A cyber security mass education perspective

Sorin TOPOR, Adrian Victor VEVERA

National Institute for Research & Development in Informatics – ICI Bucharest,
8-10 Maresal Averescu Avenue, sector 1, Bucharest, Romania

sorin.topor@ici.ro

Abstract: *Cyber security education is extremely important for a digital society. The research aims to identify some benchmarks and formulate some proposals for the realization of an adequate mass education in the field of cyber security.*

Keywords: Cyber security, Mass education, Education through entertainment.

1. Introduction

Ensuring cyber security is a major concern for any digital society. In the view of the President of Romania, Klaus Iohannis, the new organizational models of the educational system must be able to respond to the majority of contemporary social changes (President of Romania, 2018).

Romania's first cyber security strategy (2013) established a series of objectives for the protection of cyber infrastructures belonging to governmental, public and private institutions (H.G. no. 271/2013). In 2021, the new strategy aims to increase the level of resilience and the formation of a solid culture of population security (Government of Romania, 2022).

Our research aims to identify some benchmarks and formulate some proposals for the realization of an adequate education in the field of cyber security.

2. Critical analysis of the state of national cyber security

The last few years have seen a staggering evolution of cyber threats (Zamfiroiu, 2022) on the Internet. Malware, IoT malware and cryptojacking, ransomware, as well as AI and quantum attacks, supported by new languages and powerful platforms, have enabled an expansion of cyber-attack tactics forcing specialists to identify advanced solutions for an infrastructure to be prepared to bear and to revitalize them.

Specialized structures continuously monitor and systematically publish analyses of all identified cyber threats. Specialists at SonicWall Capture Labs pointed out that ransomware threats have grown at an annual rate of 21%, of which Ransomware-as-a-Service (RaaS) is the most present.

https://doi.org/10.58503/icvl-v18y202322

The Network and Information Security (NIS) Directive on cyber security (revised), adopted in July 2016, allowed many European states to replace their existing legislation to facilitate cyber risk management and created the framework for forming a cooperative network for mutual learning based on best practices (EUR-Lex, 2016).

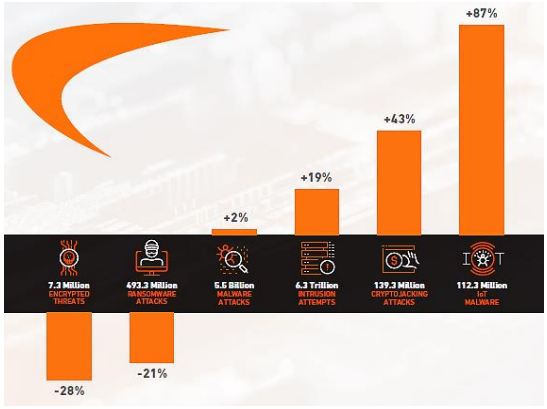

Figure 1. Cyber threat analysis for the year 2022 (SonicWall, 2023)

In order to ensure a state of normality in the cyber space, Romania proposes the establishment and operationalization of a National Cyber Security System (Government, 2022). According to GEO no. 104/2021, the National Cyber Security Directorate was established, which took over the duties of CERT-RO and can face, dynamically, the challenges in the field of cyber security through efficient, flexible and proactive mechanisms, procedures and capabilities (Government of Romania, GEO no. 104/2021).

A strong support of cybersecurity innovation and research is achieved through the establishment of the European Cybersecurity Competence Center as the authority responsible for managing EU funds for the adoption of cybersecurity work programmes. (GSG, 2021).

With the launch of Russia's Special Operation on Ukraine (2022), cyber threats have diversified. Their convergence with electronic warfare has made it easy for phishing attacks to move out of the spam e-mail realm of the Internet into products applicable to any social communication platform. Smishing messages (SMS phishing) have a rate of approx. 98% (Sara, 2020). The State of the Phish report shows that the average for 2022 was 300,000-400,000 daily attempts to deliver mobile-oriented attacks, with August peaking at 600,000 attacks per day (proofprint, 2023). On the Ukrainian front, the cyber-attacks identified (Schwart M.J., 2023), especially in the first phases of the fighting, were voice phishing (vishing). Originating from the environment of organized crime, they facilitated the identification of commanders and the degradation of troop morale. The victim is encouraged to provide personal data over the phone based on a narrative story (Barza, 2018).

Under these conditions, European states and NATO have adopted a series of urgent security and proactive cyber defense measures. Among these is the need to allocate funds for investment in cyber security education.

Reforms in education were proposed and implemented, the legal framework was created for the training of specialists, cyber security strategies were adapted and modernized, which generated a lot of plans and measures to maintain a state of normalcy in cyberspace.

Centres and institutions were created with the role of monitoring and rapid specialized intervention with the role not only of limiting cybercrime but also of informing about new threats in cyberspace.

