Fast overview about the CERT-TCC

Helmi Rais
CERT-TCC Team Manager
Helmi.rais@ansi.tn
FIRST Teams around the world

By countries | By team name | 189 Teams across 41 countries
Les IT en Tunisie: Quelques Statistiques

Le nombre d'ordinateurs à l'échelle nationale

<table>
<thead>
<tr>
<th>Année</th>
<th>Nombre d'ordinateurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1997</td>
<td>128,149</td>
</tr>
<tr>
<td>1998</td>
<td>153,967</td>
</tr>
<tr>
<td>1999</td>
<td>196,816</td>
</tr>
<tr>
<td>2000</td>
<td>207,874</td>
</tr>
<tr>
<td>2001</td>
<td>255,245</td>
</tr>
<tr>
<td>2002</td>
<td>335,325</td>
</tr>
<tr>
<td>2003</td>
<td>400,372</td>
</tr>
<tr>
<td>2004</td>
<td>472,132</td>
</tr>
<tr>
<td>2005</td>
<td>568,106</td>
</tr>
<tr>
<td>2006</td>
<td>634,840</td>
</tr>
</tbody>
</table>

Nombre d'utilisateurs d'Internet

<table>
<thead>
<tr>
<th>Année</th>
<th>Nombre d'utilisateurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>150,000</td>
</tr>
<tr>
<td>2000</td>
<td>250,000</td>
</tr>
<tr>
<td>2001</td>
<td>410,000</td>
</tr>
<tr>
<td>2002</td>
<td>505,500</td>
</tr>
<tr>
<td>2003</td>
<td>630,000</td>
</tr>
<tr>
<td>2004</td>
<td>835,000</td>
</tr>
<tr>
<td>2005</td>
<td>953,770</td>
</tr>
<tr>
<td>2006</td>
<td>1,294,910</td>
</tr>
<tr>
<td>Mars 2007</td>
<td>1,446,000</td>
</tr>
</tbody>
</table>
end 1999: Launch of a UNIT (a “Micro-CERT”), specialized in IT Security

Objective:
- sensitize policy-makers and Technical staff about security issues.
- Assists in Monitoring the security of highly critical national applications and infrastructures.
+ creates a first Task-force of Tunisian Experts in IT Security

From End 2002 (“certification of the role of IT security as a pillar of the « Information Society ») :
- The unit starts the establishment of a strategy and of a National Plan in IT Security
  (national survey, for fixing: priorities, volume of actions, needed logistic, supporting tools, ...).

January 2003:
- Decision of the Council of Ministers, headed by the President, and dedicated to informatics and IT Security, of:
  - The creation of a National Agency, specialized in IT Security
    (The Tool for the execution of the national strategy and plan)
  - The Introduction of Mandatory and Periodic Security audits
    (Pillar of our strategy)
  - The creation of a “body of certified Auditors” in IT Security

+ A lot of accompanying measures (launch of masters in IT security, ...)
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.
• CERT-TCC is a sub-structure of the National Agency for Computer Security

• CERT-TCC is the Gov Tunisian CERT
Services Provided

• Information and alert
• Education and awareness
• Enterprise support (security self-assessment)
• Electronic Surveys on security and Participation in International organizations
• Training
Threat alert:

- Analyse the state of Internet security and convey that information to the system administrators, network managers, and wide public in the Internet community.

- Monitor sources of vulnerability information and regularly sends reports and alerts on those vulnerabilities (mailing-lists, publication on the web site).

- We analyze the potential vulnerability and try to work with other CERTs and technology producers to track the solutions to these problems. We also make vulnerability information widely available through a vulnerability database.
630 Vulnerabilities published in 2007
25 Malwares published in 2007
13 Minor Alerts in 2007

• Microsoft Word 0day (CERT-TCC/Vuln.2007-045)
• Sun Solaris Worm (CERT-TCC/Vuln.2007-66)
• Microsoft Windows DNS Service (CERT-TCC/Vuln.2007-190)
• Firefox et Netscape Navigator 0day (CERT-TCC/Vuln.2007-368)
• Propagation of "Storm Worm" "Zhelatin.LJ (CERT-TCC/MAL-2007-009)
• RSTP QuickTime Vulnerability (CERT-TCC/Vuln.2007-577)

• Netmonster : The First Virus « made in Tunisia » (CERT-TCC/Malw.2007-023)
• More than **7000 Voluntary** subscribers

• More than **800** calls Monthly served

• More than **600** e-mails sent Since 2005
  – Vulnerabilities
  – Malwares
  – Spam & Hoax
  – Open Source
  – Books
  – Tools
  – Announces
Information:

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, World Wide Web site, brochures and Knowledge bases, News).

