INTERNEWS

RITI dot-Gov

USAID FROM THE AMERICAN PEOPLE

Report on creating a Romanian governmental CERT (Computer Emergency Response Team)

10-Feb-2005

Thanks to
Liviu Nicolescu – MCTI
Iulia Bumbac – MCTI
Gheorghe Serban –ANISP
For their input to this discussion paper

Introduction

About CERTs (Computer Emergency Response Team)

On the 2nd November 1988 five percent or approximately 85,000 users of the Internet experienced fatal system crashes. The world's first major Internet incident became known as the Internet or Morris worm, taking the name of the programmer who wrote and launched the incident. The US Department of Defence was determined that such an event should never again occur and in 1989 funded the first ever Computer Emergency Response Team (CERT) now known as CERTCC (CERT Co-Ordination Centre) www.cert.org.

CERT activities mean prevention and detection of computer security incidents as well as providing information about them. CERT is an abbreviation of the words Computer Emergency Response Team. There are several CERT organisations throughout the world. CERT organisations cooperate by submitting information about security incidents for information system users mainly via the Internet. The aim of CERT activities is prevention of security threats related to information systems from being carried out and response to the threats as objectively and efficiently as possible.

Computer security incidents mean situations where an organisation's, a company's, an association's or a private person's information system availability, integrity or confidentiality is illicitly changed. This may comprise, for instance, that another person's or organisation's information system operability is prevented or impeded on purpose. A computer security incident may also be a situation where an organisation's, a company's, an association's or a user's data or information systems are used without permission.

Today, different kinds of CERTs exist in different types of organizations all over the world. They have been formed in the private sector, in the public sector and sometimes in a combination of a Public-Private Partnership.

Actually we may identify 3 major types of CERT organisations:

- private CERTs that take care only of computer security incidents within a company or their customers (see BT CERT - http://www.btcert.bt.com/)
- CERT from the academic or research networks (see SURFnet-CERT - http://cert.surfnet.nl)
- public CERTs that take care of computer security incidents within the government institutions, and sometimes also receive complaints from the general public. The proactive services are playing a very important role. (see BSI – Bund - http://www.bsi.bund.de/certbund/)

International trends

The international cooperation between the different type of CERTs from different countries and continents is becoming essential in an IT security activity.

Usually, there are very close relations between the present CERTs. But also the new ones are welcome in this family and can benefit from the experience and expertise already gained.

This is why it is important to present the major international cooperation structures:

FIRST

In 1990, eleven Computer Emergency Response Teams mostly from the United States army and research formed the first founding members of FIRST (Forum of Incident Response and Security Teams). Today, FIRST has 170 members that come together within a closed and trusted community of teams, sharing both technical resources and vital information in the prevention and fight against Internet and computer network crime. Within the FIRST, community organisations see themselves as collaborators rather than competitors. Within FIRST, Computer Emergency Response Teams combine their joint efforts to protect their own individual organisational brand names, reputation and data.

TF-CSIRT

The **TF-CSIRT** Task Force is established under the auspices of the TERENA Technical Programme to promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. The aim of the Task Force is:

- to provide a forum for exchanging experiences and knowledge
- to establish pilot services for the European CSIRTs community
- to promote common standards and procedures for responding to security incidents
- to assist the establishment of new CSIRTs and the training of CSIRTs staff.

The activities of TF-CSIRT are focused on Europe and neighbouring countries, in compliance with the Terms of Reference approved by the TERENA Technical Committee on 15 September 2004.

TF-CSIRT also provides an extensive list of all European CSIRTs made known to the Trusted Introducer, formally known as TI "listed" CSIRTs (formerly "Level 0"). All

data there are given without warranty and are only passively maintained by the TI, with the exception of those CSIRTs that have the "accredited" (and "accreditation candidate") status: the latter are fully maintained by the TI.

European Government CERTs (EGC) group

The European Government CSIRTs group (EGC) is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.

To achieve this goal, the ECG group members will:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Encourage formation of government CSIRTs in European countries
- Communicate common views with other initiatives and organizations

Current members of the European Government CSIRTs group:

CERTA - France
CERT-Bund - Germany
CERT-FI - Finland
GOVCERT.NL - The Netherlands
SITIC - Sweden
UNIRAS - United Kingdom

ENISA

The European Network and Information Security Agency, ENISA, is a new agency of the European Union, which formally came into being on 15 March 2004.

The Agency's work is essential to achieve a high level of network and information security within the Community. It will also seek to develop a culture of network and information security for the benefit of citizens, consumers, business and public sector organisations in the European Union. This will also contribute to the smooth functioning of the internal market.

As its in-house expertise grows, ENISA shall help the Commission, the Member States and, consequently, the business community to address, respond and especially to prevent network and information security problems.

The Agency shall also assist the Commission in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

RITI dot-Gov proposal

MCTI has done commendable work on creating *IT security incident response capacity* within the Ministry. At the same time, the individuals working with IT security incidents are also engaged in a number of other important tasks. Probably, the present structure could benefit from improved organisational stability and financial security.

In order to identify the main issues to consider, but also to learn from other countries experiences, a study visit was made by RITI dot-Gov together with officials from MCTI and the Romanian private sector to the Swedish CERT – SITIC. A report from the study-trip that is summarizing the Swedish IT security framework and the lessons learned can be found in Annex 1 - page 14.

The present document is presenting the main findings on IT Security Incident Response capacity building for Romania. The study is focusing on the main considerations behind the RITI dot-Gov suggestion to create a Romanian independent governmental CERT. We try to identify the major issues that could be raised by the creation of such an institution and to give some suggestion on these issues.

1) Romanian IT security policy

The present context shows that the interconnection of the public networks with the private ones, the convergence of the media, IT and communications domains and the common use of resources have considerably increased the difficulty of having proper control over these. Moreover, in some cases, in designing the information and communication systems, their security has been neglected.

The protection of the information systems is essential for each sector of the economy. The targets are:

- the prevention of actions directed against information systems and communication networks,
- the decrease of vulnerability to these attacks,
- the diminishing of the damages and of the recovering time after attacks.

