CERT-FI
First Five Years – and the Next Ten...

Erka Koivunen
Head of Division
CERT-FI

CERTs in Europe, Brussels
2006-10-05

Agenda

• Founding of Finnish National CERT

• CERT-FI Today
  • What’ve Achieved
  • Why we Need to Readjust

• Next Steps
Founding of CERT-FI

- Initial discussion in 2000 – 2001
  - Should a Nation Have a CSIRT Body? Why?
  - What Services Should National CSIRT Offer? To Whom?
  - Under What Authority Should National CSIRT be Placed?

- Sponsor Candidates for CERT-FI
  - Academia: Funet CERT was already established in 1995?
  - Intelligence: Finnish Security Police?
  - Defence: Finnish Defence Forces?
  - Ministry of Finance: Government IT Security (VAHTI)?
  - FICORA: TeleCom Regulator

CSIRT within FICORA

- DoB 2002-01-01

- Focus on Communications Networks and Services

- Regulatory Authority over TelCos
  - Special Legal Mandate
  - Mandatory Incident Reporting

- Some Services Accessible to all Citizens
  - Public Situational Awareness Services
  - Voluntary Incident Reporting
CERT-FI Today

What has been Achieved?

• Incident Response Service up 24/7/365

• (Mostly) Positive Domestic Media Coverage

• Good Connections to TelCos and ISPs

• Credible and Easy-to-Approach Image

• Major VulnCoord Successes (mostly thanks to OUSPG!)

• Excellent Operational Relations Internationally
Major Services Today

NB: Confined to Technical Information Security

1. Incident Response and Incident Reporting Point

2. National Information Security Situation
   • Situational Awareness Service

3. Vulnerability Co-ordination

Why Need for Change?

• CERT-FI Severely Understaffed

• Funding Base Seen Unsustainable

• Growing Demands from non-TelCo sectors
  • Particularly from CIP Sector and Public Administration
  • Situational Awareness Considered Top Priority

• Ever Growing Reliance on ICT

• Information Security Management Getting More Mature?
The Future

Major Enablers

- Changes to the Funding Base from 2007-01-01
  - TelCos 100% → 25%
  - NESA 0% → 75%
  - At the same time the total budget is being doubled

- Projected Staffing
  - 3 Senior Security Specialists
  - 5 Security Analysts
  - 6 Customer Service Advisers
  - 2 Legal Advisers
  - 2 Administrative Persons
Next Steps 1/2

• Establishing Relations and Building Trust
  • New Customers and People
  • New Technologies and Business Models
  • New Approaches to Threat and Risk Assessment
  • New International Partners

• Expectation Management
  • “We Want Everything at Once!”
  • We can Provide Information to AID in Decision Making. However, You Make the Actual Decisions.

Next Steps 2/2

• Other Projects
  • Enhancing Situational Awareness Services
  • National Honeynet
  • Information Correlation and Automated Analysis
  • Automated Abuse Report Dissemination
  • National SMTP Whitelisting
  • New Ways to Facilitate Information Sharing
  • Ticketing System Development
  • Malware Reverse-Engineering and Library
  • ..
Contact Information

- Telephone: +358 (0)9 6966510 (6-14 UTC)
- Email: CERT@FICORA.fi
- WWW: www.CERT.fi

CERT-FI public alerts are available (in Finnish) via:

- Email alert service
- SMS alert service (pay-per-subscription)
- CERT-FI WWW pages
- RSS newsfeed
- YLE teletext page 848