CONSIDERATIONS REGARDING THE PROTECTION OF CLASSIFIED INFORMATION IN ELECTRONIC FORMAT

Teodor ŞTEFĂNESCU*

Abstract

A common understanding of activity regarding the protection of classified information based on standards and policies is critical. In this respect the classified information protection in electronic format (INFOSEC) plays a vital role. In general terms, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms as information security, computer security and information assurance are frequently incorrectly used. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences cover primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. The paper describes the activity regarding the protection of classified information in electronic format (INFOSEC). The covered domains are as follows: Legal framework; Security classification for information; INFOSEC essentials; INFOSEC components.

Keywords: *Classified information, INFOSEC, vulnerabilities, threats, accreditation, certification*

Introduction

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Confidential information about a business' customers or finances or new product line could fall into the hands of a competitor, or a breach of security could lead to lost business, or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures. The field of information security has grown and evolved significantly in recent years.

* Ph.D. Eng., Ministerul Economiei, Comerţului şi Mediului de Afaceri, teodor_stefanescu@yahoo.com

Legal Framework

Below is a partial listing of governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.

• UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU member must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.

• The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. cracking - sometimes incorrectly referred to as hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.

• EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.

• The Family Educational Rights and Privacy Act (FERPA) is a USA Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

• Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.

• Gramm-Leach-Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.

• Sarbanes-Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.

• Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

• State Security Breach Notification Laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.

• Personal Information Protection and Electronics Document Act (PIPEDA) - An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision ActThant is in fact the case.

Romanian relevant laws in this regard:

• Law no. 51/1991- national security

• Law no. 182/2002- the national standards concerning the protection of classified information;

• Law no. 544/2001 – the access to public information.

• Law no. 677/2002; 682/2002;506/2004;102/2005- the protection of personal data.

•Law no. 8/1996; EO no 123/2005 – the copyright

• Law no. 161/2003; 64/2004- the computer crime.

Key Concepts

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) as the core principles of information security. Many information security professionals firmly believe that Accountability should be added as a core principle of information security.

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

Integrity. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Availability. For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

Authenticity. In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

Non-repudiation. In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

Security classification for information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- In the business sector, labels such as: Public, Sensitive, Private, and Confidential.
- In the government sector, labels such as: Unclassified, Sensitive but Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, which consists of: White, Green, Amber and Red.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

Infosec essentials

INFOSEC - all measures and structures for the protection of classified information processed, stored or transmitted through communications and information systems and other electronic systems, against threats and other actions that may endanger confidentiality, integrity, availability, authenticity and non- repudiation of classified information, as well as any actions that may affect the functioning of the information systems, no matter if they are accidental or intentional.

The INFOSEC measures cover computer security, transmission and emission security, cryptographic security, as well as detection and prevention of threats to which information and systems are exposed to.

Information in electronic format – texts, data, images, sounds, recorded on storage devices or magnetic, optical or electric supports, or transmitted as waves, tension, or electromagnetic field, in the atmosphere or communications networks.

System of automated data processing – ADPS - all interdependent elements including: computing equipment, basic software products and applications, methods, procedures, and, if applicable, the personnel, organized in such a way as to ensure the functions of storage, automated processing and transmission of information in electronic format, and which are under the coordination and control of a single authority. An ADPS can comprise subsystems some of which can be in their turn ADPS.

Specific security components of an ADPS, necessary to ensure an appropriate level of protection for classified information which is to be stored or processed in an ADPS, are:

- hardware / firmware / software functions and characteristics;
- operation procedures and modes;
- accountability procedures;
- control of access;
- definition of an ADPS operation area;
- definition of working stations operation area/remote terminals;
- restrictions imposed by the management policy;
- physical structures and devices;
- means of control for personnel and communications.

Data transmission networks – ***DTN*** – all interdependent elements including: communications equipment, programs and devices, hardware and software technique, methods and procedures for transmission and reception of data and network control, and, if applicable, the relevant personnel. They are organized to ensure the functions of transmitting information in electronic format between two or more ADPS - or to allow interconnection with other DTNs. A DTN may use the services of one or more communications systems; more DTNs may use the services of a single communication system.

The security features of a DTN comprise: security features of individual ADPS connected, together with all components and facilities associated to the networks - communication network facilities, mechanisms and procedures of identification and labeling, access control, programs and procedures of control and revision - necessary to ensure an appropriate level of protection for classified information transmitted through DTN.

Local DTN - data transmission network interconnecting more computers or network equipment, situated in the same perimeter.

Communications and informatics system - CIS - informatics system through which information in electronic format is stored, processed and transmitted, composed of at least an ADPS, isolated or connected to a DTN. It may have a complex configuration, made of more interconnected ADPS and/or DTNs.

