Interview with Mr. Teodor CIMPOEȘU

Mr. Teodor CIMPOESU is a seasoned information security professional, with a background formation in management and marketing as well. For the past 5 years he held the position of managing director for Kaspersky Lab Romania and Bulgaria, building upon other previous 5 years of technical and project and product management experience inside the company.

Since mid-2014 he now holds the position of CyberSecurity Director with CERTSIGN, an UTI Grup company, leading the business unit responsible of delivering cyber security services on a MSSP model, along with complex infosec projects and formal training.

1. UTI organized the Conference Cybersecurity Day in October 2014, an event which launched the first private CERT from Romania. What role will play this private CERT and how will cooperate with CERT-RO and other similar structures?

Any CERT system has to be able to respond quickly and most effectively to any cybersecurity incident and to be the leading provider of security services in such situations. Exactly this is the role I attributed to this CERT. In addition, certSIGN wants to assert its position, together with CERT-RO, as the main source of education and awareness both companies and the general public about the dangers of cybercrime and security on the main measures to be considered.

Relationship with CERT-RO is and will continue to be one of closely collaboration and completion. Also, given that, in the fight against cybercrime collaboration and cooperation is essential, we should mention that we started working with other similar structures, both national and international.

2. How fast will be the response of this private CERT in case of large-scale cyber-attacks?

The reaction time is extremely short. The size of logistics and the quality of the experts in this structure allow an extremely fast reaction time. But some clarifications should be made in the sense that the CERT, as a structure, has a role of information and dissemination rather than reaction. certSIGN has developed through the SOC (Security Operation Center) an important reactive capacity. A key factor to the success of a reaction is the institutional cooperation with similar institutions, both governmental and private.

3. Cyber-attacks are becoming day by day more sophisticate. How do you think these attacks will evolve in Romania in the coming years?

Things have changed considerably in recent years. If a few years ago we were discussing pretty much about malware and related offenses, today we are facing concepts like cyber war and cyber espionage. Basically, we are witnessing an increased involvement of large states in this area. If we make a parallel with the 80s we witness a new arms race, only this time the playground is the Internet. Given the above, we believe that in the next years attacks will focus mainly on the cyber infrastructure of national interest (so-called critical infrastructure). At the same time we should carefully watch for the attacks on domestic devices (Internet of Things).

4. Multiple systems in Romania were the target of APT attacks. What methods of prevention and response would exist if such attacks occur?

An interesting fact is that these attacks were mainly going after government computer systems. We believe that this happened for two reasons: on the one hand, the attackers had an appetite for this area, obtaining governmental confidential information and on the other hand, insufficient security measures available at this time created a vulnerability for the hackers. As ways of prevention and response, is essential to create a legal framework for cooperation between the governmental and private in information security area. If we look at other countries it is obvious that security is the result of a good cooperation in this direction.

5. Lately it was reported a massive increase in cyber-attacks targeting bank accounts. How to protect bank customers from programs created for stealing financial information? How safe are online transactions?

In this case we are talking about a simple fact. Nowadays, we can’t talk about governmental or private actors with attributions in the area of information security, but ordinary people who want to make online transactions and secure payments. First, we consider that it takes a minimum safety culture, as a comparison when before the meal, you should wash your hands, and on the other hand the ability of the banks to invest in safe systems. Another important aspect is that banking environment need to impose greater transparency in the sense of reporting attacks on its systems or its clients. You can’t protect yourself from something that obviously you do not know anything about and that security through obscurity is no longer an option.

6. What solutions should people apply in order to guarantee the authenticity, integrity and confidentiality of data transmitted electronically?

The answer is straightforward and widely recognized internationally: digital certificates and electronic signatures. Now, the electronic signature with encryption are the only methods that provide guarantee authenticity, integrity and confidentiality of data.

However, users should be aware that these data are transmitted in a volume higher increasingly via mobile devices. They must also be secured and certSIGN provides customers security solutions data transmitted via mobile devices (voice, text messaging) and mobile electronic signature.

7. For years tax returns may be submitted online, through a service on the website of the National Agency for Fiscal Administration, by those who have a digital certificate. Why would you recommend taxpayers to have its own digital signature to file statements online and not ANAF counters?

The electronic signature will make them more efficient. With its help they will give legal value to any type of digital document; not only tax returns.

There will be no need, therefore, to print documents, to sign and stamp them, process them, send them by courier etc. Costs related to the handling of these items will be removed, and the time required for their manufacture will be substantially reduced. Instead, they will save time and communicate faster, better and safer.

The electronic signature will also provide coverage in case of dispute. Under the current legislation, the electronic signature has indisputable legal value. Therefore, if the organization comes to court and the documents' authenticity is being questioned, the validity of the electronic signature used is easily demonstrated and can’t be challenged.

Equally important, the electronic signature provides non-repudiation, integrity and confidentiality. Using it, they can be sure that the organizations' data will get where they must, guaranteeing that there have not been viewed or altered by unauthorized persons.

8. One of the latest trends is the use of cloud computing technology, allowing companies to outsource data and applications to virtual platforms. What kind of advantages will have the Romanian companies if they use this technology? Are there any security risks?

Cloud computing is a new challenge for security. It is obvious that, for reasons of business optimization, a number of companies are choosing to move their cloud infrastructure. We're talking about optimization, cost reduction and flexibility. However, the security risks associated are not trivial and in 99% of cases they are related to the cloud provider. In other words, if you trust the provider to move your infrastructure to the cloud, if not, and you still want to do this move, you should better have a good lawyer. Risks are primarily related to data privacy and the fact that there are no viable technical mechanisms to ensure this in the case of processed data and how corporate data is processed/used by the cloud provider.

Interview made by Ioan-Cosmin MIHAI
Vice President of RAISA