Incident Response and FIRST

We all need CSIRTs in Africa

David Crochemore - Member of the FIRST Steering Committee - David@crochemore.org

AFNOG Conference - May 23rd, 2004 - Dakar, Senegal

Agenda of the Presentation

1. Security of Information Systems
2. Security Incidents and Incident Response
3. What is a CSIRT (aka CERT)
4. The FIRST (Forum of Incident Response and Security Teams

Security of Information Systems

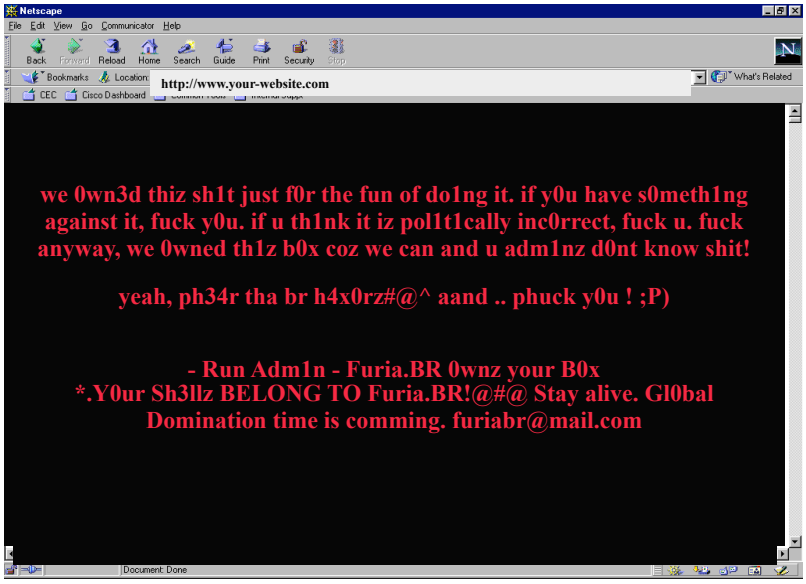
Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

in WSIS *Declaration of Principles*, Geneva, December 2003

Confidentiality

Revealing the information in the system is prohibited

Integrity



Modifiying the information is prohibited

Availability

The information is available whenever it is authorized

Mafiaboy
February 2000

Security Incidents and Incident Response

Need to keep in Mind

1. Any Operating System or software has bugs
2. There are a lot of websites providing tools to exploit those bugs

The Threats

- Root Compromise
- Port Scans
- Spam Relay
- Denial of Service
- Web Defacement
- Warez
- Viruses/Worms

Why respond to a Security Incident?

To limit the Impact

1. Loss of Data

   Research and Development, Databases, etc...

2. Loss of Time

   Time to restore, Time of work lost, Time to explain

3. Loss of Production

   Business stopped

4. Loss of Fame

   Not only for the Banks

The Need for Incident Response

1. a general increase in the number of computer security incidents being reported
2. a general increase in the number and type of organizations being affected by computer security incidents
3. a more focused awareness by organizations on the need for security policies and practices as part of their overall risk-management strategies
4. new laws and regulations that impact how organizations are required to protect information assets
5. the realization that systems and network administrators alone cannot protect organizational systems and assets

from http://www.cert.org/csirts/Creating-A-CSIRT.html

What is a CSIRT?

A Computer Security Incident Response Team (CSIRT) is a team that coordinates and supports the response to security incidents that involve sites within a defined constituency.

In order to be considered a CSIRT, a team must:
- Provide a (secure) channel for receiving reports about suspected incidents.
- Provide assistance to members of its constituency in handling these incidents.
- Disseminate incident-related information to its constituency and to other involved parties.

in RFC 2350 *Expectations for Computer Security Incident Response*

What does a CSIRT do?

Preventive Role

- Information Providing
- Technology Watch
- Vulnerability Analysis
- Risk Analysis
- Training
- Security Audit
- Tools Development

Curative Role

- Point of contact
- (Consolation)
- Incident Resolution
- Coordination
- Post-mortem Analysis
- Restarting
- Legal Information

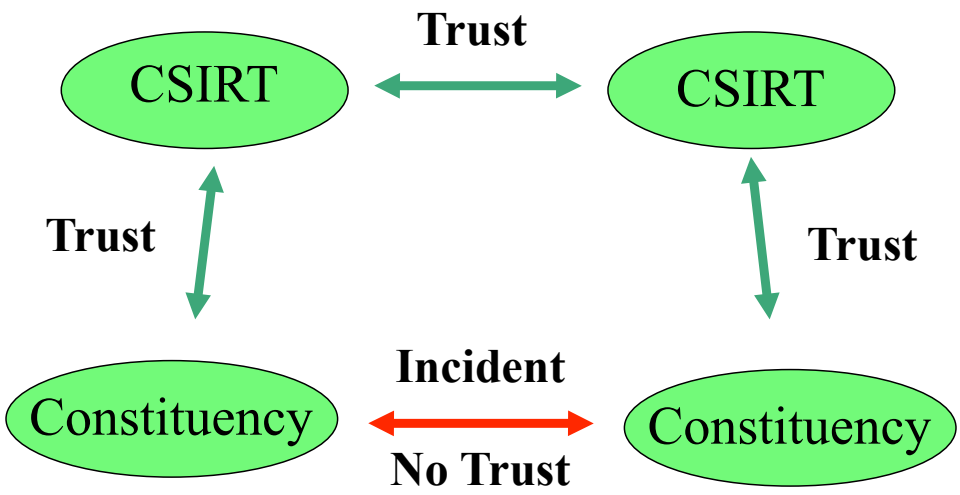
Why a CSIRT for an ISP?

Whether or not an ISP has a CSIRT, they should have a well-advertised way to receive and handle reported incidents from their customers.

In addition, they should clearly document their capability to respond to reported incidents, and should indicate if there is any CSIRT whose constituency would include the customer and to whom incidents could be reported.

in RFC 3013 *Recommended ISP Security Services and Procedures*

Trust is a Key Issue



The FIRST

Forum of Incident Response
and Security Teams

What is FIRST?

Forum of Incident Response and Security Teams (FIRST), brings together a variety of CSIRTs from government, commercial, and academic organizations.

FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

Created in 1990, FIRST has currently more than 150 members, from more than 30 countries

The Missions of FIRST

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

What does FIRST do?

- **FIRST Annual Conference** (open to anyone)

  June 13th-18th in Budapest Hungary

  http://www.first.org/conference/2004
- **Technical Colloquium** (for members only)

  with Hands-On Classes, twice a year
- **FIRST Best Practice Guide Library**
- Closed **Mailing Lists** (for members only)
- **Training Program**

  Ongoing Project in Asia-Pacific and Latin America (why not Africa in the future?)
- Other projects (Research, Outreach)

What have I been here for?

1. Convince you that you need a CSIRT in your organization
2. Convince you that this CSIRT will need to join FIRST
3. Answer all the questions you may ask

Questions?

References

- **IETF Request for Comments** (http://www.ietf.org)
  - RFC 2350 - *Expectations for Computer Security Incident Response*
  - RFC 3013 - *Recommended ISP Security Services and Procedures*
- **Useful Documents**
  - *Handbook for CSIRTs* / Moira J. West-Brown ; Don Stikvoort ; Klaus-Peter Kossakowski. - http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf
  - CSIRT FAQ - http://www.cert.org/csirts/csirt_faq.html
- **Useful Web Sites**
  - http://www.first.org (FIRST)
  - http://www.cert.org (CERT Coordination Center)
  - http://www.certa.ssi.gouv.fr (in french)
  - http://www.rnp.br/cais/ (in portuguese)