Tunisia's experience in establishing the first public CSIRT in Africa, as a case example for developing countries, and some guidelines and schemes for International cooperation

Prof Nabil SAHLI
Head of Cert-Tcc,
CEO of the National Agency for Computer Security,
Advisor to the Minister of Communication Technologies,
E-mail : n.sahli@ansi.tn,

Abstract: As a case example for developing countries, we will give a brief overview of Tunisia's experience in ICT Security before presenting the main activities of the Cert-Tcc (Computer Emergency Response Team - Tunisian Coordination Center). We will conclude by presenting an overview of the urgent needs of developing countries and the interest of a regional approach, and close with a set of key points to consider when building CSIRTs in those countries, coming from the Tunisian experience in the field.

Key-words: Tunisian CSIRT activities, developing countries, international cooperation, regional CERT, guidelines.

I- Introduction: Brief historical overview of Tunisia's experience and strategy in ICT security

In December 1999 a Unit (a "micro-CERT") specialized in ICT Security was launched, with the objective of sensitizing policy-makers and administrators of information systems, after the Y2K bug, on security issues and creating the nucleus of a task-force of Tunisian experts, specialized in the field.

In 2002 after certification of the role of ICT security as a pillar of the emerging Information Society, this unit was in charge of drafting a strategy and a national plan an ICT Security. A national survey was done, to fix priorities and the required actions and logistics.

In January 2003, the Council of Ministers, headed by the President, decided on:

-the creation of a national agency, specialized in ICT Security, as the executive tool implementing the ICT security national strategy and plan.

-the introduction of mandatory and periodic security risk assessment, one of the main pillars of our strategy

-the creation of a "body of Certified Auditors" in ICT Security,

and some other accompanying measures (launching of Masters in ICT security, etc.).

In addition to previous laws (Law on electronic signature and e-commerce, Law on cyber-crime, Law on protection of privacy and personal data), a new law related to ICT security was passed in February 2004 (Law N° 5-2004 and its 3 relatives decrees [1]). This law made it compulsory for national companies (all public and big private companies) to do periodic (now annual) security audits of their information systems, under the supervision of certified auditors from the private sector. The related decrees defined the certification process for auditors and the process of the audit.

Concerning incident handling, the Law made it compulsory to declare security incidents that could affect other national information systems, with a guarantee of confidentiality.

The Law also defined the missions of the National Agency for Computer Security (ANSI), which was created under the Ministry of Communication Technologies and which clearly does not deal with national security and defence concerns.

II- Missions of the Cert-Tcc

With the increasing complexity of attacks and the bigger damages involved, it was decided in 2002 to establish the nucleus of a CSIRT in Tunisia; this led in 2004 to the official launching of Cert-Tcc

(Computer Emergency Response Team – Tunisian Coordination Center), a public CSIRT hosted by the National Agency for Computer Security (Ministry of Communication Technologies).

Cert-Tcc has initiated actions with the following objectives:

- Increase awareness and understanding of information security and computer security issues throughout the two communities of professionals and citizens and initiate proactive measures
- Provide a reliable, trusted, 24-hour 7days/week, single point of contact for emergencies, to help handle security incidents and ensure protection of the national cyber-space and the continuity of critical national services in the face of successful or failed attacks.
- Provide high level training and certification for trainees and professionals
- Inform about best practices and about security organizational aspects, with a special focus on audit and risk management
- Inform about vulnerabilities and corresponding responses and serve as a trusted point of contact for collecting and, as a future step, identifying vulnerabilities in computer systems
- Inform about security mechanisms and tools, including those available from the open-source field, and ensure that appropriate technology and best management practices are used
- Implement mechanisms that enable quick alerting and response actions and help organizations and institutions develop their own incident management capabilities
- Facilitate communication between professionals and experts working in the security field and build relationships and stimulate cooperation among and across government agencies, public/private businesses, and academic organizations
- Collaborate with the international and national community in detecting and resolving computer security incidents
- Promote or undertake the development of education, awareness and training materials appropriate for a variety of different audiences to further improve the skills and technical knowledge of IT users and security professionals.

