Institutul European din România

Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu

Ioan-Cosmin MIHAI (coordonator)
Costel CIUCHI
Gabriel-Marius PETRICĂ

STUDII DE STRATEGIE ȘI POLITICI - SPOS 2017 - **NR. 4**

Institutul European din România

Studii de Strategie și Politici SPOS 2017

Studiul nr. 4

Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu

Autori:

Ioan-Cosmin MIHAI (coordonator)

Costel CIUCHI

Gabriel-Marius PETRICĂ

București, 2018

Coordonator de proiect din partea Institutului European din România: Mihai Sebe

Bd. Regina Elisabeta, nr. 7-9
Sector 3, București
www.ier.ro

Grafică și DTP: Monica Dumitrescu

ISBN online: 978-606-8202-60-0

Despre autori:

Ioan-Cosmin Mihai este cercetător în domeniile securității și criminalității cibernetice, conferențiar, formator și speaker. Este conferențiar universitar în cadrul Academiei de Poliție „Alexandru Ioan Cuza", profesor asociat al Universității Politehnica din București și profesor onorific al CT University, India, unde predă discipline legate de tehnologia informației, securitate și criminalitate cibernetică. Este formator acreditat în cadrul Centrului Român de Excelență în Combaterea Criminalității Informatice, cercetător al laboratorului „Calitate, Fiabilitate și Tehnologii Informatice" din cadrul Universității Politehnica din București și vicepreședinte al Asociației Române pentru Asigurarea Securității Informației. Cu un doctorat și un postdoctorat în domeniul securității cibernetice și un master în cooperare internațională, organizat de CEPOL – Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii, a dezvoltat numeroase proiecte de cercetare, a publicat 15 cărți și a scris peste 50 de articole științifice. Din 2012 este redactor șef al revistei științifice IJISC - International Journal of Information Security and Cybercrime, indexată în numeroase baze de date internaționale.

Costel Ciuchi este Senior Information Technology Expert în cadrul Direcției pentru Tehnologia Informației din Secretariatul General al Guvernului cu responsabilități în dezvoltarea infrastructurii guvernamentale, securitatea serviciilor şi resurselor informatice (INFOSEC), coordonarea activităţilor de dezvoltare a aplicaţiilor guvernamentale și a registrului de domenii GOV.RO. Profesor asociat al Facultății de Electronică, Telecomunicații și Tehnologia Informației din Universitatea Politehnica din București, susține prelegeri de curs și ore de aplicații în domeniile structurilor de date, programarea sistemelor de calcul, securității serviciilor internet. Este autor / coautor a numeroase articole și lucrări în domeniul modelării proceselor decizionale - business intelligence, managementul riscurilor și al securității sistemelor informatice. Coordonator al sectorului IT pentru Summitul NATO de la București din 2008, participă activ ca expert în diverse granturi și proiecte în sectorul IT (PHARE, Banca Mondială), și desfășoară activități de dezvoltare în domeniul structurării proceselor decizionale și a datelor complexe (big data, open data), cybersecurity (reziliența și survivabilitate) și managementul riscului de securitate.

Gabriel-Marius Petrică este specialist IT, absolvent al Facultății de Electronică și Telecomunicații, Universitatea Politehnica din București - UPB (1998) și al programului de studii aprofundate Ingineria Calității și Fiabilității din cadrul aceleiași facultăți (2000). A publicat, ca autor sau coautor, 4 cărți și peste 20 de articole științifice în reviste indexate BDI și volume ale unor conferințe internaționale, având ca principale teme tehnologiile Internet și managementul datelor electronice. Este membru fondator și director executiv al Asociației Române pentru Asigurarea Securității Informației și membru în Consiliul Editorial al revistei International Journal of Information Security and Cybercrime. În prezent desfășoară activități didactice și de cercetare în Facultatea de Electronică, Telecomunicații și Tehnologia Informației - ETTI, UPB și este doctorand al Școlii Doctorale ETTI din UPB, tema cercetărilor sale fiind studiul securității sistemelor informatice în mediul online.

About the authors:

Ioan-Cosmin Mihai is a cybersecurity and cybercrime researcher, lecturer, trainer and conference speaker. He is Associate Professor at "Alexandru Ioan Cuza" Police Academy and University Politehnica of Bucharest, Romania, and Honorary Professor at CT University, India, where he is teaching subjects related to information technology, cybersecurity and cybercrime. He is a certified trainer at The Romanian Centre of Excellence for Cybercrime, researcher at "Quality, Reliability and Information Technology" Laboratory from University Politehnica of Bucharest, and Vice President of Romanian Association for Information Security Assurance. With a PhD and postdoctoral studies in cybersecurity and a European Joint Master Programme in international cooperation, organized by CEPOL – European Union Agency for Law Enforcement Training, he has developed many research projects and published 15 books and more than 50 scientific articles. Since 2012 he has been editor-in-chief of the scientific journal IJISC - International Journal of Information Security and Cybercrime, indexed in international databases.

Costel Ciuchi, PhD, is a Senior Information Technology Expert in the Information Technology Directorate of the General Secretariat of the Government with responsibilities in developing governmental infrastructure, managing security of IT services and resources (INFOSEC), coordinating governmental applications development and GOV.RO Domain Registry. Associate Professor at the Faculty of Electronics, Telecommunications and Information Technology at University Politehnica of Bucharest, holds lectures and courses in the fields of data structures, computing systems programming, Internet services security. He is author / co-author of numerous articles and papers in the field of decision-making modeling - business intelligence, risk management and security of IT systems. Coordinator of the IT sector for the NATO Summit in Bucharest in 2008, he actively participates as an expert in various IT research grants and projects (PHARE, World Bank) and conducts development activities in the field of decision making and complex data (big data, open data), cybersecurity (resilience and survivability) and security risk management.

Gabriel-Marius Petrică, IT specialist, has received the B.Sc. degree in Applied Electronics from University Politehnica of Bucharest (UPB), Faculty of Electronics and Telecommunications (1998) and the M.Sc. degree in Quality and Reliability Engineering from UPB (2000). He is lead author or co-author of 4 books and more than 20 scientific articles published in journals and proceedings of international conferences, on topics related to Internet technologies and electronic data management. He is a founding member and executive director of the Romanian Association for Information Security Assurance and a member of the Editorial Board of International Journal of Information Security and Cybercrime. Currently, he performs teaching and research activities at the Faculty of Electronics, Telecommunications and Information Technology (ETTI) - UPB and is a PhD student at The Doctoral School of the Faculty of ETTI - UPB, his area of interest being the research on cybersecurity in the online environment.

CUPRINS

Listă figuri

Listă tabele

EXECUTIVE SUMMARY

We consider that the research project "*Current challenges in the field of cybersecurity – the impact and Romania's contribution to the field*" was in itself a "challenge" for the authors, not only on a technical level, achieving the analyzes and elaborating the considerations, but also on a professional level. The opportunity offered by the European Institute of Romania to write this study has allowed us to carry out an extensive, timely, and objective analysis of the state of our country in the field of cybersecurity.

The current context links us indissolubly by the Internet, used to conduct daily activities, at office or home, and to transfer information between all entities, from companies, organizations, and government agencies to end-users. Cyberspace generates opportunities to develop the information society, as well as risks to its functioning. The existence of vulnerabilities in computer systems, which can be exploited by organized clusters, makes securing cyberspace a major concern for all the entities involved. Potentially vulnerable to cyber-attacks are not only the physical environment - mobile equipment, computer systems, smartphones, etc., but also logical environment - operating systems, applications, e-mail services, information transfers between companies or cloud operations.

The general objective of this research project is to analyze current cyberspace challenges, identifying threats, vulnerabilities, and risks to cybersecurity. Romania's capacity to respond to the threats present in the virtual environment, both at national, European, and regional levels, is being studied.

The specific objectives of the project are to identify and classify vulnerabilities and risks present in cyberspace, to analyze the evolution and structure of cyberattacks, to identify best practices to prevent and mitigate the effects of these attacks, to research Romania's preparedness to counteract the risks and challenges from the cyberspace, to analyze the public-private cooperation in the field of cybersecurity and to propose cybersecurity policies for harmonizing the Romanian regulatory framework with the European recommendations in the field.

The research accomplished in this study used both qualitative and quantitative methods. The methods used in the qualitative research were participatory observation, case studies, comparative studies, and analysis of the specialized bibliography. Quantitative research has been directed towards verifying the obtained theories through qualitative research and used surveys as research methods.

Presentation of the study

The first chapter, "***General Aspects of Cybersecurity***", starts from identifying the concept of ***cybersecurity***, that state of normality of digital information, resources and services provided by public or private entities in the virtual space. Protecting IT&C (Information Technology and Communications) systems and their content has been well known as cybersecurity, an extended concept which implies the assurance of confidentiality, integrity, availability, authenticity and non-repudiation of information, services, resources, or actions. The state of cybersecurity can be achieved by applying proactive security measures and reactive policies, security standards and models, risk management, and deploying solutions for network and information systems protection.

The threats to cybersecurity can come from various attackers, depending on the aims pursued: from simple criminals looking for financial gains and spies who intend to steal classified or proprietary information to cyber terrorists who engage in attacks as a form of war, whether or not supported at governmental level.

The chapter goes on to present the vulnerabilities of cyber infrastructures at physical level (unauthorized access to restricted areas, natural disasters, or accidents), hardware (the use of

hardware components and fault-tolerant systems), software (providing additional, illegal access rights), and, not least, of human nature related vulnerabilities.

Since the technology is ubiquitous in almost all areas of modern society, the risk management for IT systems is considered to be fundamental to ensuring an efficient IT security. Risk management is defined by specialized literature as "the process of identifying vulnerabilities and threats within an organization and developing measures to minimize their impact on information resources." Basically, risk management focuses on the treatment, acceptance and communication of risk, general management-specific activities.

The four component stages of the risk management process are generally represented by the risk evaluation, the coordination of the decision-making process, the controls implementations and measuring the effectiveness of the program. The European Agency for Security of Information and Data Networks (ENISA) proposes a set of criteria for assessing risk management methodologies based on the fundamental elements: identification, analysis, evaluation, estimation, acceptance, treatment, and communication.

Further, the structure of cyber-attacks was defined by Lockheed Martin researchers using the *Cyber Kill Chain* intrusion model. According to the terms used to describe the attack on a cyber infrastructure or to spy traffic from a computer network, the above steps consist of: recognition, arming, delivery, exploitation, installation, command and control, actions on targets.

The chapter concludes with issues pertaining to the protection of critical infrastructure against cyber-attacks. The growing number and complexity of cyber-attacks highlights an immediate need to change the way in which critical infrastructure security is being examined. The development of resilient infrastructures to threats and risks is a necessity by adopting “secure by design” and “security by default” approaches in the sectors declared to be of great importance.

The second chapter of the study evaluates ***Romania's readiness according to the European framework in the field of cybersecurity*** and presents the European and national framework in the field of cybersecurity.

The European Union has taken some measures to increase resilience and preparedness in cybersecurity. The European Union's cybersecurity strategy, adopted in 2013, sets out strategic objectives and concrete actions aimed at achieving resilience, reducing cybercrime, developing cyberdefense capabilities, and establishing an international cyberspace policy. Other important measures in the field of cybersecurity were the second mandate of ENISA and the adoption of EU Directive on security of network and information systems (NIS Directive).

The European Union's 2016-2020 cybersecurity strategy and the adopted national strategies reflect the need for a unified approach to cybersecurity, the need for collaboration/disclosure and the continued updating of policies and mechanisms to ensure the security of the European cyber space.

On 6 July 2016, the European Parliament and the Council of the European Union adopted Directive (EU) 1148/2016 (NIS) on measures for a high common level of network and information security across the Union. The purpose of this Directive is to ensure a common level of network and information system security in the European Union and requires operators and digital service providers to take appropriate measures to prevent cyber-attacks and risk management and to report serious security incidents to competent national authorities.

An important aspect of security at EU level is the protection of personal data. To this end, the European Parliament and the Council adopted on 27 April 2016 Regulation (EU) 2016/679 on the protection of individuals regarding the processing of personal data and the free movement of such data and to repeal Directive 95/46/EC (GDPR - General Data Protection Regulation). Regulation (EU) 2016/679 entered into force on May 2016 and its provisions will be applicable in all EU Member States, as of 25 May 2018.

Many cybersecurity incidents and the evolution of cyber-attacks lately have led to the need to adopt cybersecurity policies and strategies at international level. These strategies underline the need to develop country-specific capabilities to counteract cyber-attacks and set the general framework for action and cooperation to limit their effects.

Romania adopted the Cyber Security Strategy in 2013, having a common approach at the level of the European Union, in order to provide a prompt response to the attacks in the cyberspace. The objective of Romania's Cyber Security Strategy is to define and maintain a secure cyberspace with a high degree of resilience and trust. This strategy presents important principles and directions for action to prevent and combat the vulnerabilities and threats to Romania's cybersecurity.

The Ministry of Communications and Information Society launched in public debate on 3 October 2017 the *Draft Law on ensuring a high common level of security of networks and information systems*. This draft act proposes the adoption of a set of rules aimed at establishing a unified national framework for cybersecurity and the response to security incidents occurring at the level of the networks and computer systems of key service providers and digital service providers, in line with the NIS Directive requirements.

In the last part of this chapter, we make an analysis of cybersecurity alerts processed at national level by CERT-RO (Romanian National Computer Security Incident Response Team). The data reported for the year 2016 on the website www.cert.ro indicates:

- 38.72% of total unique IP addresses allocated to Romania have been affected;
- 81.39% of the alerts collected and processed are related to vulnerable information systems;
- 12.81% of alerts collected and processed are related to systems infected with different variants of malicious software (malware), such as botnets;
- 58.98% of the total number of incidents resulting from the processing of alerts are related to vulnerable systems;
- 40.96% of the total number of incidents resulting from the processing of alerts are related to systems that are part of botnet networks;
- 10,639 ".ro" domains have been reported to CERT-RO as being compromised in 2016, down about 40% compared to 2015 (17,088 domains).

The third chapter of the study approaches ***public-private sector cooperation in cybersecurity***. The increasing number and complexity of cyber threats requires measures and actions to strengthen the international cooperation to contribute to the development of innovative and secure products and services. As of 2013, a "mechanism for cooperation between Member States and the European Commission is set as a priority measure at EU level, to share/distribute early warnings on risks and incidents, to exchange information and counter NIS threats and incidents."

The final version of the NIS Directive focuses on "increasing cybersecurity cooperation between EU Member States" and introduces the need to adopt "security measures and incident reporting obligations for digital service providers and essential service providers who own critical national infrastructure."

In the field of cybersecurity, the cooperation is done through point-to-point agreements between the organizations, horizontally (national sectoral) or vertical (international/national structures). The most recommended ways to achieve an effective cooperation are by bilateral agreements (international organizations or punctual with other countries) and multilateral ones, such as the collaboration model of the Nordic CERTs in Denmark, Finland, Iceland, Norway, and Sweden through NORDUnet CERT and NCIRC CC - NATO's Cyber Security Communication and Information Agency.

Another plan to be developed is that of the civil-military cooperation and the examination of ways in which both areas may learn from each other in terms of training and exercise, to enhance resilience and response capabilities. Several directions that can be followed are:

- the development of education platforms, common cyber exercises with the objective of exercising and assessing cyber-mode management, operational, tactical, and strategic response;
- optimizing the cooperative process to identify and limit the impact of incidents through simplified approaches.

A special subchapter is dedicated to fighting cybercrime. The evolution of organized crime in Romania in recent years is closely linked to the evolution of cybercrime and the increased use of information technology and communications in committing crimes. At national level, cybercrime manifests itself in the following aspects: cyber-attacks (malware, ransomware, DDoS attacks), computer fraud (fake goods auctions, compromising user accounts of e-commerce sites or creating phishing sites for banking data collection) and bank cards frauds (compromising ATMs and extracting confidential information from customers' cards). The Service for Countering Cybercrime is the specialized structure of the Romanian Police, which has competence in the prevention, investigation, and prosecution of cybercrime, and it operates within the Directorate for Combating Organized Crime. The service functions as a central structure, with tasks of coordinating and controlling the activity in the field nationwide.

The third chapter ends with aspects related to the concept of coordinated vulnerabilities disclosure. The number of cybersecurity incidents exploiting program, services, and system vulnerabilities is growing, owing to the lack of a vulnerability assessment methodology. Cooperation between institutions, organizations and the cybersecurity community can be useful in finding and establishing vulnerabilities. The objectives of a CVD (Coordinated Vulnerability Disclosure) policy include ensuring that identified vulnerabilities are addressed, minimizing the security risk from identified vulnerabilities, providing sufficient information to assess the risks of system vulnerabilities, and setting expectations to promote communication and positive coordination among the parties involved.

The last chapter of the study contains ***recommendations regarding the development of the national cybersecurity culture in the current European context***. The good practices mentioned in this chapter aim to establish and maintain robust and well-implemented cybersecurity awareness and ensure that end-users are aware of the importance of protecting sensitive information and the risks of misuse of information.

An extended subchapter is dedicated to the importance of cybersecurity education and research. Issues organized in the following directions are analyzed:

- academic programs in the field of cybersecurity;
- educational programs in computer security at the level of high school studies;
- post-academic and “lifelong learning” programs;
- the work of non-governmental organizations in the field of cybersecurity;
- publications in the field of cybersecurity;
- Web platforms to promote and raise awareness of cybersecurity;
- public events on cybersecurity topics;
- the research and development activity within companies.

Within the subchapter referring to public cybersecurity policies, it is highlighted that adoption and development of public cybersecurity and operational management policies will provide a better understanding of the challenges in the field and will provide the instruments needed to influence shaping of cyber threats management processes. It also offers the possibility of accurately estimating the financial effort required to implement technical and non-technical measures in the field of cybersecurity.

International cooperation plays an indispensable role in the development of the public-private partnership at the national level. Protecting virtual space is a shared responsibility

that can be efficiently achieved through collaboration between the Government and the private sector, which often owns and operates much of the infrastructure. In order to ensure national security, governments need to manage cybersecurity in collaboration with the private sector, taking into account the fact that the success of the collaboration implies a number of conditions to be created, such as trust, real benefits and clear understanding of mutual roles.

The chapter concludes with assessments of current cooperation mechanisms at the European level. As the Member States cannot act isolated against a major IT attack, networks in cooperation with international partners are essential for combating global threats. The importance of cooperation at the European and the international level is recognized by all stakeholders (administration, military, business), but because of the national approaches and incidents they have faced, only some formal agreements between states and a few public-private partnerships have been agreed to the exchange data/information in the field of cybersecurity.

The "***Conclusions***" chapter summarizes the current state of cybersecurity in Romania and identifies the areas where action can be taken to enable our country to cope with imminent challenges at all levels: technical, legislative, social, educational, or governmental.

An ***Annex*** to this study presents a questionnaire designed to identify the level of maturity of the cybersecurity processes at the level of public administration institutions in Romania. The 14 questions in this questionnaire cover topics such as security risk management, organizational culture, cybersecurity responsibilities or tasks, or infrastructure tools. Some of this questionnaire results are found in the study, as a support for the highlighted aspects and statements or for issuing conclusions.

Conclusions

Romania undergoes a continuous process of strengthening cybersecurity nationwide, both from a legal, institutional, and procedural point of view, and efforts are being made by the authorities with responsibilities in this field.

The current legislative regulations, as well as the degree of their operationalization at the level of the Romanian public institutions, currently do not allow the prevention and countering of medium and high level cyber threats with maximum efficiency. Strengthening the legislative framework in the field of cybersecurity is a national priority, so that optimal conditions for rapid response to cyber incidents can be ensured.

In 2016, Romanian National Computer Security Incident Response Team collected and processed 110,194,890 cybersecurity alerts, with 61.56% more than in 2015 and 154.89% more than 2013. In addition to the growing number of cybersecurity alerts, we can see that the most common forms of malware in Romanian computer systems were detected many years ago and, although they should have been eradicated, they continue to infect old and outdated operating systems in Romania.

Romania is a cybersecurity incident generator, with a transit (proxy) role for attackers, according to CERT-RO annual reports, but it has also become lately a target of APT, DDoS or ransomware cyber-attacks.

The Global Cybersecurity Index 2017 has as a modeling approach 5 strategic pillars on cybersecurity, namely: legal/judicial, technical, organizational aspects, capabilities, and cooperation. From the point of view of the country index, Romania needs the following:

- updating the regulatory framework;
- developing / adopting standards for organizations;
- adopting security assessment metrics;
- improving the legislative framework for vocational training, research and development programs, startups;
- the signing of bilateral and multilateral agreements.

Many of the cyber defense systems used by critical infrastructure operators in Romania are outdated and ineffective to avoid or counteracting possible attacks. In the absence of adequate measures and coordination of critical infrastructure security efforts, these systems remain extremely vulnerable, unauthorized individuals being able to gain control over vital systems for the functioning of a state. In this respect, it is absolutely necessary to periodically analyze, monitor, assess and optimize the critical infrastructure domain by starting a process of identification of critical infrastructure at the level of public administration. The rapid evolution of the domain and of the various vital sectoral components requires the updating of the national strategy on the protection of critical infrastructure, in accordance with the European and international recommendations in the field.

In the general context of discussions on cybersecurity at the national level, we highlight the importance of a conceptual separation of the main directions of action: cyberdefense, cybercrime, national security, critical infrastructure and emergencies, international cyber diplomacy, and Internet governance. It is necessary to clearly define the roles and responsibilities of each responsible national institution.

Another segment requiring to be developed is the professional training in the field and taking of actions on awareness/understanding of the field at the level of the decision makers within the public organizations.

