to remember, how interesting and how stimulating it is. People consider the very rare causes of death (e.g. murder) to be more frequent than they are in reality and consider the very common causes (e.g. heart disease) to be less frequent than they actually are. [10]

It is a typical and dangerous error when a specialist is overconfident in the correctness of their judgment *(overconfidence effect).* This group tends to trust too much in the results of science and fail to recognize the excessive complexity of the operating mechanisms of technical systems. Because of this feeling of security the experts are not encouraged to doubt their own opinions or to obtain additional information. [10] It is essential to bear this in mind because human behaviour is more complex and unknown than technical systems. The overconfidence effect can be experienced when the management is satisfied with the introduction of new security measures, but compliance with them is not checked.

The *wish for certainty* leads people to reduce the anxiety caused by uncertainty with an exaggerated and unfounded sense of security. Victims of flooding (wrongly) believe that the same disaster cannot happen to them again. [10] In information technology, it is the case that some people do not care about secure password management, despite the fact that their e-mail address or account for a social network has been used illegally previously.

CONCLUSION

Quantitative research is suitable for the investigation of certain areas, but we cannot rely only on surveys conducted among managers, because they examine information security from the point of view of the actions taken and planned, so they form a picture about the position they would like to reach, rather than the real state of affairs. Therefore, more emphasis should be placed on an analysis of the real situation, evaluating the results obtained and with continuous monitoring. In addition to the collection of questionnaire data, empirical research should be carried out, because responses may also be distorted unwittingly, as an inherent result of human nature.

„Too many cooks spoil the broth." I consider it to be a serious problem that IT professionals also believe that if a separate information security department has been created in their companies, then they do not have to deal with this area. In particular, because in many cases within the company the tasks of the information security department are interpreted in different ways. Many people expect this department only to ensure IT security, but in some companies its primary task is only the prevention of industrial espionage, while in others, this department only concentrates on checking the employees.

However, there is considerable overlap between information security and IT security, so the IT department is obliged to deal with confidentiality, integrity and availability as part of their duties, even if other departments carry out these tasks in the rest of the company.

The effect of the Internet also can be felt in relation to the careless handling of data, because in cyberspace, people give personal information to strangers more readily than if for example somebody went up to them in the street. The lack of personal contact reduces caution, and makes establishing contacts easier and less inhibited. This allows information to be extracted from unsuspecting users.

As my survey also revealed, despite the existence of strict information security rules the users do not always respect them. Security could be increased by reducing the human factor. There are various technical solutions which would remove the process of identification from people and thus reduce the danger of unauthorised persons gaining access. One possibility is

the use of biometrics, but people's aversion to such technologies and the lack of an appropriate legal framework still cause difficulties.

This article is supported by tender TÁMOP 4.2.2./B-10/1 (Risks and Answers in the Field of Talent Maintenance: "KOVÁSZ")

References

[1] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve. Verlag Dashöfer Szakkiadó, Budapest, 2000-2005

[2] Symantec: Norton Cybercrime Report 2012 http://us.norton.com/cybercrimereport/promo (16.06.2013)

[3] CIO, CSO, PwC: Changing the game. Key findings from The Global State of Information Security Survey 2013 http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf (10.06.2013)

[4] ISACA Információbiztonsági helyzetkép 2011 http://www.kpmg.com/HU/hu/IssuesAndInsights/ArticlesPublications/Documents/Informaciobiztonsagi-helyzetkep-2011.pdf (10.06.2013)

[5] ISACA Információbiztonsági helyzetkép 2012 http://letoltes.etrend.hu/Hetpecset/ppt_LIV_5/InfoBizt_helyzetkep.pdf (10.05.2013)

[6] Babbie, Earl: A társadalomtudományi kutatás gyakorlata. Balassi Kiadó, Budapest, 2003.

[7] KSH population census 2011: Population by citizenship and sex http://www.ksh.hu/nepszamlalas/docs/tables/regional/00/00_1_1_2_2_en.xls (26.02.2014)

[8] KSH népszámlálási adatok 2011.: A népesség számának alakulása, népsűrűség, népszaporodás településtípusonként http://www.ksh.hu/nepszamlalas/docs/tablak/demografia/04_01_01_01.xls (26.02.2014)

[9] KSH population census 2011: Population by education and age group http://www.ksh.hu/nepszamlalas/docs/tables/regional/00/00_1_1_4_1_en.xls (26.02.2014)

[10] Zoltayné Paprika Rita: Döntéselmélet. Alinea Kiadó, Budapest, 2005.

[11] Kaspersky Lab: Global IT Security Risks: 2012 www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf (16.06.2013)

[12] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról