Aspisec

BPF cyber security IGF 2018

Author: Andrea Chiappetta, PHD
CEO
ASPISEC srl
a.chiappetta@aspisec.com

1. How do you define a culture of cybersecurity?

The culture of cybersecurity is still far to be reached correctly from governament and companies due to the lack of knowledge and personnel involved in this specific topic. In several institutions (Public and private) the cybersercurity is considered as a branch of the IT, but security and cybersecurity have different needs.

2. What are typical values and norms that are important to you or your constituents?

The cybersecurity values can be identified in two main categories: 1) provide security to the company and their customers 2) cybersecurity can't be considered as a extraordinary costs but as operational and fundamental to be in the world markets.

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.

Being specialized in cybersecurity with a focus on critical infrastructure protection, what I saw during my activities is the lack of knowledge. At the moment we have several good ideas and main general rules to be followed. What Is totally far from the security issues is the definition of common standard in particular for the IoT or SCADA/ICS/PLC etc, I fundamental issue is the role of FIRMWARE and how the vendors and the end users doesn't know his importance.

4. Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?

In the framework of Critical infrastructures that use firmwares, we saw that no one have launched a real programme to the check it, amend it and finally hardenize it. This problems affects several sectors from trasports to energy and telco.

5. Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?

NA

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

For sure the introduction of the NIS directive at EU level will provide an important legal framework but to general.

7. Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

Absolutely yes, we don't have a common framework. US use their approach, EU doesn't have a common standard, China is setting up their requirements.

Aspisec

www.aspisec.com