Cybercrime@EAP III

Արևելյան Գործընկերություն
Східне партнерство Eastern
Partnership აღმოსავლეთ
პარტნიორობა Parteneriatul Estic
Şərq tərəfdaşlığı Partenariat
Oriental Усходняе Партнёрства

3608_25 Seminar on CSIRT/CERT Regulations and Operational Environment

5-7 July 2017, Minsk, Belarus

Provided under the Cybercrime@EAP III project

Outline

Background and justification

In the world of today, increasing number of attacks against computer systems and data is a growing concern for both cyber security professionals and the law enforcement. Attacks against critical infrastructure, whether government-owned or private, represent particular concern for both communities. The growing threat of cybercrime is further exacerbated by difficulties of accessing and securing electronic evidence, especially if information vital for criminal investigations is in the hands of private companies. However, even where realization of these threats and challenges by policy makers and professional communities is as strong as ever, successful response to these is often hampered by lack of coordination and common approaches between cybersecurity and law enforcement communities to what should be the ultimate common goal – ensuring safer cyberspace for all.

The Cybercrime@EAP III project, implemented by the Cybercrime Programme Office of the Council of Europe, features strong focus on public-private cooperation in cybercrime and electronic evidence. It is recognized that sometimes the key to cooperation is readiness to exchange information between various national counterparts, such as cybersecurity community and investigative authorities, in order to initiate or support ongoing criminal investigations. There are numerous sources from which this information may come, both national and international, such as national exchange of information between industry, critical infrastructure and government on incidents and crimes, international databases run by global cybersecurity companies, open-source intelligence, exchange of data and intelligence between CSIRT/CERT teams, online incident/crime reporting frameworks, possibilities to submit and support evidence from different media/social networks, etc.). The methods and toolkits used by CSIRTs/CERTs in putting this data into action is another important aspect of their work that needs to be known to the law enforcement in terms of similar handling of electronic evidence in criminal investigations.

Strategic insight on cybersecurity and cybercrime as two interconnected domains is also important, as it allows the national authorities to address the problem of cooperation in the long-term. The lack of dedicated cybersecurity/cybercrime strategies in Belarus makes for an important opportunity to address the subject, and to exchange knowledge, experience and best practices on the subject, including necessary regulatory framework in which cybersecurity community can operate and cooperate with the law enforcement.

Expected outcome

Carried out under Result/Immediate Outcome 2 of the Cybercrime@EAP III project (*A structured process of public/private cooperation on cybercrime underway and agreements concluded*), the even aims to strengthen the understanding of the need to exchange information between different professional communities of cybersecurity experts and the law enforcement. The goal is also to demonstrate the need for cooperation and partnerships in cybercrime and cyber-security to get access to data held by private companies, and to encourage the use of common approaches and methods for processing electronic evidence in both cybersecurity incident handling and criminal/financial investigations on the basis of internationally accepted standards, such as the Council of Europe Convention on Cybercrime.

More specifically, the seminar will look into the following subjects:

- Strategic approach to cybersecurity and cybercrime;
- Regulatory framework for cybersecurity: defining critical infrastructure, legal basis for operations and enabling factor for cooperation with the law enforcements;
- Cyber incident handling frameworks and best practices;
- Open-source intelligence: threat analysis;
- Information from international vendors and CSIRT community: threat analysis and use cases;
- Joint operations with the law enforcement: best practices;
- Operational environment for CSIRT/CERT action: tools and equipment used;
- Penetration testing: tools and methods used, and prevention of cybercrime;
- Live data forensics as an example of support to law enforcement operations;
- Other topics and subjects of interest to participants.

By the end of the event, the participants will be able to have up-to-date knowledge of CSIRT operating and regulatory environment, have solid understanding of the opportunities for operational exchange of data, intelligence and crime reports between CSIRT/CERT and law enforcement, and establish closer links between professional communities of cybercrime investigators and cybersecurity in preventing, detecting and investigating cybercrime.

Participants

The event will be attended by the following participants:

- International CSIRT/CERT experts;
- Project country team members;
- Cybercrime unit of the Ministry of Interior and other investigative units dealing with cybercrime or electronic evidence;
- Investigative Committee;
- Computer data forensics experts;
- Financial intelligence experts;
- CSIRT/national CERT experts;
- Private sector/critical infrastructure (banking, ISPs, etc.);

- C-PROC staff.

Administrative arrangements and location

The event will take place at Beijing Hotel Minsk (36 Krasnoarmeiskaya Street), Minsk, Belarus.

Programme

Wednesday, 5 July 2017

9h00	*Registration*
9h15	Opening session: why exchange of data and operational cooperation matters for public-private cooperation • Giorgi Jokhadze, Council of Europe Cybercrime Programme Office
9h30	Strategic approach to cybersecurity and cybercrime • Daniel Ionita, CERT-RO (40 min) • Giorgi Jokhadze, Council of Europe (20 min)
10h30	*Coffee break*
11h00	Regulatory framework for cybersecurity: operations/cooperation • Daniel Ionita, CERT-RO (1 hr) • Giorgi Jokhadze, Council of Europe (1 hr)
13h00	*Lunch*
14h00	Incident handling frameworks and solutions: best practices • Alexandru Stoian, CERT-RO (45 min) • CERT.GOV.GE expert (45 min)
15h30	*Coffee break*
16h00	Open source intelligence: threat analysis (practical exercise) • Alexandru Stoian, CERT-RO (30 min) • CERT.GOV.GE experts (15 min) • Practical exercise – threat analysis – give tasks to particiapnts (1 hr 15 min)
18h00	End of day 1

Thursday, 6 July 2017

9h00	• Results of homework: discussion by experts (30 min) National and international sources of information for CSIRT/CERT • CERT.GOV.GE experts (30 min) • Daniel Ionita, CERT-RO (30 min)
10h30	*Coffee break*
11h00	CSIRT/CERT toolkit for incident handling and threat analysis • Overview and examples of used tools: Alexandru Stoian, CERT-RO (1 hr) • Overview and examples of used tools: CERT.GOV.GE experts (1 hr)
13h00	*Lunch*
14h00	Penetration testing (practical exercise) • CERT.GOV.GE expert (40 min) • Alexandru Stoian, CERT-RO (20 min) • Pen test – live demonstration by CERT-RO and CERT.GOV.GE (1 hr)
16h00	*Coffee break*

16h30	Live data forensics (demonstration/practical exercise) • Demo of live forensics tools: Alexandru Stoian, CERT-RO (1 hr) • Practical exercise: give homework to participants: CERT-RO (30 min)
18h00	End of day 2

Friday, 7 July 2017

9h00	• Results of homework: discussion by experts (30 min) Law enforcement operations • Examples of joint operations with the law enforcement: Daniel Ionita, CERT-RO (40 min) • Examples of joint operations with the law enforcement: CERT.GOV.GE experts (20 min)
10h30	*Coffee break*
11h00	Conclusions and findings • Q&A session led by all experts
11h30	Consultative meeting with the Belarus country team • Giorgi Jokhadze, Council of Europe Cybercrime Programme Office
13h00	*End of mission*

Contacts

At the Council of Europe:

Giorgi JOKHADZE
Project Manager (CyberCrime@EAP III)
Cybercrime Programme Office
Tel: +40-21-201-784
Giorgi.Jokhadze@coe.int

Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest, Romania
www.coe.int/cybercrime