ADPS, DTN and CIS security - implementation of security measures at ADPS, DTN and CIS in order to prevent or hamper extraction or change of classified information stored, processed or transmitted through them - by intercepting, alteration, destruction, unauthorized access with electronic means, as well as invalidation of services and functions, by specific means.

Confidentiality - to ensure access to classified information only based on the security clearance, in compliance with the secrecy level of the information accessed and the permission resulted from the enforcement of the need-to-know principle.

Integrity - interdiction to change - by deleting or adding - or to destroy classified information without authorization;

Availability - to ensure the conditions necessary to find and easily use classified information, whenever necessary, with the strict observance of its confidentiality conditions and integrity;

Authenticity - to ensure the possibility to check the presumed identity of an ADPS or DTN user.

Non-repudiation - measure to ensure that after the emission/reception of information in a secured communications system, the originator/beneficiary cannot misleadingly deny, that he sent/received the information.

Security risk - probability that a threat or vulnerability of ADPS or DTN - CIS actually exist.

Risk management **-** has as a purpose to identify, control and minimize the security risks and it is a continuous activity meant to establish and maintain a security level in the field of communication and information technology - (CIT) in an organization. Starting from risk analysis, the threats and vulnerabilities are identified and assessed, and appropriate measures are taken to counter the risks, designed at a cost price corresponding to the consequences deriving from disclosure, change or delete of information that should be protected.

The "two-men" rule - obligation that two persons cooperate to fulfill a specific duty.

Security informatics product - security component incorporated in a ADPS or DTN - CIS, used to increase or ensure confidentiality, integrity, availability, authenticity and non-repudiation of the stored, processed or transmitted information.

Computer security - COMPUSEC - implementation at the level of each computer of the hardware, software and firmware facilities, in order to prevent unauthorized disclosure, handling or unauthorized delete of classified information or unauthorized invalidation of certain functions.

Communication security - COMSEC - implementation of security measures in telecommunications with a purpose to protect messages in a telecommunication system that might be intercepted, studied, analyzed, and by reconstruction, may lead to disclosure of classified information. COMSEC represents all the procedures including:

- transmission security measures;
- TEMPEST security measures;
- cryptographic coverage measures;
- physical, procedural, personnel and document security measures;
- COMPUSEC measures.

TEMPEST - all measures of testing and ensuring the security against information leakage through parasite electromagnetic emissions.

Assessment consists in a detailed technical and functional examination of the security aspects of an ADPS, DTN - (CIS) or of the security products, by an appropriate authority.

The assessment process verifies:

(a) the existence of the required security facilities/ functions;

(b) the absence of compromising secondary effects resulting from the implementation of the security facilities;

(c) the overall functionality of the security system;

(d) the fulfillment of the specific security requirements for an ADPS and DTN-CIS;

(e) the determination of the trust level of ADPS or DTN-CIS or of the implemented computer security products;

(f) the existence of the security performances of the computer security products installed in ADPS or DTN-CIS.

Certification **-** the issuance of a finding document, to which an analysis document is attached, reporting the assessment and its results. This finding document mentions the extent to which ADPS and DTN-CIS meet the security requirements as well as the extent to which the computer security products meet the requirements referring to the protection of classified information in electronic format;

Accreditation is a stage when an ADPS or DTN-CIS is authorized or approved to process classified information within its operational environment/space.

The accreditation stage shall take place after all appropriate security procedures have been implemented and after a sufficient level of system resources protection has been achieved. Accreditation is mainly made on the basis of the Specific Security Requirements (SSR), including the following:

• justifying statement upon the objective of system accreditation; classification level(s) of information to be processed and handled; recommended protected operational mode(s);

• justifying statement upon the risk management - mode of risk treatment / accounting / solving - identifying the threats and vulnerabilities, as well as the adequate countermeasures;

• the detailed description of the security facilities and recommended procedures designed for ADPS or DTN - CIS. This description shall represent the essential element for completing the accreditation process;

• the plan for the implementation and maintenance of the security features;

• the plan for carrying on security test, assessment and certification stages, regarding ADPS or DTN - CIS;

•certificate and, where required, supplementary elements of accreditation.

ADPS area - represents a working area, containing one or more operating computers, their local peripheral and storage units, control units and specific network and communication equipment. ADPS area does not include the separate area in which remote peripheral devices, terminal or workstations are located, even though these devices are connected to the central computing equipment of the ADPS area;

Remote terminal/workstation area represents an area - separated from ADPS area - including:

(a) computing technique equipment;

(b) local peripheral devices, terminals or remote workstations connected to the equipment within the ADPS area ;

(c) communication equipment.

