HADMÉRNÖK

VIII. Évfolyam 2. szám - 2013. június

Attila Schüller
schuller.a@gmail.com

INFORMATION SECURITY ANOMALIES IN THE IT SYSTEMS OF HUNGARIAN PUBLIC EDUCATION

Abstract

IT systems in public education involve information security risks due to recurrent security incidents. The author has carried out case studies to demonstrate that the reason for these incidents is the human factor. Public education is part of the critical infrastructure through its link with the public administration and associated IT infrastructure. Therefore greater attention should be paid to the information security of these systems. However, it should also be borne in mind that if the public administration authorities are negligent with the national systems our protection in more endangered fields may not be sufficient to counteract cyber terrorism.

A közoktatásban kötelezően előírt informatikai rendszerek számos információbiztonsági kockázatot rejtenek magukban, melyek miatt visszatérő biztonsági incidensek fordulnak elő. A szerző esettanulmányokat készített, melyen keresztül rávilágít, hogy ezen incidensek oka kizárólag a humán faktor. A közoktatás egyrészt a közigazgatáson keresztül, másrészt a hozzá kapcsolódó informatikai infrastruktúrán keresztül épül be a kritikus infrastruktúrába. Emiatt kiemelt figyelmet kellene fordítani a működéséhez szükséges rendszerek információbiztonsági és informatikai védelmére. Továbbá elgondolkodtató, hogy ha a közigazgatási szervek ennyire hanyagul kezelnek országos rendszereket, akkor a cyber terrorizmus által még inkább veszélyeztetett területeken vajon elegendő védelemmel rendelkezünk-e.

Keywords: *information security, public education, human factor ~ információbiztonság, közoktatás, emberi tényező*

INTRODUCTION

The importance of this topic was highlighted by the near-paralysis of the system through which textbooks can be ordered. The system of the Library Supplier Non-profit Organisation (Könyvtárellátó Kiemelten Közhasznú Nonprofit Kft. – KELLO) which received 354 million forints of aid from the Hungarian Government [1][2], and which got coverage in the media, in many ways proved unsatisfactory but I analyze it specifically from the aspect of information security. I compared this case with other incidents that happened to public education institutions, among other things with what happened last November, when the Information System of Public Education (Köznevelési Információs Rendszer – KIR)[1] was modified, when for example there were cases of unavailability and data losses because the badly designed system was overloaded.

Another recent event that occurred was when the IT network of public education institutions (Sulinet) operated by the National Information Infrastructure Development Institute (Nemzeti Információs Infrastruktúra Fejlesztési Intézet – NIIF) changed the firewall settings of schools, thereby risking the local and national IT systems.

In the cases examined all the information security policy recommendations defined in the ISO 27001 standard – confidentiality, integrity, availability – were compromised and there were cases in which more than one of the above factors was insufficiently taken account of.

DEFINITIONS

There are mainly three key aspects of information security often referred to as the CIA triad: confidentiality, integrity and availability. [3] The ISO 27001 standard defines the three components of the triad as follow:

Confidentiality: Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

Integrity: To preserve the integrity of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it.

Availability: Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the context of this standard, assets include things like information, systems, facilities, networks, and computers. All of these assets must be available to authorized entities when they need to access or use them. [4]

The Hungarian Privacy Act regulates as follows: through appropriate measures the data must be particularly protected from unauthorised access, modification, transfer, disclosure, deletion or destruction, accidental destruction and damage as well as disabled access occurring due to changes to the technology applied.[5]

The information society is unworkable without a modern IT infrastructure. However these systems can also stop working or be disturbed if they are exposed to malicious attack. [6] Another functioning source of harm, however, can be of internal origin and unintentional. This type of harm, arising from carelessness, can endanger the system just as much as an external, deliberate attack.

Public education forms part of public administration[2], and because of this belongs to the critical infrastructure, as does the information system needed to make it function. To an outside observer it may seem that the school system is not of such critical importance, but as I

[1] The Information System of Public Education is operated by the Office of Education. Under an agreement with the Office of Education the operational and data processing tasks are carried out by the Educatio Nkft.

[2] Area as part of the social function. [7]

show later, the huge amount of data handled and the need to ensure confidentiality of personal data, require special attention. Incidents in the public education system can endanger elements belonging to the critical infrastructure, due to interdependence[3], from the information infrastructure needed to make it function, which arises and intradependence[4], which is a result of the centralised handling of data.

