SECURITATEA DATELOR

DATA SECURITY

Ileana ŞTEFAN[1]

[1]Universitatea "Petru Maior" din Tîrgu–Mureş

Str. Nicolae Iorga, nr.1, Tîrgu – Mureş, MUREŞ, 540088, România

e-mail: stefan.ileana@yahoo.com

Abstract: *Formarea specialiştilor în domeniul securităţii informaţiilor şi a administratorilor de securitate pentru sistemele informatice reprezintă o prioritate importantă, cerută atât de mediile guvernamentale şi de administraţia centrală şi locală, cât şi de mediul privat – companii, bănci. Acestea sunt responsabile în implementarea unor servicii şi sisteme informatice, dar şi beneficiare ale acestora, cu aplicabilitate în domenii ca: e-guvernare, e-administraţie, e-banking, e-commerce, e-payment, în care rolul comunicaţiilor şi tehnicii de calcul şi al Internet-ului, este foarte important.*

Cuvinte cheie: securitatea informatiilor; controlul accesului la informatii, date cu caracter personal

Clasificare JEL: K OO, K23

Abstract: *Training specialists in the field of data security and security administrators for the information systems represents a significant priority demanded by both governmental environments and the central and local administrations, as well as by the private sector – companies, banks. They are responsible for implementing information services and systems, but they are also their beneficiaries, with applicability in fields such as: e-government, e-administration, e-banking, e-commerce, e-payment, where the role of communication and computer technology and the Internet is extremely important.*

Keywords: information security, control access to information, personal data

JEL Classification: K OO, K23

1 INTRODUCERE

Din punct de vedere a problemelor de protecţie a datelor, utilizatorii se tem mai mult, în comparaţie cu anul trecut, de ceea ce se poate întâmpla în timpul desfăşurării unor activităţi online, cum ar fi folosirea serviciilor bancare sau de cumpărături, a unor căutări pe Internet dar şi în timpul folosirii adresei personale de e-mail.

Politica de securitate a informaţiei[1], are scopul de asigure a:

- integrităţii care constă în păstrarea acurateţei şi completitudinii informaţiilor, precum şi a metodelor de procesare,
- confidenţialităţii şi anume asigurarea accesibilităţii informaţiei numai celor autorizaţi să aibă acces;
- disponibilităţii informaţiei care asigurară faptul că utilizatorii autorizaţi au acces la informaţie, precum şi la resursele asociate, atunci când este necesar, în scopul furnizării de încredere în relaţiile cu mediul intern si extern organizaţional.

Fiecare utilizator autorizat al sistemului informatic este răspunzător pentru aplicarea întocmai în activitatea sa a regulamentelor şi procedurilor de securitate interne în vigoare, elaborate şi aprobate, conform cu documentele cadru internaţionale, legislaţia naţională specifică şi reglementările interne de funcţionare. De asemenea, orice utilizator autorizat al sistemului are obligaţia

1 INTRODUCTION

From the standpoint of data protection problems, compared to last year, users fear more what could happen during online activities, such as using banking or shopping services, Internet searches, but also while using one's personal e-mail address.

The information security policy[1], is intended to ensure:

- integrity, that is to preserve the accuracy and completeness of both information, and processing methods,
- confidentiality, that is providing accessibility to information only to those authorized to have access;
- the availability of information which provides the fact that authorized users have access to information, as well as to related sources, when necessary, in order to provide trust in the relations with the internal and external organizational environment.

Each authorized user of the information system is responsible for the effective enforcement, in his activity, of the internal security regulations and procedures in force, elaborated and approved in accordance with international framework documents, the specific national legislation and the internal operational regulations. Also, each authorized system user is obliged to report any security incident.

raportării oricărui incident de securitate.

2. LEGISLAŢIA NAŢIONALĂ

In conformitate cu dispozitiile Legii nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date si ale Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private, orice furnizor de astfel de servicii care utilizează aceste date are obligatia de a administra in conditii de siguranta si numai pentru scopurile specificat,e datele personale pe care utilizatorul le furnizează.

Deasemenea, furnizorul de servicii are obliga sa pastreze confidentialitatea datelor personale furnizate asa cum prevad dispozitiile Legii 677/2001 cu modificarile ulterioare privind protectia datelor personale.