Threat - an accidental or deliberate potential compromise of ADPS or DTN - CIS by loss of confidentiality, integrity or availability of information in electronic format or by affecting the functions ensuring the authenticity and non- repudiation of information.

Vulnerability - weakness or lack of control that would allow or facilitate a technical, procedural or operational man oeuvre, which would threat a specific asset or target.

Infosec components

Hardware and software security

Computer security – COMPUSEC - is the implementation at the level of each computer of the hardware, software and firmware facilities, in order to prevent unauthorized disclosure, handling or unauthorized delete of classified information or unauthorized invalidation of certain functions.

Hardware, firmware and software security mechanisms can contribute individually as well as blended to computer security.

Hardware and firmware security uses security features that are provided by the manufacturer trough physical components of computers and refers to:

a) security procedures and documentation for start / stop computing equipment

b) instructions and safety procedures for connecting / disconnecting equipment in / from the network

c) procedures for periodic checks of the seals on equipment and ensuring that hardware modules are kept under lock and key, in case of equipment

d) pieces of the computer configuration to ensure the functioning in different conditions (for example, must be specified what terminals / workstations or peripherals can be connected or disconnected in a specific operational situation)

e) security procedures of configuration computer that is planned for maintenance and repair

f) procedures in case of hardware breakdown, including the commissioning of responsibilities and description of appropriate actions in order to secure the computer while disconnecting (also activities regarding the secure information and data stored on)

Software security comprises the use and control of any safety features provided by operating system, and utility programs as well as application programs, as follows:

a) identification methods of users, procedures for establishing user accounts (individual or groups), procedures for the allocation of user ID and delete user accounts whenever the situation requires

b) authentication methods, including protection of authentication information (eg, access password), control procedures and as well as procedures to change authentication mechanisms

c) access control mechanisms and procedures to implement user access control for the use of information systems services and resources

d) records of software, of versions of operating systems, of utility programs and those that will be used in special situations

e) control on copy or modify of data facilities related to: operating system, software tools and application programs

f) precautions before and after data processing or during preparation of various types of classified activities scheduled, including main memory erasing routines, declassifying rules or overwriting of previous versions and as well as procedures to ensure that buffers are cleared and all data files audit logs and records of open sessions of users are listed, and overwritten

Security of information storage media

In a computer and communication system the amount and density of information stored or processed, their accessibility, ease and speed of copying the information, sometimes from remote stations, underscores the need for measures to security of information, as well as the information storage media. These measures aim:

a) appropriate procedures for classification of media storage

b) responsibilities and procedures for recording, control and record storage media

All storage media classified as "secret of state" are identified and controlled according to appropriate level of secrecy (classification). For unclassified information or restricted information are applied separate internal security regulations. Identification, record and control storage and media require:

• means of identification consisting of: number, series and marking the level of classification, for each such storage media, separately

• well-defined procedures for issuing, receipt, removal, destruction or preservation information storage media

• existence manual or printed records concerning the content and classification level of information that is recorded on storage media.

For the levels "strict secret" and "strict secret de importanta deosebita", the detailed information on storage media, including the content and classification level of information, is held in an appropriate register

c) procedures for acquisition, storage, record and control storage media for computers

d) procedures to receive, exchange and dissemination of electronic documents, including procedures for checking for the existence of computer viruses and harmful software, applied to all media from outside the computer system

f) responsibilities and procedures for declassification / destruction of electronic documents and media storage.

When a storage media is planned to be unused (disbanded), it has to be declassified erasing any classification markings, then this can be used as an unclassified storage media

Classified information recorded on reusable storage media are deleted only in accordance with security operational procedures. If a storage media can not be declassified, then it must be destroyed by an approved procedure.

Declassification and reuse of storage media containing information " strict secrete de importanță deosebită" are forbidden, they can be destroyed only in accordance with security operational procedures. Classified information in electronic form stored on a medium disposables, cards, punched tapes can be destroyed as provided for operational security procedures.

Communications security

Communications security consist of applying security measures in telecommunications in order to protect messages in a telecommunication system, which could be intercepted, studied, analyzed and, by reconstitution, may lead to the disclosure of classified information. Communications security is a set of procedures, including: transmission security measures, security measures against radiation (TEMPEST), cryptographic security measures.

Transmission security

All means used to transmit classified information through radio and are subject to communications security regulations issued by the designated national institution for protection of classified information. Security transmission mechanisms conduct to ensuring the availability and confidentiality information by appropriate means in order to counteracting unauthorized interceptions, jamming, interferences, misleading, traffic analysis

Specifically, for a computer system these problems occur on wireless networks when sharing data between the server and other components of the network is via radio equipment, not wired.