EVENTS LEADING TO INFORMATION SECURITY INCIDENTS

In what follows below, I have described the information security incidents that occurred the in the public education system over the last year or that increased the probability of such incidents occurring.

1. In November 2012 the KIR system containing records of personal data was modified. The system was expanded to contain extra data, but the schools were given a very tight deadline to provide the missing data. However, the information background was not planned with sufficient care and because of this the system became overloaded and in some cases impossible to reach. [9][10]
2. Another problem was that on several occasions there were data losses in some schools, the recorded data were partially or completely lost, so the administrator had to record this data again. [9][11][12]
3. On worrying incident happened in connection with the Educatio Nkft. when after a previous system failure of the KIR system the help desk operator asked for the login data in order to do the login procedure based on this information, they wanted to check that is was really impossible to use the software according to the prescriptions.
4. At the beginning of each school year every school has to allocate the different subjects5 to be taught, which for the schools maintained by the capital necessitates using the F2 school administration system. As the deadline for the allocation of subjects approaches the software was modified continuously. In one case after solving a program failure the sum of the hours that could be allocated – which the software had earlier calculated – was decreased. This led to the whole completed job having to be modified. In another case the software was changed after the deadline, as a result of this all data had to be sent again to the city government.
5. During the centralisation of public education institutions the software of the feeding service was modified in such a way that both the software and the connected database folder were synchronized with the feeding service centre by DropBox6. During an update, which had not been signalled in advance, the school administrator opened the old program, while it was being replaced by the software provider at another location. As a result of this the data recorded during this activity were lost.
6. The textbook ordering system operated by KELLO caused several major problems. The system development was delayed so that the schools received the login data only a few days before the deadline determined by law. As a result of human failure there

[3] Interdependence: the different types of infrastructure do not operate in isolation, but often closely interact with each other. Through the interconnection of the different types of infrastructure problems can accumulate and they can cause unexpected and more serious operational problems in essential state services. The interconnections and interdependencies of the infrastructure make it vulnerable to attacks, disturbances, and attempts to destroy it. [8]

[4] Intradependence: interdependence within the infrastructure.

[5] Allocation of the different subjects is necessary for the financial planning of the public education institutions, and is also required by law. [13] The law also has regulations relating to its content.

[6] DropBox is a type of software that allows to synchronising a folder of a local PC with a folder of a remote server.

was at least one educational institution which received all the login data of all the schools within their educational district via e-mail. [14]

7. Although the institutions had their own login data because the system was not planned properly it was unreachable even on the first day due to overloading. Later, the number of the logged-in users was limited to 1 000, but more than 3 000 schools were still unable to work with it, and the system was also overloaded in the evening hours as well. The lucky ones who managed to enter the system, could record their data only very slowly because of the insufficient program speed. [15] Because of several cases of program patching the ordering interface was unreachable.
8. Each establishment was given only one login name and password to use the textbook ordering system. If several users would like to work in the system (for example: job sharing) they could enter only with the same login data.
9. A part of the students' personal data was copied centrally from the KIR database into the textbook ordering system, but each student's grade and address for the invoices, which had previously been registered by the KIR had to be registered again. Later, some days after the opening of the system some records[7] were migrated into the textbook ordering system. But the schools were not informed about this operation.
10. The user interface of the software is not clear, a little inattention can easily cause data losses and wasted work. [16]
11. After the deadline the recorded data were still accessible. In this period during a check of the recorded data it came to light that the previously recorded data had changed and the sum of the orders shown by the system when this was made exceeded the sum of the orders actually made. [17] The helpdesk could not give proper information about the state of the system. All that they said was, that there was a failure in the system, troubleshooting is in progress, the data should not be modified and sometime later the system will show the actual orders placed.
12. On 1 of January 2013, the NIIF took over the operating of the Sulinet network which ensures the Internet access of public education institutions. [18] Without any warning of schools, through remote access they removed the restrictions from the firewalls of the schools. A part of the institutions have no other firewall, or they employed a dual firewall[8] solution for the DMZ[9].
13. The Centralized Payroll System (Központosított Illetmény-számfejtési Rendszer – KIR3) does not work in the recent Java environment. For "solution" you have to remove the currently used Java and install an older, non-supported version. Schools were not notified about this change and were no informed about the troubleshooting. [20]

[7] This migration process was done in the case of addresses that were not filled in or less than 5 characters-long.