Research and education in the field of cybersecurity must be priorities of public policies. Strengthening information security research, improving education, and developing trained workforce are essential to achieving the overall cybersecurity policy objectives. Research and education policies will be effective only if they include the multilateral and multidisciplinary nature of cybersecurity as a fundamental and ubiquitous element in culture, approaches, technical systems, and infrastructures.

International cooperation plays a key role in this area, as cybersecurity challenges go beyond boundaries, extending to globally interconnected systems. Collaboration with European and international entities is absolutely necessary, whether it is about educational establishments, research centers, private companies or government institutions. Cooperation between institutions, organizations and the cybersecurity community can be useful in finding and fixing vulnerabilities. A proven cooperation mechanism is, for example, the coordinated disclosure of vulnerabilities.

The adoption of coherent public policies at Member State level on coordinated disclosure of vulnerabilities and coordinated cross-sectoral action/cooperation mechanisms will provide the necessary ecosystem to ensure the security of the community.

The opening of communication channels, the setting up of working and public consultation groups, the involvement of civil society and the public-private partnership are key directions that public policies should focus on.

In conclusion, the adoption of comprehensive and updated cybersecurity legislation to support the development of state defense capabilities is a national priority. Ensuring a secure cyber space is the responsibility of both the State and the competent authorities, the private sector and civil society. For the development of the cybersecurity culture, the most important levers are: education and research, public-private partnerships, and cooperation mechanisms at the European level.

SINTEZA STUDIULUI

Considerăm că proiectul de cercetare „*Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu*” a constituit el însuși o „provocare” pentru autorii săi, nu doar la nivel tehnic, de realizare a analizelor și elaborare a considerațiilor, ci și la nivel profesional. Oportunitatea oferită de Institutul European din România de a concepe studiul de față ne-a permis realizarea unei analize extinse, actuale și obiective privind stadiul în care țara noastră se află în domeniul securității cibernetice.

Contextul actual ne leagă indisolubil de mediul online în desfășurarea activităților zilnice, la serviciu și acasă, și transferul informațiilor între toate entitățile, de la companii, organizații și agenții guvernamentale până la utilizatorii finali. Aflat în plină evoluție, mediul virtual generează deopotrivă oportunități de dezvoltare a societății informaționale, dar și riscuri la adresa funcționării acesteia. Existența vulnerabilităților sistemelor informatice, ce pot fi exploatate de grupări organizate, face ca asigurarea securității spațiului cibernetic să constituie o preocupare majoră pentru toate entitățile implicate. Potențial vulnerabile la atacuri cibernetice nu sunt doar mediul fizic - echipamente mobile, sisteme informatice, smartphone-uri etc. - ci și cel logic - sisteme de operare, aplicații, poșta electronică, transferurile de informații între companii sau operațiile în cloud.

Obiectivul general al acestui proiect de cercetare îl reprezintă analiza provocărilor actuale prezente în domeniul spațiului cibernetic, identificându-se amenințările, vulnerabilitățile și riscurile la adresa securității cibernetice. Este studiată capacitatea României de reacție la amenințările prezente în mediul virtual, atât la nivel național, cât și la nivel european și regional.

Obiectivele specifice ale proiectului sunt identificarea și clasificarea vulnerabilităților și a riscurilor prezente în mediul cibernetic, analiza evoluției și structurii atacurilor cibernetice, identificarea bunelor practici privind prevenirea și limitarea efectelor acestor atacuri, cercetarea gradului de pregătire a României pentru contracararea riscurilor și provocărilor prezente în spațiul cibernetic, analiza cooperării dintre sectorul public și cel privat în domeniul securității cibernetice și propunerea unor politici de securitate cibernetică privind armonizarea cadrului normativ din România cu recomandările europene în domeniu.

Cercetările realizate în cadrul acestui studiu au utilizat atât metode calitative, cât și metode cantitative. Metodele folosite în cadrul cercetărilor calitative au fost observația participativă, studii de caz, studii comparative și analiza bibliografiei de specialitate. Cercetările cantitative au fost orientate spre verificarea teoriilor obținute prin intermediul cercetărilor calitative și au utilizat sondajele ca metode de cercetare.

Prezentarea studiului

Primul capitol, „***Aspecte generale privind securitatea cibernetică***”, pornește de la identificarea conceptului de ***securitate cibernetică***, acea stare de normalitate a informațiilor digitale, resurselor și serviciilor oferite de entitățile publice sau private în spațiul virtual. Activitatea de protejare a sistemelor TIC (Tehnologia Informației și Comunicațiilor) și a conținutului acestora a devenit cunoscută sub numele de securitate cibernetică, un concept extins care presupune asigurarea confidențialității, integrității, disponibilității, autenticității și nerefuzării informațiilor, serviciilor, resurselor sau acțiunilor. Starea de securitate cibernetică poate fi obținută prin aplicarea unor măsuri de securitate proactive și reactive ce includ politici, standarde și modele de securitate, prin managementul riscului și prin implementarea unor soluții pentru protecția rețelelor și sistemelor informatice.

Amenințările la adresa securității cibernetice pot proveni de la atacatori din diverse categorii, în funcție de scopurile urmărite: de la simpli criminali care urmăresc câștiguri financiare și spioni care intenționează să fure informații clasificate sau proprietare până la teroriști cibernetici care se angajează în atacuri ca o formă de război, susținut sau nu la nivel de stat.

Capitolul continuă cu prezentarea vulnerabilităților infrastructurilor cibernetice la nivel fizic (accesul neautorizat în zone restricționate, catastrofe naturale sau accidente), hardware (se are în vedere aici utilizarea unor componente hardware și structuri tolerante la defectări), software (care oferă drepturi de acces suplimentare, nelegitime) și, nu în ultimul rând, al celor care țin de natura umană.

Dat fiind că tehnologia este omniprezentă în aproape toate domeniile societății moderne, gestionarea riscului pentru sistemele informatice este considerată fundamentală pentru asigurarea unei securități informatice eficiente. În literatura de specialitate, managementul riscului este definit ca „procesul de identificare a vulnerabilităților și amenințărilor din cadrul unei organizații și de elaborare a unor măsuri de minimizare a impactului acestora asupra resurselor informaționale". Practic, managementul riscului se concentrează pe partea de tratare, acceptare și comunicare a riscului, activități în general specifice managementului.

Cele patru etape componente ale procesului de management al riscului în general sunt reprezentate de evaluarea riscului, coordonarea procesului decizional, implementarea controalelor și măsurarea eficacității programului. Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) propune o serie de criterii de evaluare a metodologiilor de management al riscului bazate pe elementele esențiale: identificare, analiză, evaluare, estimare, acceptare, tratare și comunicare.

În continuare, structura atacurilor cibernetice este analizată prin intermediul modelului de intruziune *Cyber Kill Chain* creat de cercetătorii de la Lockheed Martin. Conform termenilor folosiți în descrierea atacului asupra unei infrastructuri cibernetice sau în spionarea traficului dintr-o rețea de calculatoare, etapele constau în: recunoaștere, înarmare, livrare, exploatare, instalare, comandă și control, acțiuni asupra obiectivelor.

Capitolul se încheie cu aspecte ce privesc protecția infrastructurilor critice la atacuri cibernetice. Numărul tot mai mare și complexitatea atacurilor cibernetice evidențiază o nevoie imediată de schimbare a modului în care se examinează securitatea infrastructurilor critice. Dezvoltarea unor infrastructuri reziliente la amenințări și riscuri reprezintă o necesitate, prin adoptarea unor abordări de tipul „secure by design" și „security by default" în sectoarele declarate ca fiind de importanță deosebită.

În cel de-al doilea capitol al studiului se face ***evaluarea gradului de pregătire a României în conformitate cu cadrul european în domeniul securității cibernetice*** și se prezintă cadrul european și cel național în domeniul securității cibernetice.

Uniunea Europeană a luat o serie de măsuri pentru a spori reziliența și gradul de pregătire în ceea ce privește securitatea cibernetică. Strategia de securitate cibernetică a Uniunii Europene, adoptată în 2013, stabilește obiective strategice și acțiuni concrete menite să permită obținerea rezilienței, reducerea criminalității cibernetice, dezvoltarea capabilităților de apărare cibernetică și stabilirea unei politici internaționale în ceea ce privește spațiul cibernetic. Alte măsuri importante în domeniul securității cibernetice au fost al doilea mandat al ENISA și adoptarea Directivei NIS privind securitatea rețelelor și a sistemelor informatice.

Strategia pentru securitate cibernetică 2016-2020 a Uniunii Europene și strategiile naționale adoptate reflectă necesitatea unei abordări unitare a domeniului securității cibernetice, nevoia de colaborare/divulgare și actualizarea continuă a politicilor și mecanismelor în vederea asigurării siguranței spațiului cibernetic european.

La 6 iulie 2016, Parlamentul European și Consiliul Uniunii Europene a adoptat Directiva (UE) 1148/2016 (NIS) privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice. Scopul acestei directive este de a asigura un nivel comun de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și cere operatorilor, respectiv furnizorilor de servicii digitale, să adopte măsuri adecvate pentru prevenirea atacurilor cibernetice

și managementul riscului și să raporteze incidentele grave de securitate către autoritățile naționale competente.

Un aspect important al securității la nivelul UE este reprezentat de protecția datelor cu caracter personal. În acest sens, Parlamentul European și Consiliul au adoptat în data de 27 aprilie 2016 Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - RGPD). Regulamentul (UE) 2016/679 a intrat în vigoare pe 25 mai 2016, iar prevederile lui vor fi aplicabile în toate statele membre UE, având caracter obligatoriu începând cu data de 25 mai 2018.

Numeroasele incidente de securitate cibernetică și evoluția atacurilor cibernetice din ultima vreme au determinat necesitatea adoptării la nivel internațional a unor politici și strategii în domeniul securității cibernetice. Aceste strategii subliniază necesitatea dezvoltării unor capabilități proprii fiecărei țări pentru contracararea atacurilor cibernetice și stabilesc cadrul general de acțiune și cooperare pentru limitarea efectelor acestora.

România a adoptat *Strategia de securitate cibernetică* în anul 2013, având o abordare comună la nivelul Uniunii Europene, pentru a putea oferi un răspuns prompt la atacurile din spațiul cibernetic. Scopul Strategiei de securitate cibernetică a României este de a defini și menține un spațiu cibernetic sigur, cu un înalt grad de reziliență și de încredere. Această strategie prezintă principiile și direcțiile importante de acțiune pentru prevenirea și combaterea vulnerabilităților și amenințărilor la adresa securității cibernetice a României.

Pe 3 octombrie 2017, Ministerul Comunicațiilor și Societății Informaționale a lansat în dezbatere publică *Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*. Proiectul propune adoptarea unui set de norme menite să instituie un cadru național unitar de asigurare a securității cibernetice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale în conformitate cu cerințele Directivei NIS.

În ultima parte a acestui capitol este făcută o analiză a alertelor de securitate cibernetică procesate la nivel național de CERT-RO (Centrul Național de Răspuns la Incidente de Securitate Cibernetică). Datele raportate pentru anul 2016 pe site-ul www.cert.ro indică:

- 38,72% din totalul IP-urilor alocate României au fost afectate;
- 81,39% din alertele colectate și procesate vizează sisteme informatice vulnerabile;
- 12,81% din alertele colectate și procesate vizează sisteme informatice infectate cu diferite variante de software malițios (malware) de tip botnet;
- 58,98% din numărul total de incidente rezultate din procesarea alertelor de securitate cibernetică reprezintă sisteme informatice vulnerabile, acestea putând fi utilizate în derularea de atacuri cibernetice asupra unor ținte din Internet;
- 40,96% din numărul total de incidente rezultate din procesarea alertelor reprezintă sisteme informatice ce fac parte din rețele de tip botnet;
- 10 639 domenii „.ro" au fost raportate la CERT-RO ca fiind compromise în anul 2016, în scădere cu aproximativ 40% față de anul 2015 (17 088 domenii).

Cel de-al treilea capitol al studiului abordează ***cooperarea dintre sectorul public și cel privat în domeniul securității cibernetice***. Numărul tot mai mare și complexitatea amenințărilor cibernetice necesită măsuri și acțiuni în vederea consolidării cooperării internaționale pentru a contribui la dezvoltarea unor tehnologii, produse și servicii inovatoare și sigure. Începând cu anul 2013, la nivelul UE se stabilește ca măsură prioritară „crearea unui mecanism de cooperare între statele membre și Comisia Europeană pentru a împărtăși/distribui avertismentele timpurii privind riscurile și incidentele, pentru a face schimb de informații și a combate amenințările și incidentele NIS".

În versiunea finală a Directivei NIS este pus accentul pe „creșterea cooperării în domeniul securității cibernetice între statele membre ale UE” și se introduce necesitatea adoptării „măsurilor de securitate și a obligațiilor de raportare a incidentelor pentru furnizorii de servicii digitale și operatorii de servicii esențiale care dețin infrastructură națională critică”.

În domeniul securității cibernetice, cooperarea se realizează prin acorduri punctuale între organizații, pe orizontală (sectoriale naționale) sau verticală (structuri internaționale/naționale). Cele mai recomandate modalități de realizarea a unei cooperări eficiente este prin acorduri bilaterale (organizații internaționale sau punctual cu alte țări) și multilaterale, cum ar fi modelul de colaborare a CERT-urilor naționale din țările nordice Danemarca, Finlanda, Islanda, Norvegia și Suedia prin NORDUnet CERT și NCIRC CC - NATO Communication and Information Agency’s Cyber Security.

Un alt plan necesar a fi dezvoltat este cel al cooperării între părțile civilă și militară și examinarea modalităților prin care ambele domenii pot învăța unele de la altele în ceea ce privește formarea și exercitarea, pentru a spori capacitățile de reziliență și de reacție la incidente. Câteva direcții care pot fi urmate sunt:

- dezvoltarea unor platforme de educație, poligoane pentru exerciții cibernetice comune având ca obiective exersarea și evaluarea modului de gestionare a incidentelor cibernetice, răspunsul la nivel operațional, tactic și strategic;
- optimizarea procesului de cooperare în vederea identificării și limitării impactului incidentelor prin abordări simplificate.

Un subcapitol special este dedicat combaterii criminalității informatice. Evoluția crimei organizate în România în ultimii ani este strâns legată de evoluția criminalității informatice și de folosirea tot mai intensă a tehnologiei informației și comunicațiilor în comiterea de infracțiuni. La nivelul României, criminalitatea informatică se manifestă sub următoarele aspecte: atacuri cibernetice (malware, ransomware, atacuri de tip DDoS), fraude informatice (licitații fictive de bunuri, compromiterea conturilor utilizatorilor pe site-uri de comerț electronic sau realizarea unor site-uri de phishing pentru colectarea datelor bancare) și fraude cu carduri bancare (compromiterea bancomatelor și extragerea unor informații confidențiale din cardurile clienților). Serviciul de Combatere a Criminalității Informatice este structura specializată din Poliția Română ce are în competență prevenirea, investigarea și cercetarea criminalității informatice și funcționează în cadrul Direcției de Combatere a Criminalității Organizate. Serviciul acționează ca o structură centrală, cu atribuții de coordonare și control al activității în domeniu, la nivelul întregii țări.

Capitolul trei se încheie cu aspecte corelate conceptului de divulgare coordonată a vulnerabilităților informatice. Numărul incidentelor de securitate cibernetică ce exploatează vulnerabilități ale programelor, serviciilor și sistemelor informatice este în continuă creștere din cauza lipsei unei metodologii de testare a vulnerabilităților. Cooperarea dintre instituții, organizații și comunitatea online creată în jurul topicului „securitate cibernetică” poate fi utilă în găsirea și stabilirea vulnerabilităților. Obiectivele unei politici coordonate privind divulgarea vulnerabilităților (CVD - Coordinated Vulnerability Disclosure) includ asigurarea abordării vulnerabilităților identificate, minimizarea riscului de securitate provenit de la vulnerabilitățile identificate, furnizarea unor informații suficiente pentru evaluarea riscurilor legate de vulnerabilitățile sistemelor și stabilirea așteptărilor privind comunicarea și coordonarea pozitivă între părțile implicate.

Ultimul capitol al studiului conține ***recomandări privind dezvoltarea culturii de securitate cibernetică la nivel național în actualul context european***. Bunele practici menționate în cadrul acestui capitol au drept scop stabilirea și menținerea unei conștientizări robuste și bine implementate privind securitatea cibernetică și asigurarea că utilizatorii finali sunt conștienți de importanța protejării informațiilor sensibile și de riscurile de gestionare greșită a informațiilor.

Un subcapitol extins este alocat importanței educației și cercetării în domeniul securității cibernetice. Sunt analizate aspecte organizate pe următoarele direcții:

- programe academice în domeniul securității cibernetice;
- programe educaționale în securitate informatică la nivelul învățământului preuniversitar;
- programe post-universitare și „lifelong learning";
- activitatea organizațiilor neguvernamentale în domeniul securității cibernetice;
- publicații în domeniul securității cibernetice;
- platforme online pentru promovarea și conștientizarea securității cibernetice;
- evenimente publice pe subiecte corelate domeniului securității cibernetice;
- activitatea de cercetare-dezvoltare în cadrul companiilor.

În cadrul subcapitolului referitor la politicile publice de securitate cibernetică se evidențiază faptul că adoptarea și dezvoltarea acestor politici și ale managementului operațional vor aduce o înțelegere mai bună a provocărilor din domeniu și vor oferi instrumentele necesare pentru a influența modelarea proceselor de management/gestionare a amenințărilor din spațiul cibernetic. De asemenea, oferă posibilitatea unei estimări corecte a eforturilor financiare necesare a fi realizate în vederea implementării măsurilor tehnice și non-tehnice din domeniul securității cibernetice.

Cooperarea internațională joacă un rol indispensabil în dezvoltarea parteneriatului public-privat la nivel național. Protejarea spațiului virtual prezintă de fapt o responsabilitate partajată și care poate fi eficient realizată prin colaborarea dintre Guvernul României și sectorul privat, care de multe ori deține și operează o mare parte a infrastructurii. Pentru a asigura securitatea națională, guvernele trebuie să gestioneze securitatea cibernetică în colaborare cu sectorul privat, ținând cont de faptul că succesul colaborării implică o serie de condiții ce urmează a fi create, cum ar fi încrederea, beneficiile reale și înțelegerea clară a rolurilor reciproce.

Capitolul se încheie cu aprecieri privind mecanismele de cooperare la nivel european. Deoarece statele membre nu pot acționa în mod izolat în fața unui atac informatic major, rețelele în colaborare cu partenerii internaționali sunt esențiale pentru combaterea amenințărilor globale. Importanța cooperării la nivel european și internațional este recunoscută de toți actorii implicați (administrație, militar, business), dar, din cauza abordărilor naționale și incidentelor cu care s-au confruntat, au fost convenite doar formal acorduri între state și puține parteneriate public-privat pentru schimbul de date / informații în domeniul securității cibernetice.

Capitolul „***Concluzii***" sintetizează starea actuală a securității cibernetice în România și identifică domeniile în care se poate acționa pentru ca țara noastră să poată face față iminentelor provocări la toate nivelurile: tehnic, legislativ, social, educațional sau guvernamental.

Ca ***Anexă*** a acestui studiu este prezentat un chestionar conceput pentru identificarea stadiului de maturitate a proceselor din domeniul securității cibernetice la nivelul instituțiilor din administrația publică din România. Cele 14 întrebări ale acestui chestionar acoperă zone precum managementul riscului de securitate, cultura organizațională, responsabilități/sarcini în domeniul securității cibernetice sau instrumente la nivelul infrastructurii. O parte din rezultatele acestui chestionar se regăsesc în cadrul studiului, ca suport pentru aspectele evidențiate și susținerea unor afirmații sau formularea unor concluzii.

Concluzii

România se află într-un proces continuu de consolidare a securității cibernetice la nivel național, atât din punct de vedere legal, instituțional, cât și procedural, în acest sens fiind întreprinse eforturi susținute de către autoritățile cu responsabilități în domeniu.

Reglementările legislative existente, precum și gradul de operaționalizare al acestora la nivelul instituțiilor publice din România, nu permit în prezent prevenirea și contracararea cu maximă eficiență a unor amenințări cibernetice de nivel mediu și ridicat. De aceea, consolidarea cadrului legislativ în domeniul securității cibernetice constituie o prioritate națională, astfel încât să poată fi asigurate condițiile optime de reacție rapidă la incidentele cibernetice.

Centrul Național de Răspuns la Incidente de Securitate Cibernetică a colectat și procesat în anul 2016 un număr de 110 194 890 alerte de securitate cibernetică, cu 61,56% mai multe față de anul 2015 și cu 154,89% mai multe față de anul 2013. Pe lângă numărul în creștere de alerte de securitate cibernetică, observăm că cele mai răspândite forme de malware în sistemele informatice din România au fost detectate acum mulți ani și, deși ar fi trebuit să fie eradicate, continuă să infecteze sistemele de operare neactualizate din România.

România este o țară generatoare de incidente de securitate cibernetică și cu rol de tranzit (proxy) pentru atacatori din afara spațiului național, conform rapoartelor anuale ale CERT-RO, însă a devenit în ultima vreme și o țintă a atacurilor cibernetice de tip APT, DDoS sau ransomware.

The Global Cybersecurity Index 2017 are ca model de abordare 5 piloni strategici privind securitatea cibernetică și anume: aspectele legale/juridice, tehnice, organizaționale, capabilități și cooperare. Din punct de vedere al index-ului de țară, pentru România se evidențiază necesitatea:

- actualizării cadrului normativ;
- dezvoltării / adoptării de standarde pentru organizații;
- adoptării de metrici de evaluare a stării de securitate;
- îmbunătățirii cadrului legislativ pentru formarea profesională, programe de cercetare și dezvoltare, startup-uri;
- stabilirii de acorduri bilaterale și multilaterale.