Un furnizor poate dezvalui datele cu caracter personal catre terti daca acest lucru este cerut de lege sau in cazurile de buna-credinta in care aceste actiuni sunt necesare pentru conformarea la dispozitiile legale. Datele cu caracter personal vor putea fi dezvaluite fara consimtamantul dumneavoastra in caz de litigi/dispute privind fraudele, institutiilor abilitate.

Protecţia datelor cu caracter personal reprezintă un domeniu important pentru spaţiul legislativ din România. Conţinutul său priveşte, într-o formă

2. NATIONAL LEGISLATION

In accordance with the provisions of Law no. 677/2001 for the protection of persons regarding personal data processing and the free movement of such data and of Law no. 506/2004 regarding personal data processing and the protection of private life, any supplier of such services using these data is forced to safely administer, and only for specified purposed, the personal data the user is providing.

Also, the services supplier is forced to maintain the confidentiality of the personal data provided, as required by the provisions of Law 677/2001 with the subsequent modifications regarding personal data protection.

A supplier may reveal personal data to third parties if this is required by law or in cases of good-faith when these actions are necessary for complying with legal dispositions. Personal data may be revealed to competent institutions without your consent in cases of litigation/disputes regarding frauds.

Personal data protection represents an important field for the Romanian legislative environment. Its content focuses, in a generic form, upon the natural person’s right to have those characteristics leading to his identification protected and the state’s correlative obligation to adopt adequate measures to ensure an efficient protection.

generică, dreptul persoanei fizice de a-i fi apărate acele caracteristici care conduc la identificarea sa şi obligaţia corelativă a statului de a adopta măsuri adecvate pentru a asigura o protecţie eficientă.

În acest scop, a luat fiinţă în România, o autoritate centrală abilitată cu astfel de atribuţii de control, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal[2]. Înfiinţată, prin Legea nr. 102/2005, Autoritatea îşi exercită competenţa stabilită în principal de Legea nr. 677/2001, în condiţii de independenţă faţă de orice autoritate publică sau entitate de drept privat.

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal are ca obiectiv apărarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţă intimă, familială şi privată în legătură cu prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Acest drept are un conţinut complex, de mare importanţă pentru libertatea şi personalitatea cetăţeanului, iar în ţara noastră este garantat prin Constituţie (art. 26).

Prin Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date a fost transpus acquis-ul reprezentat de Directiva 95/46/EC, care reglementează cadrul juridic general al protecţiei datelor personale la nivelul Uniunii Europene.

To this purpose, a competent central authority emerged in Romania with such control attributions, the National Supervisory Authority for Personal Data Processing[2]. Founded by Law no. 102/2005, the Authority exercises its competence set mainly by Law no. 677/2001 independently from any public authority or private entity.

The National Supervisory Authority for Personal Data Processing aims at protecting the natural persons' fundamental rights and liberties, mainly the right to an intimate, family and private life regarding personal data processing and the free movement of such data. This right has a complex content, of great importance for the citizen's liberty and personality, and in our country it is guaranteed through the Constitution (art. 26).

Law no. 677/2001 for the protection of persons regarding personal data processing and the free circulation of such data implemented the acquis represented by Directive 95/46/EC, which governs the general legal framework of personal data protection at the level of the European Union.

The attributions of the National Supervisory Authority for Personal Data Processing[3] are specific to any control institution, being able to investigate personal data processing which fall under the incidence of Law no. 677/2001 and apply sanctions in case it finds violations of the legal provisions by the personal data operators, following ex officio complaints or based on

Atribuţiile Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal[3] sunt specifice oricărei instituţii de control, putând investiga prelucrările de date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 şi aplica sancţiuni, în cazul în care constată încălcarea dispoziţiilor legale de către operatorii de date cu caracter personal, în urma sesizărilor din oficiu sau pe baza unor plângeri depuse de persoanele lezate în drepturile lor.

Deoarece, aplicarea corectă a unui act normativ nou presupune cunoaşterea corespunzătoare a prevederilor sale, se consideră că prin intermediul informaţiilor furnizate prin intermediul site-ului atât operatorii de date cu caracter personal, cât şi persoanele fizice ale căror date personale sunt prelucrate, au ocazia de a aprofunda şi înţelege care sunt obligaţiile şi, respectiv, drepturile reglementate

In conformitate cu dispozitiile Legii nr. 677/2001, persoanele inregistrate, in calitatate de persoane vizate, au urmatoarele drepturi[4]:

- dreptul la informare (art.12)
- dreptul de acces la date cu caracter personal (art.13);
- dreptul de interventie asupra datelor cu caracter personal (art.14);
- dreptul de opozitie (art.15);
- dreptul de a nu fi supus unei decizii individuale (art.17);
- dreptul de a se adresa justitiei (art.18).

complaints filed by persons aggrieved in their rights.