EduRank classifies as the best six universities in Romania that offer specialist training programs for cyber security as follows (EduRank, 2023): the Polytechnic University of Bucharest (121st place in Europe and 403rd in the world); the Polytechnic University of Timișoara (222nd place in Europe and 674th in the world); the Alexandru Ioan Cuza University in Iași (230th place in Europe and 713th in the world); the Technical University of Cluj-Napoca (245th place in Europe and 781st in the world); the Bucharest Academy of Economic Studies (259th place in Europe and 820th in the world); the Bucharest University (276th place in Europe and 890th in the world). The ranking is based on the universities' performance in scientific research in the field, based on publication ratings, without distinguishing between undergraduate and postgraduate programs.

2. Education markers according to the age of the population

Through education, the citizens of a state develop their knowledge and skills in various fields that belong to the real sciences and/or humanities, ethics and morals, but also in other contexts such as: in the family, through the media, through the Internet, through discussions with friends, etc.

The particularities of education classified by age are (Eurydice, 2022):

1. Pre-schoolers: Retain isolated words and accept routine; Not being able to write, instructions are memorized through pictures, real objects, songs etc.; They need a protector (educator, pedagogue, teacher, etc.) who gives them parental affection in order to feel comfortable; Technology is a novelty that attracts them with colour and movement.

2. Schoolchildren/children: Learn from drama activities and short stories to keep them interested; Competitiveness is stimulated through games, contests and competitions; The technology is used for games.

3. Adolescents/Young People: They are pragmatic and need to understand what they are learning for; Appreciates freedom of expression and autonomy in selecting topics; They need external stimuli: interesting subject, dynamic and engaging knowledge transfer style, appreciation of results; Use technology for learning and networking.

4. Adults: Are self-motivated to achieve performance for a well-defined target determined by their performance and social status; Learning is based on schemes, rules and logical explanations; They pay attention to the quality and performance of technology and use it mainly for professional purposes, for networking and entertainment.

5. Seniors: Do not learn out of obligation; Prefers short and well-directed forms of learning to find answers to problems arising in daily activity; Values review and recapitulation as a form of repeated exposition of knowledge for long-term fixation; Appreciates informal discussions in the native language; Use technology only when needed.

3. Research results

The results obtained are based on the interpretation of statistical data published in various profile reports and discussions with specialists. We note that:

1. Cyberattacks aimed exclusively at children are relatively few. With parental control functions, the responsibility of ensuring cyber security rests with parents, family and tutors (for institutionalized education).
2. For teenagers a ban without proper justification will attract them and not deter them. They will not have the patience to understand the effects of the action but will seek to stand out by demonstrating that they have the skills to achieve a goal. Many open-source tools are available on the Internet. Networking is mainly on social media platforms. Looking at cyber security learns about specific events in which members of the social groups they activate are involved.
3. Adults understand the need to apply cyber security measures. Their expectations are that IT and computing applications include cyber security and that identified vulnerabilities are automatically corrected through patch solutions. Most adults follow the rules of cyber security. However, due to professional, social or family grievances or, simply, by elusions the cyber hygiene rules, they can create cyber security breaches.
4. Seniors initially reject cybersecurity solutions. Self-direction and self-determination become the main factors of organizing their evolution. Past experiences cannot be bypassed. Information technologies are considered complementary and not supplementary elements.

4. Conclusions and proposals

Another future work would consist in finding solutions to others methods (developments of actual methods) and collecting more important information about the enterprises (Dumitrache, 2020) and their educational particularities.

A mass education in the field of cyber security is possible if it is organized distinctly, through programs by categories of learning ages.

We propose the following solutions:

1. For children (school and preschoolers) specific education can be achieved through physical and online games. Kids can control a character on an itinerary with various suggestive challenges. Games must educate them to follow the rules of internet navigation and parental controls.
2. Teenagers are big consumers of cyber services and applications. Strategy games can be a solution. We give the example of the "Hacker Evolution" series which, even though the game is based on the simulated use of hacking techniques, teaches users where the vulnerabilities and cyber security problems are. Following the players networks it can create new scenarios or improve them.
3. For adults, education in the field of cyber security must follow two priority directions: education in support of his profession and societal education. An adult has a wide range of physical and online data libraries at his disposal. In addition to its education, we propose the use the TV entertainment. For example, "MasterChef Romania" (MasterChef International franchise) raised the level of education in the art of cooking. "Romanians have talent" (Reality TV Show Got Talent franchise) identifies and prepare potential artists. Fashion education is done through "Bravo, you have style!" (concept TV Show "My Style Rocks"). We believe the same recipe can be applied to cybersecurity education. When a televiewer sees how quickly access to a poorly protected account can be broken, they will understand the need to use complex key password. Moreover, the cyber security spectacle will deter hackers from further using their skills on an educated community.
4. The writing of instructions and user manuals of all products for seniors must be in the native language, well organized and with a legible narrative content, because many vision problems appear with advancing age. Seniors are no longer willing to learn what is required of them. In addition, in order to avoid becoming victims of vishing attacks, a radio show should be created that systematically repeats tips from lessons learned and the experience of others.

The solutions offered are a start for identifying new forms of mass education in the field of cyber security, in support of traditional education. These prospects require entrepreneurs willing to take large doses of risk in the future. However, investing in education is and will be the most profitable business for a healthy environment.

