Centre for Security Cooperation

Conference on
"Computer Emergency Response Teams (CERTs-CIRTs-CSIRTs)"
-Present cooperation among regional CERTs, and how it could be further enhanced-

06-07 May 2014, Zagreb, Croatia
IRC-05-P

Activity Background

With the aim to promote and increase cooperation by using dialogue and exchange of information, transfer of knowledge, views and ideas, as well as to disseminate international standards, RACVIAC – Centre for Security Cooperation conducted a Conference entitled "Computer Emergency Response Teams (CERTs- CIRTs-CSIRTs) - Present cooperation among regional CERTs, and how it could be further enhanced".

This activity was a continuation of a series of events dedicated to the topic of cyber threats and critical information protection where CERTs (CIRTs, CSIRTs) are recognized as a key instrument as they act as security service providers for the government.

A very good level of cooperation among CERTs (CIRTs, CSIRTs) and different entities, in terms of critical information protection, exists but still there is room for improvement of cooperation between CERTs (CIRTs, CSIRTs) on the national and regional level.

Knowing that the Internet doesn't recognize national borders this cooperation has become a necessity with regard to information sharing and incident response.
Trying to implement their capabilities, it is understandable that CERTs (CIRTs, CSIRTs) face some challenges or barriers regarding mutual cooperation, which are mainly political, financial, organizational and legal in nature.

The purpose of this event was to bring together representatives and equivalent representatives of CERTs (CIRTs, CSIRTs) from the SEE region in order to facilitate the exchange of experience and regional cooperation. Moreover, the aim was to expose the participants from the SEE region to experiences of experts from international organizations and countries of the region.

The Conference objectives were:

- To update participants on new developments in cyber security,
- To enable participants to exchange knowledge, experience and know-how, as well as to facilitate networking among them,
- To raise awareness of the importance of cooperation in response to cyber threats on the national and regional level.

Activity Venue, Duration and Participation

The Conference took place in Rakitje-Zagreb (Croatia) from 06–07 May 2014 on RACVIAC premises.
It comprised seven sessions which were designed to include both presentations and discussions.
The participants and lecturers included representatives from: Albania (2), Bosnia and Herzegovina (2), Croatia (6), Serbia (2), the Former Yugoslav Republic of Macedonia[1] (3), Montenegro (3), Romania (2), Slovenia (1), Turkey (3), EU Institutions (2), and RACVIAC (6).

Conference Opening

Opening Session, HE Amb. Branimir Mandic, Director of RACVIAC

At the beginning of the Conference Director of RACVIAC, Ambassador Branimir Mandic welcomed distinguished speakers and all participants and reminded them that this event is a continuation of a series of events dedicated to the topic of cyber security organized by RACVIAC - Centre for Security Cooperation.
Ambassador Mandic continued, "We are aware that many steps are undertaken on a national, regional and global level to prevent cybercrime, but we are also witnesses that the rate of cybercrimes and the cost of prevention are on the rise. A lot of theoretical work has been done in the field of cyber security but real protection can be expected from those who implement theories and who do physical operational work on the ground. Many countries have recognized how important this is and that's why they created cyber response units, computer response teams, incident response teams, etc. on a national level. However, when it comes to this kind of threat, it is impossible for one nation to protect itself without close

[1] *Turkey recognizes the Republic of Macedonia with its constitutional name*

cooperation with its neighbors and cooperation on a global scale. To make cooperation as strong as possible, not only in cyber security but also in some other security domains, we face challenges or barriers which are mainly of a political, financial, organizational and legal nature. The best way to overcome those obstacles is to communicate with each other, and act together."

HE Amb. Mandic emphasized that this event was a great chance for those of you coming from the countries who are in a phase of establishment of computer response teams to exchange views and ideas as well as to learn from experiences of colleagues where these teams are already established.
Furthermore, this was a good opportunity to discuss possible mentorship between those CERTs already instituted and those teams which are in a stage of development.

Panel I: - Cooperation among regional CERTs, and how it could be further enhanced -

Mr.Gorazd Božič

The conference started with a presentation given by Mr. Gorazd Božič, Head of SI-CERT, who acted as Chairman of the European CERT Group TF-CIRT from 2000-2008.
Mr. Božič recalled certain cyber-attacks in the past which are having a huge impact on cyber security nowadays and he also presented new trends in cyber-attacks and cyber security emphasizing that computer security today is much more important than twenty years ago. New trends show that more and more cases of cyber-attacks are related to attacks on governments and other critical infrastructure computer networks. For this reason in particular it is important to have CERTs to respond to those attacks.
As potential cooperation within the region regarding cyber security Mr. Božič suggested possibilities to organize joint training (courses) for personnel dealing with cyber security.
He suggested to those countries who are still in the phase of establishing CERTs to find a partner in the region that they feel comfortable with, make a contact and learn from their experience how to establish effective CERTs.

Panel II: - Strategic values of CERT teams, models and legal basis for cooperation -

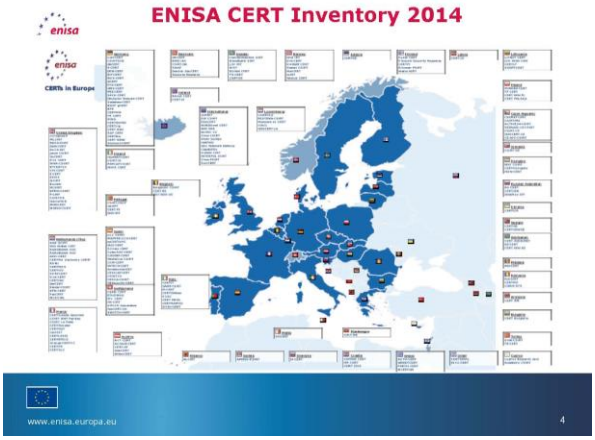
The second presentation was given by Ms. Andrea Dufkova, who is an Expert in network and information security from the European Union Agency for Network and Information Security (ENISA).
First, Ms. Dufkova presented ENISA's work as an advisory body to the EU institutions regarding information security issues. She mentioned that ENISA is also focused on capability building for CERTs and close cooperation in the fight against cybercrime, including training on specific topics.


Ms Andrea Dufkova

Presenting the map of already established CERT teams in Europe, Ms. Dufkova underlined that it is not that important how many teams (in different sectors) exist in Europe but how many of them are recognized by other teams and how they can offer support to each other. Face to face meetings can make this cooperation more efficient especially if this cooperation occurs in the region where some barriers such as language are not a problem, and, in addition, regional cooperation could be cheaper because of travel and other costs.

She continued her presentation explaining that for a governmental or national team it is necessary to meet certain capabilities starting from formal capabilities such as mandate, definition of roles and responsibilities then going on to operational and organizational capabilities and moving on to cooperation capabilities on the national, regional and other levels. For new established teams it is necessary to establish communication and information partners.

Ms Andrea Dufkova concluded that ENISA has the capacity and will to help those countries which are in a phase of establishing their CERT teams, but as she said it is not just fancy stuff to have a CERT team but that team must also be ready and proven in cyber security.



<u>Panel III: - The role and importance of information clearinghouse and coordination point for information security on the national, regional and global level</u> -

Mr. Predrag Pale from the Faculty of Electrical Engineering and Computing – University of Zagreb was the next speaker who emphasized how much people rely on new technologies and how difficult it is to resist using it but due to speed of change and global scope of changes impossible to predict what is next and what the consequences might be.

Mr. Predrag Pale

Precisely for that reason intensive and fast learning is required and first of all networking on all levels, as he said, to know who is who which will make the establishing of communication channels and trust easy.

Besides knowledge and will to solve the cyber security problem we need tools and technologies, the legal system (framework) to be in place and cooperative institutions such as CERTs, academic institutions, and channels to share information on time.

Panel IV: - CERT-EU Overview and lessons learnt -

Mr. Freddy Dezeure, Head of CERT-EU presented some practical examples of cyber threats and advice how to solve them, which was valuable for the participants in the event who face cyber security challenges in their work every day.

Mr Freddy Dezeure

He also emphasized the necessity to create the so-called Trusted Circle for Information Sharing. No matter whether we already have established CERTs or not we have to share information that is of common interest and form common benefits. To improve regional cooperation, Mr Dezeure advised to organize regular expert meetings among countries in the region and discuss issues regarding cyber security because in that way a community of experts will be created in the region. He also offered practical help from CERT-EU in the capacity that they have to provide it.

Panel V: - Cyber security strategy as a "Must" for the SEE Region -

Addressing cyber security challenges is a complex task. Modern and complex threats that stem from interconnected and interrelated environments have urged strategic thinkers around the globe to shift the approach to overall national security, stated Col Metodi Hadji-Janev, Associate professor of law and the Vice Dean at the Military Academy „General Mihailo Apostolski" – Skopje in his presentation.

In his conclusion, Col Hadji-Janev said: "Contemporary security dynamics have urged many countries and organizations to consider cyber security as a top security priority. Marching toward modernity and following their own ambitions for Euro-Atlantic integrations, among others, SEE countries have pledged serious efforts to improve their own information and communication technologies. The growing interdependence of these technologies and cyberspace in SEE, nevertheless, has not been matched by a parallel focus on security.