More than 30 Guides and Manuals

Home Users
Open Source Solutions
Best Practices
Security Policy
Security Chart
Technical Documents / Tips
Technical specification models for security solution acquisitions
Tender of offers for Security Audit Missions
Internal Workflow Solutions

Vulnerability and Malware Database into CERT-TCC Back Office Website

RSS Reader, Filter, Task Management

→ Free and Open Source

Vulnerability and Malware Database into CERT-TCC Back Office Website
• Decision Makers
• CSOs
• Professionals
• Technicians / Engineer
• Trainers
• Students
• Tunisian Cyber Community
• Home Users
• Journalists
• Jurists

Hacking Simulation
Trojans
Vulnerability Exploits
Phishing attacks
XSS
SQL Injection
Password Sniff
• **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.

• **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.

• **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.
Services Provided

Youth and Parents Awareness

- 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...)**
- 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”).

- 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**
Our urgent and big problem is the present lack of specialized experts and trainers in the various fields of information system security. This CERT is first concentrated on the organization of trainings (in Tunisia and in International institutes) for trainers in the field of specialized Information systems security trends and also for the judicial and investigation staff.

Afterwards, we organize very specialized training courses in Tunisia (and some in foreign centers) for technical staff and managers of computer security incident response teams as well as for system administrators of highly critical systems.
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, ..).

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 17799 and ISO 27000 Families.

Wireless Security

CBK Security

Open Source Solutions

Intergrating Security into SDLC

Specialized courses for judicial and investigation staff
Incident handling and assistance

CERT/TCC provides:

- A CSIRT team in charge of providing (free of charge) Assistance for Incident Handling
- Call-center, available 24Hours/24 and 7 days/week

**Article 10** of the Law No. 2004-5 relative to IT security
(Public & Private institutions, must inform the National Agency for Computer Security about any Incident, which can affect other Information Systems)

**Article 9** of the Law No. 2004-5 relative to IT security Stipulate that The employees of the National Computer Security Agency and security auditors are Responsible about the preservation of confidentiality and are liable to penal sanctions

→ Private and public organizations should trust the CERT/TCC
→ Call for assistance

- A “Citizen’s assistance service”, To which Home users can bring their PC to solve security problems or install security tools (anti-virus, PC firewall, anti-spam, ..), free for domestic use.
- Acting for the emergence of corporate CSIRT in some sensitive sectors (E-gov, E-Banking → Energy, Transportation, Health )
Computer forensics
Evidence analysis
Investigation (Log, Hard Drive, memory dump, …)
On-site
Incident handling process
Evidence collection
A Watch-center (based on open-source solutions), which permits to monitor the National Cyber-Space security in Real time

→ For the early Detection of potential threats and evaluation of their impact.
(First prototype, deployed at the level of ISP, during phase 2 of WSIS)

→ For Vulnerabilities exploitation and malwares propagation evals
Saher – Web: Tunisian Web Sites monitoring

Saher – SRV: Internet services availability monitoring (Mail server, DNS, ...)

SAHER–IDS: Massive attack detection

- Web defacement
- DoS Web
- Deterioration of web access
- ...
- Mail Bombing
- Breakdown of DNS servers
- DNS POISONING...
- Viral attack
- Intrusion
- DDoS
- ...

System developed based on a set of Open Source tools
Event Gathering Database

Gathering and Filtering of large sets of network data to identify unauthorized and potentially malicious activity (Worms, attacks, scans ...).

- Intrusion Detection
- Anomaly Detection
- Traffic Analysis

Corporate Networks

IDCs

ISP

Darknet

Vuln. Exploit. Evaluation

Malw. Propag. Evaluation

Critical Node Monitoring (Integrity, Availability)

Web, Pop, SMTP, DNS

Log Correlation Server

Automatic Alert-Triggers
Scripts for Traces Correlation.
- Trace Tools.
- Scripts for “Smart Honey-Potting”
- Technical proactive and Counter-measures.

National Reaction Plan

Alerting the Community

Gathering and Filtering of large sets of network data to identify unauthorized and potentially malicious activity (Worms, attacks, scans ...).
NRP
National Reaction Plan
- “Formal” Global Reaction Plan.
- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Access Providers).

With CERT/TCC acting as a **coordinator** between them.
was deployed 7 times,

During Sasser & MyDoom worms attack, during suspicious hacking activity and, proactively, during big events hosted by Tunisia (only with ISPs and telecommunication operator)

ONU Conference about Terrorism