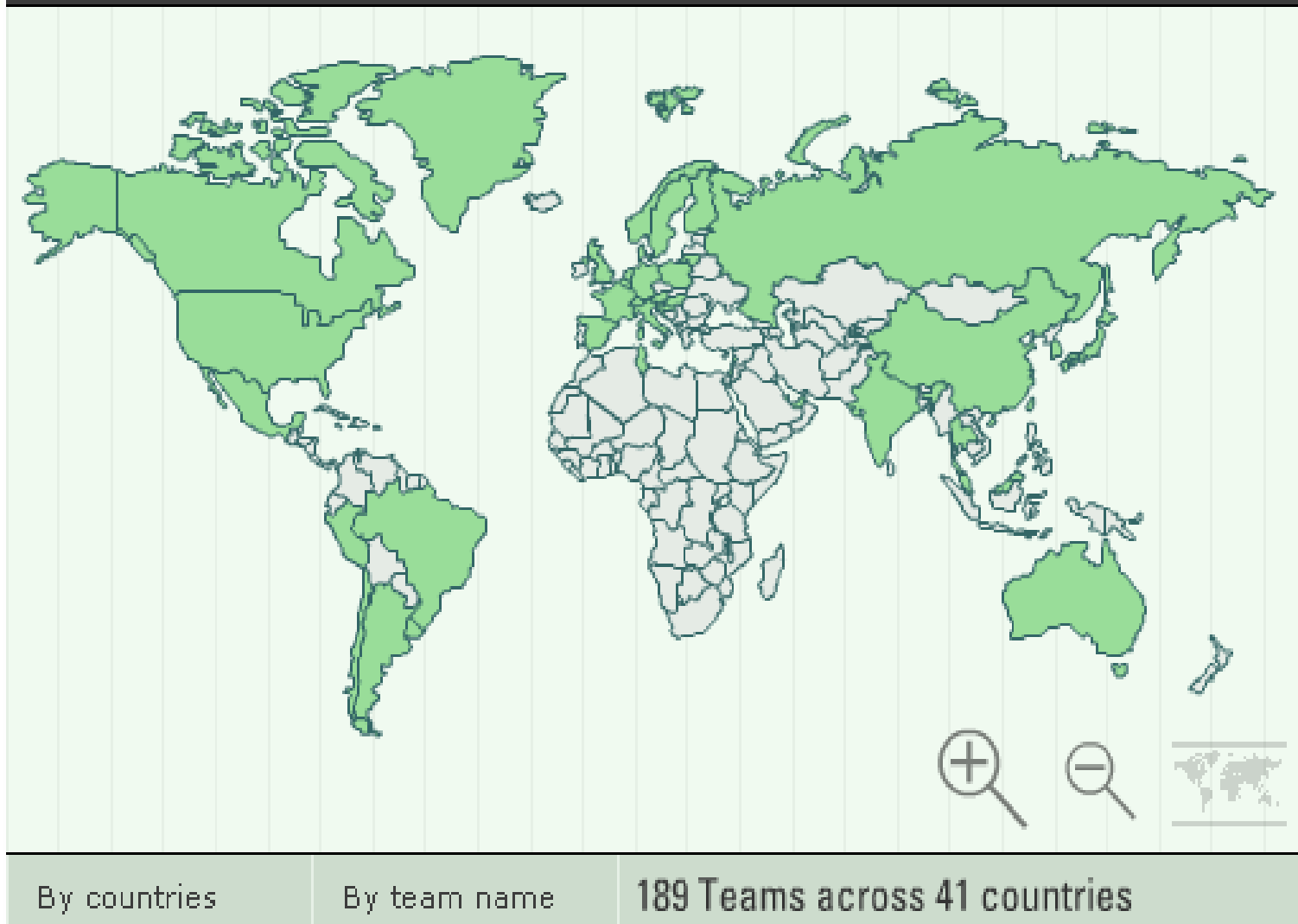




Promoting a Cybersecurity Culture: Tunisian Experience
ITU Regional Cybersecurity Forum for Eastern and Southern Africa
Lusaka, Zambia, 25-28 August 2008

Helmi Rais
CERT-TCC Team Manager
National Agency for Computer Security , Tunisia
helmi.rais@ansi.tn helmi.rais@gmail.com

FIRST Teams around the world

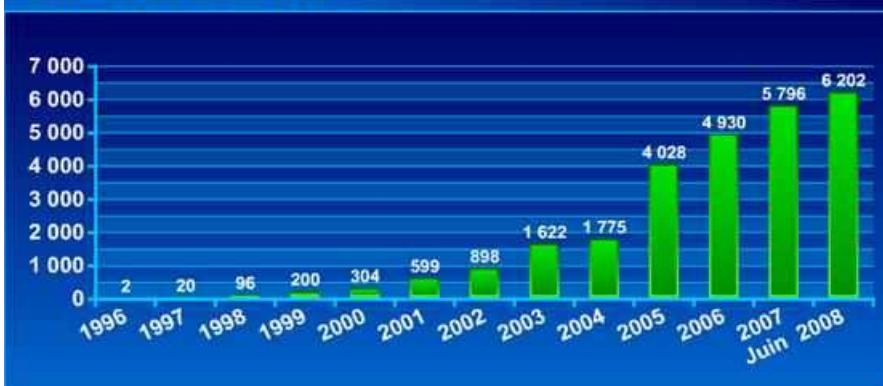


- The National Agency for Computer Security is the ICT Security Organisation in Tunisia (ICT Security Strategy, CIIP, ...)
- CERT-TCC is a sub-structure of the N.A.C.S
- CERT-TCC is the Gov Tunisian CERT
- CERT-TCC was created in 2004 (a micro-cert was in activity since 1999)
- CERT-TCC is the First african CERT
- CERT-TCC is a FIRST Member since 2007 (Forum of Incident Response and Security Teams)
- CERT-TCC is Secretary of OIC-CERT since 2006
- CERT-TCC is a CNUCED/UNCTAD Center of Excellence (UN)

