



EUROPE

# ***EC CSIRT Handbook update***

**Lorenzo Valeri, RAND Europe**

**TERENA/TFCISIRT Meeting**

**Lisbon, 16 September 2005**

## ***Aim of the study***

- Produce a first update of the 2003 Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries ('CSIRT Handbook')
  - Take into account recent developments in legal framework of EU
  - Extend its scope to ten new Member States
- Products will be a Handbook & Web service / CD-ROM application

# *Structure of Project*

- Incident Taxonomy
- User Survey
- Information Retrieval System
- Dissemination

# ***Incident Taxonomy***

- **Defining incidents remains difficult due to the rapidly evolving field and great varying approaches legally and practically**
- **Categories selected:**
  - **Target Fingerprinting**
  - **Unauthorised Access to Transmission**
  - **Unauthorised Access to Information**
  - **Unauthorised Modification of Data**
  - **Malicious Code**
  - **Denial of Service**
  - **Account Compromise**
  - **Intrusion Attempt**
  - **Unauthorised Access to Communication Systems**
  - **Spam**

# *Users Survey*

- Analysis of
  - Types of users (CSIRT teams, Law Enforcement, System Admins, Network Admins etc)
  - How the Handbook will be used (what properties to search under)
- Draft online survey available at:  
<http://web3.rand.org/resurvey/TakeSurvey.asp?SurveyID=9MH4o3KL3o6KG>

# Screenshot of survey

CSIRT Handbook update Survey - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://web3.rand.org/resurvey/TakeSurvey.asp?DisplayHeader=8&SurveyID=5KL893KL7925G&PreviousActualPageNumber=3&PreviousDisplayPageNumber=3&PreviousQuestion> Go Links

Google Search Web 375 blocked AutoFill Options

## CSIRT Handbook update

Page 4 of 12

General Questions

9. Who do you think are the targeted users? (Tick as many as relevant)

- IT Security Managers
- CSIRT Members
- Cybercrime Units personnel
- Court Case Managers
- Other, please specify

10. What specifications have you already expressed as to your needs for such information? Please give details.

11. In which ways is such information best communicated to you (formats, dissemination channels)?

- Electronic CD-ROM
- Folder or book
- Website
- Email

Done Internet 12:40

# ***Structure of Handbook***

- 1. Overview of legislation
- 2. Table (incidents mapped to sanction and penalty)
- 3. Law Enforcement bodies
  - Police
  - Courts
- 4. Reporting
  - Competent Authorities
  - Contact Details
  - Other reporting mechanisms
- 5. Forensics
- 6. References

# Screenshots of new structure

The screenshot displays a Microsoft Word document titled "EC-CSIRT\_D1v01.doc". The document content is structured as follows:

- Spam
- 2.2 Law en
- 2.2.1 Police (v
  - Belg
  - com
  - the
  - Eco
  - Crim
  - cybe
  - the l
  - poss
  - and
- 2.2.2 Courts (v
  - The
  - crim
  - app
  - s

The main content is a table with the following data:

Relevant Incidents	Applicable provision	Description	Sanction
Target fingerprinting	Article 314bis Criminal Code	Interception of private communication or data communication without the agreement of all parties involved.	Imprisonment of 1 year (2 years if the offender is a government officer) and/or a fine up to EUR 50,000
Malicious code	Article 210bis Criminal Code	Changing or deleting electronic data so that their legal scope changes and the deliberate use of such data	Imprisonment between 6 months and 5 years and/or a fine up to EUR 500,000. Attempts are subject to imprisonment between 6 months and 3 years and a fine up to EUR 250,000.
	Article 550bis Criminal Code	The (even unintentional) causing of damage to a computer system or to data stored on, processed or transmitted by such a system after unauthorised access thereto	Imprisonment between 1 and 3 years and/or a fine up to EUR 250,000
Denial of service	Article 210bis Criminal Code	Changing or deleting electronic data so that their legal scope changes and the deliberate use of such data	Imprisonment between 6 months and 5 years and/or a fine up to EUR 500,000. Attempts are subject to imprisonment between 6 months and 3 years and a fine up to EUR 250,000.
Account compromise	Article 550bis Criminal Code	Unauthorised access and maintenance of access to a computer system (outsiders), even with no intention to cause harm	Imprisonment between three months and one year (two years in case of intent) and/or a fine up to EUR 125,000
Intrusion attempt	Article 550bis Criminal Code	Preparatory measures in view of unauthorised access	Imprisonment between 6 months and 3 years and/or with a fine up to EUR 500,000
Unauthorised access to information	Article 550bis Criminal Code	Unauthorised access and maintenance of access to a computer system even with no intention to cause harm	Imprisonment between three months and one year (two years in case of intent) and/or a fine up to EUR 125,000