[8] The first firewall must be configured to allow traffic destined to the DMZ only. The second firewall allows only traffic from the DMZ to the internal network. [19]

[9] In computer security, a DMZ (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet. [19]

ANALYSIS OF THE CASES SURVEYED

I analyze the cases described in previous paragraphs from the aspect of the ISO 27001 standard, categorising them by confidentiality, integrity and availability.

Confidentiality

In case 6 access data were leaked. The careless data officer allowed not only the possibility of unauthorized data recording but also gave access to the personal data of students who go to the affected school, because these data were migrated from the KIR system (without the addresses). The fact that a serious human failure could happen in a national IT system which is operated by a government organization shows that it is not enough that there are well-defined standards and recommendations if they are not used in practice.

Point 3 shows that the central help desk ask for the users' login data. Due to the fact that the service providers cannot control the system without asking for the users' passwords – which, according to the information security recommendations, should not be handed over, even in this case – they risk leaking of the passwords and make it possible for a third person to cheat the users out of their login data by social engineering[10]. It is essential that the service providers should have a higher access level so that they can check the database and have the possibility to make modifications without asking for login information from the users.

The Hungarian Privacy Act stipulates that: during the course of the automated processing of personal data, the controller and data processor should ensure by taking additional measures the following: prevention of unauthorised data entry, the ability to control and determine which personal data have been registered in the automatic data processing systems, when this was done and who did it. [5] Because every school has only one own user identifier per establishment (see section 8), if several people work in the system (for example an administrator helps in the work connected with textbooks) then it is not possible to check it and to establish who recorded data in the system and what was recorded. Furthermore based on experience if several users use identical access data there is a greater chance that the passwords will fail into the wrong hands.

A supplement to the previous cases: using textbook ordering and also the modules of the KIR system the authentication and other data transfer communication flow via an unencrypted http protocol so a third person could get the data easily.

The modification on firewalls in point 12 risks poses a direct risk to confidentiality and through this to integrity and availability. If a school used a dual firewall solution in such a way that the firewall of Sulinet was the outer firewall, then its servers inside the DMZ were endangered and the protection from the Internet was eliminated. If, however, they did not operate an extra firewall and relied on the firewall of Sulinet to provide protection they the whole local network was endangered. The root cause of this problem is purely the human factor; it only needed a prior warning to give the schools time to prepare for the elimination of the protective firewall. Only establishing a safety system is insufficient; it should be reviewed in every time there is a modification in order not to decrease the level of defence. Even if the modification of the firewall rules was necessary, an examination should have been made of the effects on the systems of the schools and the Sulinet.

The last case is a similar problem. By forcing schools to use a software environment that is no longer supported, unauthorised persons were given the chance to exploit the vulnerabilities of the outdated system and gain access to the computer and the managed data, at the same time compromising integrity and availability.

[10] Social engineering is a type of attack that takes advantage of human credulity and co-operation. Although it is used in all aspects of life, social engineering is aimed explicitly at the acquisition of information and in particular focuses on the data stored on IT devices. [21]

Integrity

In each of these systems data loss or alteration occurred. This fact in itself means that the systems are unreliable from the point of view of information security. So they make work more difficult, they cause additional costs (the administrator could do more useful work in the meantime) and there is a risk of the possibility of damage to important data (for example data used for graduation certificates). It is noteworthy that data alterations after the deadline may result in the recipient seeing other information than that approved by the sender (for example in cases 4 and 11).

In cases (e.g. point 5) where the data loss is caused by duplication of work, the program must first be modified in order to be able to provide multi-user operation. If this is not possible for some reason, then before the software maintenance is begun the service user must be notified in good time and should be prevented from logging into the system before the end of the operation. Failure to do this poses the risk that similar incidents may also occur in the future, the person recording data will not notice the loss of data, which may cause errors that are difficult to detect.

The users should have been informed in case 9 too, before the late migration was done centrally. Not only would the schools have been spared making unnecessary data records but the solution that was implemented would also have increased the risk of data loss.