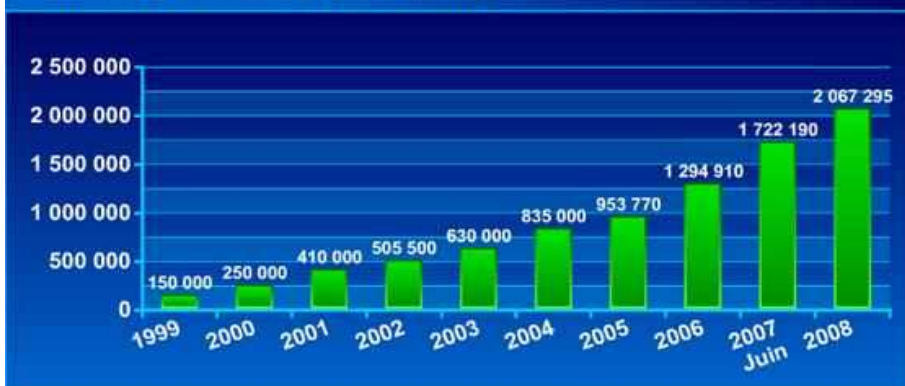
ICT in Tunisia: Statistics

Source: infocom.tn

Nombre de sites web



Nombre d'utilisateurs d'Internet

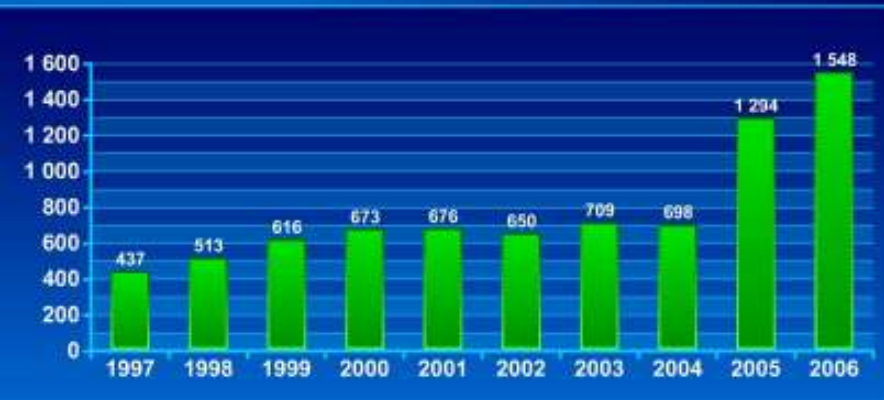


ICT in Tunisia: Statistics

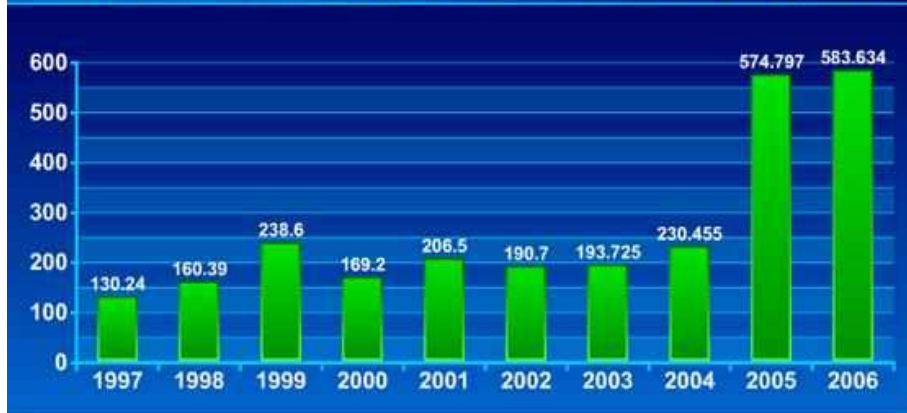
Source: infocom.tn

www.ansi.tn
cert-tcc@ansi.tn

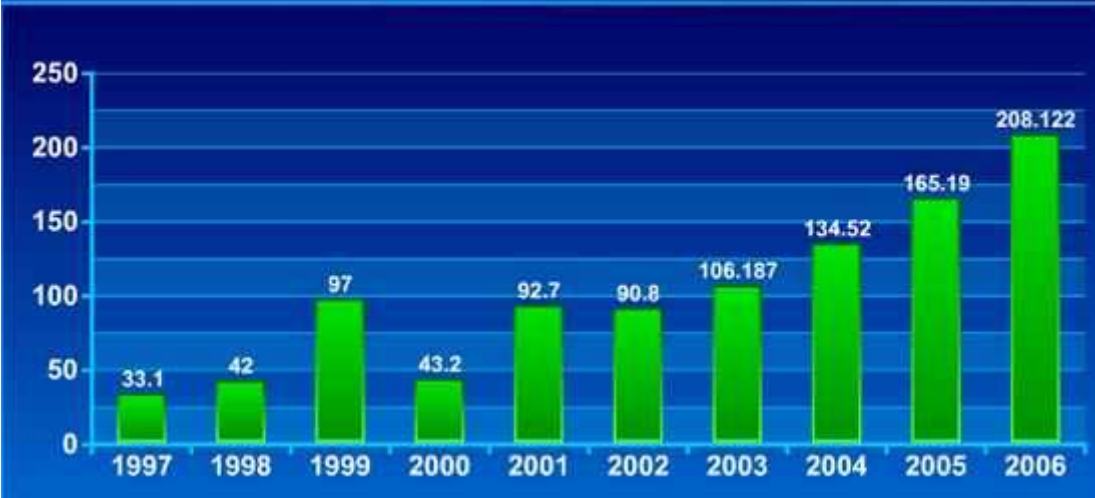
Nombre de SSII



Chiffre d'affaires déclaré par les Sociétés Informatiques (en MDT)



Chiffre d'affaire déclaré par les Sociétés de Services en Ingénierie Informatique (en MDT)



Promoting a cybersecurity culture Tunisian Experience

Lack of Awareness :

Necessity of a pragmatic approach :

- Raise Awareness of Politicians and policy-makers
- + Provides Funds (Loans, donation via “AID” programs)& Technical Assistance,

→ Launch of “Nucleus” of local CERTs,

Which provides a first “Nest” of local experts, which will be in charge of :