Although on the short term security involves fulfilling attributes of integrity, availability and confidentiality, on the long term the following measures are necessary to protect the values of the organisations and to ensure the continuity of services:

- **Preventive measures**:
    - implementing control activities within the organisations
    - informing and creating public awareness,
    - creating a natural security culture for an easier identification and awareness of risks and threats,
    - codes of conduct,
    - training of users.

- **Protective measures**:
    - technical protection measures, use of secured equipment and devices,
    - regulations,
    - recovery plans in case of disaster.

- **Reaction / fighting measures**:
    - creation and specialisation of legal bodies,
    - prompt and coherent response of authorities to incidents,
    - cooperation between the public and the private sectors
    - international cooperation.

- **Continuous reviewing and improving measures:**
    - periodical checks,
    - follow up of technological progress,
    - adaptation to new technologies.

According to MCTI strategy for the development of Romanian until 2025, taking into consideration the present technologies but also the practices used during the last 20 years in the advanced countries, the following actions can be considered:

- institutional construction,
- implementation of PKI national infrastructure
- compliance with European and international standards,
- security of non-material financial transaction
- control upon products with dual use,
- safe networks and services,
- monitoring of the evolution of and fighting cyber crime.

2) **Private sector activities in Romania**

The private sector in Romania has clearly signalled that "information security" issues must be treated very seriously. Several companies (especially large ones) and organisations from various domains of activity have started to implement security systems and applications. There is no organised forum of discussions of the "IT security" issues and such discussions occur during various events (see ROCS- Romanian Open Computer Show). There is no mechanism either to signal and analyse information security incidents at the level of the communities in various activity domains.

We will further on refer to IT security concerning electronic communication operators, especially ISPs.

Certain specific channels to signal IT security incidents are developed but they are not particularly consistent and they are nor based on a set of rules. We consider there are also some connections and collaborations between the operators of these communication channels but they are less formal, due to various reasons:

- the fear of increased attacks towards one company or other
- the lack of investment and collaboration in creating regular contacts
- the fear of negative advertising that might be caused to a company the recognition of having suffered from IT security incidents.

It should be left to the business community to decide on their own internal activities to increase IT security.

There are communication channels with the competent state authorities. However there are quite a lot of situations when IT security incidents, although they are offences and contraventions, are not reported to the competent authorities that might take measures in this sense.

ANISP has a Work Group to discuss various issues related to electronic communication security. There was an attempt at ANISP level to create a larger informal work group (attracting specialists from outside its members) that should try to address the problem of IT security and develop, in time, proper communication and information means: recommendations in IT security domain, a specific site etc.

At the level of electronic communication operators, ISPs in particular, security officers, people dedicated to IT security. Usually these attributions are the responsibility of network administrators. ANISP believe however that dedicated persons, with a well defined professional profile, with specific responsibilities and resources should deal with such aspects related to the prevention and fighting against IT security problems. Furthermore, these people should collaborate at the level of the community within an organised framework.

ANISP is interested in initiating a work group to initiate discussions in view of creating a CERT type body within the community of the electronic service providers, especially ISPs. The organisation hopes to attract companies offering security technologies and services as well.

A series of companies[1] developed in the private sector provide various services related to IT security, some of them similar to those the CERT type offers.

In the banking sector there are several banks having made public the fact that they have implemented IT security systems and applications. Organisations from other sectors of activity have also implemented IT security systems and applications. However there is no mechanism to signal and analyse IT security incidents in the banking community or other sectors of activity.

[1] See Softwin, Gecad, Provision, Business Information Systems, UTI, Omnilogic etc

3) The need for a state operated CERT

During the last years the number of information systems installed in various institutions belonging to the local and central public administration in Romania has increased exponentially. The presence of an information system within a town hall or a Ministry is certainly nowadays a necessity.

Such a system should include a security component since normally both personal data and confidential information are stored and used. At the same time, various implemented e-government projects as well as the necessity of transparency in the public sector make it necessary to allow public access to these information systems within the boundaries imposed by the individual project.

Having the above in view and the more and more diversified and sophisticated information attacks, the IT security component of the information systems implemented in the governmental sector becomes a critical issue in the achievement and maintenance of safe and operational IT systems. Unfortunately the security component is however normally underestimated or uncovered. Thus, an updated anti-virus and activated firewall are no longer sufficient protection measures. The more complex the implemented systems are the more the security necessities increase.

The State has an overall responsibility for security issues, including for the IT environment. In many sectors of society private resources are used to add to the State level security without diluting the state responsibility as such. But a possible private participation doesn't undermine the overall state responsibility as such.

International experience, such as the Swedish example, demonstrates that a constructive cooperation can be established between public and private partnership regarding IT security and where the public responsibilities can effectively be performed through a state operated CERT.

In Romanian the public sector cannot presently afford to pay for security activities performed by private enterprises. This fact further strengthens the need for a Romanian state controlled and operated CERT. The CERT would collect information and knowledge on IT security problems at the entire governmental level and use that to prevent further attacks and incidents. By preventing attacks and incidents at the governmental level the CERT will most likely prevent losses of millions of dollars.

IT security at the governmental level make the few dedicated resources be used inefficiently, many of the problems being similar in various public institutions.

The existence of such units in other countries proves that they are more and more present and useful at the level of the governmental sector under the conditions of an increased number and complexity of IT systems implemented in the public sector.

Mandate for a Romanian CERT

It was agreed that SITIC can serve in general terms as a model, however a careful analysis is necessary to make sure that we propose something of relevance for Romania. RITI dot-Gov will come up with a first proposal.

Mission Statement

CERT.ro mandate shall support the Romanian society in working with protection against IT incidents and be the central report and coordination point for relevant security incidents for the government. CERT.ro shall collect and facilitate the exchange of information regarding IT incidents between organisations in society and disseminate information about new problems that could potentially impede the functionality of government IT systems. In addition, CERT.ro shall provide information and advice regarding proactive measures and compile and publish statistics.

