GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

CSIRTs and criminal justice authorities – good practices of collaboration on cybercrime and electronic evidence

Webinar 11 May 2020 – Questions and Answers

Are there any commonalities between the Council of Europe’s training materials on cybercrime and e-evidence for LEA's and judges and those from ENISA?

The materials have been prepared separately and without coordination between institutions involved (i.e. Council of Europe and ENISA), thus there are no specific commonalities between those. This is further evident from the cursory overview of both, as they also refer to different legal standards - *Budapest Convention on Cybercrime* – in the Council of Europe case, and EU documents and standards in ENISA’s case - as the basis for response and cooperation. This is perhaps a reflection of the fact that ENISA’s mandate exclusively extends to the EU members states. At the same time, there is no specific discrepancy either as these two are largely compatible.

From the technical and operational standpoint, there are more tangible differences as the training materials of the Council of Europe (available on the Octopus Cybercrime Community site) are structured along the path of criminal justice response to threats of cyberspace - i.e. what could be loosely referred to as cybercrime/electronic evidence investigations. On the other hand, ENISA’s approach is centered upon the handling of cyber incidents - at least those materials that look into the cooperation between criminal justice authorities and the CSIRTs.

PALESTINE: The Palestinian MoI was asked how to reach the network, if there are some possibilities to set up a CSIRT and receive some support.

The CSIRTs Network is established by the NIS Directive (see Article 12) “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation”. It is composed of EU Member States’ appointed CSIRTs and CERT-EU. For more information on the CSIRTs Network, please see: https://csirtsnetwork.eu/, Contacts: Secretariat: cnw@enisa.europa.eu; Chair: csirts-network-chair@enisa.europa.eu

If by “network” we refer to CSIRT fora, you might consider having a look at:

- Europe-wide level: the website of the TF-CSIRT;
- global level: the website of FIRST (Forum of Incident Response and Security Teams) that has members from around the world. (ENISA is also represented in the FIRST’s Board of Directors - FIRST Members)

For an overview of ENISA CSIRT training materials see here. Concerning the setting up of a CSIRT, ENISA’s website has some training material addressing specifically how to set up a CSIRT – see in particular here. In addition, please also note that ENISA is currently developing a new guide on setting up a CSIRT and SOC. This guide will be available by end of 2020. For more specific questions please contact: CSIRT-Relations@enisa.europa.eu

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L’EUROPE

Implemented
by the Council of Europe

NIGERIA: I am a Police Officer from Nigeria Police Force is there any way I can be a part of CERTs and what is the requirement?

For information about CSIRTs and related contacts in your country you might find it useful to consult the members' map for FIRST (Forum of Incident Response and Security Teams). This includes also information on ngCERT (Nigerian Computer Emergency Response Team).

LEBANON: Can ENISA provide consultancy support for countries planning to set up a new national/Organizational CSIRT?

Concerning the setting up of a CSIRT, some training material addressing specifically how to set up a CSIRT is available on ENISA's website. For an overview of ENISA CSIRT training material please see here. In addition, please also note that ENISA is currently developing a new guide on setting up a CSIRT and SOC. This guide will be available by end of 2020. For more specific questions please contact: CSIRT-Relations@enisa.europa.eu

You might also find useful to consult the ENISA material on CSIRT Capabilities and Maturity available here

CERT-MU provides consultancy services to countries which are planning to set-up their national CERT/CSIRT. In this context, we have assisted Senegal with the concept development of setting up the Senegalese national CERT following the request of the Council of Europe. Other countries that have benefited from the assistance of CERT-MU include Tonga, Madagascar, Ivory Coast, and the Philippines.

MEXICO: Can ENISA provide support for countries in Latin America? Can we receive support for the training of various sectors, private, academic and government?

Because of its mandate, ENISA focuses on the EU Member States. However, the ENISA CSIRT training material is online, publicly available, and you can access it here.

Are there any relevant decision(s) issued by the ECHR regarding the electronic evidence, in particular concerning their admissibility or other aspects?