Acknowledgment

The research for this article is conducted within the project "PN 23 38 04 01 Resilient and Interoperable Communication Systems based on Distributed Technologies and Self-Sovereign Digital Identity (RoDID)", funded by the Advanced Research Program based on Emerging and Disruptive Technologies - Support for the Society of the Future (FUTURE TECH).

REFERENCES

Barza, V. (2018) *CERT-RO avertizează asupra vishing-ului, o tentativă de păcălire a utilizatorilor cu ajutorul apelurilor telefonice*. HotNews.ro, EUROfonduri, https://economie.hotnews.ro/stiri-it-22706173-cert-avertizeaz-asupra-vishing-ului-tentativ-lire-utilizatorilor-ajutorul-apelurilor-telefonice.htm [Accessed 22 May 2023].

Dumitrache, M. at al. (2020) Re-modeling and Simulation of an Economic Map System Based on System Dynamic Principles – Case Study in Southern Romania. *Studies in Informatics and Control*. 29(2), 255-264. https://sic.ici.ro/wp-content/uploads/2020/06/Art.-10-Issue-2-SIC-2020.pdf [Accessed 21st April 2023].

EduRank. (2023) *6 Best universities for Cyber Security in Romania*, https://edurank.org/cs/cybersecurity/ro/ [Accessed 22nd May 2023].

EUR-Lex. (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems in the Union [Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune]. *EU Oficial Journal*. L. 194. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=OJ:L:2016:194:TOC [Accessed 11th May 2023].

Eurydice. (2022) *Organisation of the education system and of its structure*, https://eurydice.eacea.ec.europa.eu/national-education-systems/romania/organisation-education-system-and-its-structure [Accessed 12th June 2023].

Government of Romania. (2021) GEO no. 104 of September 22, 2021, regarding the establishment of the National Cyber Security Directorate (Ordonanță de urgență nr. 104 din 22 septembrie 2021, privind înființarea Directoratului Național de Securitate Cibernetică), *M.Of. nr. 918/2021*, https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652 [Accessed 19th May 2023].

Government of Romania. (2022) Romania's cyber security strategy of December 30, 2021 for the period 2022-2027 (Strategia de securitate cibernetică a României din 30 decembrie 2021 pentru perioada 2022-2027). *M.Of. nr. 2bis/3.01.2022*. https://legislatie.just.ro/Public/DetaliiDocument/250235 [Accessed 17th May 2023].

Government. (2022) Romania's security strategy of December 30, 2021, for the period 2022-2027 (Strategia de securitate a României din 30 decembrie 2021,

pentru perioada 2022-2027). *MOf nr. 2/2022*. https://legislatie.just.ro/Public/DetaliiDocument/250235 [Accessed 19th May 2023].

GSG. (2021) The General Secretariat of the Government is completing the establishment of the European Cyber Security Center in Bucharest (Secretariatul General al Guvernului duce la bun sfârșit înființarea la București a Centrului european de securitate cibernetică). https://sgg.gov.ro/1/secretariatul-general-al-guvernului-duce-la-bun-sfarsit-infiintarea-la-bucuresti-a-centrului-european-de-securitate-cibernetica/ [Accessed 19th May 2023].

H.G. no. 271/2013 for the approval of the Cyber Security Strategy of Romania and the Action Plan at the national level regarding the implementation of the National Cyber Security System (H. G. nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică). *M. Of. Partea I nr. 296/23.05.2013.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf. [Accessed 07 June 2023].

President of Romania. (2018) EDU Romania educated, Project of the President of Romania, Klaus Iohannis, Vision and strategy 2018-2030 (EDU România educată, Proiect al Președintelui României, Klaus Iohannis, Viziune și strategie 2018-2030), http://www.romaniaeducata.eu/wp-content/uploads/2018/11/Romania-Educata-Viziune.pdf [Accessed 06 June 2023].

Proofpoint. (2023) *State of the Phish, an in-depth exploration of user awareness, vulnerability and resilience*. Report, p.5, https://www.proofpoint.com/us/resources/threat-reports/state-of-phish [Accessed 22nd May 2023].

Sara. (2020) *Email Marketing Vs SMS Marketing – Where To invest?* NotifyVisitors blog, https://www.notifyvisitors.com/blog/email-marketing-vs-sms-marketing/ [Accesed 22nd May 2023].

Schwart, M. J. (2023) Ukraine Facing Phishing Attacks, Information Operations, Russia's Invasion Tactics Include Creating Fake Hactivist Groups, Researcher Find, BankInfo Security, https://www.bankinfosecurity.com/ukraine-facing-phishing-attacks-information-operations-a-21704 [Accesed 22nd May 2023].

SonicWall. (2023) *SonicWall Cyber Threat Report, Charting cybercrime's shifting frontlines*. (Contact sales) https://www.sonicwall.com/2023-cyber-threat-report/ [Accessed 17th May 2023].

Zamfiroiu, A. et al. (2022) Using Learning Analytics for Analyzing Students' Behaviour in Online Learning. *Studies in Informatics and Control*. 31(3), 63-74. https://sic.ici.ro/wp-content/uploads/2022/09/Art.-6-Issue-3-2022.pdf [Accessed 15th March 2023].