→ raising awareness of IT Managers & administrators,
whom will be the task force in charge of “Attacking” IT users
& Finally, the broad Population, by a progressive approach (with
care to not frightening).

→ Establishing a National strategy and plan for treating cyber-security
issues, accordingly to the state of development of each country.

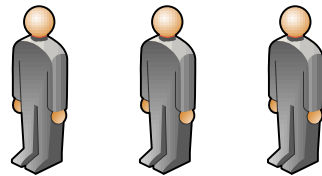
Lack of Experts

-Necessity to help the Set-Up of a first Task-force of local Experts → Need for training

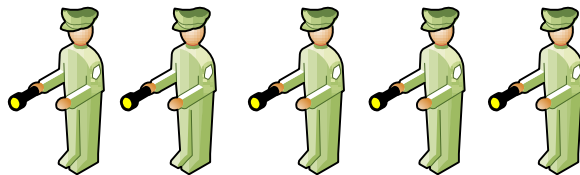
Lack of “Money”

- Search for Funds, loans (World Bank)
- Focus on Open Source Solutions

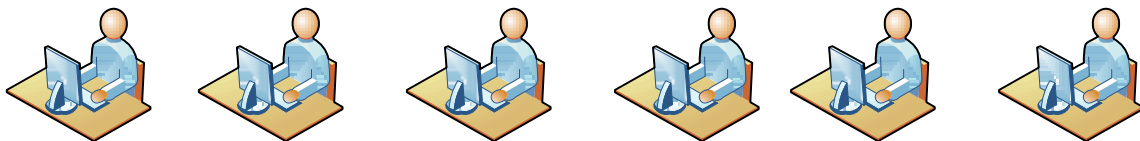
Concerned Communities



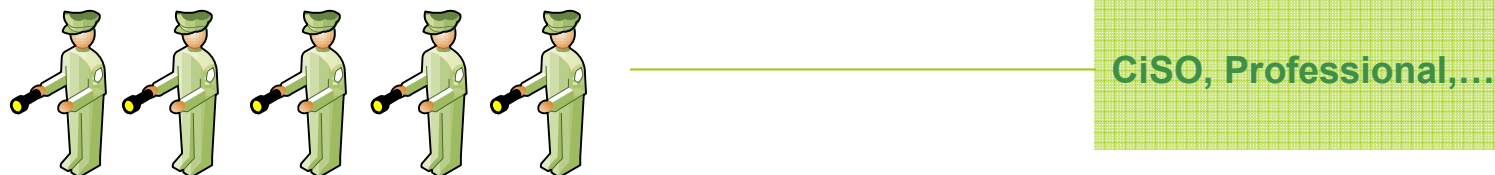
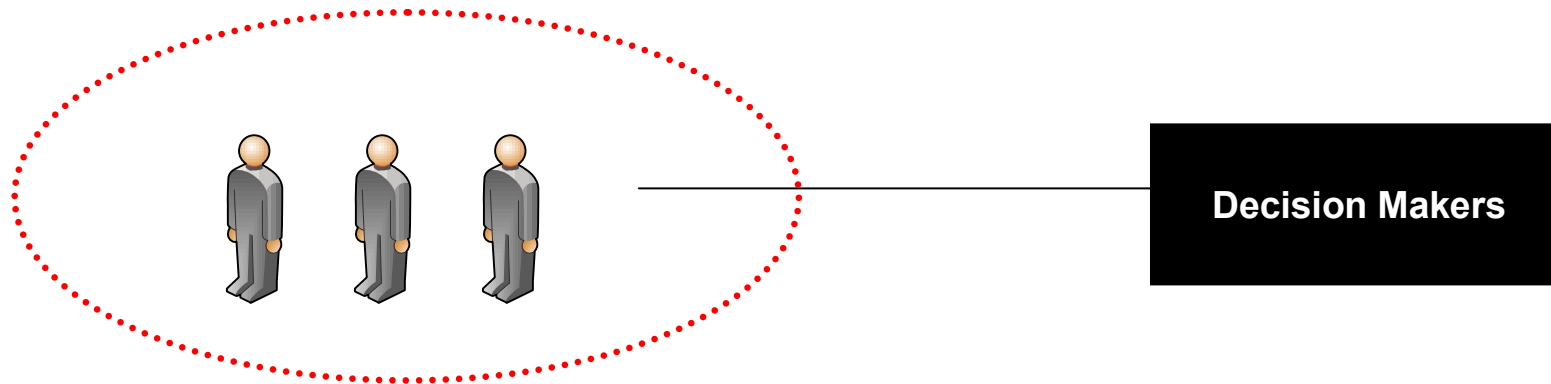
Decision Makers



CiSO, Professional,...