Cert-Tcc offers free help and assistance, 24h/24 and 7 days a week, to users and administrators in dealing with computer security problems and in responding to computer security incidents. For that task, it provides the necessary logistics and high level executives. CERT-TCC is composed of three teams:

- a team in charge of vulnerability and Artifact analysis and response coordination. This team circulates information about vulnerability and malicious activity and provides online assistance (through a call-center and by e-mail) for citizens and professionals. It is also in charge of developing awareness material and organizing awareness and training events
- a second team, in charge of Incident Analysis and Incident Coordination and Response on Site and in charge of deploying the national reaction plans, in case of emergency
- a third team, in charge of Incident and artifact detection, which develops and manages a monitoring system for the national cyberspace, based on open source solutions. It is also in charge of giving technical assistance and to help for the deployment of open-source solutions.

As a public Cert, all services provided by Cert-Tcc are offered free of charge to the whole national community (professionals and citizens), and one of its tasks is to motivate the launching of private CSIRTs, by showing the profitability of such activities. All the activities related to the support of professionals will be progressively dispatched to private CSIRTs, progressively collapsing Cert-Tcc's activities into the monitoring of the national cyber-space and awareness activities and assistance to citizens.

III- Overview about Cert-Tcc's main activities

Incident handling and assistance

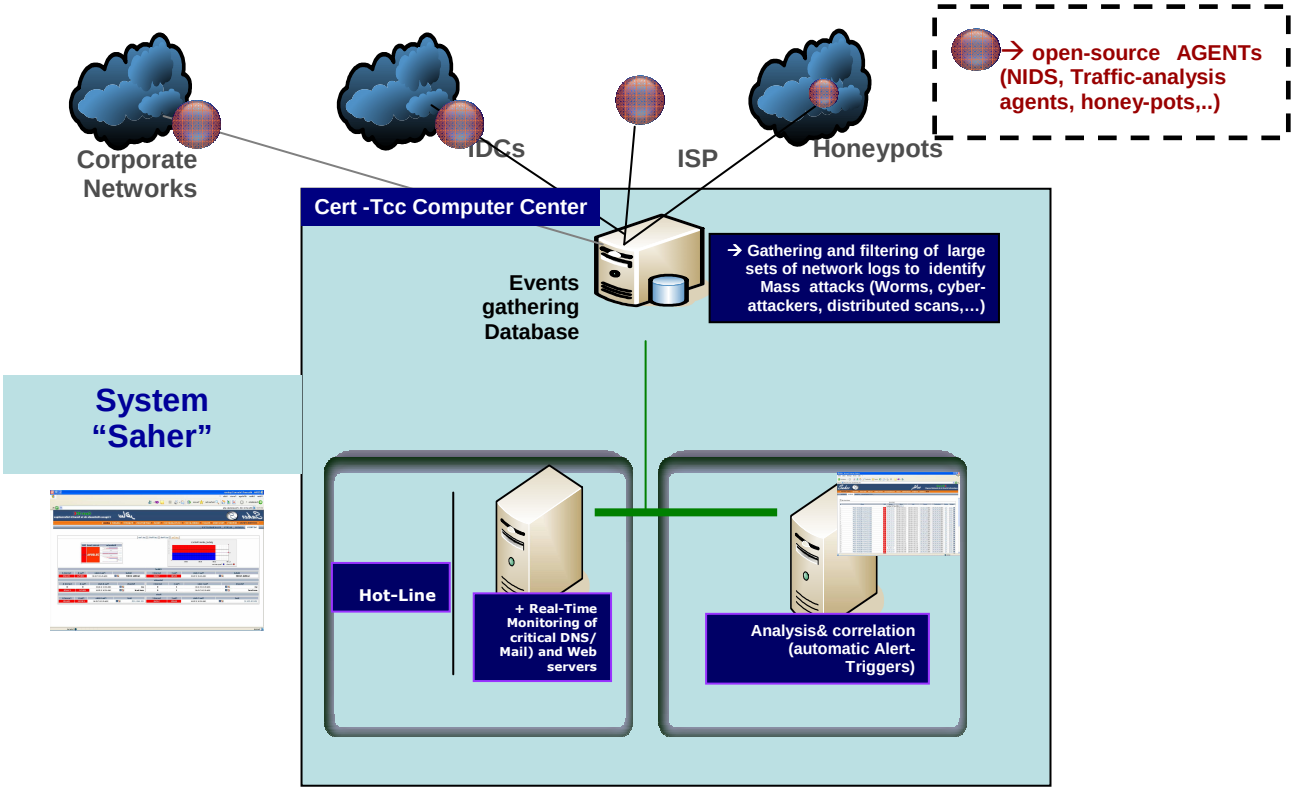
By law (Article 10 of Law n° 2004-5, related to computer security), private and public corporations must inform the National Agency for Computer Security (Cert-Tcc) about any incident which may impact other national information systems, with a guarantee of confidentiality, in compliance with Article 9 of that Law, which stipulates that the employees of the National Computer Security Agency and security auditors are liable, in case of infringement to confidentiality, to penal sanctions. So private and public organizations should trust Cert-Tcc, since we are obliged by law to keep their identities and the sensitive information provided confidential. We also try to be neutral, which enables us to work with commercial entities and government agencies without bias.

