Editorial

Cybersecurity - a Romanian Perspective in the European Context

Gabriel Petrică
Faculty of ETTI, University POLITEHNICA of Bucharest, Romania

Cyber security is a current and high interest concern, its challenges being the emergence of new vulnerabilities (in operating systems and Web applications) or threats (like APT) and the permanent change of the attackers' interest regarding their targets.

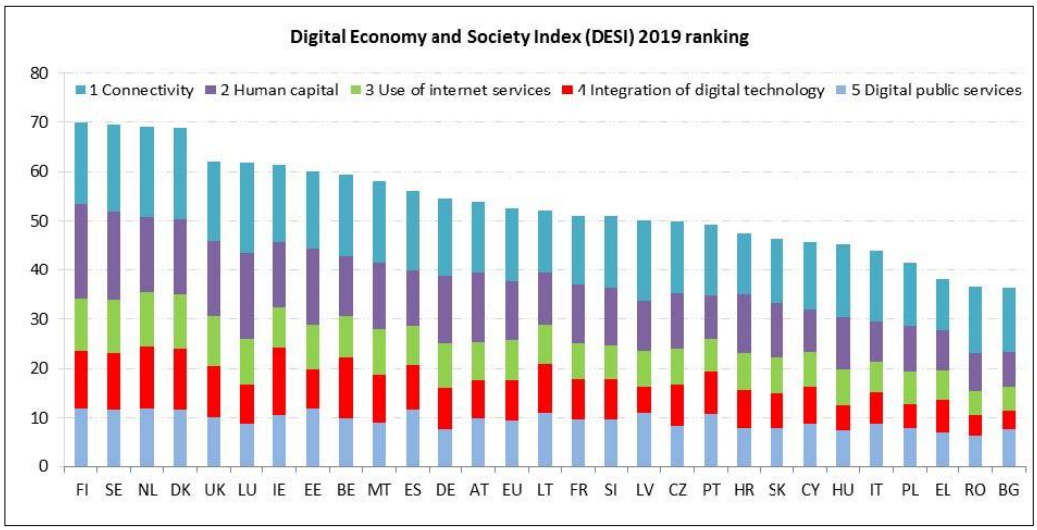
According to ENISA's Threat Landscape Report 2018[1], some changes in the cyber threat hierarchy occurred in 2018: the number of Denial of Service, Botnets, Data Breaches and Information Leakage threats increased, while threats like Spam and Ransomware have declined. Specific to 2018 was the emergence of a new motivation of the attackers, namely the monetization of their actions, which led to a new entry in the top of threat: Cryptojacking. However, the most common types of threats have remained the same as in 2017, in order: Malware, Web-based Attacks, Web Application Attacks and Phishing.

The recent evolution of cyber threats in Romania is presented by the analysis elaborated by the Romanian National Computer Security Incident Response Team (CERT-RO) for 2018[2]. At national level it is noteworthy that the main class of cyber incidents is represented by the vulnerable systems (unsecured, incorrectly configured or which needs updating) - 80.57%, followed by botnet malware (11.91%) and compromised systems (7.02%). Like the general trend, also in Romania there has been a significant increase of Cryptojacking attacks, the most common malware being MoneroMiner, CoinMiner and BitcoinMiner. The CERT-RO analysis also reveals that the cyber-attacks originated from countries from almost all areas of the world.

In the European Commission's Digital Economy and Society Index (DESI) country report for 2019[3], Romania is placed on the same penultimate place among the states of the European Union (27th place), yet scoring higher than in 2018 (36.5 vs. 35.4), while in the European Union the average score for 2019 was 52.5 (increasing from 49.8 in 2018). Romania's best rank is in the chapter of fixed and mobile Connectivity (22nd

[1] ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[2] CERT-RO, Threats evolution in the Romanian cyberspace 2018, https://cert.ro/vezi/document/cert-ro-cyberthreats-2018
[3] Digital Economy and Society Index (DESI) - 2019 Country Report - Romania, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59905

place in the EU), mainly due to the high-speed and very high-speed broadband fixed networks (implemented especially in the urban areas). For the other 3 considered domains in the country index, Romania occupies the last places (Human capital - 27th place, Use of Internet services - 28th place, Integration of digital technology - 27th place).