You can find a rather good summary of ECtHR cases relevant to the subject here. I would particularly point out to K.U. vs Finland (2009), as it was a landmark case in many respects. However, from what I know, there has not been any specific case challenging the admissibility of evidence as part of ECHR Article safeguards related to fair trial, as most of the cases dealt with Articles 8 and 10 (right to privacy and freedom of expression). I do also believe that extensive practice of the Strasbourg Court in relation to surveillance of communications (a string of cases dating back to Klass v. Germany) should be also of relevance for this particular aspect, where electronic media/data/evidence is involved.

AZERBAIJAN: regarding hacked/fake social media accounts - what is the CERT-MU role/task in handling this type of incidents? How does it cooperate with international social media operators such as Facebook? Is there any special channel?

CERT-MU serves as a central point for reporting and responding to/handling of computer security incidents/cybercrimes both at national and international levels. These include technical incidents and also those occurring on social media.

The types of incidents handled by CERT-MU occurring on social media include:

- Phishing
- Scams
- Fake accounts

- Fake news
- Hacked accounts
- Sextortion
- System Compromise
- Identity Theft
- Offensive Content
- Online Harassment

Hacked and fake accounts incidents are very common and are regularly reported through the reporting platform developed by and housed at the level of CERT-MU: Mauritian Cybercrime Online Reporting System (MAUCORS).

As a national CERT, CERT-MU has forged a working collaboration with Facebook for the reporting and resolving of such incidents. Facebook also provides a special channel to national CERTs for the reporting of incidents occurring at their level.

Being affiliated with international Forum such as FIRST may also be an advantage in resolving incidents occurring at cross border levels.

Does the Mauritian population show interest in reporting cyber incidents? Similarly, I would like to know if the judges are issuing sentences against cybercrime?

Since the set-up of CERT-MU in May 2008, the population has shown a general increasing interest in reporting cybersecurity incidents. Over the years, the number of incidents reported at CERT-MU has increased considerably. The types of incidents reported have already been elaborated in a previous question. However, it is noteworthy to state that ever since the launch of online incident/cybercrime reporting platform developed by the CERT-MU – the Mauritian Cybercrime Online Reporting System (MAUCORS), we have seen a drastic rise in the reporting of incidents. This system allows the constituency to report diverse types of incidents, be they technical or those which require legal intervention. The incident is channeled to the respective agencies for its resolution, without the intervention of the reporting party. The citizen can also track the status of their report by using the incident tracking number automatically provided to them.

Regarding the second part of your question, the rate of sentences is not that high at the moment.

In terms of legislation, is there a law similar to the General Data Protection Regulation in Mauritius?

Yes – Mauritius has the Data Protection Act 2018 which has been amended to be in line with the European Union’s General Data Protection Regulation (GDPR).

Questions addressed during the webinar:

- requirements to establish a national CERT
- Are all countries allowed to be part of CERTs community, or only EU countries? What criteria do they have to meet?
- possibility for non-EU countries to receive ENISA training: Is it possible for non-EU citizens to participate in ENISA/CSIRT's training programs and be employed at ENISA?
- Is there an interrelation between, for example, the CERT-MU and ENISA?
- handling online child sexual exploitation materials: what are CERTs supposed to do if they came across with child sexual abuse material on websites – inform the Police/LEAs or they have to communicate with other CERTs to make other steps? If so, what are these steps.
- possibility for CSIRTs to counter-attack: What about the practice of using data collected

during CSIRT's counter-cyberattack on perpetrator's computer or other devices as electronic evidence? Is it legal in EU jurisdictions?

- how can INTERPOL reach out to the international CSIRT community – this is a new capability for INTERPOL - we are working on threat identification, and then a form of causal disruption, through a coordinated response with member countries. I am keen to understand how best we can work closely with the CSIRTs?
- elaborate on the synergies and dependence between ENISA's cross-sectoral cybersecurity work and the cybersecurity and online protection work of sectoral regulators (e.g. financial sector, energy, etc.)?

PANEL

Dr. Silvia PORTESI, Network and Information Security - Research and Analysis Expert, European Union Agency for Cybersecurity (ENISA)

Dr. Alexandra MICHOTA, Officer in Network and Information Security, ENISA

Giorgi JOKHADZE, Project Manager, Cybercrime Programme Office of the Council of Europe (C-PROC)

Sachindra REECHAYE, Information Security Consultant, CERT-MU, Mauritius

www.coe.int/cybercrime