Multe dintre sistemele de apărare cibernetică folosite de operatorii de infrastructură critică din România sunt depășite și ineficiente pentru evitarea sau contracararea posibilelor atacuri. În lipsa unor măsuri adecvate și a unei coordonări a eforturilor privind securitatea infrastructurilor critice, aceste sisteme rămân extrem de vulnerabile, persoane neautorizate putând obține controlul asupra unor sisteme vitale pentru funcționarea unui stat. În acest sens, este absolut necesar ca domeniul infrastructurilor critice să fie periodic analizat, monitorizat, evaluat și optimizat, demarându-se un proces de identificare a infrastructurilor critice la nivelul administrației publice. Evoluția rapidă a domeniului și a diverselor componente sectoriale vitale necesită actualizarea strategiei naționale privind protecția infrastructurilor critice, în concordanță cu recomandările europene și internaționale în domeniu.

În contextul general al discuțiilor privind securitatea cibernetică, la nivel național este importantă separarea conceptuală a direcțiilor principale de acțiune: apărare cibernetică, criminalitate informatică, securitate națională, infrastructuri critice și situații de urgență, diplomație cibernetică internațională și guvernanța internet-ului. Este nevoie să se stabilească foarte clar rolurile și responsabilitățile fiecărei instituții naționale responsabile în parte.

Un alt segment ce necesită a fi dezvoltat este reprezentat de formarea profesională în domeniu și realizarea unor acțiuni de conștientizare/înțelegere a domeniului la nivelul factorilor decizionali din cadrul organizațiilor publice.

Cercetarea și educația în domeniul securității cibernetice trebuie să reprezinte priorități ale politicilor publice. Consolidarea cercetării în domeniul securității informatice, îmbunătățirea

educației și dezvoltarea forței de muncă instruite sunt esențiale pentru atingerea obiectivelor generale ale politicii privind securitatea cibernetică. Educația, învățarea și instruirea profesională pe tot parcursul vieții reprezintă nu doar obiectivele unui program propus la nivelul Uniunii Europene, ci scopuri în sine, care îmbunătățesc experiența personală a fiecăruia dintre noi.

Politicile în cercetare și educație vor fi eficiente doar dacă includ natura multilaterală și multidisciplinară a securității cibernetice ca element fundamental și omniprezent în cultura, abordările, sistemele și infrastructurile tehnice.

Cooperarea internațională joacă un rol-cheie în acest domeniu, deoarece provocările privind securitatea cibernetică depășesc granițele, extinzându-se până la nivelul sistemelor interconectate la nivel global. Colaborarea cu entități europene și internaționale este absolut necesară, fie că este vorba de unități de învățământ, centre de cercetare, companii private sau instituții guvernamentale. Cooperarea dintre instituții, organizații și comunitatea de securitate cibernetică poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilităților.

Adoptarea unor politici publice unitare la nivelul statelor membre privind divulgarea coordonată a vulnerabilităților și a unor mecanisme coordonate de acțiune/cooperare transsectoriale vor asigura ecosistemul necesar asigurării securității în spațiul comunitar.

Deschiderea canalelor de comunicare, crearea de grupuri de lucru și consultare publică, implicarea societății civile și parteneriatul public-privat devin direcții cheie pe care politicile publice trebuie să se axeze.

Concluzionând, adoptarea unei legislații comprehensive și actualizate în domeniul securității cibernetice, care să sprijine dezvoltarea capacităților de apărare ale statului, reprezintă o prioritate națională. Asigurarea unui spațiu cibernetic sigur este responsabilitatea atât a statului, cât și a autorităților competente, a sectorului privat și a societății civile. Pentru dezvoltarea culturii de securitate cibernetică, cele mai importante pârghii sunt educația și cercetarea, parteneriatele public-private și mecanismele de cooperare la nivel european.

INTRODUCERE

Mediul cibernetic, aflat în plină evoluție, generează deopotrivă oportunități de dezvoltare a societății informaționale, dar și riscuri la adresa funcționării acesteia. Existența vulnerabilităților sistemelor informatice, ce pot fi exploatate de grupări organizate, face ca asigurarea securității spațiului cibernetic să constituie o preocupare majoră pentru toate entitățile implicate.

La nivel european au fost întreprinse demersuri pentru a adopta noi politici privind lupta împotriva criminalității informatice și asigurarea securității cibernetice. *Directiva NIS privind securitatea rețelelor și a sistemelor informatice*[1], adoptată de Parlamentul European și Consiliul Uniunii Europene la data de 6 iulie 2016, a intrat în vigoare în luna august a aceluiași an și beneficiază de o perioadă de 21 de luni pentru a fi implementată de statele membre. Scopul Directivei NIS este de a asigura un nivel comun de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și cere operatorilor, respectiv furnizorilor de servicii digitale, să adopte măsuri adecvate pentru prevenirea atacurilor cibernetice și managementul riscului, și să raporteze incidentele grave de securitate către autoritățile naționale competente. [12] Pentru implementarea directivei NIS până în toamna anului 2018, România are obligația de a institui autorități naționale competente, puncte unice de contact și echipe de intervenție în caz de incidente de securitate cibernetică, precum și să se stabilească cerințele de securitate și de notificare a incidentelor care se aplică operatorilor de servicii esențiale și furnizorilor de servicii digitale. [3]

La nivel național a fost adoptată *Strategia de securitate cibernetică a României* în anul 2013, cu scopul de a defini și a menține un mediu cibernetic sigur, cu un înalt grad de siguranță și de încredere. Această strategie își propune adaptarea cadrului normativ și instituțional la dinamica amenințărilor mediului virtual, stabilirea și aplicarea unor cerințe minimale de securitate pentru infrastructurile cibernetice naționale, asigurarea rezilienței acestora și dezvoltarea cooperării în plan național și internațional. Realizarea strategiei de securitate cibernetică are la bază principii de coordonare a planurilor de acțiune destinate asigurării securității cibernetice, de cooperare între toate entitățile implicate, atât din mediul public, cât și din cel privat, de prioritizare a securizării infrastructurilor critice naționale și de diseminare a informațiilor, a expertizei și a bunelor practici în scopul protejării infrastructurilor cibernetice. [22]

O atenție sporită este acordată atât capacității de răspuns la atacurile cibernetice, cât și prevenirii și combaterii acestor atacuri. Combaterea fenomenului de criminalitate informatică reprezintă o prioritate pentru noi toți, atât în ceea ce privește intruziunile în sfera noastră privată sau în datele cu caracter personal, cât și în cazul furtului de identitate sau al fraudei. Prevenirea acestor atacurilor reprezintă o necesitate pentru autoritățile publice, care trebuie să aibă capacitatea de a proteja infrastructura critică pe care cetățenii României se bazează în activitatea lor zilnică.

Obiectivul general al acestui proiect de cercetare îl reprezintă analiza provocărilor actuale prezente în domeniul spațiului cibernetic, identificându-se amenințările, vulnerabilitățile și riscurile la adresa securității cibernetice. Este studiată capacitatea României de reacție la amenințările prezente în mediul virtual, atât la nivel național, cât și la nivel european și regional, România participând în calitate de stat-lider la Fondul de Sprijin pentru dezvoltarea capacității de apărare cibernetică a Ucrainei.

Obiectivele specifice ale proiectului sunt identificarea și clasificarea vulnerabilităților și riscurilor prezente în mediul cibernetic, analiza evoluției și structurii atacurilor cibernetice, identificarea bunelor practici privind prevenirea și limitarea efectelor acestor atacuri, cercetarea gradului de pregătire a României pentru contracararea riscurilor și provocărilor prezente în spațiul cibernetic, analiza cooperării dintre sectorul public și cel privat în domeniul securității cibernetice

[1] *Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană*

și propunerea unor politici de securitate cibernetică privind armonizarea cadrului normativ din România cu recomandările europene în domeniu.

Actualitatea temei de cercetare este dată de analiza necesității transpunerii prevederilor Directivei NIS în legislația națională, Ministerul Comunicațiilor și Societății Informaționale lansând în dezbatere publică, la data de 3 octombrie 2017, *Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*. [40]

Cercetările realizate în cadrul acestui studiu au utilizat atât metode calitative, cât și metode cantitative. Metodele folosite în cadrul cercetărilor calitative au fost observația participativă, studii de caz, studii comparative și analiza bibliografiei de specialitate.

Cercetările cantitative au fost orientate spre verificarea teoriilor obținute prin intermediul cercetărilor calitative și au utilizat sondajele ca metode de cercetare. Sondajul realizat în cadrul studiului (a se vedea *Anexa*) a tratat stadiul de maturitate a proceselor din domeniul securității cibernetice la nivelul instituțiilor din administrația publică din România având în vedere următoarele direcții: responsabilități și sarcini în domeniul securității cibernetice, managementul riscului de securitate (politici, planuri și proceduri), instrumente și automatisme la nivelul infrastructurii, cadrul privind stabilirea obiectivelor, indicatorilor și a mecanismelor de cooperare, cultura organizațională (dezvoltarea de expertiză la nivelul organizațiilor prin programe de instruire, conștientizare și comunicare).

CAPITOLUL I
ASPECTE GENERALE PRIVIND SECURITATEA CIBERNETICĂ

Securitatea cibernetică reprezintă starea de normalitate a informațiilor digitale, resurselor și serviciilor oferite de către entitățile publice sau private în spațiul cibernetic. [22] Această stare presupune asigurarea următoarelor obiective:

- *confidențialitatea* - proprietatea ca informațiile, serviciile sau resursele sistemelor informatice să nu fie disponibile unor persoane sau procese neautorizate;
- *integritatea* - proprietatea de păstrare a acurateței informațiilor, serviciilor sau resurselor sistemelor informatice;
- *disponibilitatea* - proprietatea ca informațiile, serviciile sau resursele sistemelor informatice să fie accesibile persoanelor sau proceselor autorizate;
- *autenticitatea* - proprietatea de asigurare a identificării și autentificării persoanelor, dispozitivelor și serviciilor sistemelor informatice și de comunicații;
- *non-repudierea* - proprietatea ca o acțiune sau un eveniment să nu poată fi repudiat (negat, contestat) ulterior. [24]

Starea de securitate cibernetică poate fi obținută prin aplicarea unor măsuri de securitate proactive și reactive ce includ politici, standarde și modele de securitate, prin managementul riscului și prin implementarea unor soluții pentru protecția rețelelor și sistemelor informatice.

1.1. Studiul amenințărilor la adresa securității cibernetice

Tehnologia este omniprezentă și tot mai complexă pentru aproape fiecare aspect al societății moderne. Progresul exponențial în ultima jumătate de secol în ceea ce privește puterea de procesare și capacitatea de memorare a făcut hardware-ul IT nu numai mai rapid, dar și mai mic, mai ușor, mai ieftin și mai ușor de utilizat. Industria IT inițială a convers tot mai mult cu industria comunicațiilor într-un sector combinat, denumit în mod obișnuit Tehnologia Informației și Comunicațiilor (TIC).

Dispozitivele și componentele TIC sunt, în general, complexe și interdependente, iar întreruperea unuia poate afecta funcționarea celorlalte. În ultimii ani, experții și factorii de decizie și-au exprimat îngrijorarea din ce în ce mai mare cu privire la protejarea sistemelor TIC în fața atacurilor cibernetice, acțiuni deliberate ale unor persoane neautorizate de a accesa sistemele în scopuri de furt, întrerupere, distrugere sau alte acțiuni ilegale.

Activitatea de protejare a sistemelor TIC și a conținutului acestora a devenit cunoscută sub numele de *securitate cibernetică*. Un concept larg și, probabil, insuficient explicat, securitatea cibernetică poate fi un termen util, dar nu poate fi identificat printr-o definiție precisă. De obicei se referă la unul sau mai multe din următoarele aspecte:

- un set de activități și măsuri menite să protejeze - de atacuri, întreruperi ale funcționării sau alte amenințări - sistemele de calcul, rețelele de calculatoare, componentele hardware/software aferente și informațiile pe care acestea le conțin sau transmit (inclusiv aplicații software, date și alte elemente din spațiul cibernetic);
- starea sau calitatea de a fi protejat împotriva acestor amenințări;
- domeniul extins de eforturi menite să pună în aplicare și să îmbunătățească aceste activități și calitatea serviciilor.

Securitatea cibernetică este legată, fără a fi în general considerată identică, cu conceptul de securitate a informațiilor. Acest ultim termen poate fi definit drept activitatea de protejare a informațiilor și a sistemelor informatice împotriva accesului neautorizat, utilizării, dezvăluirii,

întreruperii, modificării sau distrugerii, pentru a asigura integritatea, confidențialitatea și disponibilitatea informațiilor.

Uneori, securitatea cibernetică este necorespunzător asociată cu alte concepte, cum ar fi confidențialitatea, schimbul de informații, colectarea de informații și supravegherea. Cu toate acestea, securitatea cibernetică este un instrument important în protejarea vieții private și prevenirea supravegherii neautorizate, iar schimbul de informații și colectarea de informații pot fi instrumente utile pentru asigurarea securității informatice.

Gestionarea riscului pentru sistemele informatice este considerată fundamentală pentru asigurarea unei securități informatice eficiente. Riscurile asociate cu orice atac depind de trei factori: amenințările (cine atacă), vulnerabilitățile (punctele slabe pe care le atacă) și impactul (ceea ce face atacul).

Amenințările cibernetice pot proveni de la persoanele care practică sau ar putea efectua atacuri cibernetice. Atacatorii se încadrează în una sau mai multe din următoarele categorii:

- criminali care intenționează să obțină câștiguri financiare din activități precum furtul sau extorcarea;
- spioni care intenționează să fure informații clasificate sau proprietare, utilizate de entități guvernamentale sau private;
- războinici la nivel guvernamental, care dezvoltă capacități și realizează atacuri cibernetice în sprijinul obiectivelor strategice ale unei țări;
- „hacktiviști" care realizează atacuri cibernetice din alte motive decât cele financiare;
- teroriști care se angajează în atacuri cibernetice ca o formă de război, susținut sau nu la nivel de stat.

Securitatea cibernetică este în multe privințe o cursă între atacatori și apărători. Atacatorii analizează constant punctele slabe, care pot apărea în diferite contexte. Apărătorii trebuie să reducă punctele slabe, dintre acestea deosebit de importante și provocatoare fiind actele (intenționate sau nu) produse de persoane din interiorul sistemului (*insiders*) și vulnerabilitățile necunoscute anterior (*zero-day vulnerability*). Totuși, în cazul unora dintre vulnerabilitățile cunoscute, la care există metode de rezolvare, acestea nu pot fi implementate în multe cazuri din cauza constrângerilor bugetare sau operaționale.

Un atac reușit poate compromite confidențialitatea, integritatea și disponibilitatea unui sistem TIC și ale informațiilor pe care acesta le gestionează. Fenomene precum furtul sau spionajul cibernetic pot duce la obținerea unor informații financiare, personale sau profesionale, adesea fără cunoștința victimei. Atacurile de tip DoS (Denial-of-Service) pot încetini sau împiedica accesul utilizatorilor legitimi la un sistem informatic. Printr-un malware de tip botnet, un atacator poate comanda un sistem pentru a fi utilizat în atacuri cibernetice asupra altor sisteme. Atacurile asupra sistemelor de control industriale pot duce la distrugerea sau întreruperea echipamentelor pe care le controlează (generatoare, pompe, centrale), cu efecte grave la nivel regional sau statal.

Cele mai multe atacuri cibernetice au un impact limitat, însă un atac de succes asupra anumitor componente ale infrastructurii critice ar putea avea efecte semnificative asupra securității naționale, economiei, mijloacelor de subzistență și siguranței cetățenilor. Reducerea acestor riscuri implică, de obicei, eliminarea surselor de amenințare, abordarea vulnerabilităților și diminuarea impactului.

Deși este recunoscut că atacurile cibernetice pot fi costisitoare pentru indivizi și organizații, impactul economic poate fi dificil de măsurat, iar estimările acestor impacturi variază foarte mult. Dacă în 2004 piața produselor și a serviciilor în domeniul securității cibernetice la nivel global a fost de 3,5 miliarde dolari, în 2017 se estimează la circa 120 miliarde dolari (o creștere de aproape 35 ori în decursul a 13 ani). Cybersecurity Ventures estimează o sumă de 1 000 miliarde dolari, cumulată pe perioada 2017 - 2021, alocată pieței securității cibernetice. Se observă o creștere

substanțială, datorată în special extinderii continue a infrastructurii TIC prin intermediul IoT (Internet of Things) și al altor platforme noi și emergente.

Gestionarea riscurilor generate de atacurile cibernetice implică de obicei:

- eliminarea sursei amenințării (de exemplu, prin închiderea rețelelor de tip botnet);
- abordarea vulnerabilităților prin întărirea activelor TIC (prin patch-uri software sau instruirea angajaților);
- diminuarea impactului prin atenuarea daunelor și restabilirea funcțiilor (de exemplu, prin disponibilitatea unor resurse de rezervă pentru continuitatea operațiilor ca răspuns la un atac).

Nivelul optim de reducere a riscurilor va varia în funcție de sectoare și organizații. De exemplu, nivelul de securitate cibernetică pe care îl așteaptă clienții poate fi mai mic pentru o companie din sectorul de divertisment decât pentru o bancă, un spital sau o agenție guvernamentală.

Acțiunile legislative și executive sunt concepute în mare măsură pentru a aborda câteva necesități bine stabilite pe termen scurt și mediu în domeniul securității cibernetice: prevenirea dezastrelor și a spionajelor cibernetice, reducerea impactului atacurilor reușite, îmbunătățirea colaborării inter și intra sectoriale, clarificarea rolurilor și a responsabilităților agențiilor și combaterea criminalității informatice. Aceste nevoi există în contextul provocărilor mai dificile pe termen lung legate de proiectare, stimulente economice, consens și mediu:

- *Proiectare*: Experții consideră că o securitate eficientă trebuie să fie parte integrantă a design-ului TIC. Cu toate acestea, din motive economice, dezvoltatorii se concentrează în mod tradițional mai mult pe caracteristici și facilități și mai puțin pe securitate. De asemenea, multe dintre nevoile viitoare de securitate nu pot fi estimate, ceea ce reprezintă o provocare dificilă pentru proiectanți.
- *Stimulente*: Structura stimulentelor economice pentru securitatea cibernetică este distorsionată. Criminalitatea informatică este considerată ieftină, profitabilă și relativ sigură pentru criminali. În schimb, securitatea informațiilor poate fi costisitoare, este prin natura ei imperfectă, iar rentabilitatea economică a investițiilor este adesea nesigură.
- *Consens*: Securitatea cibernetică înseamnă lucruri diferite pentru diferiții actori interesați, adesea fără o înțelegere totală și comună asupra sensului, implementării și riscurilor. Există și impedimente culturale importante, nu numai între sectoare, ci și în interiorul aceluiași sector sau în cadrul organizațiilor. Abordările tradiționale ale securității pot fi insuficiente în spațiul cibernetic, dar consensul asupra alternativelor s-a dovedit evaziv.
- *Mediu*: Spațiul cibernetic a fost numit cel mai rapid spațiu tehnologic în evoluție din istoria omenirii, atât ca scară, cât și ca proprietăți. Proprietățile și aplicațiile noi și emergente - în special echipamentele mobile și concepte precum social media, big data, cloud computing sau IoT - complică și mai mult mediul amenințărilor cibernetice, dar pot reprezenta și posibile oportunități de îmbunătățire a securității informatice, de exemplu prin economiile oferite de cloud computing și analizele big data.

Cercetarea și dezvoltarea în domeniul securității informatice pot îmbunătăți proiectarea TIC, cadrul NIST (National Institute of Standards and Technology) poate facilita realizarea unui consens privind securitatea cibernetică, iar inițiativele legislative în domeniul IT (managementul și transferul datelor, media share, cloud computing și alte noi componente ale spațiului virtual) pot contribui la îmbunătățirea securității cibernetice.

1.2. Vulnerabilitățile infrastructurilor cibernetice

Vulnerabilitatea este o slăbiciune a unui sistem hardware sau software ce permite utilizatorilor neautorizați să obțină acces asupra sa. [24] Principalele vulnerabilități în cadrul sistemelor informatice sunt de natură fizică, hardware, software sau umană.

Sistemele informatice sunt vulnerabile în primul rând la atacurile clasice, atunci când un atacator reușește să pătrundă fizic în incinta sistemelor de calcul și să sustragă informații confidențiale. Pentru a preîntâmpina acest lucru trebuie să se asigure securitatea fizică a echipamentelor de calcul prin plasarea acestora în zone sigure, restricționate personalului neautorizat. Accesul la aceste zone trebuie făcut prin folosirea interfoanelor, cardurilor de acces sau dispozitivelor de scanare a datelor biometrice pentru autentificarea utilizatorilor cu permis de intrare. O altă vulnerabilitate a sistemelor informatice o reprezintă dezastrele naturale (cutremure, inundații, incendii) sau accidentele precum căderile de tensiune sau supratensiunile ce pot duce la distrugerea fizică a echipamentelor de calcul. De aceea trebuie avute în vedere și amplasarea echipamentelor pentru reducerea riscului față de amenințările mediului înconjurător. [24]

O atenție deosebită trebuie acordată componentelor hardware pentru ca acestea să nu afecteze ulterior buna funcționare a sistemelor informatice. În cazul serverelor ce furnizează servicii în Internet trebuie alese componente hardware tolerante la defectări pentru a oferi disponibilitate serviciilor și datelor partajate în rețea și pentru a reduce riscul vulnerabilităților de tip hardware. Aceste vulnerabilități sunt întâlnite cel mai des la sistemele de stocare a datelor, fiind cele mai sensibile componente hardware. Din acest punct de vedere se recomandă salvările de siguranță atât la nivelul informațiilor, cât și la nivelul sistemului de operare, pentru repunerea rapidă a acestuia și a serviciilor configurate în caz de defecțiune.

