INFO-1046
Primljeno / Received: 2008-05-06

UDK: 007:681.3:37
Professional Paper / Stručni rad

INFORMATION SYSTEMS IN SCHOOLS AND DATA PROTECTION

INFORMACIJSKI SISTEMI U ŠKOLAMA I ZAŠTITA PODATAKA

Lina Dečman, Olga Dečman Dobrnjić**, Metod Černetić****

Iskraemeco, Kranj, Slovenia*, National Education Institute of Republic of Slovenia**, Faculty of Organizational Sciences, Kranj, University of Maribor, Slovenia ***

Iskraemeco, Kranj, Slovenija*, Zavod za školstvo Republike Slovenije**, Fakultet za organizacijske znanosti, Kranj, Sveučilište u Mariboru, Slovenija***

Abstract

The steady growth of computer and communication sciences makes schools as organizations more and more dependent on information systems. Schools are organizations and thus they too must comply with the legal requirements concerning the data security. This paper deals with the topic of data protection in the schools information system. While the schools apply the information systems, the information is easier accessible to a growing number of people. Parallel to it, the opportunities of data abuse e.g. computer fraud, espionage, malevolent code etc. are more frequent. Under data protection we understand the data as well as information protection as they are almost always not just pure information but have certain value. The information protection is based above all on three basic principles: integrity, confidentiality and availability. It is suggested that the organization declares its adopted policy and guidelines for management of electronic operations and at the same time assures that they are properly implemented.

Sažetak

Nezaustavljiv razvoj u polju računalstva i komunikacije utječe i na funkcioniranje škole koja postaje svakodnevno ovisna o različitim informacijskim sustavima. Budući da su brojni važni službeni podaci dostupni sve većem broju ljudi, a time i mogućoj zlouporabi – računalne prevare, zlouporabe koda i dr., od škole kao javne organizacije očekuje se da prati zakonske odredbe o zaštiti podataka. U radu se raspravlja o sustavu informacijskog poslovanja škola kao i o sustavu zaštite službenih podataka koji moraju slijediti najmanje tri osnovna načela pouzdanost i dostupnost. Predlažemo da škola kao organizacija kreira poslovnu politiku koja respektira temeljne smjernice upravljanja elektroničkim poslovanjem ali i da se osiguraju uvjeti potrebni da postavljena pravila i ciljevi budu i realno izvedivi.

1 Data and Information

Data and information are two words denoting two different meanings. Data mean presentation of information in a formal way suitable for communication, interpretation and processing by man or machine. Data can be presented by means of symbols or analogue quantities which are ascribed or may be ascribed a meaning. Information is knowledge about objects e.g. facts, events, things, processes or ideas including concepts that have within a context a certain meaning (ISO).

For protection of information and data we may say that both data and information are protected. Contemplated from the "physical" point of view the data are actually protected but they may always represent information for someone. In most cases we may say that we protect information behind which there are naked data.

2 Information and Data Security

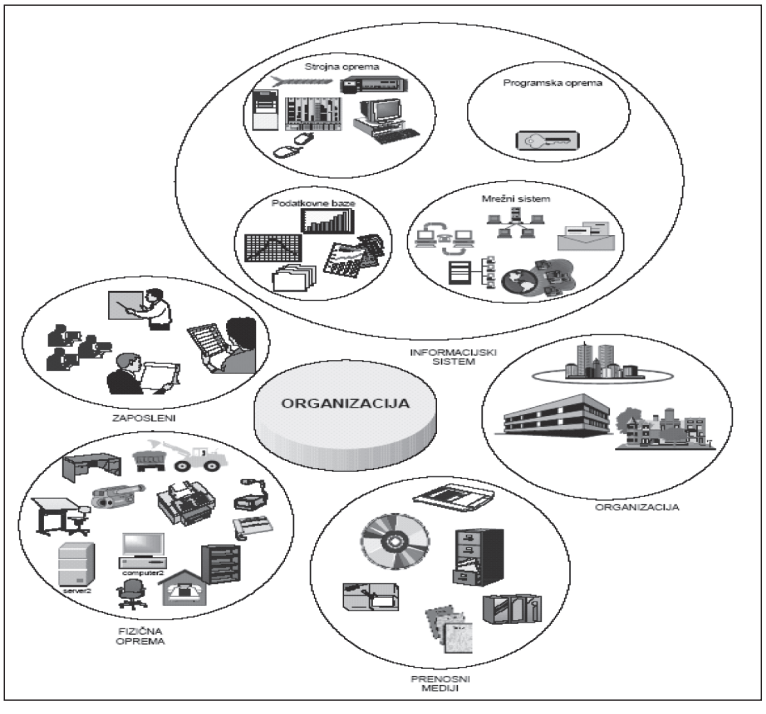
As mentioned above when saying protection of data and information we mean protection of them both. There are assets with certain value which need to be adequately protected. Protection of information assets eliminates various risks to assure safe and continuous operation and restricts the damages to the lowest possible level. Information may turn up in different forms: written on paper, saved on electronic media, sent by mail, or they may just be conveyed during the conversation. Independent from the form and media through which they are conveyed the need to be properly protected.