Constituency

CERT.ro constituency covers all hosts in the government domain as well as all addresses assigned to any local or national governmental body.
CERT.ro does not respond with technical assistance to individual users incidents.

It is important to mention that CERT.ro will not work directly with the private sector or with the individual users. However, some of the proactive services of CERT.ro (information, advice on IT security, statistics) should be available for everyone, especially via the website provided by the CERT.ro. or via the public distribution mailing lists.

4) Confidentiality issues

All documents related to a CERT.ro should be public with the following exceptions:

- Classified documents
- Correspondence resulted from discussions related to topics from the above type of documents;
- documents (even unclassified) illustrating certain situations of imminent crisis/danger to certain systems at a certain moment which, by being revealed, would make the systems vulnerable to threats;
- documents which, as a result of contract terms, are confidential;
- documents that need a third party agreement in order to be revealed;
- other documents considered confidential at a certain moment (similar to the above list).

5) Staffing: number and qualifications

We suggest a maximum number of 10 members to be part of CERT.ro staff. The number can be lower in the beginning of CERT.ro activity and can increase later to the maximum number, if necessary.

We provide below a short description of each function. A detailed overview, including the minimum qualifications required for each job and the essential functions can be found in Annex II.

1. Director, CERT-Ro

This position is responsible for planning, developing, and implementing operational strategies, initiatives, policies, and programs that further the mission of the CERT-Ro Program. He (she) tracks and assesses success of CERT-Ro in meeting its strategic plan.

2. Internet Security Analyst, Networked Systems Survivability Program

This position is responsible for providing technical and strategic leadership into the research, examination, and analysis of Internet computer security trends and topics. Duties include:
- Testing and analyzing malicious code, vulnerable software, security tools, and patches.
- Developing external relationships to ensure the adequate collection of data for analysis.
- Developing or providing oversight of development of internal systems and processes to conduct analyses.
- Analyzing and identifying security trends based on incident activity, including the analysis of incident activity and artifacts during major events, analysis of publicly available information, and other collaborative interactions with security subject matter experts.
- Working on the development of white papers describing best practices for system and network administrators, technology managers, and other technology professionals.
- Representing the CERT-Ro in various technical forums.
- Providing expert technical guidance and mentoring to other members of the CERT-Ro.
- Contributing to the development of the strategic plans and direction of the CERT-Ro.
- Developing processes and procedures to monitor the health of the Internet by, for example, monitoring routing information and changes in routing information, monitoring key DNS servers.
- Publishing information to public and private parties on the state of the routing infrastructure and the state of the DNS infrastructure.
- Publishing papers and creating presentations, in collaboration with internal and external parties, on advanced network and Internet infrastructure security issues.

3. Vulnerability Researcher, Networked Systems Survivability Program

This position is responsible for researching, examining, analyzing, reporting on, and effecting change in the current state of software engineering. Duties include detailed software vulnerability research, correspondence with software vendors, researchers, sponsors, and other stakeholders, specification and development of tools and processes to meet team goals, provide leadership in setting the strategic direction for vulnerability research, and identifying and implementing novel approaches to identify, analyze and

prevent software vulnerabilities. The candidate is expected to be a technical leader, both internally and externally.

4. Vulnerability Remediation Specialist, Networked Systems Survivability Program

This position is responsible for researching, examining, analyzing, reporting on, and effecting change in the current state of Internet security. Duties include detailed software vulnerability analysis, correspondence with software vendors, researchers, sponsors, and other stakeholders, specification and development of tools and processes to meet team goals, provide leadership in setting the strategic direction for vulnerability remediation, and identifying and implementing novel approaches to identify, analyze and prevent software vulnerabilities. The candidate is expected to be a technical leader, both internally and externally.

5. Practices, Development, and training, Networked Systems Survivability Program

The individual in this position will work as a member of the Practices Development and Training Program to develop and teach security improvement practices and curricula in information assurance and survivability for system and network administrators and managers. The candidate will be expected to work well in a collaborative team environment and to communicate effectively with others. Activities will include close work with customers from a variety of organizations, including government agencies and critical infrastructures.

6. Analyst, Networked Systems Survivability Program

The Network security Statistical Analyst will apply sound statistical principles in the development of analysis tools for the study of network situational awareness. Primary responsibilities include building prototype analysis tools, contributing to the development of a high-level research agenda for network security data analysis, and serving in a consultative role in support of team members conducting statistical analyses in the research efforts. Prototype analysis tools will provide the following capabilities:

- Trend analysis: tracking changes in network traffic composition and volume over time
- Anomaly detection: finding data points which violate normal network traffic behavior
- Behavioral-based source clustering: identifying sources exhibiting coordinated attack behavior
- Data integration: unifying a wide variety of data types for analysis and inference.

7. System Administrator

This position is responsible for supporting users and maintaining software and equipment in the CERT-Ro Computing Laboratory. This includes understanding the needs of the teams using the lab, designing and developing lab services to meet those needs, planning equipment acquisitions, overseeing configuration and maintenance of equipment,

overseeing set-up and breakdown of equipment for experiments, assisting in experiments as needed.

8. Information Developer
Strong Romanian writing and grammar skills required. Technical writing experience is advantageous but not mandatory for this position. The applicant should also have a solid grasp of general IT concepts and computer terminology in English and Romanian. Understanding other languages is helpful but not required. Some image editing/manipulation skills and general web design/development skills would be advantageous.

9. Security Consultant

2-4 years experience in a consulting environment with demonstrated experience as a System or Network Administrator within a Windows or UNIX environment. Knowledge and experience in system architecture, total security solutions, and Internet protocols and applications. Experience in configuring and implementing technical security solutions (firewalls and intrusion detection systems). Excellent customer interface skills. Strong oral and written communication skills. Excellent Project management skills. Knowledge of common Internet protocols and applications. Associate's degree or equivalent experience. Certifications such as MSCE, CCNA, CISSP, CISM or CISA desirable.

