European Alliance Against Coronavirus

Wednesday 8th July 2020 at 8:30

Cybersecurity in times of COVID-19

Working format is based on "*Gilles Rules*":

1. conceptual framework
2. needs and disruptions
3. solutions

Speakers:

- Eduardo Gistau, Mutua MAZ, Cluster IDiA

Link to session´s recording

1. CONCEPTUAL FRAMEWORK

Real word vs. online word

Speaker Eduardo Gistau has twenty years of experience in cybersecurity. He works for Mutua MAZ, a Spanish company founded in 1905 active in the healthcare and insurance field. It is part of the cluster IDiA.

He stated his speech the differences between fighting crimes in the real and internet world. In the real word, malicious attacks are solved with a superior number of police and deterrent weapons, while in the internet word the companies feel alone in battling the cyber attacks, without real time help from the public sector. Cyber crimes are an "automated" industry and they take advantage of all opportunities: it is a business and the companies are the best customers.

Cybersecurity matters

During the COVID-19 crisis, there was more remote work than usual. This meant that more credentials were exposed, as employees partly had to switch to personal devices. MAZ registered 700 attacks per day (one every 2 minutes) – nearly double the attacks of "normal" times. For the defense, they use a technology from the global market, which is dominated by the USA and China. This creates a strong dependence for EU from these countries, as there is no strong European solution.

Another important issue is the regulatory framework. In the real word, self-defence is allowed while the laws on cybersecurity do not cover to return an attack. The speaker expressed that EU should work on new laws and protocols in order to protect its companies.

Policies on European level

Marek Przeor from DG GROW shared the following information with the group:

- In April 2019 was decided to setup ENISA European Union Agency for Cybersecurity: https://www.enisa.europa.eu/

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA: https://eur-lex.europa.eu/eli/reg/2019/881/oj
- Smart Specialisation Platform, Cybersecurity: https://s3platform.jrc.ec.europa.eu/cybersecurity
- Team responsible: Cybersecurity Technology & Capacity Building (Unit H.1): https://ec.europa.eu/digital-single-market/en/content/cybersecurity-technology-capacity-building-unit-h1

---

2. IDENTIFICATION OF DISRUPTIONS

First disruption: increase of cyberattacks during COVID-19 pandemic

Source: Eduardo Gistau, Mutua MAZ

Evidence: Criminal organizations have several areas where to hit. Over the years, more and more criminal organizations have moved towards the web world because they are less exposed to checks and law enforcement. During the COVID-19 pandemic, there was an increase in smart working and in all activities managed remotely. People use their personal devices more with a greater exposure of credentials and private information. This has generated a sharp increase in cyberattacks. The problem of the increase in cyberattacks within companies is often due to an incorrect update of information systems. Companies don't always have the time and resources to stay protected. In industries, these attacks involve stopping production, logistics and turnover, among other things. For companies it is always a trade-off between the operations flexibility and the systems security. Cybercriminals have always taken advantage of opportunities and they do it even more in times of crisis. The hardest attacks to defend are the personalized ones. The main way that is used for attacks are e-mails (6% of attacks). 90% of cyberattacks are easier to defend, though even more advanced techniques as Artificial Intelligence and Machine Learning are used.

Geographical impact: EU

Stage of value chain: data protection

Character of the disruption: increase of cyberattacks

Time frame: short term

EU actions needed:

- For cybersecurity mechanisms, the European countries need to agree and act together, as web criminality does not know boarders. There is a need for a clearly communicated international governance model for cybersecurity.

Recommendation:

- The collaboration between the private and public entities needs to be strengthened. Ideally, the public entities establish a real-time defense support for the European companies, as time is crucial in this area.

- Need to raise awareness in SMEs and employees about the need for proper security, especially when working remotely.

Second disruption: strong technology dependence on China, Israel, and USA

Source: Athanasios Konstandopoulos, Eduardo Gistau

Evidence: In terms of technology used for protection, the speakers indicated a strong dependence on China, Israel, and the US, both for software and hardware. Up to date, there is no strong technological solution developed in Europe, which could be used by the European companies.

Geographical impact: EU

Stage of value chain: data protection, operations

Character of the disruption: dependence

Time frame: medium - long term

Recommendation:

- Strengthen the effort to create European cyber-defense technologies
- Another path would be to redefine common ways and use new technologies to work online

Third disruption: skill gap in cybersecurity

Source: Eduardo Gistau

Evidence: Highly trained professionals in cybersecurity are leaving Europe to work in the US or in Japan. There, the salaries are much higher, making it more attractive for the professionals.

Geographical impact: EU

Stage of value chain: HRM

Character of the disruption: talent

Time frame: medium - long term

Recommendation:

- Giving incentives and making the workplaces in Europe more attractive for the talents

3. IDENTIFICATION OF NEEDS

1) Public-private collaboration needs to be increased to respond faster to the attacks
2) Clusters can be involved to raise awareness about this topic in the companies

4. SOLUTIONS

1) Clusters can help in narrowing down the specific needs of the companies in Europe to increase their protection. They can build the bridge between the public authorities and the companies.