A 24-hour 7day/week hotline was established, allowing professionals and citizens to report and call for assistance in case of computer security incidents and also to request information and/or assistance on any trends related to ICT security.

An incident handling team was created and trained, including practical training inside other CSIRTs (Cert-IST) to respond to any request for assistance. Simultaneously, we are encouraging the creation of corporate incident handling teams inside sensitive and big infrastructures. For home users we have launched a "Citizens' assistance desk ", to which they can bring their PCs in case of security problems and/or to install security and parental control tools, free for domestic use.

In our vulnerability and incident handling activities, we assign higher priority to attacks and vulnerabilities that directly affect the national cyberspace.

Working in that direction we started developing a system ("Saher") that enables us to assess and predict potential big threats to the sensitive telecommunications infrastructures and the local cyberspace. This system is a major component of our ISAC system and is based on open-source tools. It enables the security of the national cyber-space to be monitored in real time for the early detection of massive attacks. The first prototype was deployed during the WSIS in November 2005. It consists of (open-source) agents deployed at the frontier of important corporate networks and at the level of ISP and access providers, permitting the gathering and centralized treatment of a high volume of network data to identify any important malicious activity related to mass attacks.



In order to insure a rapid and correct response to major attacks on our cyber-space, we have developed a Global Reaction Plan ("Amen"), based on coordinated crisis-cells at the level of the various actors in the national cyber-space (ISPs, IDCs, access providers, big corporate networks) with Cert-Tcc acting as coordinator. This Reaction Plan was deployed and tested during a mass worms attack and during big suspicious hacking activity and, proactively, during big events hosted by Tunisia.

Concerning disaster-recovery infrastructures, Cert-Tcc tried to regroup the needs of various national IDCs and is participating in developing a national project for building a national disaster recovery center (under the management of the National Computer Center), with funds from the World Bank. We are also motivating the development of disaster recovery plans for critical national applications, based on the use of that center, while motivating the launching of other sectorial centers.

Awareness

From the start of its activities, Cert-TCC has paid special attention to the awareness field:

Publications: As awareness material, we developed several brochures and small guides which explain to users simply and clearly the threats and how to protect their systems.

We also freely distribute CDs containing security and parental control tools, free for domestic use, but also voluminous Microsoft patches, dedicated for users with slow dial-up lines and CD of open-source security tools. We also broadcast short awareness ads via specialized sections of our security mailing list (rubrics: precaution, flash, tools, open-source).

Presentations: We co-organize and intervene in the national conferences and workshops related to ICT (11 during the first semester of 2007 and 62 from 2005) and organize booths at all national and regional exhibitions, with live demonstrations of attacks, to put people in touch with the reality of the risks and the importance of best practices.

Young people and parents: Concerning Young people's and parents' awareness, we prepared a first pack of awareness material and courses for schools. A manual ("Security passport for the family") including quizzes was developed. We also developed three "cartoons" and a little pedagogic game which explain to children amusingly the risks (pedophilia, virus…) and basic rules of protection. We also organize awareness events with institutions and organizations, working in the field of education and childhood (3 workshops in 2007) and developed a special section on a web site for parents and children and a mailing-list rubric for parents (parental control tools, risks etc).