Mr Metodi Hadji-Janev

While building their national cyber security strategies SEE countries must address several areas. These areas are: countering cybercrime; cyber defence; intelligence and counterintelligence; critical infrastructure protection; crisis management; cyber diplomacy and cyber governance. To avoid potential miscommunication future strategists must consider centralized planning and decentralized execution."

Panel VI: - Advance Cyber Defence Centre (ACDC) project -

Mr. Darko Perhoč, employee of the Croatian Academic and Research Network (CARNet) and Head of HR-CERT informed the participants about the ongoing project called ACDC- Advanced Cyber Defence Centre, in which CARNet has been involved from the very beginning.

Established in February 2013, the European Advanced Cyber Defence Centre (ACDC) aims to create a community of stakeholders joining forces to fight botnets.

ACDC provides a complete set of solutions accessible online to mitigate on-going attacks and target both end-users and network operators.

Mr Darko Perhoč

It also consolidates the data provided by various stakeholders into a pool of knowledge, accessible through the ACDC central clearing house.

ACDC reaches out to users across Europe through 8 national relay centres.

ACDC currently operates as a 30 months EU-supported pilot project which ends in July 2015 and aims to continue as a self-sustained infrastructure beyond the period when the project will expire. Initiated by 28 partners from 14 countries ACDC is open to industry stakeholders, the public authorities and academia across Member States.

(For more info regarding the project see: http://www.botfree.eu)

-National presentations on the current status, challenges and perspectives of national CERTs-CIRTs-CSIRTs -

This session was dedicated to the countries' representatives' presentations, who had an opportunity to present their own experiences, the current status and challenges of national CERTs.

In this session, the conference participants were addressed by:

-Ms. Jona Josifi, Albanian CIRT; AL,

-Ms. Sabina Barakovic, Professional Associate, Ministry of Security; BA,

-Mr. Darko Perhoč, CERT-HR; HR,

-Mr. Goran Bujas, Information systems security bureau; HR,

-Mr. Dimitar Bukovalov, Ministry of Information Society and Administration; MK,

-Mr. Ivan Radunovic, National CIRT; ME,

-Mr. Dan Tofan, CERT-RO; RO,

-LtC Dejan Vuletić, Strategic Research Institute; RS,

-Mr. Ugur Ozturk, Ministry of Foreign Affairs, TR.

During this session, it was recognized that the level of development of Computer Emergency Response Teams – CERTs is not the same in different countries. We could see from the presentations that in some countries, CERT teams are very successful in their work and have very good cooperation with other CERTs and similar organizations on the global level but on the other side, the Republic of Serbia and Bosnia and Herzegovina have only recently begun establishing CERT teams.

The representative from the Former Yugoslav Republic of Macedonia[2], throughout his presentation said that "the Government of the Republic of Macedonia adopted a decision on establishing a national Computer Emergency Response Team (CERT.mk)". He also said that, "An inter-sector working group was set for establishing CERT.mk which creates an additional need for closer cooperation among the countries. Currently, the Agency for Electronic Communications is working on the establishment of CERT.mk and putting it into practice."

The participants acknowledged that the information provided and issues discussed were of great benefit to them for further improvement of cooperation between CERTs (CIRTs, CSIRTs) on the national and regional level.

---

[2] *Turkey recognizes the Republic of Macedonia with its constitutional name*

Conference Closure

After the official part of the conference RACVIAC Director Ambassador Branimir Mandic addressed the participants with the following words:

"This event was a good example of social dialogue at the regional and international level. As pointed out at the beginning - it is impossible for one nation to protect itself against cyber-attack without close cooperation with its neighbors and cooperation on a global scale. This event insisted on the importance of regional and international cooperation in combating cyber crime and reviewed the possibilities and ways how the cooperation can be further enhanced.

I hope that we have recognized the importance of cooperation and information sharing as important tools which facilitate the work of CERTs and their employees because joint efforts in this area bring joint solutions and better results in both prevention and repression of cyber crime.

The designated employees of national / governmental CERTs should examine ways of promoting the importance of their work, the risks stemming from cyber crime and the importance of cyber security, especially in order to animate decision makers and politicians to overcome certain challenges.

In accordance with the conclusions of this event we should continue with activities which have aimed to fulfill the joint needs of the countries of the SEE Region, related to combating cybercrime and ensuring cyber security.

RACVIAC will also support the efforts on cyber security among SEE Region countries, especially the countries which have not yet adopted strategies on cyber security and didn't establish their CERTs."

Compiled by: LtC Josip Mlakic, the Conference Coordinator, RACVIAC – CENTRE FOR SECURITY COOPERATION.