Because the correct application of a new normative act requires the adequate knowledge of its provisions, it is considered that through the information provided by the website, both personal data operators as well as natural persons whose personal data are being processed, have the opportunity of studying thoroughly and understanding which are the regulated obligations and rights.

In accordance with the provisions of Law no. 677/2001, registered persons as targeted persons, have the following rights[4]:

- The right to information (art.12)
- The right to access personal data (art.13);
- The right to intervene over personal data (art.14);
- The right to oppose (art.15);
- The right not to be subjected to an individual decision (art.17);
- The right to address the justice (art.18).

3. INFORMATION SYSTEM SECURITY

In order to ensure the security of an information system, one must bear in mind that they have two components – that is the hardware and software component. An information system contains, besides data, a series of services and several access types. For this reason, security is

3. SECURITATEA SISTEMULUI INFORMATIC

Pentru a se asigura securitatea unui sistem informatic trebuie sa avem in vedere ca acestea contin doua componente si anume componenta hardware si componenta software. Un sistem informatic contine pe langa date si o serie de servicii si mai multe tipuri de acces. Din acest motiv securitatea este cu atat mai sigura cu cat ea este pusa pentru fiecare componenta a sistemului informatic in parte decat daca ea are ca obiect intregul sistem ca un tot unitar. In acest mod datele protejate vor fi mai greu de accesat avand in vedere ca trebuie sa se sparga mai multe nivele de securitate.

Exista doua tipuri de securitate si anume :

a. Securitate fizica ;
b. Securitate logica.

Securitatea fizica a unui sistem informatic consta in asigurarea securitatii componentelor hardware a unui sistem informatic si anume protejarea impotriva furtului sau vandalizarii acestora prin plasarea lor intr-o incapere sigura. De asemenea, trebuie asigurata paza si accesul persoanelor straine.

O alta securitate fizica care trebuie avuta in vedere este securitatea care are ca obiect copiile datele si programelor salvate (backup). Aceste copii trebuie

safer when it is applied for every information system component rather than considering the entire system as a whole. This way, the protected data shall be harder to access provided that several levels of security have to be breached.

There are several types of security, namely:

a. Physical security;
b. Logical security.

An information system physical security consists in ensuring the security of the hardware components of an information system, namely protection against theft or damage by placing them in a safe room. Also, security and the access of foreign persons must be ensured.

Another physical security which must be bore in mind is the security which focuses upon the copies of the saved data and programs (backup). These copies must be protected against theft and damage.

Logical security is necessary besides the physical security. In order to have the desired effect, they must exist simultaneously.

Given that an information system contains, besides data, a series of services and several access types, we shall have the following from the standpoint of logical security:

- Services security;
- System access security.

protejate impotriva furtului si vandalizarii lor.

Pe langa securitatea fizica este necesara si asigurarea securitatii logice. Pentru a avea efectul scontat acestea trebuie sa existe concomitent.

Avand in vedere ca un sistem informatic contine pe langa date si o serie de servicii si mai multe tipuri de acces din punct de vedere al securitatii logice vom avea :

- Securitatea serviciilor ;
- Securitatea accesului la sistem.

Din punct de vedere a unui utilizator obisnuit securitate datelor trebuie sa asigure:

- Protejarea datelor impotriva coruperii;
- Protejarea datelor impotriva furtului;
- Protejarea sistemului impotriva atacurilor.

Fiecare utilizator autorizat al sistemului informatic este răspunzător pentru aplicarea întocmai în activitatea sa a regulamentelor şi procedurilor de securitate interne în vigoare, elaborate şi aprobate, conform cu documentele cadru internaţionale, legislaţia naţională specifică şi reglementările interne de funcţionare. De asemenea, orice utilizator autorizat al sistemului are obligaţia raportării oricărui incident de securitate.

Într-o companie, managerul general are responsabilitatea securităţii informaţiilor. Angajaţilor au obligaţia de a respecta regulile

From the point of view of a regular user, data security must ensure:

- Data protection against corruption;
- Data protection against theft;
- System protection against attacks.