Press: We try to maintain close relationships with the press, being aware of its importance for reaching a wider population. We participate in weekly programs on 6 regional and national radio stations (3 in 2005) and we created a press relations position in Cert-Tcc (a journalist), who prepares and provides raw material to journalists and motivates papers on the subject. Short awareness courses are also prepared with a school and an association of journalism.

Regulatory level: Legal promulgation of mandatory annual security risk assessment (Law N°5-2004 on computer security[1]) was an important awareness instrument for ICT professionals and managers of information systems and thus it was decided that such audits must include awareness sessions by auditors for the whole staff of the audited entities. We also organize awareness sessions to sensitize policy-makers and public controllers, with the goal of avoiding procedural barriers.

Information and alert

One of our primary tasks is to detect and analyze threats and, when necessary, convey that information to system administrators and also the wider user community.

Cert-Tcc regularly circulates information and alerts about critical vulnerability and malicious activity through its mailing lists and through its web site (around 600 products vulnerabilities declared in 2006).

We try to analyze potential vulnerabilities by collecting information through monitoring multiple sources, and we are trying to work with other CSIRTs and software editors to track down solutions to these problems. So in 2007 we started collaboration with Microsoft, through the Microsoft SCP program, that helps us for all what concerns Microsoft products and platforms.

To increase awareness of best security practices, we started developing short guides and internal knowledge bases. The first publications concerned technical tips, good practices and open-source manuals that provide simple and practical guidance to professionals and also common ICT users.

Training and education

We chose to concentrate on building up a task force of trainers and creating specialized diplomas in ICT security, and encouraging professionals to pursue international certification.

To solve efficiently the problem of the lack of specialized training in ICT security, Cert-Tcc organized training for trainers, who will be in charge of reproducing those training courses on a wider scale. Over a hundred potential trainers were trained in Tunisia by specialized international training centers (loan from the World Bank) in the 3 basic fields of ICT security (network security, platforms security, methodologies and organizational aspects), creating a potential task force of trainees in these fields. For 2007, we are preparing additional training modules for trainees and managers of computer security incident response teams and for the preparation of a CISSP exam.

We also developed a certification training program for auditors from the private sector; in case of success a national certification of security auditor is awarded. Two (night) training courses were carried out enabling more than 60 professionals to pass the auditor certification exam (NACS certificate). In addition, we gave periodic training to administrators of e-gov systems, and, as motivation for the CISSP certification, we gave training sessions that covered all the chapters of the CBK.

Cert-Tcc also tries to work with professional and academic institutions to develop curricula in information security and we intend to launch a regional training center in ICT security, through a partnership with the private sector and a little support from the World Bank. The first task for this Center will be training and certification in the field of incident handling.

We are also preparing special trainings for judges, law enforcement staff and journalists.

Education: In collaboration with two academic institutions, the first Masters degree in ICT security was launched in 2004 and now seven universities (3 public universities and 4 private) offer Masters degree programs. To motivate students to attend such courses, it was decided to offer them the possibility of applying for the national security auditor certification.

We think that all students should be prepared to gain the appropriate knowledge of risks and of the existence of best security practices and tools for protection. For that purpose, we started summer awareness sessions for new high school teachers (over 800 in 2006) and we are motivating all education institutions to introduce basic awareness courses in academic programs, from high school to university. Cert-Tcc started developing awareness material and programs for high schools and we are preparing for a large-scale operation, on awareness sessions at school.

Collaboration with associations

We regularly co-organize awareness workshops and training with Non-Governmental Associations (over 20 from 2006) and we try to rely on such associations for synergy between professionals and the various national actors.

We encouraged the creation of two associations specializing in the field of ICT security. An academic association was launched in 2005 (ATSN: "Association Tunisienne de la Sécurité Numérique") and a more professional one in 2006 (ATESI: "Association Tunisienne des Experts de la Sécurité Informatique"). To motivate technical add-on from those associations, we are urging them to create technical workgroups (self risk-assessment methodologies, open-source security tools) and develop deontological rules and models (books for tenders, etc.), to attract more specialists and private investment in the field. We also want to organize, with those associations, regular surveys on important topics related to national information security systems, to perfect the national strategy in the field (identification of weakness and consequent actions needed).

International collaboration

Cert-Tcc joined FIRST as a full member in May 2007 and tries to collaborate with other CSIRTs in developing measures to deal with large-scale or regional security incidents, share information and provide collaboration in investigations.