Internet Community



- Decision Makers are key persons for promoting IT Security culture
- CERT-TCC has made different awareness actions with Ministers, CEOs, Bank Managers...
 - Government General Secretary
 - Ministers of Communication Technologies, Social Affair...

-“Hacking Exposed” **demonstration** of attacks for Decision Makers → get in touch with **reality of risks**)

Hacking Simulation

Trojans

Vulnerability Exploits

Phishing attacks

XSS

SQL Injection

Password Sniff

In addition of existent Laws :

- Ø Law on protection of **Privacy and Personal data** (Law n° 2004-63)
- Ø Law on **Electronic Signature and e-commerce** (Law N° 2000-83)
- Ø Law **Against Cyber-Crimes** (Law N° 1999-89, Art 199)
- Ø Law on consumer protection and respect of Intellectual property (Law N°1994-36)

✓ February 2004 : **Promulgation of an “original” LAW, on computer security**
(Law N° 5-2004 *and 3 relatives decrees*) :

Obligation for national companies (ALL public + “big” and sensitive private ones) to do **Periodic (Now annually) Security audits of their IS.**

➤ **Organization of the field of Security audits**

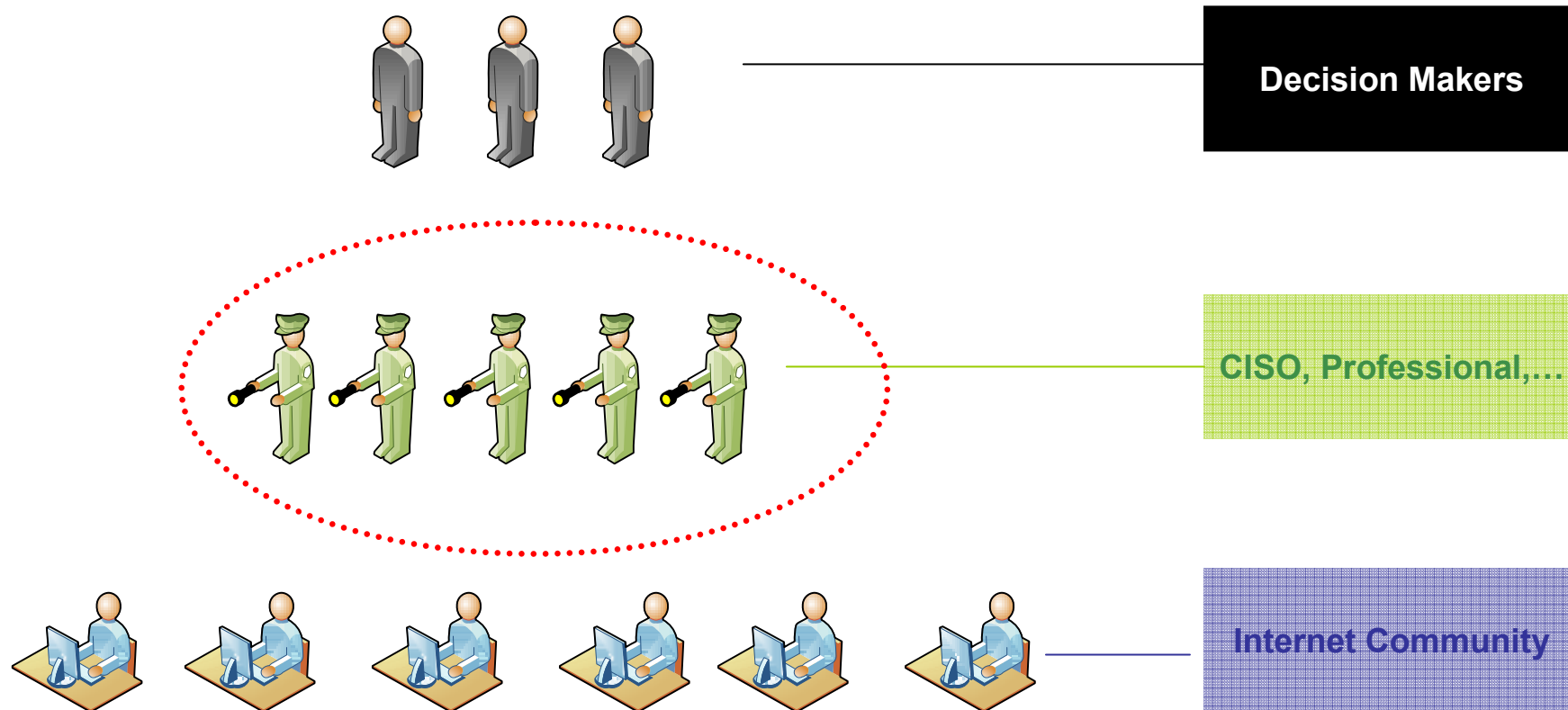
- Audits are Made by **CERTIFIED auditors** (*from the private sector*).
- *definition of the process of certification of auditors*
- *definition of the auditing missions and process of follow-up (ISO 1 77 99)*

➤ **Creation and definition of the Missions of the National Agency for Computer Security (which does not deal with National Security & Defense issues)**

(created under the **Ministry of Communication Technologies**)

➤ **Obligation to declare** security Incidents (Viral, mass hacking attacks, ..)
that could affect **others IS**, with guarantee of **confidentiality**, by law.