Primarily another area of concern, software ergonomics, was affected by the error described in section 10, that the user interface and the functions of the buttons are not clear. It will be seen from this that the human factor is also present in software developers, but it also increases the likelihood of human failures on the user's side because as people are accustomed to simple interfaces it is easy to cause damage to the recorded data. This damage, however, poses a risk for information security.

Availability

In public education information systems high availability is particularly important due to the high number of users and tight deadlines. Nevertheless, the systems of the KIR and the KELLO collapsed during their first live operation. This problem had also occurred with other modules of KIR previously but nothing was learned from this experience the IT background is not planned sufficiently. Limiting the number of users is not an option, if overloading occurs, an alternative solution would be to prevent the near-paralysis of the system. One possible way to do this would be to apply client programs that do not generate continuous data traffic would be possible if data could be imported into the on-line system from .csv and .xls files.

Lack of distributed data traffic and a bandwidth which is insufficient compared to the number of users lead to slow operation speed (as described in point 7).

In case 9 it was impossible to migrate from the KIR system the recorded data of the student's grade, and initially the addresses too, so data previously recorded by the school were not available. There is no way we can know if the importance of these data was forgotten in the planning stages or the developers had trouble drawing the appropriate software modules, but in any event this problem indicates human error.

Overloading of the computer system was also associated with the unavailability of support, so when the problem occurred, it caused a failure of the whole system, and the users did not know the reason for this and how long troubleshooting would take.

In the last case described, the KIR3 became inaccessible, moreover – as I pointed out in the confidentiality section, because of the non-supported software environment, the system is exposed to attacks that endanger each component of the CIA triad.

The Privacy Act sets out the following: the controller, as well as the data processor within their respective scope of activities, is obliged to ensure data security, institute technical and organisational measures and develop procedural rules required to enforce the present Act, as

well as other data protection and confidentiality rules. [5] This means that developers and operators are not only guilty of serious professional mistakes, but have not fulfilled their obligations as laid down in the legislation.

The controller and data processor must take account of the current level of development of the relevant technology when determining and applying measures taken to protect the data. The solution that ensures a higher level protection of the personal data must be selected from among several possible control solutions, unless this proves far too difficult for the controller. [5] For a fraction of the money received in state financial support, which I mentioned in my introduction, modern, state-of-the-art technology allows a system to be developed that complies with current standards and legislation.

The size the system also highlights the seriousness of the cases presented. For example, the Office of Education announces the following information to the KIR one of the largest national database systems:

- it contains 3.6 million citizens' personal information to which other personal information is linked through various records,
- the services used by nearly 5 600 public educational institutions, with more than 2 500 supporters of institutions, make use of thousands of organizations, the number of registered users being more than 30 thousand,
- more than 200 000 people per month visit the educational administration's dedicated portal. [22]

The Sulinet network is operated by the NIIF contains about 5 070 endpoints. [23] If the local system became vulnerable in only a fraction of the institutions concerned, then case 12 allowed a botnet[11] of such a size to be set up that could have led to serious attacks.

CONCLUSION

Based on experience, in many cases software written for Hungarian public education institutions is not preceded by careful planning. Schools can put in practice the system only shortly before the deadline prescribed to them, because the developers finish the program late. The result of all this is that all those responsible for providing information try to connect to a server with relatively small data capabilities, in a relatively tight time frame, which cannot handle the requests. In practice, attempts are made to remedy the initial crash only in an ad-hoc manner, and instead of by increasing the server capacity and bandwidth, the number of concurrent users that can be processed is limited, so the majority must wait and cannot access the data necessary for their work.

The overload of the computer system is often associated with the unavailability of the help desk. During the critical period they cannot be reached or they cannot provide any significant help. Business continuity, which is a basic requirement in the business sector, is not guaranteed, if there is a problem then disruption occurs on every channel.

An especially large problem, which is incomprehensible from the point of view of IT, is that the same data have to be recorded by a number of separate systems, sometimes with small formal differences (e.g. the surname and last name have to be recorded separately in one system and one only needs to enter the full name in the other one). Data migration between the systems concerned is allowed by law but in practice several programs do not support the exchange of data between them. In many cases, even .xls or .csv file import is not possible. However, it makes no sense to store databases in multiple locations because it can lead to a situation where data updates are not carried out in every system if data are changed (the

[11] Computers that have been infected without the user's knowledge and which can be remotely controlled without the user realising anything is amiss: referred to in computer slang as a "zombie" or "bot". A network that is generated using several computers is known as a botnet. [21]

recording person's human error!). It is also possible that different programs are managed by different individuals, and the operators do not notify each other of data changes.