Emissions security

Emissions security is a set of all testing measures, as well as getting security measures, against leakage of information through stray electromagnetic emissions, TEMPEST.

Spurious emissions occur around cables that move electricity. At a sufficient distance (several meters) of these cables and depending on the current that flows through throe cables, the electromagnetic fields can be captured with special equipment, and information can be retrieved.

This situation is valid for cable networks that are not sufficiently protected and avoid is possible only to the extent that information and communications system installation or any major change it will be executed by authorized persons in terms of security provided by standards.

The works will be permanently supervised by qualified technical personnel who have access to information at the highest level of classification that computer system will store, process or transmit.

Cryptographic security

Computer system for processing, storage and transmission of data and information at "state secret" level must be provided with the grading system (methods, means and equipment to ensure integrity, confidentiality and availability)

The way how information is presented, even if transmission uses short code or binary representation, or other form of transmission must not influenced the classification given to that information.

Physical security

A special importance should be given physical security measures in order to prevent following actions: unauthorized access to classified information, to perform unauthorized operations, locking resources and services, as well as to protect computers and computer equipment (theft, destruction, etc.).

Physical security of computing and communication systems as a component of INFOSEC, is considering the environment in which they work (the rooms are located, power supply, temperature, protection against fires, floods, functioning in emergency situations), but staff access to areas where they are located.

Any person able to enter a place that contains computers can be in a position to interact or to damage the equipment, as well as may have access to classified information processed by it.

Computer security threats can come from anyone who has professional training and adequate knowledge of computer systems and can access them. In areas where systems that process classified information are located it is necessary to apply general security measures such as:

• entry personnel and materials, and departure to / from these areas to be controlled by appropriate measures

• areas and places where computers systems security can be affected, there should never be occupied by a single authorized employee (usually rule the two)

• people who require temporary or intermittent access to these areas must have authorized access as visitors being always accompanied in order to have the guarantee that will not access classified information or equipment used

• Antivirus protection as a component of the protection systems must contain procedures and virus protection measures both manual and automatic as follows:

•Verification of installed operating systems, software packages and software tools, the presence of viruses or other harmful software, having proper procedures for removing them and if their detection;

•Always check the files / data stored in computer systems, virus checking during processing, accessing, introducing / extracting data to / from computer systems or well-established intervals

• Verification of storage media (information and software) received from external sources, with their disinfection procedures

• Constantly updated versions of antivirus software and using several antivirus products (licensed), both servers and workstations

•Reporting of incidents caused by viruses, the sender of infected storage media and security structure.

Conclusions

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

References

- Allen, Julia H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley. ISBN 0-201-73723-X.
- Krutz, Ronald L.; Russell Dean Vines (2003). The CISSP Prep Guide (Gold Edition ed.). Indianapolis, IN: Wiley. ISBN 0-471-26802-X.
- Layton, Timothy P. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.
- McNab, Chris (2004). Network Security Assessment. Sebastopol, CA: O'Reilly. ISBN 0-596-00611-X.
- Peltier, Thomas R. (2001). Information Security Risk Analysis. Boca Raton, FL: Auerbach publications. ISBN 0-8493-0880-1.
- Peltier, Thomas R. (2002). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.
- White, Gregory (2003). All-in-one Security+ Certification Exam Guide. Emeryville, CA: McGraw-Hill/Osborne. ISBN 0-07-222633-1.
- Dhillon, Gurpreet (2007). Principles of Information Systems Security: text and cases. NY: John Wiley & Sons. ISBN 978-0471450566.
- Oprea, Dumitru, Protectia si securitatea informatiilor, Ed. a II a rev., Iasi, Polirom, 2007, ISBN: 978-973-46-0927-7
- Patriciu, V.V.; Pietrosanu-Ene, M.; Bica, I.; Cristea, C., Securitatea informatica in UNIX si Internet, Editura Tehnica, Bucuresti, 1998

Web References

- Law no. 101/2003 for the approval of Government Emergency Ordinance no.153/2002 on the organization and functioning of the National Registry Office for Classified Information (ORNISS), Romania, www.orniss.ro
- Emergency Ordinance no. 153/2002 on the organization and functioning of the National Registry Office for Classified Information, www.orniss.ro
- Law no. 182/2002 on the protection of classified information, www.orniss.ro
- Government Decision no. 353/2002 on Norms on the Protection of NATO Classified Information in Romania, www.orniss.ro
- Government Decision no. 585/2002 - The National Standards on the Protection of Classified Information in Romania, www.orniss.ro
- Government Decision no. 781/2002 on the protection of restricted information, www.orniss.ro
- Protectia informatiilor clasificate, www.sri.ro