Concerned Communities



Information & Assistance

To increase awareness of security issues and help organizations to improve the security of their systems, we collect and disseminate information through multiple channels (mailing-lists, Web site, brochures and Knowledge bases, News).

More than 30 Guides and Manuals

Open Source Solutions

Best Practices (Processes, Procedures...)

Security Policy

Security Chart

Technical Documents / Tips (Configuration, deployment...)

Technical specification models for security solution acquisitions

Tender of offers for Security Audit Missions

Tender of offers model for IT Security Consulting Mode)

- CISO's Day (More than 140 CISOs)
 - New attack Technics, IT Security Technologies, Procedures, Tools
- IT Security Auditor's Day (More than 160 Auditors)
 - Standards, Methodologies, Inquiries, Problems...
- Software Developers Day (2009)
- CERT-TCC Forum (end 2008)
 - Share Knowledge, Experiences
 - Update the Collaboration Network
 - Improve Coordination procedures

Promoting Open Source Solutions

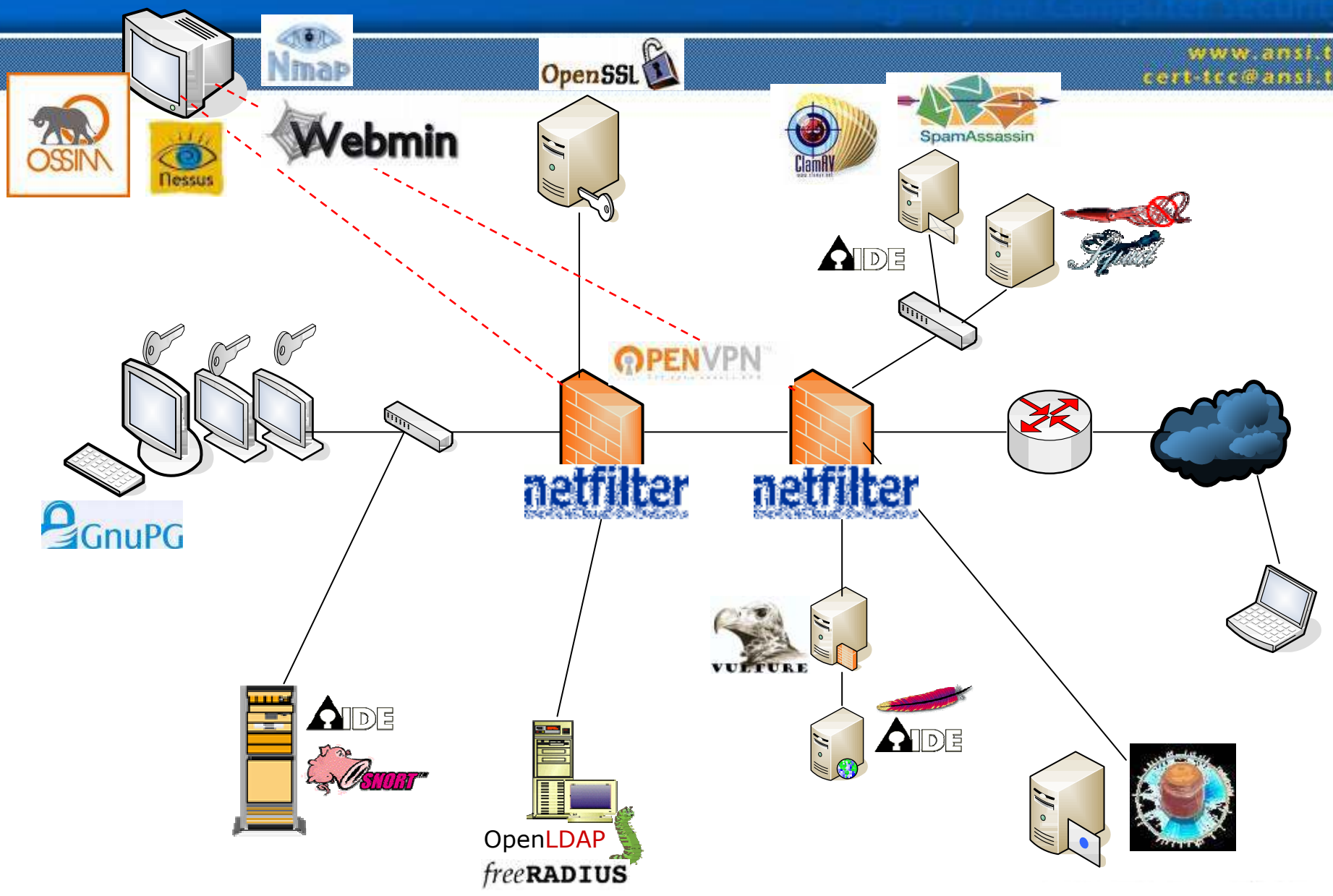
- Acting in **Raising awareness about the benefits (&limits) of the deployment of open-source tools.**
- Formulation (funds) of **4 projects for the development of security tools (from open-source) for the private sector** (including improvement of the system "Saher"). **(350 000 \$)**
- Definition of **5 federative projects of Research&Development for academic laboratories** (under the supervision of the **Ministry of Scientific Research**)
- Collaboration, with the university for the launch of a **Research laboratory** specialized in open-source security tools (Loan from the World Bank).