The concept of security covers the following basic principles:

- **integrity:** protecting the accuracy and entirety of information and of computer software

- **confidentiality:** restricting the access to information to the authorised people only
- **availability:** assuring that the information and computer services are available to the authorised staff when they need it.

The task of information security is to protect all significant information and hardware important for smooth operation of school as organization. The information and the assets to be protected shall be determined from the list. The range of the sources and assets eligible for protection are shown in the Figure 1. It s recommended that security risk policy is designed for schools (organizations).



Legend:

strojna oprema	– hardware
programska oprema	- software
podatkovna baza	- data base
mrežni system	- network
zaposleni	- staff
informacisjki sistem	- information system
fizična oprema	- furnishings, equipment
prenosni mediji	- transmission media

Figure 1: The range sources and assets eligible for protection (Source: Janežič, 2004)

While designing the security policy and introducing the protection of information, we must first analyse the risks. Based o such analysis the measures to reduce risks and to control the use of information can be prepared. The measures (the way of work, procedures, organization structures and software functions) will be part of the security policy which determines the detailed procedures for each individual field or problem. All employees should be familiar with the policy. The protection of information is a never ending process. Besides we should never be satisfied with the acquired standard of protection as the environment is highly unpredictable in this field. New software, way and systems of invading the computer network emerge daily. In short, the circumstances in which an information system operates change continuously. We must be aware of the fact that perfect security is impossible and that security depends largely on the means available in the organization for this purpose. The protection of information should originate from the objectives of the organization and shall be included in the development strategy.

3 Significance of Data and Information Protection

The information and the supporting processes, systems and networks are important business assets. The integrity, confidentiality and availability of information often plays important role in sustaining of competitiveness of the organization in the market, in creating capital flows, in demand and supply, in profitability, in compliance with law and in preserving and presentation of the overall image of schools as organizations /**1**/. The unstoppable growth of computer sciences and informational communications makes schools more dependent on information systems. While the information are easier to be accessed by more people, the possibility of abuse grows parallelly

(computer frauds, espionage, sabotage, malevolent code). Also the breakdowns in system and software errors may jeopardize the operation and even existence of schools as organizations. Besides this the most frequent reason for introduction of system of information security has recently been the requirements of auditors, governmental agents and of the central banks. It is to be expected that the same will be required by the business partners. An efficiently organized information protection reduces the risks to an acceptable level.

4 Requirements for Information Protection

4. 1 Requirements of the organization for continuous operations

With the view of protecting the significant business operation, every organization should introduce the business continuity management (BMC). It offers a protection against the impact of major errors or catastrophes and thereby reduces the work interruptions to an acceptable level. /**2**/ Business continuity management shall be an integral part of the school management. It should be planned and adopted by the management and thereby it is awarded an additional business value. The system of planning and introducing the business continuity is closely linked to all business processes in the organization which in turn are the result of risk management in a well regulated organization as shown in Figure 2. All too often the planning of these activities is left to the technical staff from the field of information technology. The security awareness of the executive officers is very important as they select the strategy of informational security in an organization. /**3**/ Even the fact that we may be insured does not suffice as the insurance will only take care of the financial side and not to prevent the accidents or for revamping or resuming the interrupted process. /**4**/The school as an organization should publish the adopted policy and guidelines for management of business continuity management and will at the same time make sure that it is properly implemented.

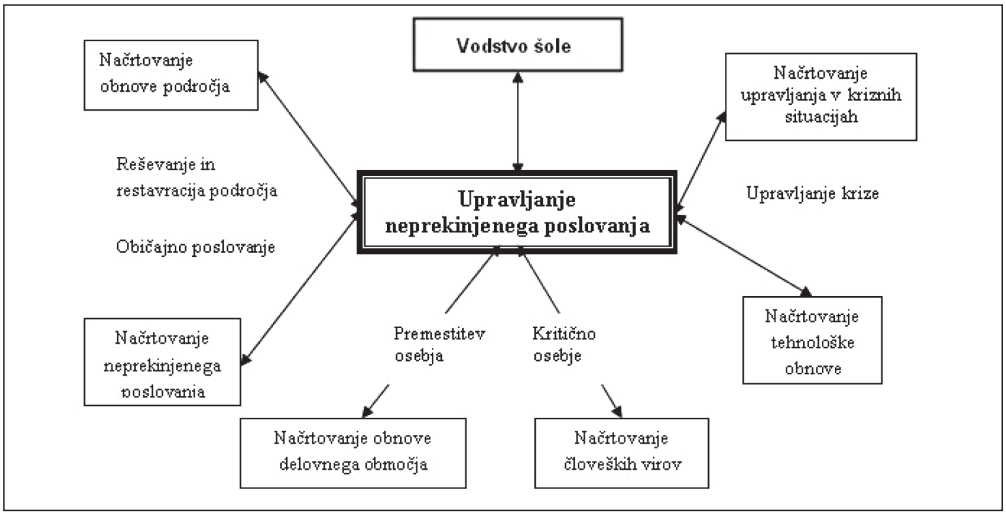


Figure 2: Relations in business continuity management (Source: Smith, 2001)