10. Security Response Engineer

BS Degree, preferably in a computer science-related field, or equivalent industry experience. The candidate is expected to display a broad range of skills, including the ability to read and understand x86 assembly code, and an understanding of TCP/IP networking, including knowledge of the major TCP/IP-based protocols. The applicant should have a minimum two years of C/C++ programming experience on the MS Windows and/or Linux platforms. In addition to the above, the role requires a working knowledge of shell scripting, PERL and/or Python programming to conduct day-to-day tasks.

6) Possible location for the CERT.ro

Our discussions on this topic considered some of the characteristics that this institution should have:

- a 100% governmentally supported project. Although we have studied the possibility of achieving a public-private partnership, the European experience and the types of activities to be developed show that such a possibility couldn't be considered presently. We can however state that an extremely well organised collaboration should exist between a governmental CERT, the private CERTs, the ISPs and other key-players on the IT security market.
- a civilian institution. There could most likely be problems for a military institution to cooperate to the extent necessary with civilian organisations.

- Part of an independent institution. This requirement is necessary for the separation of CERT type activities from the activities to establish IT security policies. The institution must however be a collaboration pole not only for MCTI, as IT security policy creator but also with the other ministries and institutions involved in the domain of IT security, including the top security level - CSAT (Superior Defence Council of the Country).
- From a pure substance point of view an independent institution could be good solution. However, due to its relatively small size (max. 10 people) the CERT would be burdened by an un-proportionally big amount of administrative tasks. Therefore, it is preferable to "place" it within the framework of another institution. .
- The employees must not be public officers. Such a statute would prevent them from being paid according to the abilities that are necessary for such a unit.

A public consultation on the organisational issue is recommended to make sure that the interest from all parties can be adequately taken into account

This document presents 2 possible solutions without excluding the possibility of another institution being chosen to host CERT.ro.

A. We consider there is the possibility to create a governmental CERT.ro within the existing National Regulatory Authority for Communications (ANRC), which meets all the above mentioned capacities.

Such a hypothesis is supported by the European experience showing that in most states such a CERT is achieved within the regulatory authorities for electronic communications, as an autonomous department with operational independence, a proper staff capability and an adequate payment for the employees.
Further more, such attributions in the domain of IT security would come to complete the provisions of Law *no. 506 of 17 November 2004 on the processing of personal data and protection of private life in the electronic communication sector* which gives ANRC the competence to establish security measures for the electronic communication service providers.

Art. 3: Security measures
(1)*The provider of an electronic communication service for the public has the obligation to take all proper technical and organising measures to ensure the service security. As regards network security, if necessary, the provider of the electronic communication service will take the respective security measures together with the public electronic communication network provider. The measures taken must ensure a security level that is proportional with the existing risk, having in view the latest technical possibilities and the costs involved by the implementation of these measures.*
(2) *The National Regulatory Authority for Communications further on referred to as ANRC, establishes the conditions under which the provider must meet the obligation stipulated in paragraph (1).*

B. Another option could be the creation of CERT.ro as an autonomous department within a new public institution that would cover other IT security issues.

The creation of a new IT institution could be considered to host a large range of IT security and related domains that are now within the attributions of MCTI or other bodies and that could be achieved within an independent institution from the Ministry[2]:

- Authorisation of remote access payment means in agreement with Order no. 218 of 14 June 2004
- Regulation and Monitoring in the electronic signature domain in agreement with the electronic signature law
- Notification for time stamping services, according to Law 451/2004
- Performing technical expertise services in the domain IT security and equipment
- Promotion of standards in the domain of IT security
- Independent audit on the e-government services
- Monitoring of the implementation for electronic commerce law in agreement with Law 365/2002 – art 17
- Managing the E-fraud portal

All these activities can be achieved within an independent institution that would IT security have as general competence domain. Part of the above activities can produce revenues (either by payment of services – as authorising payment means or by monitoring fees as for electronic signature regulating).

7) Budget

A rough estimation for the CERT.ro budget will be:

Assistance for Process, Management and Operational consulting, Recruitment management, Training.....……...120.000 euro
Communications and IT infrastructure (services, hardware and software) ....130.000 euro
Initial facility and furniture.....…….....20.000 euro
Operational expenses for 1 year.....…….....440.000 euro

Total .....…….....710.000 euro

8) <u>Source of financing</u>

The establishment of the CERT.ro could be financed from several sources

- European Union funds could possibly be used to support some of the costs of the setting-up of CERT.ro. Through PHARE 2005 such a project could be financed through technical assistance (consultancy) or investment funds (equipment,

[2] In fact, such activities could make the object of CERT.ro activity in case it is created as a department within ANRC

computers, etc) or twinning projects (where expertise from a European CERT could be shared to the new Romanian institution). The availability of such a funding and the specific requirements should be checked with the EU delegation in Bucharest starting with January 2005. Also we should be open to other sources of financing from EU, including future activities from the recently created ENISA[3]

- Other bilateral sources of financing, such as the IBD/GTZ project from the German government
- Governmental financing via the state budget
- USAID, via the RITI dot-Gov project could support the initial training to US for 4 future members of CERT.ro, including the participation to a CERT-CC training in Arlington

Depending on the timeframe of the setting-up of CERT.ro, a combination of the above-mentioned sources or with other international donors sources could be the best solution.

For the yearly operation all options are left open, including the alternatives of financing over the state budget or through fees or other contributions related to the operation as long as the latter would not be regarded as purely commercial activity.

9) <u>Co-operation with other bodies.</u>

The IT Security policy should be drafted by MCTI, after extensive consultations with the IT industry, especially the ISPs. It is important that the IT security policy is also presented and discussed among the highest level of Defence Strategy in Romania – CSAT.

The Policy should be implemented by CERT.ro in cooperation with all the public institutions that have tasks in this domain according with the national legislation.

The CERT.ro activity and the implementation of the IT Security Policy should be supervised by the IT&C Commission in the Parliament. The Commission should receive a public yearly report from CERT.ro regarding the present status of the ICT security and the implementation of the IT security policy. The Commission can ask clarifications from CERT management on a certain matter as well as CERT experts on certain technical aspects related to IT security.