CERT/TCC is Acting for sensitizing young investors (by providing "Markets"),to:

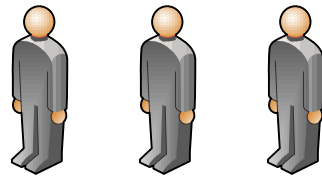
First Step : Provides support for open-source tools deployment (installation, training, "maintenance")

Then → Customization of open-source solutions (for clients specific needs)

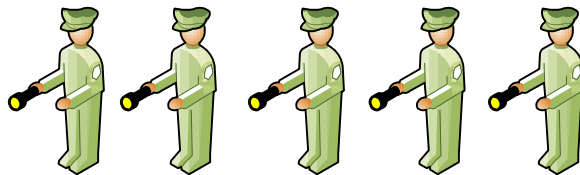
End → Launch of real **Research/Development activities**



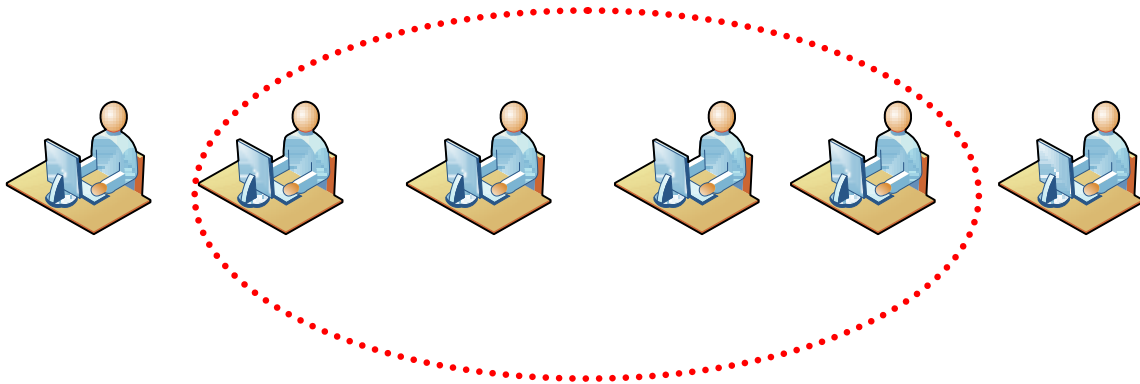
Concerned Communities



Decision Makers



CSO, Professional,...



Internet Community

Awareness Activities

- **Publications** : we also reproduce or develop and publish free electronic publications (guides, ..), to show administrators how to protect systems and networks against malicious and inadvertent compromise.
- **Presentations** : We organize and regularly give presentations at conferences, workshops, and meetings, as an excellent way to help attendees to learn more in the area of network information system security.



4 awareness
cdroms



8 aw
booklets



2008 Tips
Calendar



➔ Pensez à **sauvegarder** vos données, régulièrement et en lieu sûr !

La valeur de vos données perdues est souvent inestimable.

✉ assistance@ansi.tn



Pour déclarer vos incidents de sécurité: incident@ansi.tn
Pour avoir une assistance: assistance@ansi.tn
Pour vous abonner à notre mailing liste: abonnement@ansi.tn

A Votre Service 24h/24 et 7j/7



www.ansi.tn



N° Vert 80 100 267
Call -Center: 71 843 200



94 Av Jughurta
Mutuelle Ville 1002, Tunis



Un **incident de sécurité** est comme un iceberg,

la **partie apparente** ne reflète pas toute la mesure de son impact.

Déclarez-le !

✉ incident@ansi.tn



Pour déclarer vos incidents de sécurité: incident@ansi.tn
Pour avoir une assistance: assistance@ansi.tn
Pour vous abonner à notre mailing liste: abonnement@ansi.tn

A Votre Service 24h/24 et 7j/7



www.ansi.tn



N° Vert 80 100 267
Call -Center: 71 843 200



94 Av Jughurta
Mutuelle Ville 1002, Tunis

IT Security Awareness Posters

Awareness Activities

- **Media information** : We also work with the news media, and give them the necessary information material and support to raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves.
- **Press-Relations position** in CERT/TCC (a journalist, which prepares and provides Material to Journalists : motivation ..)



Weekly participation in 8 National Radios



Participation in 1 TV Program 2 Times per Month

الوكالة الوطنية لتسيير المعلوماتية تنشر من الرسائل الإلكترونية المشوهة الوهماء بالقرص يبيع مائة ألفاً
 تلقى مؤخراً العديد من مستعملي البريد الإلكتروني رسائل الكترونية من مصادر اجنبية ذات محتوى كاذب توهم الملتقى ببيع مبالغ هائلة كالمسحوق وتحتل على تقديم معلومات خاصة للحصول على الربح المزعوم.

