LACIGF 12 Report

Title of the session: Session 9 – INTERSECTORAL THEME – TECHNICAL COMMUNITY: Internet security under a multi-participatory approach: different realities, common challenges and convergent tools

Session summary:

The session was moderated by **Ernesto Majó (LACNIC, Uruguay)** y **Ernesto Bojórquez (LACTLD, México). Ernesto Majó** began by brief conceptualizing introduction on the proposed theme, mentioning the concept of security as a broad concept today. It has different dimensions, including Internet stability and resilience, human capabilities, and infrastructure. He believes that the human dimension is an essential factor, as well as collaboration, which he also considers as an essential factor to understand the challenges of the field. He also showed an infographic of the Internet ecosystem as an intent to give visibility to the complexity and various actors involved on it, each with different responsibilities. Ernesto Majó also mentioned that, in order to achieve a safer Internet, our reach is limited due to the fact that the nature of the Internet is characterized by the concept of cooperation, so we must solve the problems together and work with each other to find solutions.

After that introduction, the public was invited to get together in four working groups, according to participating actors.

- Technical Community;
- Civil society;
- Private sector;
- Public Sector

Each group should contribute by answering two instructions:

- What are the initiatives or protocols to identify security challenges?
- Bring critical issues, tools or protocols that we develop.

Afterwards, each group made a small presentation about the debate.

In the presentation of the technical community group, performed by **Sebastián Bellagamba (Internet Society, Uruguay)**, he commented on some of the issues that were identified from his organization, including connectivity, Internet trust and security.

The challenges associated with these issues can be divided into three parts:

1. In principle, what is associated with *Pretty Good Privacy* (PGP) and Internet security, and how to ensure default protocols for packet switching with improved security;
2. On the other hand, the theme of IoT implementation, and how to deal with the lack of knowledge in network security when it comes to the manufacturers of these products;
3. Finally, what refers to the fragmentation of the Internet and its impact, which can be both positive and negative.

On the last point in particular, Bellagamba mentioned that ISOC conducted a study about the consolidation in the Internet segments. Among them the most discussed was the segment of the service layer. Today the amount of services is innumerable, given that the cost of innovation is cheaper by cloud providers, when compared to other layers.

Collectively, the challenges they considered relevant were listed:

- Vulnerability of DNS domains;
- Routing;
- Lack of coordination in the technical community;
- Ensure the information integrity;
- Regulation;
- MANRS (How to bring nodes to national and regional instances?);
- Impossibility of IPv4 implementation traceability;
- The necessity to work on capacity building.

They also presented a list of tools and projects identified by the technical community as possibilities to contribute to safety:
- OTA (Over The Air): over-the-air programming refers to various methods for distributing new software, configuration settings and even updating encryption keys for devices such as cell phones, decoders or voice communication secure equipment;
- RPKI: issuance of cryptographic material that allows LACNIC members to demonstrate digitally that they have the right to use IPv4 and IPv6 addresses;
- CSIRTs: it means Computer Security Incident Response Team;
- BGP (Border Gateway Protocol): in telecommunications, BGP is a protocol through which routing or routing information is exchanged between autonomous systems.

Andrés Sastre (ASIET, Uruguay) made the presentation for the private sector. The following challenges were identified in his work group:

- Failure of mechanisms for the dialogue between public and private;
- High demands from states;
- Lack of innovation by companies;
- Lack of trust and misuse of safe browsing;
- Lack of products availability on the network.

Some solutions proposed by that group were:
- Requirement of minimums standards, by the industry, in broad terms;
- Digital education, to counteract distrust.

Julián Casasbuenas (Association for Progressive Communications - APC and Colnodo, Colombia) presented the discussion made in the civil society working group. Initially, they identified some security challenges in civil society:

1. Digital Appropriation / Education on digital security and data protection issues: A great ignorance in terms of security is identified in society in general. The recommendation

here is to start this process in primary education in order to teach digital security from early childhood, inviting schools to participate;

2. Create public policies originated from civil society, be more proactive than reactive. To work with multiple stakeholders for the elaboration of regulations and public policies that can also be shared with the whole society by receiving their comments;
3. Investment in security and collective create;
4. Establish proportionality in security and surveillance issues in LAC countries.

Some initiatives proposed by the working group:

1. Security protection programs.
2. Digital literacy promoted by governments and all sectors with focus in basic education;
3. Perdurable sustainable programs.
4. Share experiences and materials, using platforms that we participate.

Alejandra Erramuspe (AGESIC, Uruguay) y **Juan Cayoja Cortez (UMSA, Bolivia)** were in charge of presenting the government sector discussion. The sector was divided in two groups. On the one hand, one group proposed to generate legal measures and provisions that could allow to train new specialists and to generate a safety culture. On the other hand, The second group mentioned the need to establish legal frameworks, based on knowing the experiences of different countries.

At the end of the conclusions of each group, the main moderator, Ernesto Bojórquez, asked the following question to the audience: How do you think the different sectors could collaborate to face the proposed challenges?

After that, several participants approached the microphone to express their intervention. Experiences from countries like Peru, Uruguay and Colombia were shared. The importance and responsibility of governments to maintain public policies, beyond government changes, was also mentioned.

Outputs and other relevant links:
Full session: https://www.youtube.com/watch?v=wlipzllXLxo

By: Raysa Alanes (Las De Sistemas, Argentina) and Juliana Novaes (Artigo 19, Brazil)

Translation: Laura Gabrieli Pereira da Silva (UNESP, Brazil)

Revision: David Paredes Abanto (DIDEPTI SRL, Perú) and Luis Gustavo de Souza Azevedo (UFAC, Brazil)

Coordination and edition: Nathalia Sautchuk Patrício (NIC.br, Brazil) and Guilherme Alves (Youth Observatory, Brazil)