We also try to be active at regional (especially at the African) level and at international organizations and frameworks committed to security and to improve links with international security groups. We are trying to motivate international frameworks to launch regional collaborative actions. Cert-Tcc is active inside ITU's "Action Line C5" and is regularly invited to read papers in workshops related to this action line.

Cert-Tcc is committed to contributing with other CSIRTs on sharing our modest experience (errors, success stories) and providing, as far as is now available, assistance and logistics (hosting trainees, awareness material, open-source training, etc.) for establishing CSIRTs in developing countries and participating in setting up a regional CERT, which will help other countries in the region, especially the African region. We are also trying with other CSIRTs from the OIC, to launch an OIC-Cert, which should be financed by IDB funds.

IV- Some features and needs of developing countries and a scheme for international cooperation:

IT security is at the core of a safe and sustainable involvement in this new era of the Information Society, and the international community has to contribute significantly to its development in developing and less developing countries, so that ICT technologies and their benefits may be exploited to the desired extent.

Apart from the risk of greater digital divide, that security incidents can induce, by undermining confidence in the use of ICTs, the ICT infrastructures of developing countries are constantly abused by intruders (spam relays, botnets, phishing sites) and developing countries are becoming a potential future "reservoir" of intruders (problems of unemployment, lack of entertainment, feeling of injustice and need for expression, etc.).

That is why urgent action is needed to help those countries facing cyber security challenges, not only as a matter of 'aid' but of mutual interest to prevent the creation of criminal havens.

Characteristics and primary needs of developing countries

-Lack of experts: There is a need to set up task forces of local experts, which can be done by launching specialized entities (local CERTs,) that provides "nests" for local experts. Developing countries should be helped to launch local CSIRTs, which will be in charge of awareness actions and

the common tasks of CSIRTs in developing countries, and to participate in establishing a national strategy and plan in ICT security, accordingly to the state of development of each country

-Lack of awareness: International actors should help raise the awareness of policy-makers, starting with high-level politicians, of the impact on development of ICT security, along with making funds available from international development banks' programs.

- Lack of protection tools and funds: Software editors should foresee the possibility of providing special cheap prices (accordingly to the economic situation and as a marketing action for, hopefully, growing markets) and also study the possibility of pursuing the provision of security patches for old versions of their products.

In addition to commercial solutions, there is a need to raise awareness about the capabilities (and limits) offered by open-source security tools and to help provide trainers in the open-source field.

Also due to the lack of end-user protection tools, there should be assistance to local ISPs in offering "centralized" protection (NIDS, anti-virus) at their level and provide training for CSIRST teams and assistance in case of emergencies. ISPs connecting less developing countries should also try to pay more attention and take more preventive measures against the abuse made by « their » intruders into the communication infrastructures (botnets, spam relays, etc.) of developing countries.

The raising of user awareness and information on best practices (the "proactive approach") is more critical than in developed countries, due to the lack of protection tools. Local CSIRTs should be helped by providing awareness material and training in this direction.

An opportunity for canalizing help through the launching of CSIRT and the benefits of a regional approach

With inputs and guidance from eminent forums (FIRST, ENISA, APCERT, etc.) specializing in the field and international organizations (ITU, ODCE, WB, etc.), it is important that we try to sensitize and combine regional skills of all the stakeholders (private sector, NGOs, governments) in developed countries, and developing countries, that built some of the skills in ICT security.

One efficient way to canalize and organize help to those countries, with possible rich inputs from all stakeholders, is through CSIRTs.

The first step will be to provide help to those countries for building CSIRTs to gain skilled interlocutors and have an identified point for canalizing efficient international technical help. To this end, it is important to take into account the benefits of the "regional" approach, since this permits help to be better organized and problems that are generally common to several countries in each region (similar state of development/ language, same time/address block/, proximity, etc.) to be more efficiently addressed .

Help to developing countries in establishing CSIRTs should rely on regional CSIRTs. That is why there is a real benefit in encouraging the rapid launching of additional regional CSIRTs that will cover all regions, and assigning the task of providing help for regional developing countries in establishing local CSIRTs, besides raising the awareness of regional organizations (African organizations, Arab League, ASEM, etc.) and regional development banks (African Bank for Development, IDB, etc.).