Each authorised user of the information system is responsible for the effective implementation in his activity of the internal security regulations and procedures in force, elaborated and approved, according to the international framework documents, the specific national legislation and the internal operational regulations. Also, each authorised system user is obliged to report any security incident.

Within a company, the general manager is responsible for the information security. Employees are obliged to comply with the rules imposed by the management through specific policies and procedures.

Given the specific activity of a company and its objectives, the company leader will set a policy for the security of information. Depending on them he must decide the means in which information shall be classified. Information may be classified in:

- Non-sensitive information;
- Confidential information;
- Strictly confidential information.

Given the classification of information, the access level of the employees to each information

impuse de management prin anumite politici şi proceduri.

În funcţie de specificul de activitate al firmei şi de obiectivele acesteia conducătorului firmei îi revine sarcina de a stabili o politică de securizare a informaţiilor. Ca urmare, trebuie să decidă modalitatea în care se vor clasifica informaţiile. Informaţiile pot fi clasificate în:

- informaţii neconfidenţiale;
- informaţii confidenţiale;
- informaţii strict confidenţiale.

În funcţie de clasificarea informaţiilor, se stabileşte nivelul de acces al angajaţilor la fiecare categorie de informaţii. Fiecare angajat trebuie să aibă acces doar la acele informaţii care îi sunt stric necesare pentru îndeplinirea sarcinilor. Contractele de muncă trebuie să conţină clauze de confidenţialitate foarte bine definite pentru fiecare post.

Nivelul de acces al utilizatorilor la informaţii trebuiesc stabilite în funcţie de modalităţile de control al accesului la informaţii. Cotrolul nu înseamnă numai accesul la resursele informatice ale companiei, ci trebuie controlat şi accesul fizic, deoarece nu toate informaţiile sunt pe suport electronic. Nu mai are importanţă dacă calculatorul este parolat dacă biroul este plin de hârtii care conţin informaţii sensibile referitoare la contractele în derulare, de exemplu. Ca urmare, este necesara o procedură de stabilire a controlul accesului în reţea şi a controlului accesului fizic.

category is set. Each employee must have access only to the strictly necessary information for carrying out his tasks. Labour contracts must contain very well defined confidentiality clauses for each position.

The access level of the information users must be set according to the methods of controlling the access to information. Control does not means only access to the company's information resources, but also physical access must be controlled, because not all information is stored electronically. It does matter if the computer has a password if the desk is filled with documents which contain sensitive information about on-going contracts, for instance. Therefore, it is necessary to establish a procedure for network access control, as well as for controlling physical access.

In order to ensure information protection, one must take into account:

1) To train personnel, once every six months, until rules are strictly enforced.

2) To monitor the implementation of policies and procedures. Companies should conduct an internal audit once a year.

3) Continuous improvement. Following the conclusions of the internal audit or verifications, the organisation must take measures to adjust policies and procedures.

În vederea asigurării protecţiei informaţiei trebuie să se ţină cont de următoarele:

1) Instruirea personalului trebuie să se facă periodic, o dată la şase luni, până când regulile vor fi respectate cu stricteţe.

2) Verificarea aplicării politicilor şi procedurilor. Firmele trebuie să asigure desfăşurarea unui audit intern o dată pe an.

3) Îmbunătăţirea continuă. În urma concluziilor auditului sau a verificărilor, organizaţia trebuie să ia măsuri de ajustare a politicilor şi procedurilor.

4.CONCLUZII

Utilizatorii se tem mai mult, când vine vorba de probleme de securitate, mai ales în ceea ce priveşte protecţia lor în timpul desfăşurării unor activităţi online simple, precum folosirea serviciilor bancare sau cumpărături, a unor simple căutări pe Internet dar şi în timpul folosirii adresei personale de e-mail.

4.CONCLUSIONS

Users fear more when it comes to security issues, especially when it regards their protection while undergoing simple online activities, such as using banking or shopping services, simple Internet searches, but also while using one's personal e-mail address.

BIBLIOGRAFIE/ BIBLIOGRAPHY

[1] http://www.datasecurity.ro

[2] http://www.politiaromana.ro/protectia_datelor_cu_caracter_personal.html

[3] Decizia ANSPDCP nr. 52/2012 - prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video

[4] Legea nr. 677/2001

[5] http://www.agora.ro/conferinte