Comunicațiile prin rețeaua Internet sunt nesigure. Oricine se poate conecta la linia de comunicație și poate intercepta, altera sau chiar devia traficul de date. Pentru a înlătura aceste vulnerabilități se recomandă folosirea metodelor moderne de criptare astfel încât, în cazul în care sunt interceptate, datele să nu poată fi decriptate. [56]

Din punct de vedere software există mai multe tipuri de vulnerabilități:

- care măresc privilegiile utilizatorilor locali fără autorizație;
- care permit utilizatorilor externi să acceseze sistemul în mod neautorizat;
- care permit implicarea sistemului într-un atac asupra unui terț utilizator, de exemplu atacul DDoS (Distributed Denial of Service). [24]

O clasificare poate fi făcută după gradul de pericol pe care îl reprezintă vulnerabilitățile pentru sistemul informatic supus atacului. Astfel, în funcție de pericolul prezentat, vulnerabilitățile prezintă 3 grade notate cu A, B și C (Tabelul 1).

Tabel 1. Gradele de vulnerabilitate și consecințele lor

Grad de vulnerabilitate	**Consecințe**	**Mod de atac**
A	Permite utilizatorilor externi să acceseze în mod neautorizat sistemul informatic	troieni, viermi
B	Permite utilizatorilor locali cu privilegii limitate să-și mărească privilegiile fără autorizație	buffer overflow
C	Permite utilizatorilor externi să altereze procesele sistemelor informatice	DoS, DDoS

Vulnerabilitățile de clasă C, cele care permit atacuri prin refuzul serviciilor, sunt vulnerabilități ale sistemului de operare, în special ale funcțiilor de rețea. Aceste vulnerabilități permit utilizatorilor externi să altereze serviciile de rețea ale unui sistem informatic, sau, în anumite cazuri, transformă sistemul victimă într-un sistem *zombie* ce va putea fi implicat ulterior într-un atac de tip DDoS. Aceste vulnerabilități, dacă sunt exploatate, duc la încetinirea sau la oprirea temporară a serviciilor de rețea oferite, cum este cazul unor servere HTTP, FTP sau de poștă electronică. Vulnerabilitățile de clasă C nu sunt considerate foarte grave deoarece implică doar alterarea serviciilor, nu și a datelor. Cu toate acestea, în anumite domenii în care se pune accent mare pe disponibilitatea datelor, aceste vulnerabilități reprezintă un risc ridicat.

Vulnerabilitățile ce permit utilizatorilor locali să-și extindă privilegiile fără autorizație, vulnerabilitățile de clasă B, ocupă o poziție medie pe scara consecințelor. Prin aceste vulnerabilități, un utilizator cu un cont limitat va putea obține privilegii de administrator în sistemul informatic respectiv. Tipurile de atac care permit mărirea privilegiilor unui utilizator într-un sistem informatic sunt atacurile *buffer overflow*. În urma unor erori de programare, unele aplicații alocă un spațiu insuficient de memorie pentru stocarea informațiilor. În momentul în care spațiul de memorie este total ocupat, informațiile ce depășesc spațiul alocat sunt stocate la o altă adresă din memorie. Prin manevrarea acestor adrese, un atacator poate executa diverse comenzi cu aceleași drepturi ca ale programului respectiv. [24] Cum programul de regulă are drepturi de administrator în sistemul de operare, atacatorul care exploatează vulnerabilitatea buffer overflow poate executa comenzi în sistem cu drepturi de administrator. Vulnerabilitățile de clasă B sunt considerate vulnerabilități grave deoarece pot permite accesul unor utilizatori neautorizați la informații importante din sistem.

Vulnerabilitățile de tip A, cele mai grave pe scara consecințelor, permit utilizatorilor externi accesul la sistemul informatic. Prin atacuri cu troieni sau viermi informatici se pot deschide breșe în securitatea sistemului informatic prin care un utilizator extern se poate conecta în mod neautorizat la sistem. Sunt considerate vulnerabilități deosebit de grave deoarece permit accesul utilizatorilor la sistemul de operare și la baza de date a sistemului, aceștia putând fura sau chiar șterge datele importante.

Cauzele apariției vulnerabilităților într-un sistem informatic sunt multiple, câteva dintre acestea fiind:

- erorile existente la nivelul sistemelor de operare sau al aplicațiilor;
- configurarea necorespunzătoare a sistemului de operare sau a aplicațiilor;
- cunoștințele limitate ale administratorilor de sistem sau de rețea;
- lipsa suportului dezvoltatorilor de software în rezolvarea erorilor identificate în aplicațiile software.

Nu în ultimul rând, cele mai mari vulnerabilități sunt cele umane, date de personalul ce se ocupă de configurarea și administrarea sistemelor informatice. Prin lipsa experienței sau printr-o documentare inadecvată privind anumite configurări ale sistemului de operare sau ale aplicațiilor instalate, securitatea cibernetică poate fi total compromisă. Un tip aparte îl reprezintă vulnerabilitățile de tip *zero-day*, necunoscute dezvoltatorilor și furnizorilor de software și care pot fi exploatate de criminalii cibernetici.

Orice sistem informatic are vulnerabilități, astfel că putem spune că nu există un sistem 100% sigur. Aceste vulnerabilități sunt folosite de multe tipuri de atacuri ce vizează un sistem informatic în mod direct, cum ar fi atacurile de tip malware, sau indirect, în cazul implicării sistemului informatic într-un atac de tip DDoS.

1.3. Managementul riscului de securitate

Complexitatea tehnologică, aria largă de răspândire a datelor / informațiilor și numărul mare de amenințări și incidente la adresa securității și funcționalității sistemelor distribuite reprezintă factori care trebuie luați în considerare la dezvoltarea sistemelor informatice. Scopul principal al procesului de management al riscului pentru o organizație are în vedere protecția acesteia și capacitatea sa de a îndeplini misiunea. În acest sens, procesul de management al riscului nu trebuie tratat ca o funcție tehnică efectuată de experți care operează și gestionează sistemul informatic, ci ca un element esențial în funcționarea unei organizații. Dezvoltarea unei strategii de protecție a resurselor organizației este un proces complex și sensibil din punctul de vedere al componentelor pe care le implică managementul riscului.

În literatura de specialitate, managementul riscului este definit ca „procesul de identificare a vulnerabilităților și amenințărilor din cadrul unei organizații și de elaborare a unor măsuri de minimizare a impactului acestora asupra resurselor informaționale”. [34] În general, majoritatea organizațiilor se concentrează pe protecția fizică (în special pe vulnerabilitățile infrastructurii - rețea, sisteme de calcul) și nu reușesc să stabilească efectele asupra celor mai importante resurse.

O abordare incompletă produce un decalaj între necesarul operațional și cel al sistemului informatic, lăsând bunuri valoroase sub incidența riscului. Abordările curente pentru managementul riscului legate de securitatea informației tind să fie incomplete deoarece nu reușesc să includă în cadrul analizei toate componentele riscului (bunuri, amenințări și vulnerabilități). Managementul riscului este procesul care permite nivelului managerial să asigure un echilibru între costurile operaționale, resursele financiare necesare pentru implementarea măsurilor de protecție și atingerea obiectivelor privind protecția resurselor (infrastructura, sistemele de calcul, aplicațiile, datele) care susțin activitatea.

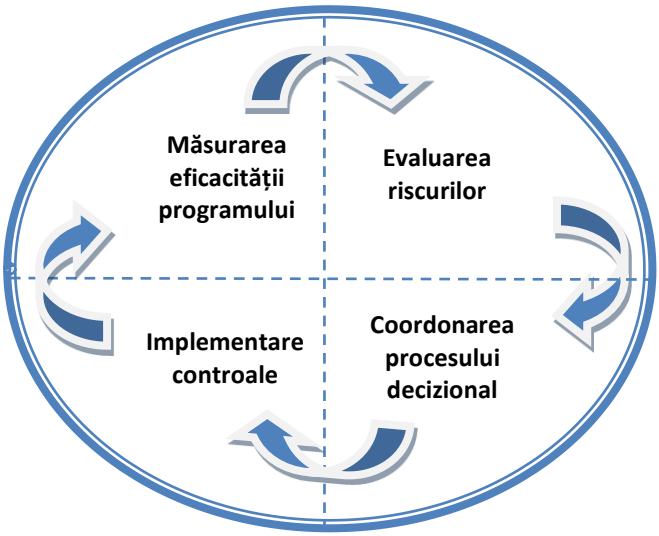
Conform NIST, managementul riscului este „procesul care permite managerilor IT echilibrarea costurilor operaționale și financiare ale măsurilor de protecție pentru a realiza un câștig în raport cu capacitatea de protecție a sistemelor informatice și a datelor care sunt suport pentru misiunea organizației”. [34] Această definiție are la bază eventualitatea ca un eveniment (neprevăzut sau anticipat de decident cu o anumită probabilitate) să se materializeze și să afecteze negativ anumite aspecte ale activității operaționale.

Planificarea managementului riscului este procesul prin care se decide modul de abordare și planificare a activităților de management al riscului. Înainte de inițierea oricăror acțiuni de management al riscurilor trebuie să se evalueze existența unui potențial de risc pentru sistemul analizat cu privire la domeniul de activitate. Această evaluare trebuie să țină cont de toate activitățile care implică sistemul și care ar putea să conțină un risc potențial. Se obține astfel o listă de activități și o clasificare a riscurilor potențiale în activități fără risc, cu risc scăzut și cu potențial de risc ridicat.

Procesul de management al riscului în general constă din desfășurarea următoarelor etape:

- *evaluarea riscului* - identificarea și clasificarea riscurilor care pot să afecteze organizațiile (planificarea și colectarea datelor legate de risc, ierarhizarea riscurilor);
- *coordonarea procesului decizional* - identificarea și evaluarea măsurilor de control ținând cont de raportul cost-beneficii (definirea cerințelor funcționale, identificarea soluțiilor de control, revizuirea soluțiilor în comparație cu cerințele, estimarea reducerii riscurilor, selectarea strategiei de atenuare a riscului);
- *implementarea controalelor* - implementarea și rularea de măsuri de control menite să reducă sau să elimine riscurile (căutarea unor abordări alternative, organizarea soluțiilor de control);

- *măsurarea eficacității programului* - analiza eficienței măsurilor de control adoptate și verificarea gradului de protecție pe care îl asigură controalele aplicate (elaborarea formularelor de risc al securității, măsurarea eficacității controalelor).



Figură 1. Procesul de management al riscului

Analiza riscurilor (identificarea și evaluarea riscurilor) reprezintă unul dintre cele mai importante aspecte ale securității [31], iar în conformitate cu bunele practici din domeniu, organizațiile trebuie să abordeze problema riscului în patru etape [42]:

- identificarea și evaluarea informațiilor importante;
- identificarea și evaluarea amenințărilor;
- evaluarea vulnerabilităților;
- evaluarea riscului.

Analiza de risc presupune un proces de identificare și clasificare a riscurilor de securitate, determinarea amplitudinii riscurilor și identificarea zonelor cu potențial mare de risc. Analiza de risc face parte din ansamblul complex de măsuri care poartă denumirea de *managementul riscului*. Evaluarea riscurilor este rezultatul unui proces de analiză a riscurilor.

Reducerea riscurilor presupune adoptarea măsurilor de prevenire în cazul manifestării acestora, iar pentru implementare sunt necesare o serie de costuri la nivel organizațional care trebuie corelate cu dimensiunea daunelor privind exploatarea vulnerabilităților astfel încât factorii manageriali să decidă riscurile care trebuie prevenite, limitate sau acceptate. Cele mai importante abordări utilizate în procesele de analiză a riscului sunt analiza cantitativă, analiza calitativă și analiza cost-beneficii.

În esență, analiza riscului reprezintă o metodă (calitativă și/sau cantitativă) utilizată pentru evaluarea impactului riscului asupra deciziilor potențiale într-o situație dată. Scopul unui astfel de demers este acela de a ghida decidentul pentru a soluționa mai bine probleme decizionale marcate de un anumit grad de incertitudine.

Analiza calitativă a riscului reprezintă un proces de evaluare prin stabilirea unei prioritizări a riscurilor în funcție de efectul lor potențial asupra sistemului (potențial de pierdere). Analiza calitativă reprezintă o modalitate de determinare a importanței riscurilor identificate și un ghid pentru măsurile de răspuns la acestea. Această metodă de abordare a analizei riscului este cea mai

răspândită, fiind utilizată doar valoarea pierderii potențiale estimate. Cele mai multe metodologii pentru analiza calitativă a riscului folosesc un set de elemente corelate: amenințări, vulnerabilități și controale, care trebuie să fie proporționale cu gradul de criticitate al sistemului informatic și probabilitatea producerii unui eveniment nedorit. [28]

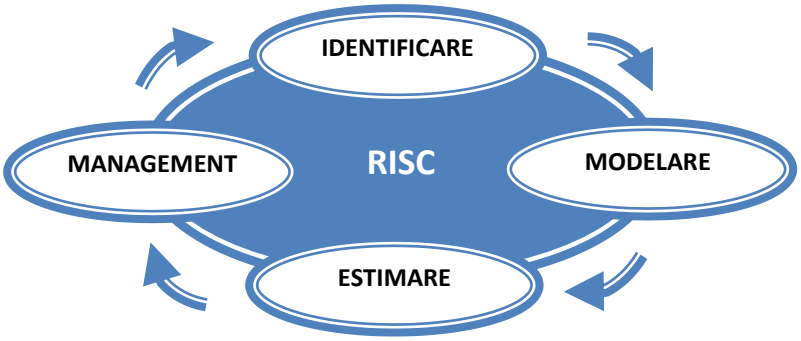
Analiza cantitativă a riscului este procesul prin care se urmărește evaluarea numerică a probabilității și impactului fiecărui risc asupra obiectivelor sistemului și influența sa în riscul general al sistemului. Acest model de analiză a riscului are ca element central determinarea probabilității de producere a unui eveniment și estimarea pierderilor probabile (impactul) pe care acesta le-ar produce. Analiza cantitativă face posibilă o ierarhizare a evenimentelor în ordinea riscului, prin calculul valorii unui eveniment și prin multiplicarea pierderilor potențiale cu probabilitatea de manifestare a evenimentului.

Analiza cost-beneficiu trebuie să fie inclusă în procesul de luare a deciziilor deoarece face o estimare și o comparație între valorile relative și costurile asociate cu fiecare control propus; practic reprezintă criteriul de eficiență folosit pentru alegerea controlului care va fi implementat. Utilizată ca instrument de fundamentare a deciziilor, analiza cost-beneficiu constă în compararea costurilor totale cu beneficiile exprimate în termeni financiari. Costurile trebuie să includă atât costul cu achiziția echipamentului, cât și costurile de operare (mentenanța, instruirea utilizatorilor, consumabile etc.) și costul de oportunitate.

Metode de evaluare a riscurilor

Sistemele informatice actuale sunt esențiale pentru desfășurarea proceselor operaționale în majoritatea organizațiilor. Deciziile cu privire la protecția infrastructurilor IT pentru obținerea unui randament optim al investițiilor în securitate implică necesitatea ierarhizării pe baza importanței în cadrul sistemului. În acest sens au fost dezvoltate o serie de metode și instrumente pentru dezvoltarea domeniului managementului riscului. Astfel, ENISA (Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor) propune o serie de criterii de evaluare a metodologiilor de management al riscului bazate pe elemente esențiale ale domeniului: identificare, analiză, evaluare, estimare, acceptare, tratare și comunicare. [18]

În accepțiunea ENISA, separarea etapelor de identificare, analiză și evaluare a riscurilor contribuie la o mai bună coordonare a procesului consolidat de management al riscului. Practic, managementul riscului se concentrează pe partea de tratare, acceptare și comunicare a riscului, activități în general specifice managementului.



Figură 2. Etapele procesului de management al riscului

Este unanim acceptat de experții din domeniul securității informațiilor că estimarea riscurilor este parte a procesului de management al riscului (care se ocupă cu estimarea, planificarea, implementarea, controlul și monitorizarea controalelor implementate) și a politicilor de securitate aplicate.

Printre cele mai utilizate instrumente și metode de estimare a riscurilor se numără metodologiile OCTAVE și NIST SP 800-30 Risk Management Guide for Information Technology Systems [92]. OCTAVE se concentrează pe estimarea riscului, iar NIST SP 800-30 are tendința de studia amănunțit probleme tactice, organizatorice, fiind mai apropiat de abordarea standardizată, în strânsă legătură cu planificarea convențională și ciclurile de dezvoltare ale sistemelor.

Adoptarea unor controale de securitate pentru a proteja resursele informatice fără o evaluare adecvată a riscurilor generează o supraprotecție a resurselor, făcând din securitate un obstacol în calea desfășurării proceselor operaționale sau o protecție neadecvată care va expune resursa cheie a organizației la diferite amenințări. NIST SP800-30 și OCTAVE permit organizațiilor să evite aceste probleme prin definirea componentelor esențiale și oferă un cadru de evaluare sistematică a riscurilor de securitate.

1.4. Analiza structurii atacurilor cibernetice

Esența unei intruziuni constă în faptul că atacatorul cibernetic trebuie să creeze o metodă prin care să penetreze sistemul de securitate, să se plaseze în mediul informatic securizat și, de acolo, să acționeze asupra obiectivelor vizate, încălcând confidențialitatea, integritatea și disponibilitatea datelor, aplicațiilor sau echipamentelor din acel mediu informatic. Structura atacurilor cibernetice a fost definită de cercetătorii de la Lockheed Martin prin modelul de intruziune *Cyber Kill Chain*. [16]

Un model de intruziune este un proces sistematic de urmărire și capturare a adversarului în vederea obținerii efectelor dorite. În doctrina militară americană sunt definiți pașii acestui proces:

- *găsire*: identificarea țintelor adverse în vederea capturării;
- *localizare*: stabilirea coordonatelor acestor ținte;
- *urmărire*: observarea și monitorizarea activităților;
- *țintire*: utilizarea armelor adecvate pentru obținerea efectelor dorite;
- *capturare*: prinderea adversarului;
- *evaluare*: estimarea efectelor produse.

Acest proces integrat, punct-la-punct, este descris ca un „lanț” (*chain*), deoarece orice deficiență, la oricare nivel, va întrerupe funcționarea întregului proces. Modelul de intruziune constă în recunoaștere, înarmare, livrare, exploatare, instalare, comandă și control și acțiuni asupra obiectivelor.

Figură 3. Modelul de intruziune *Cyber Kill Chain*

Conform termenilor folosiți în descrierea atacului asupra unei infrastructuri cibernetice sau în spionarea traficului dintr-o rețea de calculatoare, etapele de mai sus constau în:

- *Recunoaștere* - cercetarea, identificarea și selectarea țintelor - poate consta în căutarea adreselor e-mail, a relațiilor sociale sau a datelor despre o anumită tehnologie, informații afișate pe diverse site-uri Web;
- *Înarmare* - realizarea unei aplicații de tip malware care, combinată cu o breșă de securitate exploatabilă, să permită accesul de la distanță. Mai mult, fișiere de tip PDF sau specifice suitei Microsoft Office pot fi privite ca arme la dispoziția atacatorului.
- *Livrare* - transmiterea armei în mediul vizat. Principalele căi de transport sunt poșta electronică (atașarea unor fișiere infectate), platformele Web (rularea unor scripturi malware) sau memoriile USB detașabile.
- *Exploatare* - după ce arma este livrată victimei, urmează țintirea unei aplicații sau vulnerabilități a sistemului de operare. Fișierul infectat se poate folosi de facilitatea de auto-executare pentru a lansa codul malware sau poate fi executat chiar de utilizator.
- *Instalare* - infectarea unui sistem victimă cu un troian, backdoor sau altă aplicație malware de acest tip ce asigură prezența atacatorului în mediul vizat;
- *Comandă și control* - de obicei o gazdă infectată trebuie să fie accesibilă din afara rețelei locale pentru a se putea stabili un canal de comandă și control între victimă și atacator. Odată realizată această comunicare bidirecțională, un atacator are acces în interiorul mediului vizat și poate controla activitatea prin lansarea manuală a unor comenzi.
- *Acțiuni asupra obiectivelor* - după realizarea primelor șase faze, un atacator poate acționa în vederea atingerii obiectivelor propuse. Aceste acțiuni constau de regulă în colectarea informațiilor din mediul compromis, modificarea integrității datelor sau atacuri la disponibilitatea serviciilor și a echipamentelor, însă sistemul victimă poate fi folosit și ca punct de plecare în infectarea altor sisteme sau pentru accesul în rețeaua locală. [16]

Principalele tipuri de atacuri cibernetice la ora actuală sunt realizate prin aplicații malware, prin refuzul serviciilor (DoS, DDoS), prin afectarea poștei electronice și a aplicațiilor Web, o ultimă categorie fiind reprezentată de atacurile tip APT (Advanced Persistent Threat).

