Cyber Security as Business Enabler

Interview with Mr. Mihai ANDRIES, CISO at BRD - Groupe Société Générale

Mihai ANDRIES *is CISO at BRD, with over 10 years of experience in cyber security and over 20 years of banking experience. He started his activity in BRD in 2001, as IT administrator of the card payment system, then he was network engineer contributing to the design and implementation of the WAN, MAN, LAN networks of the bank. He completed his IT expertise covering the areas of technical architecture, strategy and IT processes to reach the IT Security area, initially operational and later - since 2013 - associated with cyber risk management in support of business activities.*

1. Tell us more about yourself - Can you tell us about your professional career?

I started my Banking job in 2001 as a technical administrator for Card System. My job was to deal the administration and monitoring of the system, but also to deliver technical evidences for suspect transaction investigations on POS and ATMs. This was a very interesting and challenging job. After a year, I switched to a position as network engineer. It was the time of fast and dynamic development, where communication and interconnectivity were crucial. In 2005 I was proposed to open a new function in technical architecture, consisting in ordering, normalization and standardization of technical solutions and implementing a project implementation methodology, for technical support in business projects. I was the head of technical architecture and project managers for 5 years. After that, I moved to a starting new security-linked position in Strategy Process and Security as a manager for this domain, which had an operational security component, which was a Security Operation Center (SOC).

In 2013, I was proposed to take the position of CISO. The reporting was to CIO at that time. I started the CISO function with four people, and after four years, in 2017, CISO become an executive function, in a dedicated security department directly reporting at board level.

2. Going to security basics: What is in general Cyber-security mission?

The cyber-security (or CISO) mission is to Protect and secure the Information Assets (including data, systems, networks and operations) against threats such as cyberattacks, insider, or physical security risks.

3. And what are the main leverages or tools that CISO dispose in order to achieve the mission?

There are 3 main leverages which CISO can dispose:

A) Building, enforcing and implementing the **ISP (Information Security Program**) - by understanding the Organization, Industry regulations, Business Drivers, Stake holders and Influencers, then defining the Security Charter in terms of Governance, Risk framework and Compliance, and finally executing the Program using the associate elements like Budget, Staff, Roadmap and Reporting.

B) **Operating effectively and efficiently** even in face of cyber threats and other security challenges – here is the SOC staffing, tools and procedures like Event management, SIEM, Vulnerability management, Patch management, Incident-response, etc.

C) **Prepare the Changes in an effective Change Management Process** - can be assured by Risk Management for operational changes (including Risk analysis, Exceptions management, Penetration tests, secure Code developing, etc.).

4. What are the main concepts or Security Principles a CISO should apply?

There are a few important security principles in Security:

a) Zero-trust Principle.
b) Security and Privacy by Design.
c) Minimum privileges (or need to know) Principle.
d) Segregation of Duties (or Four eyes) Principle.
e) Security in depth.

5. If we take Zero-trust principle, how is it in line with the fact that doing Business is conditioned having a Trust relation?

Today, we live in a digitalized world, dominated by the Speed of Business, Technology evolutions, and Threats emergence. The interaction between people is more and more in a digital, and virtual interaction. This is where should reign the zero-trust principle: In the virtual interaction between people, because the virtual interaction is significant less secure that the physical interaction (like it was before digitalization era). In conclusion, the trust between human remains the same, but the trust between virtual human is today a challenge.

6. And how to apply Zero-trust concretely in our virtual collaboration?

Apply Zero-trust means first of all a mindset change, respecting some non-intuitive rules when we are on digital interaction like:

- Never trust, always verify.
- Operate under the assumption of data breach.
- Verify continuous.

7. What means Security in Depth?

Security in Depth is implementing more controls harder to bypass as much approaching the trophy. In cyber security the trophy are the information assets. The succession of controls consists of Deterrent, Preventative, Detective and Corrective.

The most economical effective controls for an organization are Preventative controls. There an organization should invest with priority applying the principle that *prevention is better than cure*. But there is no 100% security ever, so override controls is possible, so we have to be prepared with Detective and Corrective controls.

8. Particularly for Romanian context, what are the main cyber security risks?

The cyber security risks are mostly similar in all countries and all sectors, even though the banking sector is more attractive. Usually, the cyber-attacks begun in Western Europe or US and then migrate to the Eastern part in a few weeks, we had the chance to see and prepare it coming. But in present, in the context due to geo-political evolutions the sense has changed. Particularly, in present there are two emerging threats manifesting:

(i) the DDoS attacks and

(ii) the Hacktivism.

Both have as objective the sabotage or negatively affect the services delivered by companies. Particularly for Hacktivism beside the classical ransomware attack, I would underline the countermeasure to secure the data by an offline backup. Anything can be rebuilt but data distorted.

9. What are the main priorities in the next years to improve the security resiliency?

One emergent is the interior threats increase so the actions to mitigate this risk are the priority. DLP and the enforcement of classification of information and its adoption by the information owners, is a driver to apply appropriate security measures in balance with the sensitivity (access to information, transfers).

Another context where is important to increase security is the DevOps to secure the code security in Continuous Integration and Continuous Delivery processes.

A constant very sensitive attention is on vulnerabilities. If we make a comparison, the vulnerabilities represent the toxic consequence of the new digitalization era, as pollution is the toxic consequence of industrialization. As, if for exposed systems organizations are very carefully to mitigate in time, for internal systems nowadays required to be more determinate in applying the specific security controls.

And last, but not the least, adopting new technologies based on AI & ML (Artificial Intelligence and Machine Learning) is a good investment. From these technologies, perspective analyzing, as example, the Internet network traffic is an effective control in case of data exfiltration and/or suspect malware traffic detection.

10. As the CISO of a big Romanian bank with all the responsibilities it includes, do you sleep well at night?

I do sleep well. The risk "Zero" does not exist but I have the satisfaction about the achievements made and I know I do the maximum. However, I must admit that if I think about something inefficient or not achieved, I may go fixing it before sleeping.

Interview conducted by Gabriel PETRICĂ
RAISA - Romanian Association for Information Security Assurance