Cert-Tcc is ready to participate with other international CSIRTs in regional cooperation programs, especially in Africa. We are preparing to host in Tunisia in 2008 a multi-stakeholder meeting which will focus on developing countries, under the sponsorship of ITU and hopefully other organisations and forums, and we are trying , with other Certs from OIC to develop a regional CERT, partially financed by IDB.

V- Some points to consider, while building up CSIRTs in developing countries:

While there are no internationally agreed standards as to what constitutes a CSIRT [6], there are a number of documents and efforts that can assist the process of defining a CSIRT team and on the certification and accreditation of CSIRTs. The CERT/CC has published a variety of documents that can

assist in the creation of a CSIRT [2,3] which were developed from knowledge and experience in incident response activities gained over the last decade. A guide, available in several languages, is offered by ENISA [4] and a review of the available literature and a pilot organizational survey of CSIRTs is offered in [5].

Countries can now leverage the experiences of international CSIRTs to help them develop and implement more effective teams. There are various organizations, such as the FIRST [7] that promote collaboration among teams and provide resources for helping new and existing teams at the international level. At the regional level, there are regional forums: the APCERT [8] in Asia, and ENISA [9] and TF-CSIRT [10] in Europe.

For an idea about the kind of actions to be launched with regard to some specific needs of developing countries, we briefly give a set of practical key points to consider, when building CSIRTs in developing countries:

- First of all: Do not wait too long, start as rapidly as possible from a small team, which should be trained and given the task of launching a national CERT. The sitting of such a team depends on where basic security skills exist in each country (national ISP, university, Ministry, etc.), but it is important that there be no relations with national defence and national security concerns.

Once launched, this public CSIRT will provide a "nest" for local experts and should be given the special task, not common for CSIRTs, of participating in defining and implementing a national ICT security strategy and plan.

It is recommended that such a team start with a small number of motivated experts and initiate a suitable subset of well-handled services (awareness activities, vulnerability alert and incident handling), since it is very important to gain the respect of the community by providing those services in a quality manner.

- Awareness

The public CSIRT launched should start by focusing on the awareness field, sensitizing policy-makers and professionals about computer security issues and their impacts. Sensitization of IT users should be done with care not to frighten them too much about the risks related to the use of ICT. Every presentation of risks should be accompanied by specifying simple preventive and technological solutions.

This CSIRT should:

- Quickly start a specialized mailing list, which should include awareness sections. This will introduce an interactive relation with users and motivate the team to start technological watch about vulnerabilities and threats.

- Initiate the development and distribution of awareness material (brochures, guides, etc.), on the web, and in classical paper and CD form (free anti-virus for domestic use, etc.). You can use existing materials developed by other CERTs, and adapt it for local requirements and languages.

- Organize regular awareness campaigns (workshops, booths at exhibitions). To put people in touch with the reality of the risks, there should be real-time simulation of intrusions and presentation of statistics, concerning frequency of attacks, associated vulnerabilities and financial losses and impacts (especially when conducting seminars for high-level authorities).

You should also target the media, by encouraging them to increase public awareness and exploit their ability to reach a wider population, and encourage the launching of security associations working in the awareness field, with which you should start co-organizing awareness events, as a way to push such important activity to the dynamic associative level.

Depending on the economic situation, there should be special attention paid to raising professionals' awareness about the advantages and limits of open-source tools and informing domestic users about the existence of free commercial security solutions.

- Training and education

- Start by focusing on enhancing the potential of trainers in ICT security by organizing training for trainers.

- Encourage the introduction of basic (awareness) courses in academic and school programs, providing programs, documentation and training for trainers, and motivate and participate in launching specialist diplomas in ICT security at the university (Masters, etc.).
- Encourage high-level certification for professionals (CISSP, etc.), by raising motivation and proposing training courses.