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)

[3] European Network and Information Security Agency - http://www.enisa.eu.int/

- Close co-operation with other public institutions that have tasks in the IT security area.

It is highly recommended to create an informal group with the other national CERTs and public institutions, that should meet at least monthly to discuss operational issues, share knowledge, present common projects. These meeting are important for the identification of overlapping activities between different institutions, but also in order to define the national objectives and perspectives on IT security.

A special collaboration needs to be created with the cybercrime law enforcement authorities. The information should flow in both directions:

- The law enforcement bodies should have a technical expertise focal point that can address technical matters that need to be cleared
- The CERT.ro team should inform the law enforcement authorities about the illegal activities that have been stopped or identified by CERT.ro

Cooperation with international structures

As the international cooperation in the domain of IT security has become a necessity, it is essential that CERT.ro should develop collaboration relationships with other CERT type organisations, as well as with their associations: FIRST, TI CSIRTS, ECG[4].

Having also into consideration the decision for Romania's European integration, a special relationship must be created with ENISA.

10) List of legislation that might be amended.

The creation of a CERT.ro type institution should be subject to a special law to specifically provide at least:

- An autonomous statute
- The management structure
- The objectives, attributions and responsibilities
- The supervision manner and the institution in charge with it
- The financing means for annual costs
- The relations with other public institutions
- The recruitment and retribution of CERT.ro personnel
- The manner of approval for ANRC cost/revenue budget on CERT activities

In case CERT.ro operates within another institution, then the normative act establishing the operation of the respective institution must me modifies.

[4] See section International trends for more information on these institutions/associations.

In terms of the activities that will be under the task of CERT.ro or the institution hosting it, the normative acts regarding that domain will have to be modified as well (e.g. electronic signature, remote access payment means etc.)

However we consider it is too early to get into details on these aspects.

Annex 1

Report from CERT related study trip October 2004

RITI dot-Gov organised a CERT (Computer Emergency Response Team) related study trip to Stockholm, Sweden, 22 October 2004. The following persons participated in the trip:

Ministry of Communication and IT
Liviu Nicolesco, General Director IT Regulation, Standards, Anti fraud and Security
Iulia Bumbac, Head of Service, Antifraud and network security

National Association of ISPs, ANISP
Gheorge Serban, Executive Director.

RITI dot-Gov
Jerker Torngren, Project Director
Bogdan Manolea, Legal expert

The First meeting was with Mr. Michael Mohr, Director and Principal Secretary of the Governmental Defence Commission.

The second meeting was with Mr. Johan Mårtensson, Head, Swedish IT Incident Centre, SITIC, which is the official Swedish CERT authority.

The Defence Commission evaluates the present system for protecting cyber security across the society and will present a proposal to the Government regarding the possible need for modifications in the present system. The Commission is strongly supported by all Ministries.

Based on a previous proposal by the Commission, the Swedish Parliament decided in 2002 on the present organisation for IT security, including the creation of SITIC. The Commission is now evaluating the efficiency of that organisation and the possible need for modifications due to changes regarding threats.

In addition the Commission has the role of co-ordinating non-military IT threats.

The core participants in the Commission are all representing the public sector but the private sector participates frequently on an ad hoc basis.

In addition to the establishment of the new agency SITIC, three other agencies have tasks regarding IT security;

- Swedish Emergency Management Agency, SEMA
- The Defence Material Equipment

- Defence Radio Agency

The Ministry of Justice is directly engaged through the National Police Force, which has a dedicated IT crime squad, providing also support to local police forces.

Co-ordination between all engaged authorities is organised through the Coordinating Group, where all the agencies meet once per month to present each Agency schedule in order to avoid the duplication of the their work.

It was pointed out that a number of private companies are doing "CERT-tasks" as well on a strictly commercial basis. Some of these companies could offer services in competition to SITIC. This situation will be further analysed by the Commission in order to create a clear split of responsibilities and engagement between public and private engagement. The further considerations in the split / duplicated engagements will be done based on the fact that the overall responsibility for security issues must rest with the public sector.

SITIC was set up as the Swedish public CERT in 2002. Although the number of CERTs is increasing globally, only 8 European countries have Government –run CERTs. However a CERT structure as such can be found in almost all EU countries through Academia or the private sector.

SITIC has 9 staff members and is organised as a department within the state regulator for Post and Telecom, PTS, primarily to benefit from the administrative services and organisation of PTS. To set up a separate authority for the tasks that are engaging only 9 persons was not considered to be efficient. The choice of host organisation wasn't obvious except for the fact that it should be a civilian organisation, not military defence related one.

The number of staff members is much related to the tasks a CERT should carry out as such and doesn't really reflect the size of the country.

SITIC is financed directly over the State Budget, and is an integrated part of the PTS budget. The yearly SITIC budget amounts to SKR 15 million, which corresponds to around 1,6 million Euro. 2/3 of this amount is spent on the wages for the staff members, by necessity being very qualified in the field of IT security. According to SITIC, a by far higher amount is yearly saved through less disruption as a result of the SITIC operations. As examples were mentioned a previous threat SITIC avoided which would have paralysed the entire national social contribution system and also a total stand still of the Stockholm Municipally.

The staff needs to have some expertise in working and managing computer networks, analysis and communication skills and some programming knowledge. They don't need to know in detail how malicious codes are written, but how these are functioning and are being developed in general. They also need to be well updated on the development in the IT security domain.

SITIC co-operates with the other agencies have tasks regarding IT security, but also with vendors, ISP's and other IT incident teams in Sweden and abroad.

The task of SITIC is to support society in the efforts against IT incidents by;

1. Being able to quickly communicate information to the community regarding new problems, potentially threatening to IT systems.
2. Providing information and advice regarding preventive efforts.
3. Aggregate and publish statistics as input to continuous improvement of the preventive work.
4. Establishing a system for information exchange regarding IT incidents between community organisations and the team.

This is done through;

- Technology area studies in order to survey/discover new IT security problems.
- Receive reports about IT incidents.
- Analysis.
- Produce statistics.
- Provide advice.