وتنشر الوكالة الوطنية لتسيير المعلوماتية في هذا الصدد من الاجابة عن جميع هذه الرسائل الالكترونية المشوهة ومن الافلاء بمعلومات خاصة مثل الاسم واللقب ورقم الحساب البنكي وغيرها من المعلومات الشخصية التي تقول القائمو بعروضات تلاعب وتحويل وتلتصق على مزيد من التوضيحات الاتصال بالوكالة الوطنية لتسيير المعلوماتية عبر البريد الإلكتروني: assistance@ansi.tn

... la production culturelle on et gratitude de l'Utap culteurs au Chef de l'Etat

(Lire en page 4)

... les grandes
 de la présidence
 çaise de l'Union
 péenne, qu'ils w
 modernet part
 tive, en phase a
 temps". Egalém
 l'étude, l'idée d'u
 férié européen f

Alerte informatique

Un virus virulent et dévastateur nommé « Hoax »

Ce virus en circulation depuis mars dernier est capable de brûler le disque dur de l'ordinateur

L'Agence nationale de la sécurité informatique informe qu'un faux message électronique intitulé "Invitation" sur la circulation d'un virus dangereux "Hoax" a été retransmis au niveau national et international et qui risque de brûler le disque dur de l'ordinateur.

L'agence avait mis en garde, plusieurs fois, contre la diffusion du virus "Invitation", à partir du mois de mars 2006, à travers un e-mail émanant de l'équipe de réponse aux urgences informatiques (cert-Tcc) sur le site Internet www.ansi.tn

Elle a également recommandé la non-transmission à d'autres personnes d'autant que l'objectif de ces faux messages d'alerte est de semer la panique et d'engorger les serveurs e-mail.



Mesures présidentielles relatives aux grandes cultures
 Les éléments d'une stratégie de réajustement



La Presse Once Plan

Le Centre de la Presse (CPC) a organisé une conférence de presse le 13 mai 2008, à l'occasion de la signature de l'accord de coopération entre le Centre de la Presse et l'Agence Nationale de la Sécurité Informatique (ANSI) pour la lutte contre les virus informatiques. L'objectif de cette conférence est de sensibiliser le public sur les dangers des virus informatiques et de promouvoir les mesures de sécurité à adopter.

Une conférence de presse a été organisée le 13 mai 2008, à l'occasion de la signature de l'accord de coopération entre le Centre de la Presse et l'Agence Nationale de la Sécurité Informatique (ANSI) pour la lutte contre les virus informatiques. L'objectif de cette conférence est de sensibiliser le public sur les dangers des virus informatiques et de promouvoir les mesures de sécurité à adopter.



Agence Tunis Afrique Presse

Mardi, 20 Juin 2008

rapport national sur les Droits de l'homme

informatique-virus

Faux message d'alerte contre un virus informatique dangereux

TUNIS, 13 mai 2008 (TAP) - L'Agence nationale de la sécurité informatique (ANSI) informe qu'un faux message électronique intitulé "Invitation" sur la circulation d'un virus dangereux "Hoax" a été retransmis au niveau national et international et qui risque de brûler le disque dur de l'ordinateur.

L'agence avait mis en garde, plusieurs fois, contre la diffusion du virus "Invitation", à partir du mois de mars 2006, à travers un e-mail émanant de l'équipe de réponse aux urgences informatiques (cert-Tcc) sur le site Internet www.ansi.tn

Elle a également recommandé la non-transmission à d'autres personnes d'autant que l'objectif de ces faux messages d'alerte est de semer la panique et d'engorger les serveurs e-mail.

L'ANSI met à la disposition du public le centre Cert-Tcc qui assure l'encadrement et le soutien en matière de sécurité informatique 24 heures sur 24, tous les jours de la semaine, à travers le numéro de téléphone vert et gratuit 80100207 au profit du public et d'un numéro d'appel 71843200 au profit des professionnels.

A noter qu'il est possible de s'abonner à la base des données de la poste électronique pour être au courant des nouveautés en matière de sécurité informatique, à l'adresse suivante: a@ansi.tn ou abonnement a@ansi.tn

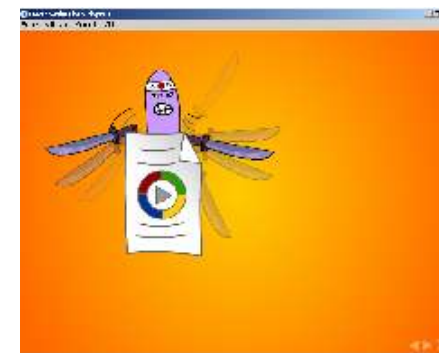
Liens utiles

La Présidence de la République
 Institutions Publiques

Bulletin Régional



- Acts for raising **Youth and parents awareness** ,In Collaboration with specialized centers and associations :
 - Preparation of a first pack of short (awareness) courses for Primary school.
 - Starts the Development of special pedagogical material for childrens&parents : 3 “Cartoons”, Quizzes
- Development of a special rubric in the Web site and Inclusion of a special Mailing-List rubric for parents (Parental control tools, risks, ..)
- **Development of special awareness tools (Cdroms, Cartoons, Games, Booklets...)**



- CONSEILS POUR LA FAMILLE
- OUTILS DE CONTRÔLE PARENTAL
- GUIDES POUR LA FAMILLE
- SECURITE INFORMATIQUE
- PASSEPORT DE SECURITE
- QUIZ POUR ENFANTS
- F.A.Q POUR ENFANTS
- LIENS UTILES

Computer Emergency Response Team
Tunisian Coordination Center

Parents et enfants



- DESSINS ANIMÉS
- Dessin 1
 - Dessin 2
 - Dessin 3
 - Dessin 4
 - Dessin 5
 - Dessin 6