Atacurile de tip malware sunt cele mai răspândite forme de atac:

- *virușii informatici* sunt aplicații cu efecte de cele mai multe ori distructive, proiectate pentru a infecta un sistem informatic. Virușii prezintă două caracteristici principale: se auto-execută și se auto-multiplică în sistemul infectat.
- *troienii* sunt aplicații ce dau impresia că efectuează operații legitime, dar de fapt încearcă să exploreze vulnerabilități ale sistemului informatic și să deschidă porturi în sistemul de operare pentru a permite accesul atacatorilor în sistem;
- *viermii informatici* sunt aplicații cu efecte distructive ce infectează sistemul informatic și se propagă prin Internet. Viermii caută sisteme informatice cu vulnerabilități, le infectează și efectuează operații dăunătoare, după care încearcă să se propage mai departe.
- *Adware* este un tip de aplicație care se instalează în sistemul de operare și transmite în mod agresiv reclame utilizatorului;
- *Spyware* este un tip de aplicație care captează pe ascuns diverse informații despre activitatea utilizatorilor pe Internet;
- *Ransomware* este un tip de aplicație malware care restricționează accesul la sistemul informatic sau fișierele infectate și cere o răscumpărare pentru ca restricția să fie eliminată. Unele tipuri de ransomware criptează datele de pe hard-disk-ul sistemului, în timp ce altele pot bloca pur și simplu sistemul informatic și afișa mesaje menite a convinge utilizatorul să plătească.
- *Rogueware* este o aplicație care induce în eroare utilizatorii să plătească bani pentru îndepărtarea unor false infecții detectate în sistemul de operare. De cele mai multe ori, acest tip de aplicații pretind că îndepărtează malware-ul găsit pe calculatoare, dar în realitate instalează aplicații cu efect distructiv.

- *Scareware* este o aplicație ce cauzează utilizatorilor stări de frică, de anxietate, cu scopul de a comercializa anumite aplicații false. [25]

Atacul prin refuzul serviciilor (DDoS) prezintă ca efect compromiterea funcționării anumitor servicii de Internet. Unul din cele mai întâlnite atacuri de tip DDoS este atacul packet flood, prin care se trimite un număr mare de pachete către sistemul victimă ce are ca efect blocarea conexiunilor deschise și încărcarea traficului de rețea, ducând până la întreruperea serviciilor oferite de sistemul atacat. [24]

Atacurile la nivelul poștei electronice au crescut exponențial în ultima perioadă. În funcție de scopul infractorilor cibernetici, atacurile ce se transmit prin e-mail sunt de mai multe tipuri:

- e-*mail bombing* constă în trimiterea repetată a unui e-mail cu fișiere atașate de mari dimensiuni către o anumită adresă de e-mail. Acest atac duce la umplerea spațiului disponibil pe server, făcând inaccesibil contul de e-mail.
- *e-mail spoofing* constă în trimiterea unor mesaje e-mail având adresa expeditorului modificată. Acest atac este folosit pentru a ascunde identitatea reală a expeditorului pentru a afla detalii confidențiale sau datele necesare accesării unui cont.
- *e-mail spamming* este un atac ce constă în trimiterea de mesaje e-mail nesolicitate, cu conținut de regulă comercial. Scopul acestor atacuri este de a atrage destinatarii e-mail-urilor să intre pe anumite site-uri și să cumpere produse sau servicii mai mult sau mai puțin legitime.
- *e-mail pshishing* este un atac a cărui amploare este în creștere, constând în trimiterea de mesaje cu scopul de a determina destinatarii e-mailurilor să furnizeze informații privind conturile bancare, cardurile de credit, parole sau alte detalii personale.

Atacurile la nivelul aplicațiilor Web se înmulțesc odată cu dezvoltarea spectaculoasă a tehnologiilor Web care au dus la conceperea unor platforme interactive, cu conținut dinamic și având o interacțiune ridicată cu utilizatorii. Aceste noi platforme prezintă însă și vulnerabilități ce pot fi exploatate de atacatorii cibernetici în scopul de a evita măsurile de securitate și de a accesa în mod neautorizat informațiile din bazele de date. Cele mai întâlnite atacuri de acest tip sunt:

- *SQLi:* injecții cu cod sursă SQL (Structured Query Language), prin care un atacator poate introduce anumite date într-o interogare SQL ce este transmisă bazei de date, schimbând logica interogării. În acest fel, atacatorul poate evita mecanismele de autentificare.
- *XSS (Cross Site Scripting):* atacatorul inserează în cadrul unui site script-uri ce sunt executate în aplicațiile browser ale victimelor în momentul în care aceștia vizitează site-ul infectat;
- *CSRF (Cross-Site Request Forgery):* atacatorul folosește relațiile de încredere stabilite între aplicațiile Web și utilizatorii autentificați. Astfel, atacatorul preia controlul asupra sesiunii victimei, având control complet asupra contului utilizatorului.
- *Man in the Middle*: atacatorul interceptează comunicarea dintre utilizator și website, putând prelua datele de acces dacă acestea nu sunt transmise criptat. [25]

Amenințările persistente avansate reprezintă atacuri cibernetice complexe prelungite, de ordinul a luni sau ani de zile, îndreptate către o țintă specifică, cu intenția de a compromite sistemul și de a obține informații din sau despre acea țintă. Țintele pot fi persoane, companii, guverne sau organizații militare. Atacul de tip APT constă, de obicei, în mai multe atacuri cibernetice diferite. Etapele unui atac de tip APT constau, de regulă, în colectarea informațiilor referitoare la țintă, identificarea unui punct vulnerabil și exploatarea acestuia, infectarea țintei și transmiterea informațiilor strategice extrase. Astfel de atacuri pot fi realizate de state sau organizații teroriste care dispun de capabilități tehnologice și resurse financiare importante, necesare derulării unor astfel de atacuri cibernetice de complexitate ridicată. [48]

1.5. Protecția infrastructurilor critice la atacuri cibernetice

În ultimul secol, infrastructurile (indiferent de domeniul de activitate - transport, energie, telecomunicații etc.) au căpătat o importanță deosebită atât din punct de vedere economic, cât și militar. Asigurarea securității nu se rezumă doar la componenta militară, protecția componentelor vitale pentru funcționarea unei societăți reprezentând obiective prioritare pentru toate guvernele și statele lumii.

Noile evoluții tehnologice la nivel mondial au evidențiat noi provocări și vulnerabilități cauzate de erori umane, dezastre naturale sau acțiuni umane premeditate (terorism). Vulnerabilitatea se definește pe imposibilitatea asigurării protecției corespunzătoare lor, dar și prin creșterea presiunilor programate, intenționate sau aleatorii asupra lor. [20] Distrugerea sau întreruperea componentelor vitale ale unui sistem / flux de lucru în procesul de funcționare și îndeplinire a misiunii pentru care a fost dezvoltat poate afecta încrederea în capacitatea de guvernare a statelor și chiar poate duce la pierderea de vieți omenești.

Diversitatea pericolelor și amenințărilor (simetrice și/sau asimetrice) și a vulnerabilităților existente la nivelul infrastructurilor suport necesită o evaluare continuă a statutului de infrastructură / componentă „critică”.

La nivel internațional, problematica protecției infrastructurilor critice a devenit un subiect important prin elaborarea de studii și analize privind asigurarea securității împotriva dezastrelor naturale sau tehnologice și a activităților teroriste.

Directiva 2008/114/CE a Consiliului Europei, adoptată la 8 decembrie 2008, privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, stabilește următoarea definiție pentru termenul „infrastructură critică”: „element, sistem sau componentă, aflat pe teritoriul statelor membre, care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, și a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacității de a menține respectivele funcții”. [13]

Importanța domeniului comunicațiilor, a rețelelor și sistemelor informatice la nivelul UE este subliniată de *Directiva 2016/1148/CE* privind securitatea rețelelor și a sistemelor informatice care subliniază că amploarea, frecvența și impactul incidentelor de securitate reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Scopul Directivei NIS este de a asigura dezvoltarea unui cadrul normativ european privind realizarea unor reglementări unitare la nivelul statelor membre referitoare la importanța comunicațiilor, rețelelor și sistemelor informatice, în domeniul cooperării și intervențiilor în cazul unor incidente majore și al managementului riscului. [12]

Pentru îndeplinirea angajamentelor rezultate din Directivă rezultă necesitatea implementării unor măsuri în vederea asigurării securității infrastructurilor critice naționale:

- măsuri tehnice și organizatorice pentru operatorii de servicii esențiale, adecvate și proporționale cu riscul la adresa securității rețelelor și a sistemelor informatice;
- măsuri care trebuie să asigure un nivel de securitate pentru rețele și sisteme informatice proporțional cu riscurile identificate;
- măsuri care să prevină și să minimizeze impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru a furniza serviciile;
- măsuri care să asigure cooperarea și intervenția în caz de incidente de securitate.

De asemenea, Directiva solicită statelor membre să dezvolte propriile strategii în materie de securitate cibernetică prin definirea politicilor în acest sens, dezvoltarea cadrului juridic la nivel național și desemnarea autorităților competente. În vederea asigurării unei colaborări

transfrontaliere eficiente, statele sunt încurajate să nominalizeze un singur punct de contact care va exercita atribuții de legătură cu celelalte state membre UE.

În cadrul Anexei II din Directivă au fost stabilite entitățile publice sau private care necesită măsuri speciale de protecție din diverse domenii de importanță deosebită, interconectate și care susțin activitățile vitale necesare funcționării unui stat: energetic (instalații, rețelele de producție și distribuție), tehnologia informației (telecomunicații, Internet, rețele de comunicații ale statelor membre), sănătate (spitale, laboratoare și producția de produse farmaceutice, servicii de urgență, de căutare și de salvare), transport (feroviar, rutier, aerian, pe apă și infrastructurile aferente utilizate) și administrație publică.

La nivel național, începând cu anul 2010 au fost adoptate acte normative în domeniul protecției infrastructurilor critice, dintre care amintim: [33]

- *O.U.G. nr. 98 din 03.11.2010* privind identificarea, desemnarea și protecția infrastructurilor critice (aprobată cu modificări prin Legea nr. 18 din 11.03.2011, modificată și completată prin Legea nr. 344/2015);
- *H.G. nr. 718 din 13.07.2011* privind Strategia națională de protecție a infrastructurilor critice;
- *H.G. nr. 1154 din 16.11.2011* pentru aprobarea pragurilor critice aferente criteriilor intersectoriale ce stau la baza identificării potențialelor infrastructuri critice naționale și privind aprobarea Metodologiei pentru aplicarea pragurilor critice aferente criteriilor intersectoriale și stabilirea nivelului de criticitate;
- *H.G. nr. 1198 din 4.12.2012* privind desemnarea infrastructurilor critice naționale (modificată și completată prin H.G. nr. 639 din 19 august 2015);
- *H.G. nr. 683 din 19.09.2016* privind desemnarea infrastructurilor critice europene și pentru modificarea Hotărârii Guvernului nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor.

În domeniul tehnologiei informației, începând cu anul 2012 a fost adoptată „*Metodologia de identificare a infrastructurilor critice naționale din sectorul tehnologia informației și comunicații*" la propunerea MCSI, care stabilește cadrul și normele privind identificarea, desemnarea și protecția infrastructurilor critice.

Metodologia de organizare și funcționare este bine structurată, având definită o schemă logică privind procesul de evaluare și identificare a infrastructurilor critice naționale din sectorul TIC și grile de evaluare a serviciilor esențiale pentru sectoare cum ar fi: voce și date, Internet, servicii publice electronice, infrastructuri de securitate și servicii poștale.

Infrastructurile critice la nivel național sunt deținute și exploatate atât de sectorul privat, cât și sectorul public. Prin urmare, oriunde se află infrastructura, statul însuși nu mai poate asigura o securitate globală a infrastructurii critice și depinde în mare măsură de sectorul privat în asigurarea acesteia. Dezvoltarea unui parteneriat public / privat este esențial pentru definirea de politici sectoriale de protecție a infrastructurilor critice. [54]

Identificarea infrastructurilor necesare susținerii actului de guvernare și a serviciilor administrației publice necesită automatizarea unor procese privind monitorizarea și implementarea de controale regulate prin dezvoltarea de centre specializate de monitorizare NOC (Network Operations Center).

În acest sens, în cadrul departamentelor de specialitate (public/privat) care operează infrastructuri critice este necesară implementarea unei componente specializate, cu capacități și cunoștințe specializate în dezvoltare și aplicare de politici privind modelarea, simularea și analiza riscurilor (backup, disaster recovery), monitorizare și gestionare a sistemelor de protecție

(firewall-uri, antivirus, sistemelor de prevenire a intruziunilor), precum și evaluarea și raportarea partajată a amenințărilor.

Modelarea fluxurilor de cooperare in cazul incidentelor cibernetice reprezintă o componentă vitală a proceselor de management pentru rețelele și sistemele informatice. Dezvoltarea unui ansamblu coerent de măsuri privind cooperare sectorială în domeniu, detecție, răspunsul, recuperare automată și asigurarea de capacități de protecție va reprezenta fundamentul pentru trecerea la un model național specific privind infrastructurile critice.

Numărul tot mai mare și complexitatea crescută a atacurilor cibernetice evidențiază o nevoie imediată de schimbare a modului în care se examinează securitatea infrastructurilor critice. Dezvoltarea unor infrastructuri reziliente la amenințări și riscuri reprezintă o necesitate, prin adoptarea unor abordări de tipul „secure by design” și „security by default” în sectoarele declarate ca fiind de importanță deosebită.

CAPITOLUL II

EVALUAREA GRADULUI DE PREGĂTIRE A ROMÂNIEI ÎN CONFORMITATE CU CADRUL EUROPEAN ÎN DOMENIUL SECURITĂȚII CIBERNETICE

2.1. Cadrul european în domeniul securității cibernetice

Multitudinea incidentelor din ultimii ani au evidențiat o creștere continuă a numărului de amenințări, în special din spațiul virtual. Protecția infrastructurilor critice la nivel de stat a devenit o preocupare majoră care a depășit domeniul tehnic, fiind un subiect de actualitate aflat pe agenda publică a guvernelor.

Uniunea Europeană a luat o serie de măsuri pentru a spori reziliența și gradul de pregătire în ceea ce privește securitatea cibernetică. *Strategia de securitate cibernetică a Uniunii Europene,* adoptată în 2013, stabilește obiective strategice și acțiuni concrete menite să permită obținerea rezilienței, reducerea criminalității cibernetice, dezvoltarea capabilităților de apărare cibernetică și stabilirea unei politici internaționale în ceea ce privește spațiul cibernetic. Alte măsuri importante în domeniul securității cibernetice au fost al doilea mandat al Agenției Uniunii Europene pentru Securitatea Rețelelor și Informațiilor (ENISA) și adoptarea *Directivei (NIS) privind securitatea rețelelor și a sistemelor informatice*.

Comisia Europeană a adoptat în 2016 Comunicarea privind „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator", în cadrul căreia a anunțat noi măsuri de intensificare a cooperării, informării și schimbului de cunoștințe și de consolidare a rezilienței și pregătirii Uniunii Europene. Această comunicare a propus ideea de a se institui un cadru de certificare de securitate pentru produsele și serviciile TIC în scopul de a spori securitatea pieței unice digitale și încrederea de care se bucură aceasta. Certificarea de securitate cibernetică a TIC capătă astfel o importanță deosebită, având în vedere utilizarea pe scară tot mai largă a tehnologiilor care necesită un nivel ridicat de securitate cibernetică, cum ar fi automobilele inteligente, dispozitivele electronice pentru sănătate sau sistemele industriale automate de control.

În octombrie 2017, Parlamentul European și Consiliul Uniunii Europene propun Pachetul de securitate cibernetică, care cuprinde Regulamentul privind ENISA – „Agenția U.E. pentru securitate cibernetică" și de abrogare a Regulamentului (U.E.) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor. Propunerea de regulament prevede un set cuprinzător de măsuri care se bazează pe acțiuni anterioare și promovează obiective specifice care se consolidează reciproc:

- sporirea capabilităților și a nivelului de pregătire ale statelor membre și ale întreprinderilor;
- îmbunătățirea cooperării și a coordonării dintre statele membre și instituțiile, agențiile și organele U.E.;
- sporirea capabilităților la nivelul U.E. care să completeze acțiunea statelor membre, în special în cazul unor crize cibernetice transfrontaliere;
- sporirea gradului de sensibilizare a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică;
- sporirea a transparenței asigurării securității cibernetice a produselor și serviciilor TIC în scopul de a consolida încrederea în piața unică digitală și în inovarea digitală;
- evitarea fragmentării sistemelor de certificare în UE și a cerințelor de securitate aferente, precum și a criteriilor de evaluare în toate statele membre și în toate sectoarele. [46]

Propunerea de regulament revizuiește mandatul actual al ENISA și stabilește un set reînnoit de sarcini și funcții, cu scopul de a sprijini eforturile depuse de statele membre, instituțiile U.E. și alte părți interesate pentru a asigura un spațiu cibernetic sigur în Uniunea Europeană.

Noul mandat propus urmărește să atribuie agenției un rol mai puternic și mai proeminent, în special în ceea ce privește acordarea de sprijin statelor membre în punerea în aplicare a Directivei (NIS) privind securitatea rețelelor și a informațiilor, contracararea într-un mod mai activ a amenințărilor specifice și dobândirea statutului de centru de expertiză care acordă sprijin statelor membre și Comisiei cu privire la certificarea de securitate cibernetică. [46]

Pentru a răspunde provocărilor din prezent și din viitor în materie de securitate cibernetică, este necesară o abordare holistică a aspectelor digitale pentru a face față provocărilor celei de a patra revoluții industriale. Această abordare a necesitat punerea în aplicare a Strategiei privind piața unică digitală și revizuirea Strategiei de securitate cibernetică.

2.1.1. Strategia europeană pentru securitate cibernetică

Obiectivele strategice cuprinse în Strategia europeană pentru securitate cibernetică 2016 - 2020 sunt derivate din reglementări europene, contribuții relevante din partea statelor membre și a comunităților, inclusiv din sectorul privat. În sprijinul statelor membre și al instituțiilor Uniunii Europene, ENISA propune, în mod prioritar, dezvoltarea următoarelor direcții:

- *expertiză* - colectarea, analiza și punerea la dispoziție a informațiilor / datelor cu privire la aspectele esențiale ale direcției NIS care ar putea avea un impact potențial asupra UE;
- *politică* - promovarea securității rețelelor și a informațiilor ca o prioritate a politicii UE, prin asistarea instituțiilor Uniunii Europene și a statelor membre în elaborarea și punerea în aplicare a politicilor și legislației UE referitoare la NIS;
- *dezvoltarea de capabilități* - actualizarea și diversificarea capacităților de securitate și a rețelelor existente la nivel european, prin asistarea statelor membre și a organismelor Uniunii Europene în vederea consolidării capabilităților de protecție și răspuns;
- *comunități* - promovarea comunității emergente în domeniul IT prin consolidarea cooperării la nivelul UE între organismele sale, statele membre și sectorul privat;
- *implicare* - consolidarea coordonării instituționale ENISA, prin îmbunătățirea gestionării resurselor în mod eficient cu părțile interesate, inclusiv cu statele membre și cu instituțiile Uniunii, dar și la nivel internațional.

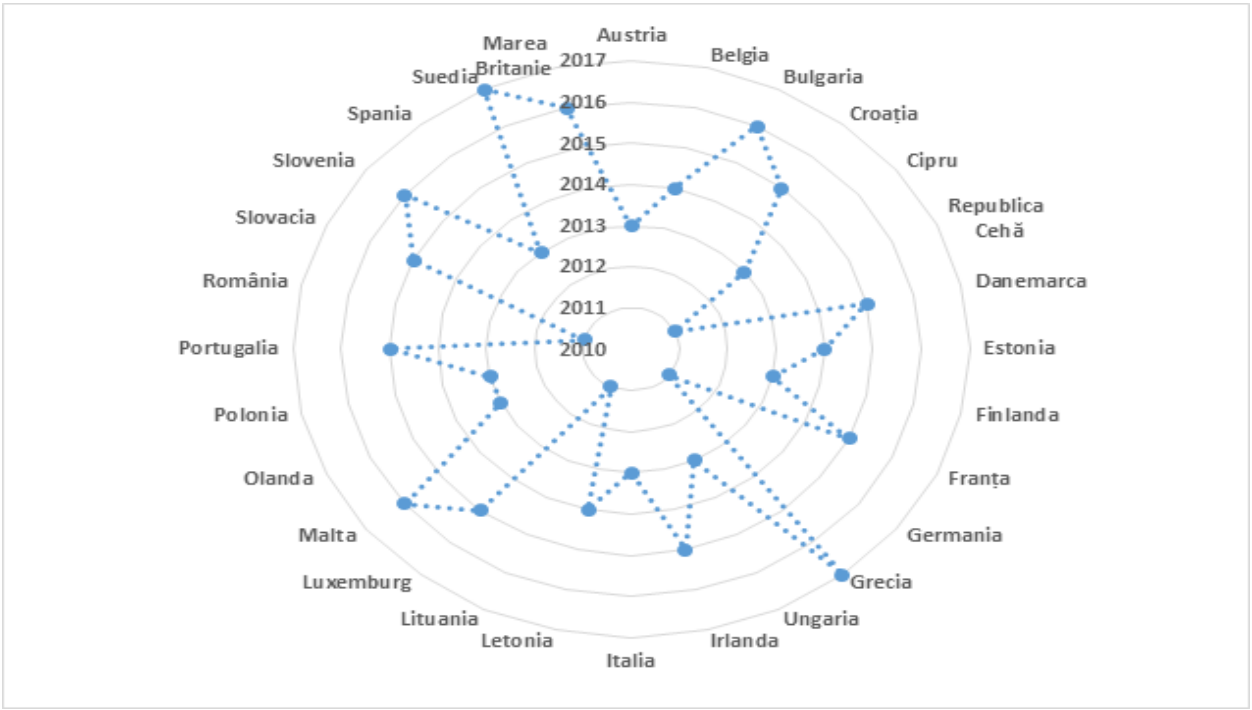
Astfel, ENISA realizează, începând cu anul 2012, un ghid de bune practici privind dezvoltarea, implementarea și evaluarea strategiilor de securitate cibernetică la nivelul statelor membre. Grupul de experți NCSS (National Cyber Security Strategy) din cadrul Agenției Europene elaborează seturi de recomandări menite a fi instrumente utile și ghiduri practice pentru autoritățile de reglementare, factorii de decizie politică, responsabili și alți actori implicați în strategiile de securitate cibernetică.