It is not considered necessary to conduct this kind of work on a daily 24 hours basis. SITIC is consequently only operating during normal working hours.

It was pointed out by SITIC that the functions of a CERT are often mistaken with those of the Antivirus producers or other IT security consultants. The difference lies in the approach that those organisations have in connection with the malicious codes that appear everyday.

The Antivirus producers or other IT security consultants are giving information on all possible vulnerabilities, which can be over 4 000 / year.

SITIC on the other hand focus on the main software and hardware products and concentrate their activities and alerts on that pattern and deals with around 200 vulnerabilities on a yearly basis, assisting the target audience to patch the security holes or repair the vulnerability before the vulnerability is used.

Annex 2
Indicative Job profiles

1. Director, CERT-Ro

Qualifications:

MS degree in computer science or equivalent.

Fifteen plus years of progressively responsible experience in a technology- or research-based organization in higher education, industry or the government. At least 10 years software development experience including hands-on development, development team leadership, and project management. Demonstrated management experience with responsibility for projects, people, budgets, and contracts.

Mastery and broad understanding of computer systems, computer security practices, and information security evaluation methods, as well as broad understanding of organizational goals, management, etc.; ability to manage diverse areas and large, complex projects; ability to influence, work with, and manage technical staff; able to respond quickly and effectively to changing priorities; excellent analytical, organizational, supervisory, reasoning, and problem solving skills; ability to interact effectively with diverse constituencies internally and externally; excellent verbal and written communication skills; computer literacy.

Ability to meet inflexible deadlines, remain calm during difficult situations, work under pressure, and work with frequent interruptions.

Must be able to pass a background check and obtain government security clearance.

Essential Functions:

Manages **CERT-Ro** programs to effectively implement the **CERT-Ro** strategic plan, goals, and objectives and manage day to day functional business activities of **CERT-Ro**. Develops, implements, and tracks short and long term operational plans (financial, staffing, infrastructure, project). Resolves scheduling conflicts for external customer priorities.

Provides guidance to and monitors the success of **CERT-Ro** employees in meeting strategic goals. Assesses performance of direct reports and makes salary recommendations for all staff in areas of responsibility. Serves as primary liaison to internal SEI functions and programs.

Leads strategic planning process and contributes to the development of **CERT-Ro** strategic plan. Insures annual update of strategic plan; reviews feasibility of plan, identifies risks and defines risk mitigation strategy. Articulates vision for internal and external audiences.

Candidates must be able to pass a background investigation, obtain a security clearance, and be a Romanian citizen.

2. Internet Security Analyst, Networked Systems Survivability Program

Qualifications

NOTE: Candidate must have the ability to pass a background check investigation, obtain a security clearance, and be a Romanian citizen.

PhD with six years of related experience or MS in Computer Science or related field with 8 or more years experience.

BS in Computer Science or related field with ten years experience.
Experience: Expert knowledge of at least several of the following topics:

- security tools
- system and/or network administration
- extracting security information from network monitoring tools/applications
- operational details of multiple operating systems
- software development experience
- programming experience in multiple languages

Expert knowledge is required in all of the following:

- computer systems and Internet security issues
- operation and limitations of technologies used by organizations as key network security defences, such as firewalls, intrusion detection systems, proxies, scanners, and encryption
- core Internet protocols (TCP/IP, UDP, BGP, DNS, SMTP, etc.).
- Internet routing protocols and security issues related to Internet routing
- DNS server operations, including root DNS servers, and the impact on the Internet infrastructure on how DNS servers operate
- detailed knowledge of methods used by intruders to attack systems networks
- IP address space and global domain name management issues
- operation of the core Internet infrastructure
- best practices for secure code development
- reverse engineering of malicious code
- computer security forensics
- development of tools to assist system and network administrators
- collecting, summarizing, and analysing Internet traffic and incident data for security trends.

Additionally, in-depth knowledge or familiarity with most or all of the following topics is required:

- security tools
- system administration
- core Internet protocols (TCP/IP, UDP, DNS, SMTP, etc.).
- incident response handling (encompasses more than just IR)
- common vulnerabilities
- theoretical underpinnings of computer security
- cryptography and encryption tools
- intrusion detection
- software engineering
- Published papers or documents, and formal presentations in several of the following topic areas:
- BGP and other routing protocol security issues
- best practices for the secure operation of DNS servers, systems used in the routing infrastructure
- possible improvements to DNS or routing protocols
- discovering vulnerabilities in software
- secure programming practices
- reverse engineering of software
- forensic analysis of computer systems or other electronic devices
- analysing large volumes of intrusion detection system data or network data

Skills/Abilities

The ability to provide technical leadership to junior and entry level staff; the ability to set priorities in a variety of technical domains; demonstrated experience in public speaking and effective communications with a large number of external, international collaborators and partners; the ability to serve as a facilitator in coordinating with many different parties involved in the security of the Internet infrastructure, and to help groups reach technical consensus.

The ability to work well under pressure of deadlines. The ability to manage technical and management (or non-technical?) interactions with a large number of colleagues of varying seniority.

Essential Functions

Technical development and implementation of results; transition activities, including incident, artefact and vulnerability analysis. Oversight of the collection of data to support analysis efforts.
Mentoring of junior level staff.

Research into areas of technical interest.

Representation of **CERT-Ro** in other groups (conference presentations, technology working groups, etc.).

Incident response and vulnerability handling.

Other duties as required.

3. Vulnerability Researcher, Networked Systems Survivability Program

MINIMUM QUALIFICATIONS:

Bachelor of Science in Computer Science, Information Science, Information Management or equivalent, plus 10 years experience as a system or network administrator, software developer, database administrator or similarly technical occupation, or Master of Science in Computer Science, Information Science or Information Management, or equivalent plus 8 years experience as a system or network administrator, software developer, database administrator or similarly technical occupation, of a PhD in Computer Science, Information Science, or Information Management plus 6 years experience as a system or network administrator, software developer, database administrator or similarly technical occupation. We will consider other educational backgrounds of a technical nature with experience as described.