# *Study website*

- url: [www.csirt-handbook.org.uk](http://www.csirt-handbook.org.uk)
- Based on open source and open API using PHP based Content Management System (XOOPS 2) and MySQL database
- Features:
  - 3 levels of user interaction (admin, publishing author and user)
  - Guestbook, discussion forum, newsletter etc

# Screenshot of website

Computer Security Incident Response Team Handbook of Legislative Procedures

Introduction

This website reflects the 2005 project to update the 2002 Handbook of Legislative Procedures for Computer and Network Misuse. It will include confirmation and review of existing information, as well as collection of legislative information relating to the 10 new member states. This information will then be placed into an online searchable directory of legislation, to enable CSIRT teams and interested parties to query the dataset in accordance with identified requirements. This project has similar aims to the related eCSIRT.net project, which aimed to improve the efficient and effective co-operation of CSIRTs. This project, however, aims to add legal data to this co-operation, so that if necessary, CSIRTs know what laws are applicable to specific detected activities.

Structure of the project

This project is split into the following work-packages:

- WP1: Taxonomy update
- WP2: National Legislative Survey
- WP3: Information Retrieval System
- WP4: Project Management

For more information on each package, please visit the Workpackages pages, under 'Content' on the left hand side of the page.

Login

Username:

Password:

User Login

Lost Password?

Register now!

Site Search

Search

Advanced Search

POWERED BY XOOPS (C) 2002 THE XOOPS PROJECT

# *Information Retrieval System*

- **CD-ROM**

- Java Application running of read-only CD-ROM based on a HypersonicSQL RDBMS and Java SRE 2.1.5

- **Data revision options:**

- Distribution of new copy of data-files via CD or email
- Download of new application or data-files from study website

- **Online Application through the CSIRT Handbook Site**

## Update to the Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs)

v0.1a

### Details of the record

country\_id 2

Country Belgium

**Background** For cases where traditional crimes and investigation measures can not sufficiently deal with CIA offences, a law of 28 November 2000 introduced four specific computer crimes (informatics forgery, informatics fraud, data manipulation and hacking), three specific investigation measures (data seizure, network searching and expert involvement) and a provision imposing data retention obligations on operators and service providers of electronic communication .

In addition, specific laws penalise spam, the interference with military communications to hinder their functioning and the unauthorised deliberate access to the national social security database.

**Police** Belgian police consists of the federal police and 196 local police units engaged in community policing. The Belgian Federal Computer Crime Unit (FCCU) is part of the federal police, General Direction of Judicial Police, Direction of Financial and Economic Crime. The FCCU works closely together with 17 regional Computer Crime Units spread over the country, which assist the local and federal police during cyber crime related investigations. The FCCU gives technical and logistics support to the local Computer Crime Units but has no hierarchical command over them. Where possible, the FCCU also works together with other judicial services, the government and the private sector to give advice and promote preventive action.

**Courts** The court most likely to deal with computer crime is the Court of First Instance, criminal section (Correctionele rechtbank/Tribunal correctionnel). Against its decisions, appeal can be lodged with the Court of Appeal (Hof van beroep/Cour d'appel). The Supreme Court (Hof van Cassatie/Cour de Cassation) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate.

**Reporting** The FCCU should be alerted in all cases of computer crime, such as denial of service attacks, hacking, fraud and any major computer crime incidents. Smaller computer crime that has no impact on the safety of citizens or where the financial impact is low will be given a lesser degree of priority and should be dealt with by the local and federal police as part of their general duties.













**Forensics** Forensics

Evidence in Belgian criminal procedure is not regulated. All kinds of evidence may be submitted. Electronic evidence is admitted as a common form of evidence. The more authentic the evidence, the easier it will be to convince a judge during proceedings.

## Update to the Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs)

v0.1a

4 records found [delete all](#)

	provision_id	provision	criminal_code	law	precedent	country_id
  	1	Article 314bis Criminal Code				2
  	2	Article 210bis Criminal Code				2
  	3	Article 550bis Criminal Code				2
  	4	Article 14 Law of 11 March 2003				2

[Export to CSV](#)

(Total records: 4)

[Home](#) | [Insert](#) | [Search](#) | [Show all](#) | [Logout](#) | [Top](#)

app\_provision

Powered by: [DaDaBIK](#)

# *Dissemination*

- July 6 Workshop Brussels
- Other suggested events:
  - TF CSIRT Meetings
  - ENISA CSIRT related Event-Vilnius November 2006
  - TFCsirt/FIRST Meeting January 2006
- Assistance from the CSIRT Community!

**For more information contact:**

**Lorenzo Valeri, RAND Europe ([lvaleri@rand.org](mailto:lvaleri@rand.org))**

**Neil Robinson, RAND Europe ([neilr@rand.org](mailto:neilr@rand.org))**