TF-CSIRT Briefing May 29th 2003

Neil Robinson

http://www.iaac.org.uk/csirt.htm
Structure of presentation

- Background
- Scope
- Introduction
- Addressing the need
- Structure of the project
  - Task 1: User Requirements
  - Task 2: Incident survey
  - Task 3: Legal Survey
  - Task 4: Forensic survey
  - Task 5: Dissemination

http://www.iaac.org.uk/csirt.htm
Background

• Lack of clear guidance about legislative and evidential requirements for Computer Crime

• Recognised by; eEurope 2002 & 2005 Action Plans; ENISA; other legal and law enforcement initiatives (EC Draft Framework Decision on Attacks against Information Systems)

• What is needed is an easy to use guide matching incident to legal framework
Scope of the project

• Build a handbook which should advise, given a computer incident:
  – Whether it is illegal in the 15 MS
  – What form of evidence is required for action...
  – Whether law enforcement involvement is likely
  – If so, the correct procedures to follow in each country

http://www.iaac.org.uk/csirt.htm
Fulfilling the Need

• Based on expert and evidence based assessment
• Focus on computer misuse and crime
• Covering 15 Member States
• Tailored to user requirements
• Accessible format
Partners

- Sponsored by DG Information Society
- Team
  - Project Management and Dissemination: RAND Europe
  - Legal experts: TRANSCRIME - Univ. of Trento
  - Incident / technical expert: Prof Danilo Bruschi, Univ. of Milan
  - LE & Forensic expert: Pieter Van Dijken, Former NL judge & Investigator

http://www.iaac.org.uk/csirt.htm
Task 1: User Requirements Definition

• 1. Identify potential handbook users
• 2. Identify User information requirements
• 3. Ensure format, content and dissemination plan meet user requirements
• 4. Ensure incident classification scheme builds upon current initiatives
Incident Classification

- Computer Fingerprinting
- Malicious Code
- Denial of Service
- Account Compromise
- Intrusion Attempt
- Unauthorised Access to Information
- Unauthorised Access to Transmissions
- Unauthorised Modification of information
- Unauthorised Access to communication systems

http://www.iaac.org.uk/csirt.htm
Legislative Information

- Convention on Cyber-Crime
- European Draft Framework Decision on attacks against Information Systems
- Applicable law in each country
  - Computer crime law
  - General penal code

http://www.iaac.org.uk/csirt.htm
Forensic Procedures: Process

- Commercial Forensic ‘best practice’
- Interpol Computer Crime Handbook
- US DoJ Forensic guide
- Other official guides (ACPO etc)
- Personal Contacts (interviews etc)
Supporting and Forensic Information

• Contact information for Law Enforcement
  – Name of body
  – Contact person (where possible)
  – Contact details (phone, fax, etc)

• Forensic Procedures
  – Permissible methods (if not then who to get permission from..)
  – Recommended procedures & methods of collection
  – Relevant legislation (data protection, RIPA)
Format – hardcopy ‘handbook’

- Ch 1 Users guide (flowchart)
- Ch 2 Incident Descriptions
- Ch 3 Legal Terms
- Ch 4 Global Forensic Best Practices and terms
- Chapter 5-20
  - Content split according to country
Ch 5- 20 National Information

- General Introduction
- Section 1 – legislation (summary, text and links)
- Section 2 – Forensics (unique characteristics) – legislation, tools, techniques, practices
- Section 3 – reporting – who, what, where

http://www.iaac.org.uk/csirt.htm
## Belgium

<table>
<thead>
<tr>
<th>Incident Classification</th>
<th>Law</th>
<th>Criminal Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Fingerprinting</td>
<td>Art 314 bis par.1: interception of a private communication or a data communication without the agreement of all the parties involved in the communication. 1 year of prison and/or a fine 2 years of prison and/or a fine, when the offender is a government officer Art 259 bis par 1.</td>
<td>Art 314 bis par.2: disclosure of the contents of an intercepted communication 2 year of prison and/or a fine 3 years of prison and/or a fine, when the offender is a government officer Art 259 bis par 2.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Art 16 Law on Transmission Lines of 03.01.1934: it is a punishable offence to interfere with military communications line in order to hinder their functioning. Up to 3 years of prison and a fine.</td>
<td>Art 523: destruction of machinery. 3 years of prison and/or a fine.</td>
</tr>
</tbody>
</table>

[http://www.iaac.org.uk/csirt.htm](http://www.iaac.org.uk/csirt.htm)
## Denmark

<table>
<thead>
<tr>
<th>Incident Classification</th>
<th>Law Description</th>
<th>Law Punishment</th>
<th>Criminal Code Description</th>
<th>Criminal Code Punishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Fingerprinting</td>
<td>Par 263, c.1: any person who unlawfully: 1. deprives someone of a letter, telegram, or other sealed communication, or opens such a communication, or acquaints himself with its contents, 2. obtains access to places where other persons keep personal property, 3. with the aid of equipment, secretly listens to or records statements made private, telephone or other conversations, or negotiations during a meeting he is not attending or to which he has unlawfully obtained access.</td>
<td>A fine</td>
<td>imprisonment for a term not exceeding 6 months.</td>
<td>Text</td>
</tr>
<tr>
<td>Documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Classification</td>
<td>Law Description</td>
<td>Law Punishment</td>
<td>Criminal Code Description</td>
<td>Criminal Code Punishment</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>--------------</td>
<td>---------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Computer Fingerprinting</td>
<td>Art 38: a person who unjustifiably: (1) opens letter or other closed message addressed to another, (2) obtains attempt to obtain information about the content of a telephone call, a telegram, a message containing text, images or data or another comparable form of telecommunication message while it is being transmitted over a telephone network, (3) defaces, destroys, hides or conceals a closed message of the type referred to subparagraph 1 or a telemessages of the type referred to in subparagraph 2,</td>
<td></td>
<td>A fine</td>
<td>Imprisonment for at most 6 years</td>
</tr>
<tr>
<td>Documentation</td>
<td></td>
<td></td>
<td>Text</td>
<td></td>
</tr>
</tbody>
</table>
Next steps

• End of June
  – Summary layout & sample of data to be distributed to EC & CSIRTs

• September
  – Presentation of results of study to EC, 16th Sept in Brussels
  – Conclusion and dissemination to CSIRTs via paper handbook
Dissemination

- Paper Handbook due to DG INFSO
- Underlying database used for data collection
- Possible electronic (CD-ROM) based application (with Terena support?)
Sample Online Prototype

- Support, contact and guidance
- Query the system via controlled lists
- Simple import of updates via e-mail attachment
- Local administration
- Free text search for more descriptive attributes

Start page

http://www.iaac.org.uk/csirt.htm
Sample Online Prototype

- Scroll through countries
- Membership of relevant organisations (EU, Interpol etc)
- Hyperlink to full text of law
- List of known CSIRTS
- Country data

http://www.iaac.org.uk/csirt.htm
Questions?

RAND Europe Cambridge

T: +44 (0)1223 353329
F: +44 (0)1223 358845
neilr@rand.org