Source: Digital Economy and Society Index (DESI) - 2019 Country Report - Romania

Approved by the Government Decision no. 245 / April 7, 2015, the National Strategy on the Digital Agenda for Romania 2020[4] contains the measures that Romania should take in order to reach a level of development similar to the countries in the region and to integrate into Europe's digital single market from the point of view of ICT. Although the Romanian IT and telecommunications fields has been characterized in the last years by a sustained development both at technical (hardware and software) and legislative level to adapt to the requirements of the European Union, a slow progress is observed in the considered areas, and the measures taken have had a limited impact so far.

In order to improve the rank and bring as close as possible to the objectives set by the national Digital Agenda, Romania must urgently adopt a set of measures that will remove our country from the cluster of low performing countries. Regarding this objective, a strategic area that should be given special attention is lifelong education. Professional training and specialization programs within companies, as well as the public-private partnerships established between universities and companies, are aspects that stimulate education and research, but also ensure a better integration in the labor market of young graduates (at present Romania ranks 6th in Europe, with 4.9% of graduates from the ICT learning field). The existence of awareness and learning programs on cyber security and the risks exposed by Internet users is necessary for all age groups, contributing to the enrichment of the cyber culture of any user regardless his

[4] Digital Agenda for Romania 2020, https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/Strategia-Nationala-Agenda-Digitala-pentru-Romania-2020-aprobata-feb-2015.doc

age. Through public events (conferences, seminars, workshops, or hackathons) dissemination of information between specialists and stakeholders is realized, the collaborations are improved, and the horizons of knowledge are diversified.

On the occasion of the Romanian Presidency of the Council of the European Union, a mandate that was held from January 1 to June 30, 2019, our country has elaborated a working agenda focused on the following four pillars: *"1. Europe of convergence (ensuring convergence and cohesion for a sustainable and fair development for all citizens and Member States); 2. A safer Europe: making Europe safer by increasing cohesion among Member States facing new security challenges that threaten citizens' safety and by supporting cooperation initiatives in this area; 3. Europe, a stronger global actor (enhancing Europe's global role); 4. Europe of common values (stimulating EU solidarity and cohesion)."* [5]

Within the second pillar, security at European level is approached as a complex concept that concerns not only the internal security and external borders of the EU, but also the issues of migration, the fight against terrorism, the functioning of the Schengen Area or cyber security. In the latter case it is necessary to take additional measures in order to increase the resilience of the EU to cyber-attacks, starting from the current revision of the EU strategy regarding cyber security (NIS Directive and GDPR Regulation, adopted in 2016).

Ensuring the security of individuals, companies, organizations or governmental authorities in the virtual environment is a mandatory, strategic objective that must be considered in all public policies and projects carried out within the EU. A higher level of cyber security can be achieved through a better collaboration of all the entities involved in creating an environment convenient to the exchange of opinions, information, knowledge and good practices, at European level. These actions will lead to improved detection and response times to hybrid threats, defined as *"the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare."* [6]

As measures to improve cyber security can be mentioned: users training programs, awareness actions regarding threats and vulnerability, security alerts management, access rights policies, setting up networks and information systems for a high level of

[5] PROGRAMME of the Romanian Presidency of the Council of the European Union, https://www.romania2019.eu/wp-content/uploads/2017/11/en_rogramme_ropres2019.pdf

[6] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018

data security and privacy, compliance with and adoption of European and international standards in the field.

During this period, one of the public events dedicated to cyber security training and awareness is CyberEDU 2019, held under the aegis of the Romanian and Finnish Presidencies of the Council of the EU and in partnership with main European and international stakeholders. "*Generally, all decision makers agree it should take THE prime spot on the agenda and this is even reflected in the national cyber strategies all around the EU. But when discussing investments in both public and private organisations there is a proven lack of follow-up most of the time. Being under budgeted for years it leaves place for little improvement and never-ending repetition of this well-known myth 'human as the weakest link'. CyberEDU 2019 aims at creating synergies under a new paradigm 'humans as the last line of defence' in cyber security and offer more ideas for cyber skills within a lifelong learning context.*"[7]

The objectives of the current information society are represented by both the data storage and processing in the cloud and the accelerated development of the IoT and mobile devices. Classic attacks (phishing, scamming or social engineering) launched via e-mail or Web will continue to exist, but new hardware and software technologies are coming with both high performance and new specific vulnerabilities which developers and IT specialists will have to deal.

[7] CyberEDU2019: CyberEDU round table process, https://easychair.org/cfp/CyberEDU_2019