INTECO-CERT

Jorge Chinea López

INTECO-CERT relations coordinator

January, 2009

26th TF-CSIRT Meeting
FIRST Symposium
What is INTECO?

1. What is INTECO?

✓ **State-owned company** attached to the MITT (Ministry of Industry, Tourism and Trade)
✓ Development **Instrument** of the IS
✓ Management, advice, promotion and circulation of **projects**
✓ **Main pillars**: applied research, rendering of services and training

**OBJECTIVES**

✓ **Convergence** of Spain and Europe
✓ **Technological transversality** between sectors and areas of ICT knowledge
✓ High localization of **intensive knowledge and connection** with other world centres
✓ **Create an “ICT Cluster“** in León (Spain) with high capacity for innovation
2. INTECO's strategical actions

- e-Trust (Security)
- INTECO-CERT for SME’s and Citizens
- Security Technologies Show-Room
- Information Security Observatory

- SW Quality
  - Quality’s National Laboratory.
  - Training.
  - Promote TI projects.
  - Promote standards and normalization.

- Accessibility
  - Spanish National Centre for Accessibility and web standards.
  - Spanish National Centre for Accessibility Technologies.
  - R&D area in Web Accessibility.
  - Center for Management of Interactive Public Services - DTT

- Citizens and Internet.
- Innovation TIC and SME competitiveness.
3. eTrust projects

- Establish the bases for the coordination of different public initiatives in the information security area.
- Promoting applied research and specialized training activities in the TIC security area.
- Become a national IT Security Reference Centre
Objetives

Â Increase the level of awareness in the security area promoting its use in a safe and responsible way.
Â Minimize the damage caused by security incidents, accidents or failures to provide mechanisms for prevention and adequate reaction.
Â Prevent, inform, raise awareness and educate the SME and the citizens by providing clear, concise information about technology and the state of Internet security.
INTECO-CERT security services: http://cert.inteco.es

**Information Services:**
- Subscription to security reports, alerts
- News, events, topical subjects.
- Alerts and bulletins about new online viruses, vulnerabilities, viruses spread by email, spam, etc.

**Training Services:** Tutorials, manuals, online courses.

**Protection Services:** free tools, software updates.

**Response and Support Services:**
- Security Incidents management.
- Malware infections.
- Phishing/eFraud attacks.
- Legal support.
- Security forums
TF-CSIRT/FIRST meetings

- Interchange Incidents / Contacts
- Share Information
- Interchange Experiences and Innovation
- Collaboration Projects
Interchange Incidents \ Contacts

Incidencias@cert.inteco.es

PGP: A230 1EE1 F521 19DE 10E7 8E09 00F9 7042 0DCB 42640

Cert@cert.inteco.es

PGP: C82C AF18 3C23 058A EA27 F1AB 1496 A4D7 B729 A0CD

jorge.chinea@inteco.es / jchinea@cert.inteco.es

javier.berciano@inteco.es / jberciano@cert.inteco.es

http://www.inteco.es/Seguridad/INTECOCERT/Acerca_de/RFC_2350

Share Information

See Contacts ;(-)
Interchange Experiences
Prevent, inform, raise awareness and educate the SME and the citizens

http://cert.inteco.es
Interchange Experiences
Technologies Security Show-Room.

✓ To promote the use of technologies related to security in Spanish entities.

Å Catalogue of IT security solutions and services, and promotes its development (590 providers and 1065 solutions and services).
Å Tests to security products.
Å To promote the international visibility of Spanish security technologies.

http://demostrador.inteco.es
Interchange Experiences
Standard ISO 27001 - ISMS Implementation at SMEs

http://sgsi.inteco.es
Collaboration Projects

Security Sensors Network (SPAM \ Virus).

- To provide information about malware detected in e-mails by antivirus software and SPAM detected by different tools.

- 170 organizations (administration, universities, ISP, hosting, etc.).
- The sensor network consists of regularly sending a summary of the virus/spam detection log.
- Official statistics about the spam / virus in Spain.
- To notify to Spanish ISP or CERT.

https://ersi.inteco.es
Collaboration Projects

Antifraud repository.

- Collects structured information of all types of fraud from detected fraud cases. (.es protocol).

- Detailed statistics of the cases detected.
- Correlation between resources and electronic services in various cases, targeted attacks, and so on.
- Study of the evolution of electronic fraud in Spain.
- Detection of new trends in fraud.
- Assessing about the fraud incidence to the user.

(Sorry, private access)
Collaboration Projects

CONAN (CONfiguration ANalysis)

✓ Collects information from a PC suspected of being modified by malicious code in order to determine whether the PC is infected or not configured correctly.

Security pro-active sensor network

- An application for malware detection (not to protect, only to advise).
- An application for vulnerable applications detection.
- An adviser of good practice in security.
- An assessment of the security status.
Collaboration Projects

**Jennings**

- Jennings is our self-made automated malware analysis system to help the CERT staff on malware research

(Sorry, private access) ñ > see you in Kyoto!