Romanian Enforceable legislation for cyber crime, anti-spam, e-signature, privacy and consumer protection

- Preventing and Fighting against Cyber-Crime
  - Law no. 161/2003 Anti-corruption law Title III

- Electronic Signature
  - Law no. 455/2001

- Privacy and Consumer Protection
  - Law no. 676/2001
  - Law no. 677/2001
  - Law no. 506/2004

Other laws:
  - Law no. 196/2003 on Prevention and Fighting against Pornography
  - Law no. 365/2002 on Electronic Commerce
I. Legislation against Cyber Crime

- Preventing and Fighting against Cyber-Crime
  - Law no. 161/2003 Anti-corruption law Title III

Short Presentation:

Definition of:
- Information System, automatic processing of dates, electronic dates, services provider, security measures, pornography materials.

Measures to prevent cyber crime

Informatics Infractions

International Cooperation against cyber crime
Romanian Cyber Crime sites

- **eFrauda** mission is to address fraud committed over the Internet. For victims of Internet fraud, eFrauda provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected internet fraud. For law enforcement and regulatory agencies at all levels, eFrauda offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

- **eFrauda** is offered to provide a method for romanian citizens and from abroad to promptly and directly communicate their complaints to romanian government agencies that are interested in investigating and taking action against internet fraud that is reported.

- **eFrauda** function is to protect the suppliers and consumers of information society services, respecting the law establishment, reducing the bureaucracy, preventing and fighting against cyber crime, increasing the transparency in relation between the citizens and authorities.
IT Security Incidents Response and Expertise Center
www.ceris.ro

- **CERIS** is the place where IT staff within organizations could call for receiving guidance and solutions in IT security events they deal with.

- Services offered by this center

- Recommendations regarding system protection means against potential problems, which will contribute to incidents anticipation and even to quick solve;

- Providing main information about IT system security;

- Providing guidance to organization for own IT system security increase
CERIS is the place where IT staff within organizations could call for receiving guidance and solutions in IT security events they deal with.

**Services offered by this center**
- Recommendations regarding system protection means against potential problems, which will contribute to incidents anticipation and even to quick solve;
- Providing main information about IT system security;
- Providing guidance to organization on their own IT system security increase and for management of incidents resulting from vulnerability exploitation.

**The main functions of the center**
- User assistance through IT system security audit provided by "Online Information Security Audit" application;
- To guide in security incident management;
- To guide in vulnerability detection and management;
- To publish security alert;
- IT system auditing in order to evaluate compliance with ISO 17799 standard; action recommended for this compliance;
- To guide public administration IT sector in order to decrease negative impact of the IT
IT Security Incidents Response and Expertise Center
www.ceris.ro - statistics

Statistics 2002
Ernst & Young’s Information Security Survey 2002 provide useful information regarding the IT security issues, finding the answers from companies involved in IT business, as following:

- 74% of respondents believe they have an information security strategy
- 51% believe IT security is currently a priority compared to other IT projects
- 70% of organizations plan to enhance business continuity and IT disaster recovery plans
- 53% see the internal availability of specialist skills as a challenge to effective security
- only 40% of organizations are confident they would detect a system attack
- 40% of organizations do not investigate information security incidents
- critical business systems are increasingly interrupted – over 75% of organizations experienced unexpected unavailability
- less than 50% have an IT security training and awareness program
- business continuity plans exists at only 53% of organisations
- only 41% of organizations are concerned about internal attacks on system, despite overwhelming evidence on the high number of attacks from within organizations
- 60% of organizations expect to experience greater vulnerability as connectivity increases

Causes of unavailability of critical business systems
II. Legislation for e-signature

- Electronic Signature
  - Law no. 455/2001

Short Presentation:
Definition of:
electronic-signature, extended electronic-signature,
subscriber, cryptographic keys, safety device, certificates

Legal forms of e-signs and Certifications
Delivery of certifications services
Suspension of certification validation
Monitoring and controls
Recognition of certificates delivered by foreigner providers
II. European Legislation for e-signature

  - Electronic communication and commerce necessitate electronic signatures and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States management of certificates, but should also encompass any other service and productusing, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services.

  - Establish criteria for member states to determine whether a national body should be designated as responsible for the conformity assessments of secure signature-creation devices.
E-Sign
http://www.ars.mcti.ro - content

- Law on e-sign
- Law on temporal mark
- Standards for e-sign law
- Guide for using e-sign:
  - What isn’t e-sign ?
  - What is it e-sign ?
  - Who can use e-sign ?
  - Pair of public key / private key ?
  - What we need to do for using e-sign ?
  - Mechanism for creation of e-sign
  - Mechanism for verification by receiver of e-sign
  - What we can sign ?
    WORD documents, PDF documents, e-mails
III. Legislation for Privacy and Consumer Protection

- Electronic Signature
  - Law no. 676/2001
  - Law no. 677/2001
  - Law no. 506/2004

Short Presentation:

**Definition of:**
- user, e-mail, traffic data, telecommunication services,
- public network, operator, personal dates, processing of personal dates.

**Security Measures**

- Privacy of Communications
- Dates about traffic
- Detailed billing
- Automatic redirection of calls
Romanian governmental CERT (Computer Emergency Response Team) RITI dot-Gov

Cooperation with other cu national structures
The experience of other CERT units proves that in order to fulfil the objectives related to CERT mission, it is essential to have a good collaboration with:
- The community organisations (Govt. Authorities, Regional organizations and Municipalities) that should send IT incident reports to CERT.ro and receive analyses, statistics, specific advice and training
- Other IT incident teams in Romania and abroad, but also with Vendors, in order to exchange information about new problems (e.g. vulnerabilities and viruses)
- Close co-operation with other public institutions that have tasks in the IT security area.
Thank you very much for your given attention

Aurica Nazgodineanu,
Head of Statistics and Database Section
Romanian National Regulatory Authority for Communications
aurica.nazgodineanu@anrc.ro