2018 IGF BPF Cybersecurity

Marilson Mapa

marilson.mapa@gmail.com Private Sector – GRULAC

1. How do you define a culture of cybersecurity?

A culture of cyber security necessarily implies an ethical stance on the part of all actors. What characterizes the companies responsible for the Internet operation - ISPs, Registrars and RIRs - is an absolute and total lack of ethics. Their abuse teams are trained to lie and cheat the victims of spam and scam. No matter how full the complaint is - full header, full text, identification of all ISPs involved, scanner report proving scam, existence of lawsuits or convictions by Court - nothing is enough for these companies to ban or prevent their criminal client keep sending the reported messages. They protect and hide their customers by acting as accomplices to unlawful acts. It is evident the greed and lack of ethics widely proven among tech giants who are taking huge losses by action from the EU and US. This conclusion is based on an enormous amount of evidence obtained over more than four years making denunciations almost daily.

The behavior of most ISPs, Registrars and RIRs is no different from the illicit activities of companies such as Theranos, Facebook, Cambridge Analytica and Google. They characterize the current rule where ethics and respect for people have been thrown in the trash. This unbridled laissez-faire and the ends justifying the means shaped the current agenda of them: cheat as much as possible, just try not to get caught. Never before so few have done so much harm to so many.

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

Without a policy that mandates ethical behavior with punishment for proven excesses, these criminals who last year broke the 500 billion spam and scam barrier a day (Talos/Cisco) will continue to irritate and steal billions of people around the globe..

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms?

No. In defense of the victims of this system, no. They would have to act against their financial goals. That's exactly what I witnessed in RIPE and ARIN where foxes take care of the henhouse.

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?

All AUPs, ToSs and ASPs, and I know hundreds, are adequate and potentially effective. Only missing administrators who do not confuse liberalism and laissez faire with criminal acts.

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)?

All failed. No ISP, Registrar or RIR obeys your AUPs, ToSs, ASPs and Codes of Conduct. These documents are exposed on their websites to give an air of respectability that they do not have.

The current GDPR was not created to protect the populations, the taxpayers who finance the UN and the bureaucratic apparatus of the European Union. This regulation protects the companies that are victimizing the population and I could see that these companies are more arrogant and more dishonest with this regulation. And I can prove it.

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

We need effective methods to demand ETHICAL BEHAVIOR from internet providers in order to reduce the negative effects to the end users of the internet.

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?

Unfortunately I'm in Brazil. And reports of corruption explode every day. This situation generates a sense of impunity which feeds monsters in all areas. In the sector in question the absurdities go beyond the limits of what would be unthinkable. The last report I sent to the ISP Locaweb had the following subject: **Criminals in action - Season 4 - Chapter 75 (each season has 100 chapter)**. Was the complaint of No. 375. With the knowledge and complicity of Cert.br, Registro.br, Cgi.br e LACNIC (Registrar, Management Committee and RIR).

But let it be clear that what we have in my country is not so different from the grotesque spectacle practiced by tech giants and the thousands of Internet providers.