Stabilirea unor obiective clare, definirea responsabilităților și a unui cadru de evaluare a riscurilor asigură dezvoltarea unui sistem de securitate minimal la nivel european, cu scopul de a monitoriza, controla și reduce probabilitatea producerii unor evenimente nedorite.

Analiza strategiilor naționale de securitate cibernetică la nivelul UE arată o preocupare majoră a statelor membre UE pentru domeniu - peste 70% dintre statele membre au actualizat strategia națională cel puțin o dată.

Figură 4. Ciclul de viață al unei strategii naționale de securitate cibernetică

Până în prezent, toate cele 28 de state membre și-au dezvoltat propriile strategii naționale de securitate, ultima fiind adoptată în septembrie 2017 (Grecia). Experiența incidentului din Estonia (2007), precum și a virusului Stuxnet (2010), au fundamentat necesitatea unor acțiuni la nivelul statelor pentru dezvoltarea capabilităților proprii de contracarare a atacurilor cibernetice și stabilirea unui cadrul de acțiune și cooperare între diverse entități guvernamentale și nonguvernamentale pentru limitarea consecințelor.



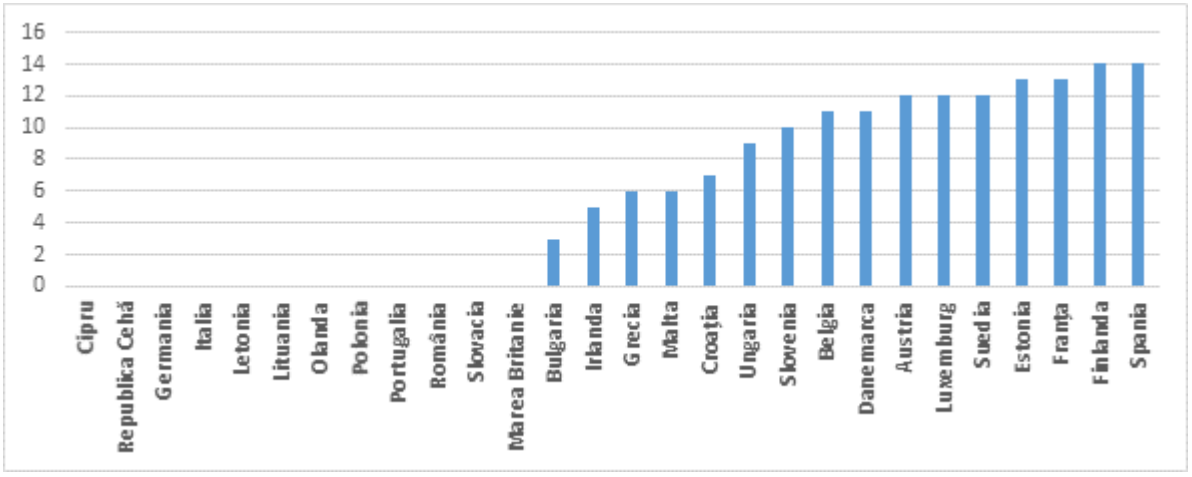
Figură 5. Dezvoltarea strategiilor naționale de securitate cibernetică la nivelul statelor membre UE

Privind din perspectiva temporală a adoptării strategiilor naționale de securitate cibernetică, majoritatea statelor membre au adoptat strategii în urmă cu 4 ani (2013 - 8 state), respectiv 2 ani (2015 - 7 state). Un număr de 4 state - printre care și România - au strategii adoptate de mai mult de 5 ani (în 2011).

Tabel 2. Stadiul strategiilor de securitate cibernetică adoptate la nivelul statelor membre UE

Membru UE	An adoptare	Număr obiective	Membru UE	An adoptare	Număr obiective
Austria	2013	12	Italia	2013	0
Belgia	2014	11	Letonia	2014	0
Bulgaria	2016	3	Lituania	2011	0
Croația	2015	7	Luxemburg	2015	12
Cipru	2013	0	Malta	2016	6
Republica Cehă	2011	0	Olanda	2013	0
Danemarca	2015	11	Polonia	2013	0
Estonia	2014	13	Portugalia	2015	0
Finlanda	2013	14	România	2011	0
Franța	2015	13	Slovacia	2015	0
Germania	2011	0	Slovenia	2016	10
Grecia	2017	6	Spania	2013	14
Ungaria	2013	9	Suedia	2017	12
Irlanda	2015	5	Marea Britanie	2016	0

Statele care au experimentat incidente cu un impact ridicat asupra infrastructurilor naționale au revizuit documentele și politicile naționale, contribuind la dezvoltarea domeniului prin lecțiile învățate. Obiectivele definite în cadrul unei strategii naționale reflectă complexitatea și domeniile abordate în ceea ce privește securitatea cibernetică. Din punctul de vedere al numărului obiectivelor definite, 16 state - cu strategii revizuite în ultimii 4 ani - au obiective, iar restul de 12 state nu au prezentate obiective.



Figură 6. Numărul de obiective definite în strategiile naționale la nivelul UE

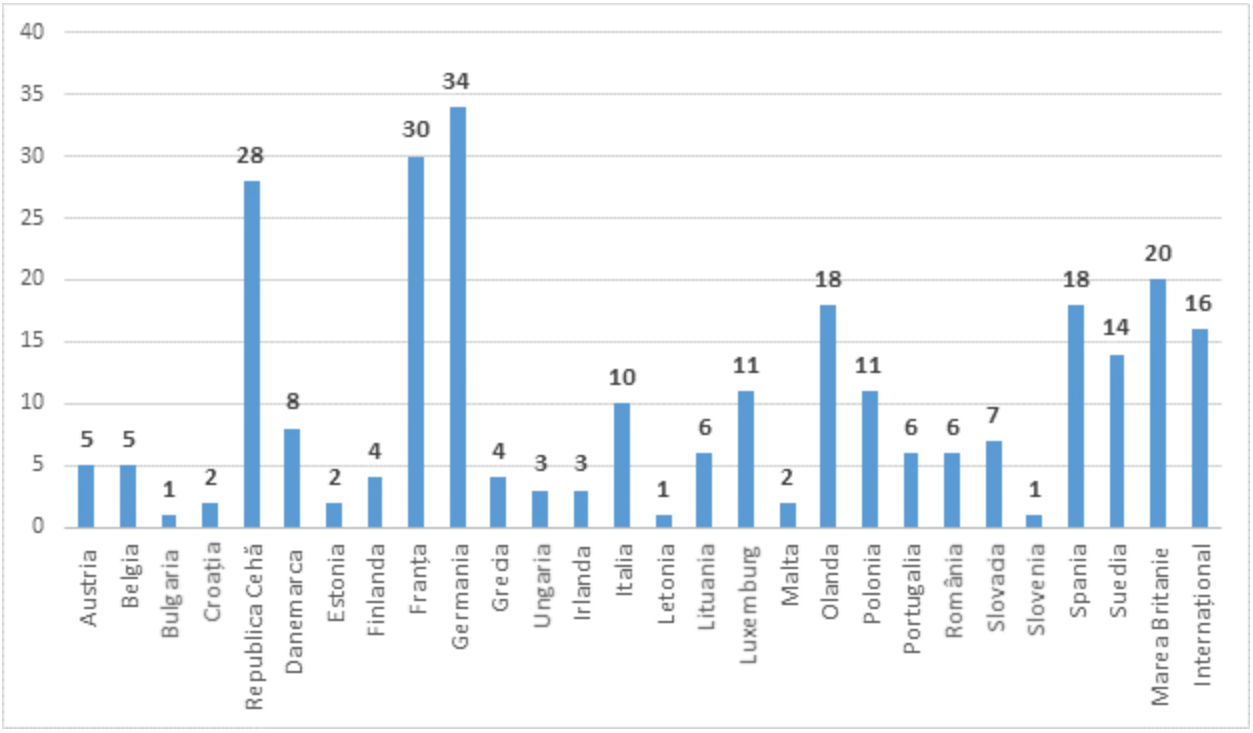
Dezvoltarea unei strategii are în vedere 3 etape (proiectare, implementare și evaluare), ultima având la bază necesitatea de a monitoriza implementarea obiectivelor. Includerea obiectivelor clare în cadrul unei strategii oferă o imagine asupra priorităților naționale din domeniu și direcțiilor de acțiune adoptate.

Diversitatea obiectivelor prezente în cadrul strategiilor arată prioritățile și punctele de vedere diferite existente la nivelul statelor membre. Astfel, principalele obiective care se regăsesc în majoritatea strategiilor sunt:

- organizarea exercițiilor de securitate cibernetică;
- stabilirea și dezvoltarea mecanismelor de raportare a incidentelor (naționale sau internaționale);
- stabilirea și dezvoltarea parteneriatelor public-privat.

Conștientizarea importanței domeniului securității cibernetice la nivel european este demonstrată de acțiunile și evenimentele de promovare a bunelor practici în domeniu (European Cyber Security Month, Data Privacy Day, Web Security Day, Safer Internet Day etc.), forumuri care au rolul de a aduna experții din domeniu în diverse campanii de prevenire și informare.

Un aspect important al strategiei europene în domeniul securității cibernetice îl reprezintă dezvoltarea capabilităților naționale ale statelor membre (prin furnizarea unor recomandări privind dimensiunile-cheie ale consolidării capacităților), orientată inclusiv pe creșterea și funcționarea eficientă a CSIRT-urilor (Computer Security Incident Response Team) naționale / guvernamentale. De asemenea, la nivelul fiecărui stat este necesară stabilirea cadrelor pentru a sprijini actualizarea sistemelor naționale de raportare a incidentelor și formarea profesională în domeniu pentru îmbunătățirea competențelor.



Figură 7. Distribuția CSIRT-urilor la nivelul statelor membre

Operaționalizarea unor echipe de intervenție în cazul incidentelor de securitate cibernetică și cooperarea între experții din domeniu, atât cei din sectorul public, cât și din cel privat, reprezintă elemente esențiale în combaterea amenințărilor din spațiul virtual. Resursele umane limitate de la nivelul CERT-urilor (Computer Emergency Response Team) naționale impun extinderea ariei de colaborare și a mecanismelor de alertă / intervenție. Existența unei evidențe și a unor criterii bine stabilite pentru constituirea / acreditarea unui CSIRT asigură un cadru bine organizat în vederea extinderii cooperării la un alt nivel.

Strategia pentru securitate cibernetică 2016 - 2020 a Uniunii Europene și strategiile naționale adoptate reflectă necesitatea unei abordări unitare a domeniului securității cibernetice, nevoia de colaborare / divulgare și actualizarea continuă a politicilor și mecanismelor în vederea asigurării siguranței spațiului cibernetic european.

2.1.2. Directiva (NIS) privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice

La 6 iulie 2016, Parlamentul European și Consiliul Uniunii Europene a adoptat Directiva (UE) 1148/2016 (NIS) privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice. Directiva NIS (Directive on Security of Network and Information Systems) este prima legislație paneuropeană privind securitatea cibernetică și se concentrează pe consolidarea autorităților cibernetice la nivel național, pe creșterea coordonării între acestea și pe introducerea cerințelor privind securitatea pentru sectoarele cheie ale industriei.

Scopul acestei Directive este de a asigura un nivel comun de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și cere operatorilor, respectiv furnizorilor de servicii digitale, să adopte măsuri adecvate pentru prevenirea atacurilor cibernetice și managementul riscului, și să raporteze incidentele grave de securitate către autoritățile naționale competente. [12]

În acest scop, Directiva NIS:

- stabilește pentru toate statele membre obligația de a adopta o strategie națională privind securitatea rețelelor și a sistemelor informatice;
- creează un grup de cooperare pentru a sprijini și facilita cooperarea strategică și schimbul de informații între statele membre și pentru a dezvolta încrederea între acestea;
- creează o rețea a echipelor de intervenție în caz de incidente de securitate cibernetică pentru a promova cooperarea operațională rapidă și eficace;
- stabilește cerințe de securitate și notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale;
- stabilește pentru statele membre obligații de desemnare a autorităților competente la nivel național, a punctelor unice de contact și a CSIRT cu atribuții legate de securitatea rețelelor și a sistemelor informatice. [12]

Directiva NIS privind securitatea rețelelor și a sistemelor informatice precizează următoarele măsuri ce trebuie luate la nivel național, de fiecare stat membru:

- adoptarea unei strategii naționale privind securitatea rețelelor și a sistemelor informatice care să definească obiectivele strategice și măsurile politice și de reglementare adecvate;
- desemnarea unei sau mai multor autorități competente la nivel național privind securitatea rețelelor și a sistemelor informatice;
- desemnarea unui punct unic de contact național privind securitatea rețelelor și a sistemelor informatice;
- asigurarea că, fie autoritățile competente, fie echipele CSIRT, primesc notificările incidentelor transmise în conformitate cu prezenta directivă. [12]

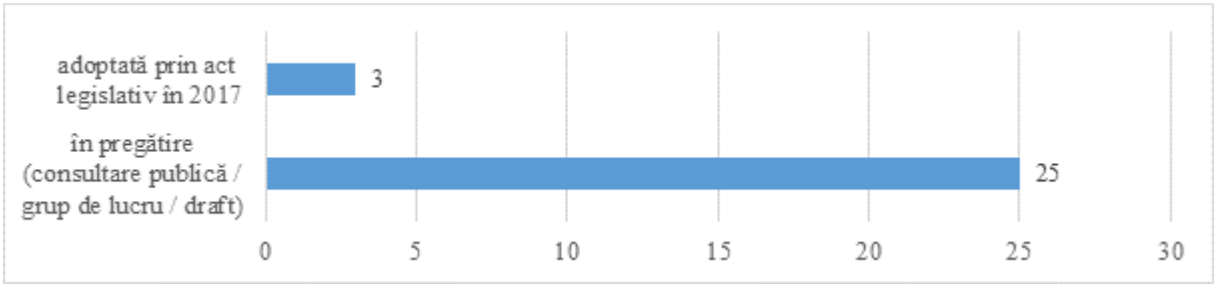
Statele membre trebuie să actualizeze lista operatorilor de servicii esențiale identificați cel puțin o dată la doi ani, din data de 9 mai 2018. Criteriile pentru identificarea furnizorilor de servicii esențiale sunt următoarele:

- furnizarea unui serviciu esențial pentru susținerea activităților societale și/sau economice de cea mai mare importanță;
- furnizarea serviciului respectiv depinde de rețea și de sistemele informatice;
- un incident ar avea efecte perturbatoare asupra furnizării serviciului. [3]

Din punctul de vedere al cerințelor de securitate și notificarea incidentelor, statele membre trebuie să se asigure că operatorii de servicii esențiale:

- iau măsuri tehnice și organizatorice adecvate pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care le utilizează;
- iau măsuri adecvate pentru a preveni și minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate;
- notifică autorității competente sau echipelor CSIRT incidentele care au un impact semnificativ asupra continuității serviciilor esențiale pe care le furnizează. [12]

Statele membre sunt obligate să transpună Directiva NIS în legislația națională, în termen de 21 de luni de la data adoptării sale. La nivelul statelor membre, odată cu adoptarea Directivei NIS au fost demarate acțiuni de transpunere a cerințelor în legislația națională. 3 state membre (Republica Cehă, Germania [37] și Franța [36]) au adoptat acte administrative la nivel de Guvern cu referire la Directiva NIS. Pentru îndeplinirea cerințelor specificate în Directiva NIS au fost modificate acte existente sau au fost emise acte de complianță cu Directiva.



Figură 8. Gradul de implementare NIS la nivelul statelor membre

Evaluarea legislației existente la nivel național în raport cu cerințele Directivei NIS este un proces în desfășurare în majoritatea statelor membre. [10] Diversitatea aspectelor abordate în legislațiile naționale demonstrează necesitatea unei prevederi legislative unitare la nivel european în vederea asigurării unui cadrul unitar legislativ și de cooperare în domeniul securității cibernetice.

Un aspect interesant al adoptării NIS la nivel european este acela că Marea Britanie, deși se află în plin proces de ieșire din Uniunea Europeană, continuă eforturile și contribuțiile la aplicarea și transpunerea Directivei NIS în legislația națională.

2.1.3. Regulamentul privind prelucrarea datelor cu caracter personal și libera circulație a acestor date

Un aspect important al securității la nivelul UE este reprezentat de protecția datelor cu caracter personal. În acest sens, Parlamentul European și Consiliul au adoptat în data de 27 aprilie 2016 Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - RGPD). Regulamentul (UE) 2016/679 a intrat în vigoare pe 25 mai 2016, iar prevederile lui vor fi aplicabile în toate statele membre UE, având caracter obligatoriu începând cu data de 25 mai 2018.

Preocupările privind asigurarea protecției datelor persoanelor în spațiul comunitar sunt elemente de bază, fiind un drept fundamental al unei persoane, garantat de capitolul II, Libertăți, art. 8 din Carta Drepturilor Fundamentale a UE și art. 16 al Tratatului UE.

Noul Regulament aduce o serie de schimbări semnificative prin consolidarea drepturilor garantate pentru persoanele ale căror date sunt prelucrate și simplificarea formalităților administrative pentru operatorii care prelucrează date cu caracter personal. De asemenea, extinde domeniul de aplicare și pentru operatorii de date care nu sunt localizați pe teritoriul Uniunii, dar care presupun prelucrarea datelor personale ale cetățenilor comunitari și conferă operatorilor posibilitatea de a interacționa cu o singură autoritate de supraveghere din statul în care este stabilit sediul principal al său.

Astfel, au fost stabilite cerințe obligatorii [47] privind:

- posibilitatea de a obține informații cuprinzătoare cu privire la scopul și temeiul legal în care se prelucrează datele personale;
- perioada de stocare datelor și drepturile de care beneficiază;
- dreptul de a fi uitat, cu aplicabilitate în mediul on-line (excepție în cazul în care este necesară pentru respectarea libertății de exprimare și a dreptului la informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public);

- obligația operatorului de a demonstra obținerea consimțământului pentru prelucrările de date personale;
- portabilitatea datelor - posibilitatea de a cere transferul datelor la un alt operator de date (obligativitatea operatorului de transfera datele într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil).

Un alt aspect cu caracter de noutate este cel al cooperării între autoritățile de supraveghere în cazul prelucrărilor de date care privesc persoane din mai multe state UE, oferind competențe autorității din statul respectiv ca, alături de autoritățile din celelalte state implicate, să se asigure că datele sunt prelucrate conform regulilor și principiilor stabilite de Regulament. Este prevăzută de asemenea o mai bună responsabilizare a operatorilor de date prin realizarea unui studiu de impact privind riscurile asociate prelucrării datelor cu caracter personal și clasificarea categoriilor de date pe care acesta le prelucrează.

Un management al riscului adecvat și o estimare corectă a impactului pe care îl poate avea asupra persoanei, dar și asupra operatorului de date ca și depozitar al datelor, vor stabili planul de măsuri tehnice și organizatorice necesare pentru prevenirea incidentelor.

Evaluarea impactului asupra protecției datelor presupune [21]:

- descrierea prelucrării de date efectuate și a scopurilor acesteia;
- evaluarea necesității și a proporționalității prelucrării de date efectuate;
- estimarea riscurilor asupra drepturilor și libertăților persoanelor vizate;
- măsuri pentru a trata riscurile și a asigura conformitatea cu dispozițiile Regulamentului nr. 679/2016.

Evaluarea impactului asupra protecției datelor permite [21]:

- realizarea unei prelucrări de date cu caracter personal sau a unui produs care respectă viața privată;
- estimarea impactului asupra vieții private a persoanelor vizate;
- demonstrarea faptului că principiile fundamentale ale Regulamentului nr. 679/2016 sunt respectate.

În acest sens au fost introduse 2 noi concepte, *privacy by design* și *privacy by default*. Principiul „Confidențialitatea / protecția datelor prin proiectare” se bazează pe abordarea privind confidențialitatea încă de la începutul procesului de proiectare a sistemelor și este o strategie preferabilă în comparație cu încercarea de adaptare a unui produs sau serviciu într-o etapă ulterioară. Abordarea conceptelor încă din procesul de proiectare sprijină luarea în considerare a întregului ciclu de viață al datelor și utilizarea acestora.

Principalele obligații pentru operatorii de date rezultate din Regulamentul (UE) 2016/679 sunt:

- *desemnarea unui responsabil cu protecția datelor* **(**este obligatorie din 25 mai 2018, raportat la dispozițiile art. 37 - 39 din Regulamentul General privind Protecția Datelor în cazul unei autorități publice**);**
- *cartografierea prelucrărilor de date cu caracter personal* (este necesară inventarierea prelucrărilor de date cu caracter personal efectuate, stabilirea scopului și a temeiului legal și păstrarea evidenței activităților de prelucrare);
- *prioritizarea acțiunilor de întreprins* **(**în funcție de riscurile pe care le prezintă prelucrările efectuate de un operator de date cu caracter personal pentru drepturile și libertățile persoanelor vizate);
- *gestionarea riscurilor* **(**clasificarea activităților de prelucrare a datelor cu caracter personal pe scara riscului luând în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii);

- *organizarea unor proceduri interne* (elaborarea procedurilor pentru obținerea consimțământului și care să garanteze respectarea protecției datelor în orice moment, luând în considerare toate evenimentele care pot apărea pe parcursul efectuării prelucrărilor de date);
- *proceduri interne* privind protecției datelor cu caracter personal încă de la momentul conceperii (*privacy by design*);
- *aplicarea de măsuri tehnice și organizatorice adecvate* pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării (*privacy by default*), sensibilizarea și organizarea diseminării informației prin stabilirea unui plan de pregătire cu persoanele care prelucrează date cu caracter personal;
- *asigurarea confidențialității și securității prelucrării* prin adoptarea de măsuri tehnice și organizatorice adecvate, incluzând printre altele, după caz [21]:
    - pseudonimizarea și criptarea datelor cu caracter personal (prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane);
    - capacitatea de a asigura continuu confidențialitatea, integritatea, disponibilitatea și rezistența sistemelor și serviciilor de prelucrare;
    - capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util, în cazul în care are loc un incident de natură fizică sau tehnică;
    - un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

2.2. Cadrul național în domeniul securității cibernetice

Numeroasele incidente de securitate cibernetică și evoluția atacurilor cibernetice din ultima vreme au determinat necesitatea adoptării la nivel internațional a unor politici și strategii în domeniul securității cibernetice. Aceste strategii subliniază necesitatea dezvoltării unor capabilități proprii fiecărei țări pentru contracararea atacurilor cibernetice și stabilesc cadrul general de acțiune și cooperare pentru limitarea efectelor acestora. Prin aceste strategii se dorește implementarea unor măsuri de securitate pentru protecția infrastructurilor cibernetice, în special pentru cele ce susțin infrastructurile critice naționale.