Experience with or substantial knowledge of

- Internet security issues
- Software testing
- Software engineering
- Common forms of malicious code
- Common development methodologies
- Common software failures (e.g. buffer overflows)
- Software development and programming in multiple languages
- System, database, and network administration
- Multiple operating systems
- Common Internet protocols (e.g., TCP/IP, ICMP, DNS, HTTP, etc.).
- Advanced cryptographic theory and practice

Published papers or documents, and formal presentations in several of the following topic areas:

- discovering vulnerabilities in software
- reverse engineering of software
- forensic analysis of computer systems or other electronic devices

Must have the following abilities and skills:

- software testing and evaluation
- originality and creativity

- outstanding written and oral communication skills
- establish priorities in working
- work within a closely coordinated team during emergencies
- work calmly and well under pressure
- recognize and deal appropriately with confidential and sensitive information
- communicate effectively under normal and stressful situations
- leadership and mentoring skills

of time.

The ability to work well under pressure of deadlines

Must be able to pass a background check, obtain a security clearance, and be a Romanian citizen.

ESSENTIAL FUNCTIONS:

1. Detailed examination and testing of software looking for new vulnerabilities.
2. Research, specification, and development of new tools, processes and techniques to improve vulnerability testing and detection for use by software engineers.
3. Writing and publishing results of the tests.
4. Correspondence with software vendors, vulnerability researchers, sponsors, and other stakeholders.
5. Represent **CERT-Ro** in other groups (e.g., conferences, workshops, etc.)
6. Provide assistance and input to other teams and projects within the SEI.
7. Mentoring junior staff.

4. Vulnerability Remediation Specialist, Networked Systems Survivability Program

MINIMUM QUALIFICATIONS:

Bachelor of Science in Computer Science, Information Science, Information Management or equivalent, plus 10 years experience as a system or network administrator, software developer, database administrator or similarly technical occupation, or Master of Science in Computer Science, Information Science or Information Management, or equivalent plus 8 years experience as a system or network administrator, software developer, database administrator or similarly technical occupation or Ph.D in Computer Science, Information Science, Information Management or equivalent, plus 6 years experience as a system or network administrator, software developer, database administrator or similarly technical occupation. We will consider other educational backgrounds in a technical discipline with experience as described.

Experience with and expert knowledge of

- Internet security issues
- common software failures (e.g. buffer overflows)
- software development and programming in multiple languages
- system, database, and network administration
- multiple operating systems
- common Internet protocols (e.g., TCP/IP, ICMP, DNS, HTTP, etc.).
- cryptographic theory and practice

Published papers or documents, and formal presentations in several of the following topic areas:

- possible improvements to DNS or routing protocols such as BGP or OSPF
- forensic analysis of computer systems or other electronic devices
- analysing large volumes of vulnerability assessment system data or network data

Must have the following abilities and skills:

- quickly evaluate evidence
- separate fact from opinion, speculation, and possibilities
- develop action plans in the absence of complete information, while preparing for any reasonable contingency
- outstanding written and oral communication skills
- establish priorities in working
- interact effectively with vulnerability reporters, system and network administrators, vendors, experts, Internet users, sponsors, policy makers, news reporters, managers and staff
- work within a closely coordinated team during emergencies
- work calmly and well under pressure
- maintain composure while dealing with difficult people
- recognize and deal appropriately with confidential and sensitive information
- communicate effectively under normal and stressful situations
- leadership and mentoring skills

The ability to work well under pressure of deadlines

Candidate must be able to pass a background check, obtain a security clearance, and be a Romanian citizen.

ESSENTIAL FUNCTIONS:

1. Development of advanced vulnerability remediation strategies, including enhancing communication strategies with software vendors, protection of the critical infrastructure, communication with the general IT community, advanced

patch management strategies, and other techniques related to remediating vulnerabilities.
2. Research, specification, and development of new tools, processes and techniques to improve vulnerability remediation techniques and to support publication, secure communication and interaction with stakeholders.
3. Writing and publishing short to medium-length document describing vulnerability mitigation strategies.
4. Correspondence with software vendors, vulnerability researchers, sponsors, and other stakeholders.
5. Represent CERT-Ro in other groups (e.g., conferences, workshops, etc.)
6. Provide assistance and input to other teams and projects within the SEI.
7. Mentoring junior staff.
8. Be on call to respond to Internet emergencies (outside of normal business hours)
9. Act as supervisor for vulnerability team

5. Practices, Development, and training, Networked Systems Survivability Program

Minimum Qualifications:

MS in Computer Science, Electrical Engineering, or Information Science with one year experience.

At least 1 year relevant experience as a system/network administrator in a TCP/IP networked environment or very strong working knowledge of managing all aspects of UNIX/LINUX in a professional training environment is required. This includes experience developing and effectively delivering technical training. Strong background and knowledge of Linux security administration to include IPTables firewall configuration, Tripwire, Syslog, TCPDump, and Snort, as well as FreeSWAN IPSEC implementations and shell/Perl scripting. Experience writing and developing Linux security courseware and training exercises. Strong programming experience in C/C++. Java, XML, and Perl.

Candidate must be able to prioritize workload and complete deliverables on time, have good technical problem-solving skills, have strong analytical and information organization skills, have excellent oral and written communication skills, and strong technical teaching skills. Candidate must be able to multitask and work effectively with multiple project teams and sponsors/customers. Technical proficiency with operating systems and detailed knowledge of network protocols are required.

Ability to pay close attention to detail, meet deadlines, work under pressure, and communicate effectively.

Candidate must be able to pass a background investigation, obtain a security clearance, and be a Romanian citizen.

Essential Functions:

1. Design and develop technical documents and instructional materials.
2. Install/configure hardware and software including promising new technologies that require examination for information security and assurance research and development.
3. Deliver technical and management training to customers.
4. Mentor, guide, and interact with team and other staff.
5. Contribute to transition planning and strategy.

6. Analyst, Networked Systems Survivability Program

MINIMUM QUALIFICATIONS:

BS in Computer Science, Information Science or equivalent with 3 years of applicable experience, MS in Computer Science, Information Science, with 1 year of applicable experience, or recent Ph.D in Computer Science, Information Science or equivalent.