Legend:

upravljanje neprekinjenega poslovanja	business continuity management
načrtovanje obnove področja	planning of revamping of the field
vodstvo šole	school administration – management
reševanje in restavracija področja	solving and restoring of the field
običajno poslovanje	ordinary business operating
načrtovanje neprekinjenega poslovanja	planning of business continuity
načrtovanje obnove delovnega območja	planning of renewal of field of work
premestitev osebja	transfer of staff
kritično osebje	critical staff
načrtovanje človeških virov	planning of human resources
načrtovanje tehnološke obnove	planning of technological refurbishment
upravljanje krize	crisis management
načrtovanje upravljanja v kriznih situacijah	planning of crisis management

4.2 Legal requirements

The schools like the majority of public institutions decide to protect the information, above all due to business but also legal requirements. Information security is closely associated to information law. It is at this point where the questions of accessibility to the software, hardware, system equipment, protection od personal data, encryption, electronic trading, and signatures, copyrights … /**5**/ The laws in Slovenia which regulate the information protection are:

- Law on Electronic Operations and Electronic Signature
- Law on Electronic Communications
- Law on protection of Personal Data
- Law on Copyrights and Similar Rights
- Law on Conditional Access to the Protected Electronic Services
- Law on Protection of Consumers
- Law on Classified (Confidential) Information

The insurance companies abroad offer insurance of the risks – perils of electronic operations. The demand was first detected in banks and companies which operate by means of internet /**6**/. These insurances are most common in America the leading area in internet trading. However the relevant companies need to know that the insurance will not be concluded for the value of data on internal servers if no proof is submitted that updated back up copies have been saved.

5 Conclusion – The environment requires the schools to assure the data security

In time the society will expect from schools as organizations a high degree of data security as they have contacts with various organizations whose data security depends on the security of the data of the relevant school. There is namely no use to have the best security of data in one's own organization but exchange them with the partner who is inadequate in terms of security. Any connecting in a network comprising schools with poor protection will jeopardize our own data security. We may be attacked exactly through such school as the weak link in the network. In our opinion, the business environment will thus force the schools to introduce the security policy of protecting their information.

References

/1/ British standard BS ISO/IEC 17799:2000: Slovenski prevod standarda, Information technology. Code of practice for information security management, Palsit. Nova Gorica, 2002.

/2/ Ibidem

/3/ Kajić Milan et al.: Mehanizmi varovanja podatkov pri elektronskem poslovanju Statističnega urada RS, Elektronsko poslovanje in statistika, Statistični dnevi 99, Radenci, 1999.

/4/ British standard PAS 56: Guide to Business Continuity Management, British Standards Institutions. London, 2003.

/5/ Berčič Boštjan: Skladnost varnostnih politik z zakonodajo, Bilten konference INFOSEC 2003, Inštitut za informacijsko varnost, Nova Gorica, 2003.

/6/ Svetič Barbara: Vam kradejo informacije?, Gospodarski vestnik, Ljubljana, 2002.

Literature

1. Berčič Boštjan (et al): Ukrepi v primeru informacijskih nesreč. Nova Gorica: Inštitut za informacijsko varnost, 2003a.
2. Černetič Metod: Management ekonomike izobraževanja. Moderne organizacija. Kranj. 2006.
3. Dečman Lina: Computer communications and protection, Novi komunkacijski izazovi u obrazovanju, Međunarodni znanstveni i stručni skup, Zbornik radova, Pula, 2006, Medulin, 10. i 11. studenog 2005.
4. Egan Mark, Mather Tim: Varovanje informacij, grožnje, izzivi in rešitve, Ljubljana.
5. Hočevar Peter: Varnosti z delnimi rešitvami ne dosežemo. Sistemi – Priloga revije Moj Mikro, Ljubljana, št. 7/8, letnik 21, julij, avgust 2005.
6. Smith, D.J.: A recipe for chaos, Risk management bulletin, 6 (1), 9-14, 2001
7. Janežič Damjan (et al): Grožnje elektronskega poslovanja – upravljanje z informacijskimi tveganji. Nova Gorica, IZIV, 2004.
8. Vavtar Bojan, Dečman Lina, Černetič Metod: Pravni in tehnični vidiki zaščite računalniških programov, 25. mednarodna konferenca o Razvoju organizacijskih znanosti Management sprememb, Portorož, 2006.