2.2.1. Strategia de securitate cibernetică a României

România a adoptat Strategia de securitate cibernetică în anul 2013, având o abordare comună la nivelul Uniunii Europene, pentru a putea oferi un răspuns prompt la atacurile din spațiul cibernetic. Scopul Strategiei de securitate cibernetică a României este de a defini și menține un spațiu cibernetic sigur, cu un înalt grad de reziliență și de încredere. Această strategie prezintă principiile și direcțiile importante de acțiune pentru prevenirea și combaterea vulnerabilităților și amenințărilor la adresa securității cibernetice a României. [22]

Principalele obiective stabilite de Strategia de securitate cibernetică a României sunt:

- adaptarea cadrului normativ la noile amenințări prezente în spațiul cibernetic;
- fundamentarea și aplicarea cerințelor minime de securitate pentru protejarea infrastructurilor cibernetice naționale;
- asigurarea rezilienței infrastructurilor cibernetice;
- realizarea campaniilor de informare și conștientizare a populației privind amenințările și riscurile prezente în spațiul cibernetic; [22]
- dezvoltarea cooperării dintre sectorul public și privat la nivel național și internațional.

Strategia de securitate cibernetică a României urmărește asigurarea securității cibernetice la nivel național, cu respectarea *Strategiei naționale de apărare* și *Strategiei naționale de protecție a infrastructurilor critice*.

Pentru asigurarea stării de normalitate în spațiul cibernetic al României, Strategia de securitate cibernetică se focalizează pe următoarele direcții:

- *stabilirea unui cadru conceptual, organizatoric și de acțiune pentru asigurarea securității cibernetice*. Pentru stabilirea acestui cadru se constituie un Sistem Național de Securitate Cibernetică, se stabilesc un set minimal de cerințe de securitate pentru infrastructurile cibernetice naționale și se dezvoltă cooperarea între sectorul public și sectorul privat, pentru schimbul reciproc de informații în domeniul securității cibernetice;
- *dezvoltarea capacităților de management al riscului și de reacție la incidentele cibernetice la nivel național*. Aceste capacități sunt dezvoltate prin implementarea unui mecanism de avertizare și alertă timpurie în cazul atacurilor cibernetice, prin sporirea gradului de reziliență al infrastructurilor, prin dezvoltarea structurilor de tip CERT și prin stimularea activităților de cercetare și dezvoltare în domeniul securității cibernetice;
- *promovarea metodelor de securitate în domeniul cibernetic*. În cadrul acestei direcții sunt derulate programe de conștientizare a factorului uman cu privire la vulnerabilitățile, amenințările și riscurile prezente în spațiul virtual, dezvoltarea unor programe educaționale privind utilizarea sigură a echipamentelor de calcul și formarea profesională a persoanelor ce își desfășoară activitatea în domeniul securității cibernetice;
- *dezvoltarea cooperării în domeniul securității cibernetice*. În acest sens se urmărește încheierea unor parteneriate de cooperare la nivel internațional în cazul unor atacuri cibernetice de amploare și participarea la evenimente și conferințe internaționale în domeniul securității cibernetice. [22]

SNSC (Sistemul Național de Securitate Cibernetică) reprezintă cadrul general de cooperare ce reunește autorități și instituții publice, cu responsabilități și capabilități în domeniu, în vederea coordonării acțiunilor la nivel național pentru asigurarea securității spațiului cibernetic. SNSC funcționează ca un mecanism unitar de relaționare și cooperare interinstituțională, acționând pe următoarele componente:

- *componenta de cunoaștere* - oferă suport pentru elaborarea măsurilor proactive și reactive în vederea asigurării securității cibernetice;
- *componenta de prevenire* - ajută la crearea și dezvoltarea capabilităților necesare analizei și prognozei evoluției stării securității cibernetice;
- *componenta de cooperare și coordonare* - asigură mecanismul unitar și eficient de relaționare în cadrul sistemului național de securitate cibernetică;
- *componenta de contracarare* - asigură reacția eficientă la amenințările sau atacurile cibernetice. [22]

Consiliul Suprem de Apărare a Țării este autoritatea ce coordonează, la nivel strategic, activitatea Sistemului Național de Securitate Cibernetică, iar Consiliul Operativ de Securitate Cibernetică (COSC) reprezintă organismul prin care se realizează coordonarea unitară a acestuia. Din COSC fac parte reprezentanți ai Ministerului Apărării Naționale (MApN), Ministerului Afacerilor Interne (MAI), Ministerului Afacerilor Externe (MAE), Ministerul Comunicațiilor și Societății Informaționale (MCSI), Serviciului Român de Informații (SRI), Serviciului de Telecomunicații Speciale (STS), Serviciului de Informații Externe (SIE), Serviciului de Protecție și Pază (SPP), Oficiului Registrului Național pentru Informații Secrete de Stat (ORNISS), precum și secretarul Consiliului Suprem de Apărare a Țării. [22]

Realizarea obiectivelor Strategiei de securitate cibernetică a României presupune conlucrarea dintre sectorul public și sectorul privat, inclusiv prin măsuri de prevenție, conștientizare și promovare a oportunităților în domeniul cibernetic.

2.2.2. Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

Ministerul Comunicațiilor și Societății Informaționale a lansat în dezbatere publică, în data de 3 octombrie 2017, Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. [40] Acest proiect de act propune adoptarea unui set de norme menite să instituie un cadru național unitar de asigurare a securității cibernetice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale în conformitate cu cerințele Directivei NIS.

Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice reglementează:

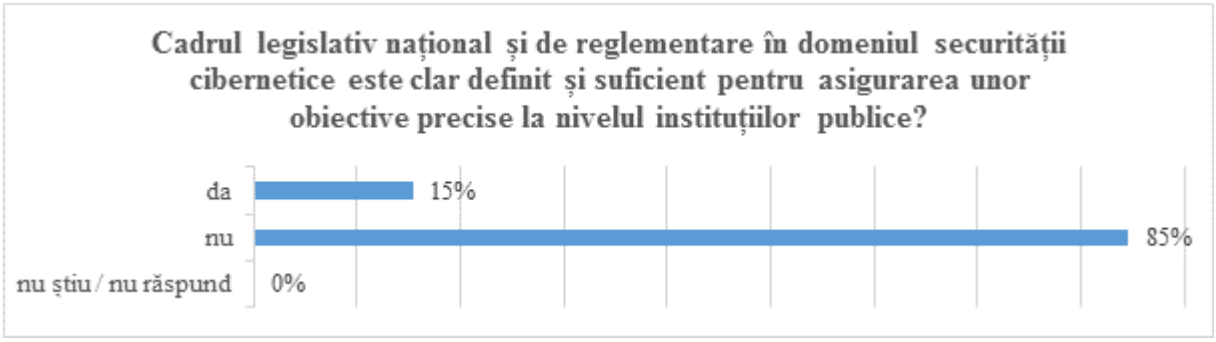
- cadrul de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice;
- autoritățile și entitățile de drept public și privat care dețin competențe și responsabilități în aplicarea prevederilor prezentei legi, a punctului unic de contact la nivel național și a echipei naționale de răspuns la incidente de securitate cibernetică;
- cerințele de securitate și de notificare pentru operatorii de servicii esențiale și furnizorii de servicii digitale precum și instituirea mecanismelor de actualizare a acestora în funcție de evoluția amenințărilor la adresa securității rețelelor și sistemelor informatice. [40]

În privința autorității competente la nivel național, a punctului unic și a echipei CSIRT naționale proiectul de lege propune dezvoltarea acestora în cadrul CERT-RO (Centrul Național de Răspuns la Incidente de Securitate Cibernetică). În vederea asigurării unui nivel ridicat de securitate a rețelelor și sistemelor informatice, CERT-RO se consultă și cooperează cu Serviciul Român de Informații (prin Centrul Național Cyberint), Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază. [40]

Pentru definirea domeniului de aplicare, proiectul reglementează operatorii de servicii esențiale și definirea acestor serviciilor esențiale. Sectoarele vizate pentru identificarea serviciilor esențiale și a operatorilor de servicii esențiale cuprind: energia, transporturile, sectorul bancar, infrastructurile pieței financiare, sectorul sănătății, furnizarea și distribuirea de apă potabilă, infrastructura digitală. Proiectul propune alcătuirea unui Registru al operatorilor de servicii esențiale, care să fie actualizat de CERT-RO la cel puțin doi ani. [40]

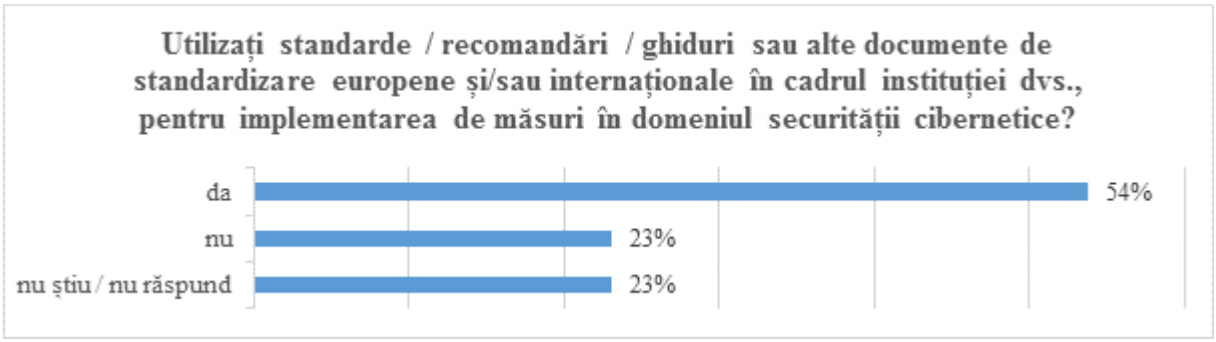
Proiectul de act normativ își propune și stimularea dezvoltării pieței de securitate cibernetică. În acest sens, sunt definite măsurile care privesc piața de audit de securitate pentru rețelele și sistemele operatorilor și furnizorilor vizați, precum și piața de servicii de securitate cibernetică de tip CSIRT. Adoptarea unui set de norme care să reglementeze un cadru național unitar de asigurare a securității cibernetice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice, reprezintă un element principal pentru îndeplinirea obiectivelor de asigurare a securității naționale a României în domeniul cibernetic. [29]

Conform sondajului realizat în cadrul acestui studiu, 85% dintre respondenți au precizat că în domeniul securității cibernetice, cadrul legislativ național și de reglementare nu este clar definit și suficient pentru asigurarea unor obiective precise la nivelul instituțiilor publice.



Figură 9. Chestionar privind cadrul legislativ național și de reglementare în domeniul securității cibernetice

La întrebarea privind utilizarea standardelor, recomandărilor, ghidurilor sau altor documente de standardizare europene și/sau internaționale în cadrul instituțiilor, pentru implementarea de măsuri în domeniul securității cibernetice, 54% dintre respondenți au răspuns afirmativ.



Figură 10. Chestionar privind utilizarea standardelor / recomandărilor / ghidurilor sau a altor documente de standardizare europene și/sau internaționale în cadrul instituțiilor

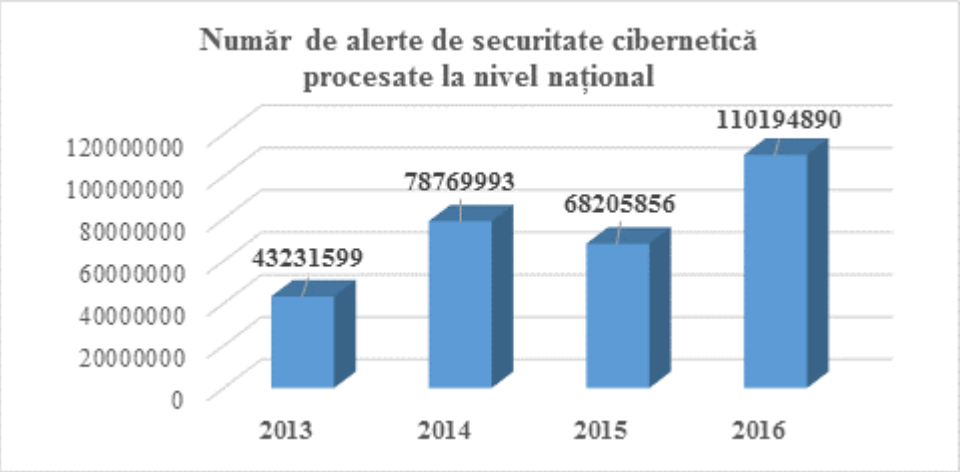
Acest studiu empiric ne arată că, la nivelul instituțiilor publice din România, cadrul legislativ național și de reglementare nu este clar definit și suficient pentru asigurarea unor obiective precise în domeniul securității cibernetice.

2.3. Studiul alertelor de securitate cibernetică procesate la nivel național

CERT-RO a colectat și procesat în anul 2016 un număr de 110 194 980 alerte de securitate cibernetică (în creștere față de anul 2015 cu 61,55%), ce au afectat un număr de 2 920 407 adrese IP unice. [43]

Tabel 3. Alerte de securitate cibernetică procesate la nivel național

An	Număr alerte
2013	43 231 599
2014	78 769 993
2015	68 205 856
2016	110 194 890



Figură 11. Alerte de securitate cibernetică procesate la nivel național

În urma analizării alertelor de securitate cibernetică colectate de CERT-RO în anul 2016, au fost constatate următoarele:

- 38,72% (2,92 mil.) din totalul IP-urilor alocate României (7,5 milioane) au fost afectate;
- 81,39% (89,68 mil.) din alertele colectate și procesate vizează sisteme informatice vulnerabile;
- 12,81% (14,12 mil.) din alertele colectate și procesate vizează sisteme informatice infectate cu diferite variante de software malițios (malware) de tip botnet;
- 58,98% (2,38 mil.) din numărul total de incidente rezultate din procesarea alertelor de securitate cibernetică reprezintă sisteme informatice vulnerabile, acestea putând fi utilizate în derularea de atacuri cibernetice asupra unor ținte din Internet;
- 40,96% (1,65 mil.) din numărul total de incidente rezultate din procesarea alertelor reprezintă sisteme informatice ce fac parte din rețele de tip botnet;
- 10.639 domenii „.ro” au fost raportate la CERT-RO ca fiind compromise în anul 2016, în scădere cu aproximativ 40% față de anul 2015 (17.088 domenii). [43]

În baza constatărilor de mai sus, pot fi formulate următoarele concluzii:

- majoritatea alertelor colectate de CERT-RO se referă la sisteme informatice vulnerabile (configurate necorespunzător sau nesecurizate) și la sisteme informatice infectate cu diverse variante de malware de tip botnet;
- oricare dintre cele două tipuri de sisteme informatice menționate mai sus pot fi folosite ca interfață (proxy) pentru desfășurarea unor atacuri asupra unor terțe ținte (din interiorul sau din afara țării), reprezentând astfel potențiale amenințări la adresa altor sisteme conectate la Internet;
- dispozitivele sau echipamentele de rețea de uz casnic sau cele care fac parte din categoria IoT, odată conectate la Internet, devin ținta atacatorilor, iar vulnerabilitățile sunt exploatate de către atacatori pentru a compromite rețeaua din care fac parte sau pentru lansarea unor atacuri asupra altor ținte din Internet;
- România este o țară atât generatoare de incidente de securitate cibernetică, cât și cu rol de proxy (de tranzit) pentru atacatori din afara spațiului național, prin prisma utilizării unor sisteme vulnerabile sau compromise, ce fac parte din spațiul cibernetic național. [43]

În pofida aspectelor tehnice ce fac imposibilă identificarea numărului exact de dispozitive sau persoane afectate din spatele celor aproximativ 2,9 mil. adrese IP sau 110 mil. alerte raportate la CERT-RO, este important de reținut că acestea acoperă aproximativ 38,72% din spațiul cibernetic național (raportat la numărul de adrese IP alocate României) și ca urmare sunt necesare măsuri de remediere a situației prin implicarea tuturor actorilor cu responsabilități de ordin tehnic sau legislativ. [43] Realizând gruparea alertelor pe incidente, a rezultat un număr de 4 035 445 incidente în anul 2016, distribuite conform tabelului de mai jos.

Tabel 4. Distribuția alertelor pe număr de incidente

Nr. crt.	Clasă alertă	Număr incidente	Procent
1	Vulnerabilități	2 380 120	58,98%
2	Botnet	1 653 096	40,96%
3	Malware	2 071	0,05%
4	Altele	158	0,01%

Statistica bazată pe agregarea alertelor colectate în incidente arată faptul că sistemele informatice ce fac parte din rețele de tip botnet (40,96%) reprezintă în continuare o problemă principală a spațiului cibernetic național, alături de sistemele informatice vulnerabile (58,98%).

Un procent de 13% din totalul alertelor colectate și procesate de CERT-RO în anul 2016 conțin și informații referitoare la tipul de malware asociat alertei (precum alertele de tip botnet sau cele referitoare la URL-uri malițioase). [43]

Tabel 5. Top 5 tipuri de malware în România

Nr. crt.	Tip malware	Număr alerte	Procent
1	Sality	4 953 615	34,16%
2	Downadup	2 570 006	17,72%
3	Nivdort	1 979 510	13,65%
4	Ramnit	1 081 592	7,46%
5	Dorkbot	830 914	5,73%

Interesant de observat sunt principalele forme de malware răspândite pe teritoriul României în ultimii 3 ani.

Tabel 6. Top 5 tipuri de malware în România în ultimii 3 ani

Nr. crt.	Tip malware 2016	Tip malware 2015	Tip malware 2014
1	*Sality*	*Conficker*	*Downadup*
2	*Downadup*	*Sality*	Zeus
3	Nivdort	ZeroAccess	*Sality*
4	Ramnit	Ramnit	Virut
5	Dorkbot	Tinba	Zeroaccess

Observăm prezente în acest Top 5 tipuri de malware în România în ultimii 3 ani [43][44][45], în special două forme de malware:

- *Sality* – virusul, descoperit pe 4 iunie 2003, infectează fișierele executabile de pe unitățile locale, detașabile sau de la distanță, încercând să dezactiveze software-ul de securitate;
- *Downadup / Conficker* – viermele, descoperit pe 21 noiembrie 2008, scanează rețelele de calculatoare pentru a infecta sistemele de operare neactualizate, cum ar fi Windows XP sau Windows 2003.

Ambele forme de malware, deși detectate în urmă cu peste 10 ani, încă sunt folosite de infractorii cibernetici, în special pentru că sunt distribuite în rețelele de tip Peer-to-Peer (P2P).

Un procent de 20,19% din totalul alertelor colectate și procesate de CERT-RO în anul 2016 conțin și informații referitoare la sistemul de operare al sistemelor informatice vizate de alerte.