Although the Privacy Act requires that a report should be compiled on errors occurring during the course of automated processing [5], but if the rest of the law has not been complied with, then probably an error report will not have been made. But this document could help a lot in the future to avoid problems similar to those described.

As already mentioned, the public education system plays a part in the critical infrastructure, and for this reason, emphasis should be placed on its information security, especially if we consider the huge amount and importance of the data it contains and the risks affecting the inter- and intradependence of the other elements.

The case studies presented have highlighted the importance of the human factor, because negligence and incompetence pose at least as much of a risk as a deliberate intent to cause damage.

References

[1] Index: Százmilliókkal tartozik a tankönyvterjesztési monopolcég. http://index.hu/belfold/2013/03/27/szazmilliokkal_tartozik_a_tankonyvterjesztesi_monopolceg/ (03.28.2013)

[2] 1120/2013. (III. 8.) Korm. határozat a rendkívüli kormányzati intézkedésekre szolgáló tartalékból a Könyvtárellátó Kiemelkedően Közhasznú Nonprofit Kft. közérdekű feladatai feltételeinek biztosítása céljából történő előirányzat-átcsoportosításról

[3] Rainer Baumann, Stéphane Cavin, Stefan Schmid: Voice Over IP – Security and SPIT. University of Berne, 2006.

[4] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[5] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[6] Dr. Haig Zsolt: Az információbiztonság komplex értelmezése. In: Hadmérnök, Robothadviselés 6. különszám, 2006. http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html (04.24.2013)

[7] Dr. Bende-Szabó Gábor, Dr. Kökényesi József (szerk.): Közigazgatási szakvizsga. Általános közigazgatási ismeretek 2. rész. Magyar Közigazgatási Intézet, Budapest, 2002.

[8] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori (PhD) értekezés. ZMNE, Budapest, 2007.

[9] http://lista.sulinet.hu/pipermail/techinfo/2012-November/076246.html (04.23.2013)

[10] http://lista.sulinet.hu/pipermail/techinfo/2012-November/075830.html (04.23.2013)

[11] http://lista.sulinet.hu/pipermail/techinfo/2012-November/076232.html (04.23.2013)

[12] http://lista.sulinet.hu/pipermail/techinfo/2012-November/076226.html (04.23.2013)

[13] 20/2012. (VIII. 31.) EMMI rendelet a nevelési-oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról

[14] http://lista.sulinet.hu/pipermail/techinfo/2013-March/079131.html (03.28.2013)

[15] http://lista.sulinet.hu/pipermail/techinfo/2013-March/079163.html (04.23.2013)

[16] http://lista.sulinet.hu/pipermail/techinfo/2013-April/079556.html (04.23.2013)

[17] http://lista.sulinet.hu/pipermail/techinfo/2013-April/079709.html (04.23.2013)

[18] 5/2011. (II. 3.) Korm. rendelet a Nemzeti Információs Infrastruktúra Fejlesztési Programról

[19] DMZ (Computing). Wikipedia the Free Encyclopedia http://en.wikipedia.org/wiki/DMZ_(computing) (04.23.2013)

[20] http://lista.sulinet.hu/pipermail/techinfo/2013-April/079717.html (04.23.2013)

[21] Dr. Kovács László (szerk): Számítógép-hálózati hadviselés: veszélyek és a védelem lehetséges megoldásai Magyarországon. Tanulmány, ZMNE, Budapest, 2010.

[22] Az adatszolgáltatás jelene a köznevelésben http://www.oktatas.hu/kozneveles/projektek/tamop311_2szakasz/projekthirek/adatszolgaltatas_jelene_a_koznevelesben (04.24.2013)

[23] 2013. március 31-től változás a helyszíni munkavégzés szolgáltatásában http://sulinet.niif.hu/node/9 (04.24.2013)

THIS ARTICLE IS SUPPORTED BY TENDER TÁMOP 4.2.2./B-10/1 (RISKS AND ANSWERS IN THE FIELD OF TALENT MAINTENANCE: "KOVÁSZ")