- Mechanisms and tools for reinforcing the security of the National Cyber-space

- Provide the needed assistance for incident handling via a hotline and by creating a specialized task force, able to intervene in case of emergency, 24 Hours and 7 day/week.
- Draft reaction plans for mass attacks, based on coordination between key actors (ISPs, access providers, IDCs).
- Start deploying a system permitting the monitoring and early detection of mass attacks (ISAC) by starting, in case of lack of funds, with solutions from the open-source field.
- In case of lack of protection tools at the level of national Information Systems, provide training for the deployment of open-source security tools.
- In case of lack of protection tools at the user level, motivate ISPs to provide "up-stream" protection at their level (anti-virus and anti-spam gateways, NIDS, etc.). There should also be assistance for domestic users, in deploying commercial security tools, free for domestic use.
- Promote and support the use of filtering, rating, parental control and related software, as well as measures for the establishment of safe environments for the use of the Internet by children.

- Additional "special" tasks

In addition to the common activities of CSIRT in developed countries, CSIRT in developing countries should also help draft national strategies and implement security plans in ICT security, and try to coordinate between all stakeholders, concerned by the reinforcement of the security of national information systems.

The CSIRT should start by launching surveys to identify priorities and assess the volume of needs, the results of which will be used to draft and perfect ICT security national strategies and plans.
An effort should be made, with all concerned stakeholders to:
- Identify national "heavy" investment to engage (disaster recovery infrastructures, mass training, etc.) and regroup efforts made to this end.
- Define rules (national information security policies, procedures and practices) for the follow-up of efficient security plans, taking into account the reality of human and financial resources.
- Reinforce the role played by the private sector (motivate the public sector to call for private services, provide training for trainers and help for certification, establish rules for fair competition, motivates private investment, etc.)
-Motivate the emergence of academic associations in the field of ICT security, with the goal of motivating national R&D in strategic fields
- Establish national cyber crime and information security councils that include the participation of all stakeholders (private sector, government authorities, telecommunications service providers, law enforcement officials, the judiciary, NGOs).

At regulatory and judicial level, the CSIRT could also help by:
- providing assistance in adopting norms and certification procedures, related to ICT security tools and procedures
- helping enhance the skills of judicial and law enforcement bodies in dealing with cyber-crime, by providing technical assistance and training opportunities and ensure that codes of conduct and best practices are reflected in the criminal procedure laws of the country, where appropriate
- participating in defining and implementing regulatory rules and mechanisms for controlling abuses (copy right, respect for privacy, consumer protection, etc.) and promotes self-regulation in the private sector
- strengthen international collaboration in dealing with cyber security incidents (mutual assistance with CSIRTs, transfer of proceedings, etc.), and encourage acceptance of, and compliance with, international legal instruments.

Conclusion:

We think that establishing CSIRTs in developing countries should be one of the pillars of developing countries' ICT security strategy. It also offers a good and practical medium for implementing efficient international technical cooperation. In that trend, we tried to attract more attention about the needs of these countries and about the benefits of a regional approach to better organize help for the launching of CSIRTs in developing countries.

We also gave an overview of the activities of the Tunisian CERT, as a case example of a developing country, which started with modest resources, taking into consideration our stage of development, and tried to contribute to the evolution of the overall situation of ICT security in the country.

Bibliography

[1] Law N°5-2004, Journal Officiel de la République Tunisienne, N°10, 3 February 2004, available in (non-official) electronic English format at http://www.ansi.tn/en/leagalframe.htm

[2] The Handbook for Computer Security Incident Response Teams (CSIRTs), Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, 2nd Edition: April 2003, CMU/SEI-2003-HB-002, www.cert.org/archive/pdf/csirt-handbook.pdf

[3] Steps for Creating National CSIRTs, Georgia Killcrece, CERT/CC, August 2004, http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

[4] ENISA, step-by-step approach on how to set up a CERT, 2006, http://www.enisa.europa.eu/pages/05_01.htm

[5] State of the Practice of Computer Security Incident Response Teams (CSIRTs), G. Killcrece, K. Kossakowski, R. Ruefle, M. Zajicek, Technical Report CMU/SEI-2003-TR-001, October 2003, http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03tr001.pdf

[6] RFC 2350, Expectations for Computer Security Incident Response, N. Brownlee ,E. Guttman, June 1998, www.ietf.org/rfc/rfc2350.txt

[7] FIRST, http://www.first.org/

[8] APCERT, http://www.apcert.org/

[9] ENISA, http://www.enisa.europa.eu/

[10] TF-CERT , http://www.terena.org/activities/tf-csirt/