Accueil > Parents et Enfants

 Sécurité informatique pour la famille

 Outils de contrôle parental

 F.A.Q pour enfants

ALERTE NATIONALE

25.09.2007
Risque Bas

 Conseils pour la Famille

 Liens utiles

 Guides pour la Famille

MAILING LIST DE SECURITE

Entrez votre adresse email

OK

 Passeport de sécurité pour la famille

QUIZZ Quiz pour enfants

 Dessins animés

Google Insights Stats

Search Volume: virus

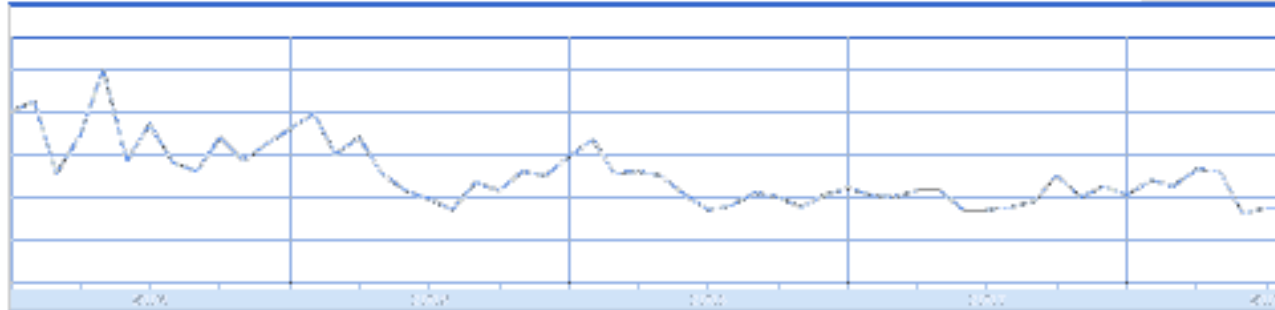
Tunisia, 2004 - present

virus

Interest over time

News headlines: [Show](#) [Hide](#)

[How can I see numbers?](#)



Regional interest for virus

[Subregion](#) [City](#)

Search Volume: faille

Tunisia, 2004 - present

faille

Interest over time

News headlines: [Show](#) [Hide](#)

[How can I see numbers?](#)



Regional interest for faille

[Subregion](#) [City](#)

Education and Training

Collaboration with academic institutions for :

-Developing Masters in IT security : (Now, A master degree in IT security permits the certification of IT Security Auditor)

- In 2004 : Launch of the first Master in IT security (Collaboration between two universities).
- In 2008 : 7 masters (3 publics & 4 privates universities/ 1 Regional).

- Introduction of security modules (awareness) inside academic and education programs.

- Universities
- Elementary Schools (in progress)

- Establishment of a Task Force of Trainers in IT Security.
 - Launch of training courses for trainers (private sector)
 - 4 Train Courses organized since 2005 (Loan of the World Bank)
 - Preparation of 4 additional training courses for trainers in 2008-2009 (Loan of the World Bank)
 - Encourage private sector to organise Advanced IT Security Trainings (CISSP, CISA, CEH, ITIL...)



Other Training Activities

- Decision Makers
- CISOs
- Professionals
- Auditors
- Developpers
- Students
- Home Users
- Journalists
- Judges and Law Enforcement Staff

- The first identified topics (trainees courses) are the following :
 - Network perimeter security technics (Secure architectures, Firewalls, IDS, secure dial-up servers, content gateways and proxies, ..) .
 - Internal Network security organization and technics (security policy development, security plan development, tools : Distributed firewalls, Anti-virus gateways, PKI, ..).
 - Secure application development and hosting technics
 - Information Survivability technologies (disaster recovery plans)
 - Technical basis for intrusion prevention (identifying and preventing intrusions and security flaws).
 - Fundamentals of Incident Handling and overview of a Computer Security Incident Response Team
 - Creating and Managing a Computer Security Incident Response Team
 - Methodologies of security self-assessment.
 - ISO 27001, 27002,...
 - CBK course. (Physical Security, Telecom and Network Security...)
 - Specialized courses for military, judicial and investigation staff

Induction of Synergy Between National actors

Motivates the creation of specialized Associations in IT security :

- An **academic** association was **launched** in 2005: “Tunisian Association for Numerical Security”.
 - A **professional** association : “Tunisian Association of the Experts in Computer Security”.
- In project : An **association of ISPs**

-Organisation of awareness actions with different associations over the country (ATIM, ATSN, JCI, ATAI, ...)

- More than 20 national seminars and workshops per year

- Participation to the National Internet Festival

● Awareness Actions
2007-2008



Motivation (funds) for the Development of Self-assessment methodologies (adapted to our STEP) & Guides of Best Practices

Implication for the Development of Models of books for Tender of offers (Insures Fair concurrency → attracts more private investments in the field)

- Publication of a “Model for tender of offers” for **Risk Assessment operations**
(With consultation and **validation** of the private sector)
- Development of Models of books for tender of offers for
 - Commercial** Security Tools acquisition (Firewalls, IDS,)
 - Open-source** Security tools deployment (Training, assistance)

Implication for Evaluation of actions & Revision of Action Plans

- Realization of **National Surveys** about IT Security
(A survey is planed for end 2007, with participation of the 2 associations)



Thank you for your attention