Total of 3 years of applicable experience in the design and analysis of complex data sets, building tools to assist in the analysis and generation of reports, and with scripting and/or programming languages such as C++, JAVA, or equivalent.

Skills and abilities are:

- Ability to manage heavy workload and effectively manage priorities
- Strong problem solving skills
- Excellent oral and written communication skills
- Ability to work both independently and with teams

Ability to work under pressure and meet deadlines; ability to establish priorities in tasks; strong learning capability; ability to assist users of varying competency; ability to interact effectively with vendors, managers, and technical staff. Good technical problem solving skills; strong information organization skills; good oral and written communication skills. Maintain confidentiality of sensitive information.

Candidates must be able to pass a background investigation, obtain a security clearance, and be a Romanian citizen.

ESSENTIAL FUNCTIONS:

1. Participate in the design of future analysis systems
2. Participate in integrated analysis of event and netflow based data

3. Lead the production of the CERT-Ro analysis report based on the collection of IDS and other data
4. Contribute to conference and meetings; marketing calls on clients; and give talks and lectures as appropriate
5. Contribute to the review of literature and commercial tools for data mining

7. System Administrator

MINIMUM QUALIFICATIONS:

BS in Computer Science, Information Science, or equivalent with 8 years of applicable experience, MS in Computer Science, Information Science, or equivalent with 5 years of applicable experience, or Ph.D. in Computer Science, Information Science, or equivalent with 3 years of applicable experience.

Project management experience, including experience creating and upgrading computing infrastructures.

System administrator level of knowledge for UNIX or Windows operating systems, as well as experience with the selection, configuration and deployment of associated hardware and software. Experience and knowledge in using system administration tools to manage dozens of machines and configurations.

Network administrator knowledge of network technologies including: TCP/IP, UDP, Ethernet, 802.11, routing protocols, DNS. Experience in network architecture and implementation.

- Ability to manage heavy workload and effectively manage priorities.
- Strong problem solving skills.
- Excellent oral and written communications skills.
- Ability to work both independently and with teams.
- Ability to effectively manage multiple projects.
- Ability to elicit technical requirements from management and staff.

Ability to work under pressure and meet deadlines; ability to establish priorities in tasks; strong learning capability; ability to assist users of varying competency; ability to interact effectively with vendors, managers, and technical staff. Good technical problem-solving skills; strong information organization skills; good oral and written communication skills. Maintain confidentiality of sensitive information.

Candidate must pass a background investigation, be eligible to obtain a Romanian Authorities Secret Clearance and must be a Romanian citizen.

ESSENTIAL FUNCTIONS:

1. Collects user requirements for lab equipment software and services needed for the Artefact Analysis and Vulnerability Handling teams.
2. Test, evaluate, and select new hardware and software for the lab in consultation with the SEI IT and lab users.
3. Work with the CERT-Ro to develop and/or implement tools and processes for managing and maintaining software and hardware in the lab, including the set-up for experiments.
4. Schedule experiments, obtaining experiment requirements, performing lab setup, assistance in experiments, and lab cleanup.

8. Information Developer

Requirements:

The Security Response Content Developer will be responsible for the final quality of content produced by the CERT-Ro Response group. This includes producing wireless and web-based security alerts and detailed technical descriptions of network- and host-based security threats and the information required for CERT-Ro customers to mitigate them.

A key part of the role is working with their peers worldwide on content development projects and to ensure consistency with security information being provided by the other Security Response sites.

Day-to-day, the candidate will liaise closely with the Security Response Engineering team to understand the technical background of issues submitted by customers and their solutions, proof reading and editing the content provided by the engineers when appropriate to adhere to guidelines. They are also responsible for monitoring competitors' websites to lead information on new threats that CERT-Ro alerting service customer require. The Information Developer is also responsible for posting the information onto the CERT-Ro website after approval.

During a security incident, the applicant will be expected to work as part of the incident response team. They will be required to put security information together based on an incomplete understanding of the nature of the threat. The Information Developer will be responsible for determining what information is important and needs to be given to customers immediately, what information is released internally and what information requires further clarification.

As CERT-Ro Security Response operates 7 x 365, the candidate may be required to work public holidays periodically.

9. Security Consultant

Requirements:

Participates on consulting and implementation projects utilizing professional concepts and company policies and procedures to evaluate and solve a variety of problems. The consultant at this level will have subject-matter expertise on a medium portfolio of CERT-Ro security solutions. Evaluate factors and exercise judgment within broadly defined practices and policies in selecting methods, techniques and evaluation criteria for obtaining results. As part of a team may lead components of a project and/or lead small consulting projects including testing, implementing and documenting total security solutions. May participate in the bid/proposal development process.

10. Security Response Engineer

Requirements:

The Security Response Engineer role combines the responsibilities of rapidly responding to new security threats in the field and of responding to customer issues submitted to CERT-Ro Security Response for review. The principal responsibility of the candidate is to review issues either directly submitted by customers to Security Response, or files retrieved from the Internet, and to create antivirus detections and information "write-ups" for them, to be posted to the CERT-Ro Security Response website. As these are typically customer issues, much of the work must be done within strict time constraints. The candidate is expected to identify new threats from these issues, to disassemble them and to quickly determine their functionality. From their own analysis, the Security Response Engineer then determines the appropriate method of detecting this threat and writes a signature based on the detection technology available in CERT-Ro's security products. A detailed document describing the threat and how to remove it from affected systems is then provided. The applicant must be able to occasionally work in high-pressure situations while remaining focused on the task to be completed. Working closely with other members of the CERT-Ro Security Response group, in many cases in geographically separate locations, requires the ability to communicate issues clearly and concisely. Excellent written and verbal communication skills are a necessary part of the job. The candidate is expected to be able to work with minimum supervision and to display the determination to ensure both customer commitments and project goals are met. Strong problem-solving, and troubleshooting skills are a must, as a full solution to many problems faced in the role may either not be apparent or may simply not exist.