Activity 1.2.1

Regional workshop on reporting mechanisms: international good practices

25 November 2016, Tirana, Albania

Outline

Background

As the use of and reliance on information technology becomes ever more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and in sophistication, but there has been a time lag in developing effective countermeasures.

The timely and efficient reporting of cybercrime to the relevant authorities and ensuring meaningful follow-up of the crime reports through the criminal justice system are perhaps one of the most important countermeasures against offences involving computer systems and data. However, cybercrime reporting remains problematic for a number of reasons, such as fragmented setup of reporting systems across different institutions, overlapping jurisdictions, lack of clear guidelines and rules for reporting, and lack of transparency in following up an initial crime report.

Objective

The purpose of the one day regional workshop is to present international good practices on reporting mechanisms of online fraud and other cybercrime, including such aspects as:

-   Types of threats to be addressed by a cybercrime reporting mechanism;
-   Expected benefits of such mechanisms;
-   Methods to collect reports and the impact of reports on criminal cases;
-   Examples of reporting mechanisms managed by the public sector; private sector; public-private and private-public cooperation.
-   Any other practical aspects related to the establishment and running of online reporting mechanisms.

Various examples of international good practices on reporting mechanisms will be discussed, showing how public/private and interagency cooperation could work against cybercrime in the context of cybercrime reporting. The impact, benefits and performance of various models of online platforms for cybercrime reporting will be considered. Building on the experience of several existing reporting mechanisms around the world, participants will get an insight into a number of examples that may serve as a model for the project countries/areas.

Participants

The target audience of the regional workshop is made of representatives of the following institutions/organisations from all 7 project countries/areas:
- Ministry of Justice, prosecutors specialised in supervision/prosecution of cybercrime cases, cybercrime units, financial intelligence units, financial investigation units;
- Ombudsperson's Office;
- Computer Emergency Response Teams;
- Internet Service Providers;
- Banking Associations.

Programme

25 November 2016 – Hotel Tirana International: Balsha meeting room	
Time	
9h30-10h00	Opening
10h00 - 11h00	**Why are separate reporting mechanisms needed for cybercrime?** - Types of threats to be addressed by a cybercrime reporting mechanism; - Expected benefits of such mechanisms; - Methods to collect reports and the impact of reports on criminal cases. Nigel JONES, Jean-Christophe LE TOQUIN, Hein DRIES-ZIEKENHEINER – Council of Europe experts
11h00-11h15	**Coffee Break**
11h15-12h15	**Reporting cybercrime and fraud: case-studies - Action Fraud (UK) and Get Safe Online** Presentations and Q&A Nigel JONES, Council of Europe expert
12h15-13h15	**Preventing and combating financial fraud: case-study – CIFAS (UK)** Presentation and Q&A Hein DRIES-ZIEKENHEINER, Council of Europe expert
13h15-14h15	**Lunch**
14h15-15h00	**Reporting spam and other types of cybercrime: case-study – Signal Spam (France)** Presentation and Q&A Jean-Christophe LE TOQUIN, Council of Europe expert
15h00-15h30	**Fraud and Internet Security Resources: case study – Hoaxbuster** Presentation and Q&A Jean-Christophe LE TOQUIN, Council of Europe expert
15h30-16h30	**Reporting child abuse online and offline: Internet Watch Foundation (IWF) and International Association of Internet Hotlines (INHOPE). Victim care – why it needs to be different?** Presentation and Q&A Nigel JONES, Council of Europe expert

16h30-16h45	**Coffee Break**
16h45-17h30	**Issues to consider: funding, partnerships, technology, security of information etc.** Facilitated discussion by Council of Europe experts
17h30-17h40	Closing