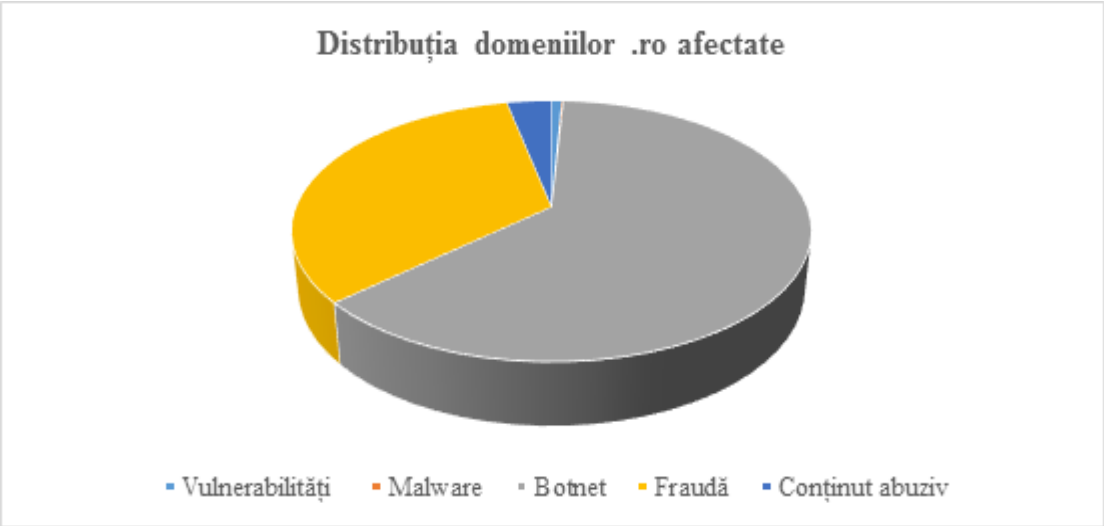
Tabel 7. Distribuție alerte totale per tipuri de sisteme de operare afectate

Nr. crt.	Sistem de operare	Procent
1	Linux	42,96%
2	Network Devices Firmware/OS	22,91%
3	Unix	24,02%
4	UPnP OS	8,08%
5	Windows	0,57%

Pentru anul 2016, CERT-RO a primit alerte referitoare la 10 639 domenii „.ro” compromise. Distribuția domeniilor afectate, după tipul de incident, se regăsește mai jos. [43]

Tabel 8. Domenii .ro compromise

Nr. crt.	Clasă alerte	Număr site-uri
1	Vulnerabilități	8 202
2	Malware	1 363
3	Botnet	677
4	Fraudă	361
5	Conținut abuziv	36
	TOTAL	**10 639**



Figură 12. Distribuția domeniilor .ro afectate

Din 896 7264 domenii înregistrate în România, în luna decembrie 2016, numărul domeniilor infectate reprezintă aproximativ 1,19% din totalul domeniilor „.ro" și aproximativ 2,52% din totalul domeniilor „.ro" active. [43]

2.4. Concluzii

România se află într-un proces continuu de consolidare a securității cibernetice la nivel național, atât din punct de vedere legal, instituțional, cât și procedural, fiind întreprinse, în acest sens, eforturi susținute de către autoritățile cu responsabilități în domeniu. Din punct de vedere al inițiativelor legislative în domeniul securității cibernetice, România a făcut mai mulți pași pentru a crește gradul de pregătire în ceea ce privește securitatea cibernetică. Astfel, România a ratificat *Convenția Consiliului Europei privind criminalitatea informatică,* prin Legea nr. 64/2004. Guvernul României a aprobat *Strategia de securitate cibernetică a României*, prin Hotărârea nr. 271 din 15 mai 2013, având astfel o abordare comună la nivelul Uniunii Europene, pentru a putea oferi un răspuns prompt la atacurile din spațiul cibernetic. La începutul anului 2014 au intrat în vigoare *Noul Cod Penal* și *Noul Cod de Procedură Penală*, care implementează standardele internaționale existente în domeniul criminalității informatice. Ministerul Comunicațiilor și Societății Informaționale a lansat în dezbatere publică, în data de 3 octombrie 2017, *Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, care propune adoptarea unui set de norme menite să instituie un cadru național unitar de asigurare a securității cibernetice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale, în conformitate cu cerințele Directivei NIS.

Conform rapoartelor anuale ale CERT-RO, România este nu doar o țară generatoare de incidente de securitate cibernetică sau cu rol de tranzit pentru atacatorii externi, din afara spațiului național, însă a devenit în ultimii ani și o țintă a atacurilor cibernetice de tip APT, DDoS sau ransomware.

Reglementările legislative existente în prezent, precum și gradul de operaționalizare al acestora la nivelul instituțiilor publice din România nu permit prevenirea și contracararea cu maximă eficiență a unor amenințări cibernetice de nivel mediu și ridicat. Din acest motiv, consolidarea cadrului legislativ în domeniul securității cibernetice trebuie să constituie o prioritate națională, pentru a fi asigurate condiții optime de reacție rapidă la incidentele cibernetice.

CAPITOLUL III

COOPERAREA DINTRE SECTORUL PUBLIC ȘI CEL PRIVAT ÎN DOMENIUL SECURITĂȚII CIBERNETICE

3.1. Importanța cooperării în aria securității cibernetice

Complexitatea sistemelor dezvoltate în ultimii ani în majoritatea domeniilor reprezintă o consecință directă a diversității subsistemelor și a elementelor componente ale acestora, ce au condus la creșterea gradului de interacțiune dintre diversele tehnologii și arhitecturi utilizate în implementarea unui sistem informatic. Asigurarea securității sistemelor a devenit un proces decizional complex, care necesită dezvoltarea unor instrumente manageriale aplicate cu privire la procesul de adoptare a deciziilor.

Ca o consecință directă, informațiile referitoare la comportamentul unui sistem complex și interacțiunile dintre subsisteme nu pot fi ușor observate și controlate de un singur operator. Prin urmare, comportamentul sistemelor complexe sau al unor părți componente poate fi uneori imprevizibil în timpul funcționării, în contradicție cu funcțiile și obiectivele pentru care acestea au fost proiectate. Dezvoltarea unui sistem care să îndeplinească misiunea pentru care a fost proiectat, în prezența unei amenințări la adresa performanțelor și securității (defect, atac cibernetic, dezastru natural etc.), precum și asigurarea funcțiilor critice ale sistemului inițial, sunt reunite în conceptele de reziliență și survivabilitate (caracteristica de supraviețuire a unui sistem).

Principalele caracteristici asociate conceptului de survivabilitate implică integritatea și disponibilitatea. Aceasta include luarea în considerare, la proiectarea sistemelor, a întrebărilor „cum” și „cât”, precum și o evaluare a riscurilor speciale. Astfel de riscuri pot fi limitate, având în vedere resursele și abilitățile sistemului pentru a oferi un nivel optim al serviciilor, prin definirea unei capacități de apărare și răspuns, cunoscute în momentul respectiv. Având o viziune de perspectivă, se presupune că provocările referitoare la performanța sistemului vor avea loc și se caută în mod activ noi modalități de combatere a amenințărilor.

Importanța domeniului calității și fiabilității sistemelor complexe critice, în special a securității și dependabilității, este subliniată de numeroasele programe și proiecte aflate în derulare la nivelul Uniunii Europene, prin Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor. Obiectivul central este de a stimula și sprijini dezvoltarea unui nivel ridicat al capacității de reacție și răspuns, de securitate și de reziliență, atât la nivelul statelor membre (național), cât și la nivel european. Această abordare a fost aprobată în linii mari de către Consiliu începând cu anul 2009. [49]

Strategia europeană și planurile de acțiune ale statelor membre, de protecție împotriva amenințărilor din spațiul cibernetic, cuprind direcții de acțiune cum ar fi pregătire și prevenire, detecție și reacție și reziliența infrastructurilor. Una din direcțiile care a căpătat o importanță deosebită este reprezentată de cooperarea la nivel național și internațional în domeniu. Astfel, începând cu anul 2013, încă de la versiunea de lucru a Directivei NIS - Network and information security across the EU - 2013/0027(COD) [41], se stabilește ca măsură prioritară „crearea unui mecanism de cooperare între statele membre și Comisia Europeană pentru a împărtăși / distribui avertismentele timpurii privind riscurile și incidentele, pentru a face schimb de informații și a combate amenințările și incidentele NIS”.

În versiunea finală a Directivei NIS [12] este pus accentul pe „creșterea cooperării în domeniul securității cibernetice între statele membre ale UE” și se introduce necesitatea adoptării „măsurilor de securitate și a obligațiilor de raportare a incidentelor pentru furnizorii de servicii digitale și operatorii de servicii esențiale care dețin infrastructură națională critică”.

Numărul tot mai mare și complexitatea amenințărilor cibernetice necesită măsuri și acțiuni în vederea consolidării cooperării internaționale pentru a contribui la dezvoltarea de tehnologii, produse și servicii inovatoare și sigure.

Cu toate acestea, nivelul de amenințare este în continuă evoluție, iar gestionarea unui incident cibernetic la scară largă, care implică simultan mai multe state, va fi o provocare. Cooperarea la nivelul european este, prin urmare, esențială pentru a face față atât atacului cibernetic pe scară largă (în mai multe state), cât și incidentelor cibernetice mai mici, dar potențial mai frecvente. Astfel, este necesar un plan pentru o reacție coordonată, bazat pe schimbul transfrontalier de informații, pentru a aborda incidentele cibernetice în cel mai eficient mod. În acest sens, domeniul securității cibernetice trebuie integrat în mecanismele și procedurile existente pentru gestionarea situațiilor de urgență, în scopul de a obține o coordonare cu celelalte sectoare potențial afectate de un incident cibernetic.

Principalele mecanisme de cooperare la nivel european sunt:

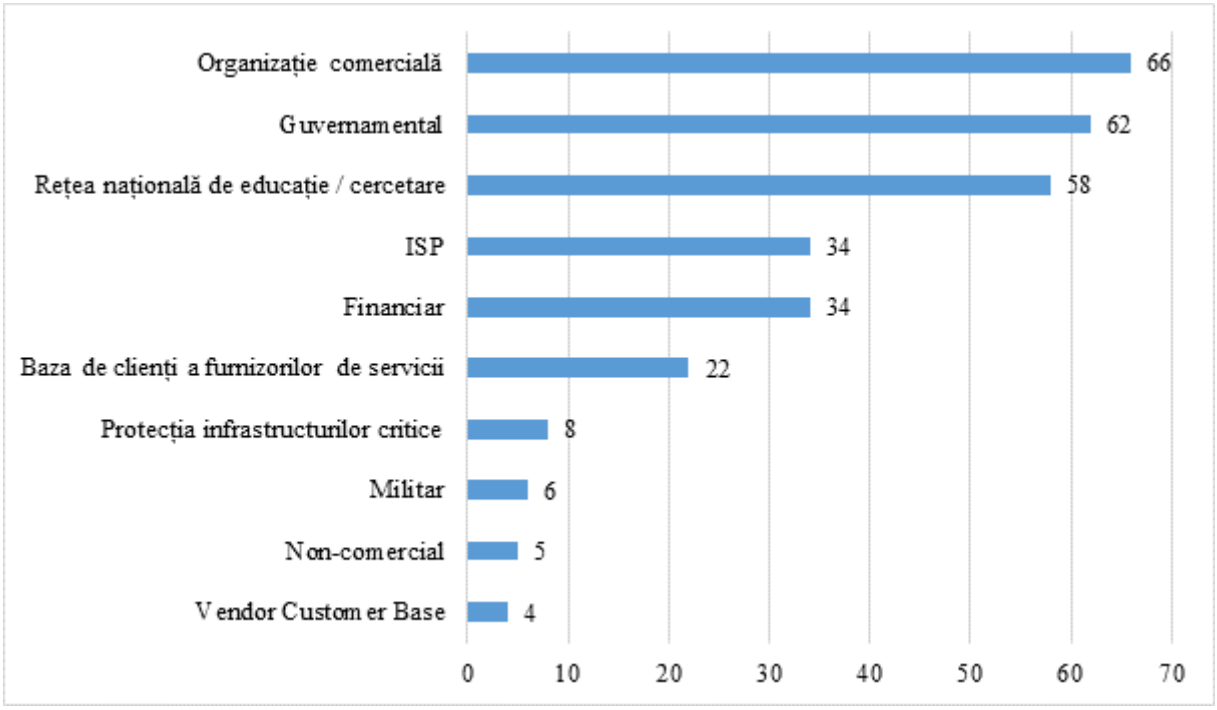
- Grupul de cooperare - sprijină cooperarea strategică și schimbul de informații relevante privind incidentele cibernetice în rândul statelor UE;
- CSIRT - rețeaua de echipe de răspuns la incidentele de securitate a calculatoarelor, care promovează o cooperare operațională rapidă și eficientă privind incidente specifice în domeniul securității informatice și al schimbului de informații.

La nivel internațional, țări ca Statele Unite ale Americii, Japonia [27] sau China [26] au adoptat strategii de cooperare în domeniu, prin definirea de mecanisme dinamice pe mai multe niveluri de colaborare cu alte state în vederea partajării informațiilor și a modalităților de contracarare a incidentelor.

Schimbul de informații privind criminalitatea informatică și colaborarea cu instituții din alte state trebuie reglementate prin stabilirea unui cadru privind cooperarea internațională pentru asigurarea securității în spațiul cibernetic. Atacurile cibernetice sunt de obicei transnaționale și dificil de atribuit, țările ar trebui să colaboreze pentru a asigura securitatea cibernetică prin cooperare constructivă și consultare continuă.

În prezent, cunoștințele și expertiza privind securitatea cibernetică sunt disponibile într-un mod dispersat și nestructurat. În acest sens, apare necesitatea unui cadru internațional agreat privind o cooperare consolidată împotriva unui atac cibernetic de scară largă prin colaborarea structurilor de specialitate naționale (CERT, CSIRT etc.). Mecanismele dezvoltate trebuie să pună accent pe partajarea cunoștințelor despre vulnerabilități și amenințări, utilizarea de proceduri și standarde comune în atenuarea acestora, valorificarea bunelor practici și a lecțiilor învățate ale altor state și încurajarea unei culturi a încrederii reciproce.

Distribuția pe domenii de activitate a CSIRT-urilor active în spațiul european arată o dezvoltare în special în zona societăților comerciale, a administrației publice și în mediul educație academică - cercetare.



Figură 13 CSIRT-uri pe domenii de activitate în UE și EFTA (European Free Trade Association)

În domeniul securității cibernetice, cooperarea se realizează prin acorduri punctuale între organizații, pe orizontală (sectoriale naționale) sau verticală (structuri internaționale / naționale). Cele mai recomandate modalități de realizarea a unei cooperări eficiente este prin acorduri bilaterale (organizații internaționale sau punctual cu alte țări) și multilaterale, cum ar fi modelul de colaborare a CERT-urilor naționale din țările nordice Danemarca, Finlanda, Islanda, Norvegia și Suedia prin NORDUnet CERT și NCIRC CC - NATO Communication and Information Agency's Cyber Security.

Un alt plan necesar a fi dezvoltat este cel al cooperării între părțile civilă și militară și examinarea modalităților prin care ambele domenii pot învăța unele de la altele în ceea ce privește formarea și exercitarea, pentru a spori capacitățile de reziliență și de reacție la incidente. Câteva direcții care pot fi urmate sunt:

- dezvoltarea unor platforme de educație, poligoane pentru exerciții cibernetice comune având ca obiective exersarea și evaluarea modului de gestionare a incidentelor cibernetice, răspunsul la nivel operațional, tactic și strategic;
- optimizarea procesului de cooperare în vederea identificării și limitării impactului incidentelor prin abordări simplificate.

Provocările și amenințările din spațiul cibernetic ignoră granițele naționale și au schimbat percepția asupra securității la nivelul unei societăți prin dependența din ce în ce mai mare de infrastructurile naționale. Interdependența economică și alte aspecte ale coexistenței moderne ar trebui să conducă și să ajute la dezvoltarea unei comunități internaționale și a unei culturi solide de cooperare în domeniul securității cibernetice.

3.2. Combaterea criminalității informatice

Evoluția crimei organizate în România în ultimii ani este strâns legată de evoluția criminalității informatice și de folosirea tot mai intensă a tehnologiei informației și comunicațiilor, în comiterea de infracțiuni. Dezvoltarea fenomenului criminalității informatice în România se manifestă sub mai multe aspecte:

- creșterea numărului de cazuri înregistrate privind criminalitatea informatică;
- preocuparea infractorilor pentru identificarea de noi moduri de operare;
- reorientarea grupărilor criminale către infracțiuni de natură informatică.

Principalii factori care au determinat orientarea grupărilor criminale către infracțiuni informatice sunt obținerea de câștiguri materiale mari într-un timp relativ scurt și cu riscuri relativ mici, caracterul transfrontalier al infracțiunilor, accesul facil la echipamente IT moderne, precum și la instrumente software și tutoriale ce pot fi descărcate ușor din zona neindexată a Internet-ului - DarkNet. [55]

La nivelul României, criminalitatea informatică se manifestă sub următoarele aspecte: *atacuri cibernetice*, ce urmăresc compromiterea diferitor rețele și sisteme informatice prin multiple moduri și instrumente (malware, ransomware, atacuri de tip DDoS sau Defacement), *fraudele informatice*, constând în licitații fictive de bunuri, compromiterea conturilor utilizatorilor pe site-uri de comerț electronic sau realizarea unor site-uri de phishing pentru colectarea datelor bancare și *fraudele cu cărți de credit*, constând în compromiterea bancomatelor și extragerea unor informații confidențiale din cardurile clienților. [55]

Persoanele implicate în activități de criminalitate informatică folosesc metode complexe de inginerie socială, conving victimele să divulge informații confidențiale sau să desfășoare acțiuni care să ducă la infectarea sistemelor informatice pe care le folosesc sau administrează. În foarte multe cazuri, sistemele informatice astfel infectate devin părți componente ale unor rețele de tip botnet, care sunt folosite la executarea unor atacuri cibernetice coordonate de tip DDoS împotriva unor infrastructuri cibernetice administrate de instituții publice.

Se observă un trend îngrijorător al implicării tot mai multor persoane de vârste fragede și chiar minore în săvârșirea infracțiunilor informatice, acestea neavând o viziune clară asupra consecințelor juridice ce decurg din astfel de acțiuni. În acest sens se impune o mai bună informare a publicului și chiar campanii derulate în școli cu privire la combaterea și prevenirea criminalității informatice în rândul copiilor și tinerilor.

Unele din cele mai frecvent întâlnite atacuri cibernetice în România, ca de altfel și în Europa, constau în infectarea sistemelor informatice cu malware de tip ransomware. Acest ransomware criptează datele de pe sistemul informatic utilizat de victimă, iar singura modalitate prin care datele se pot recupera este plata unei chei de decriptare. Atacurile ce distribuie ransomware au devenit o problemă enormă pentru securitatea cibernetică în ultimii ani. Numărul de utilizatori infectați cu ransomware crește constant, cu 718 000 de utilizatori afectați între aprilie 2015 și martie 2016, ce reprezintă o creștere de 5,5 ori față de aceeași perioadă din 2014 - 2015. [35]

Poliția nu poate lupta împotriva singură împotriva acestor forme de atacuri, în special a răscumpărării, deoarece plățile către infractorii cibernetici sunt realizate în moneda virtuală Bitcoin. Lupta împotriva ransomware-ului la nivelul Europei necesită un efort comun între poliție, departamentul de justiție, Europol și companiile de securitate IT. În acest sens, pentru conștientizarea pericolelor reprezentate de răspândirea diverselor forme de ransomware, Centrul European de Criminalitate Informatică EC3, în parteneriat cu Poliția olandeză, două companii de securitate cibernetică (Kaspersky Lab și McAfee) și cu alți parteneri fondatori și asociați, au dezvoltat portalul *No More Ransom*. Lansat în iulie 2016, acest exemplu de parteneriat public-privat internațional are ca scop nu doar lupta împotriva fenomenului ransomware, ci și educarea utilizatorilor din întreaga lume cu privire la modul de prevenire a atacurilor de acest tip.

Un alt exemplu în acest sens este colaborarea dintre Poliția Română (prin Serviciul de Combatere a Criminalității Informatice) și Bitdefender, pentru obținerea cheii de decriptare a aplicației malițioase de tip ransomware Bart. [7]

O altă tendință în România este dată de infectarea sistemelor informatice care administrează plățile prin POS cu anumite tipuri de malware, care permit atacatorilor cibernetici să controleze aceste dispozitive de la distanță, putând astfel identifica, transfera și comercializa datele cardurilor bancare. [55]

Serviciul de Combatere a Criminalității Informatice este structura specializată din Poliția Română ce are în competență prevenirea, investigarea și cercetarea criminalității informatice și funcționează în cadrul Direcției de Combatere a Criminalității Organizate. Serviciul acționează ca o structură centrală, cu atribuții de coordonare și control al activității în domeniu, la nivelul întregii țări. Serviciul realizează evaluări și analize asupra fenomenului criminalității informatice în România, asigură programe de pregătire și dotarea necesară polițiștilor care-și desfășoară activitatea în domeniul prevenirii și investigării criminalității informatice. Serviciul are atribuții de punct de contact 24/7, pentru asigurarea cooperării internaționale și luarea unor măsuri de urgență în cazuri de criminalitate informatică, împreună cu Serviciul de combatere a criminalității informatice din cadrul DIICOT (Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism). [52]

Un proiect important al Inspectoratului General al Poliției Române în domeniul combaterii criminalității informatice a fost realizarea *Centrului Român de Excelență în Combaterea Criminalității Informatice (CYBEREX),* cu sediul la Academia de Poliție „Alexandru Ioan Cuza" din București. Proiectul a reunit principalii actori implicați la nivel național în prevenirea și combaterea criminalității informatice: instituții, companii private și mediul academic. Pe lângă coordonarea la nivel național, proiectul a prevăzut, de asemenea, cooperarea la nivel european și a asumat bunele practici și lecțiile învățate din experiențele altor state membre ale Uniunii Europene în domeniu.

Obiectivul proiectului a fost de a crea premisele unei abordări strategice de prevenire și combatere a fenomenului criminalității informatice. Acest Centru Român de Excelență, inclus în rețeaua *2Centre* (*Cybercrime Centres of Excellence Network for Training Research and Education*), oferă instruire experților din domeniul criminalității informatice și asigură accesul acestora la cele mai recente evoluții și tendințe în domeniu.

3.3. Divulgarea coordonată a vulnerabilităților informatice

Numărul incidentelor de securitate cibernetică ce exploatează vulnerabilități ale programelor, serviciilor și sistemelor informatice este în continuă creștere din cauza lipsei unei metodologii de testare a vulnerabilităților. Vulnerabilitățile sunt defecte în codul software ce pot fi exploatate pentru a compromite confidențialitatea, disponibilitatea sau integritatea sistemelor afectate. Remedierea vulnerabilităților este, prin urmare, crucială pentru asigurarea securității cibernetice, iar un proces de divulgare a vulnerabilităților reprezintă un element semnificativ în reducerea riscurilor de securitate. Însă vulnerabilitățile informatice, în special cele de tip *zero-day,* sunt căutate pentru comercializare pe piața neagră, pentru a fi exploatate în atacuri cibernetice, ducând astfel la pierderi însemnate și punând în pericol datele cetățenilor și funcționarea sistemelor și serviciilor în spațiul cibernetic. [15]

În procesul de divulgare a vulnerabilităților pot fi implicate numeroase părți interesate, cum ar fi producători/furnizori de software, furnizori de securitate IT, cercetători, publicul larg, dar și infractorii cibernetici. Aceste părți interesate pot avea interese conflictuale, ceea ce poate duce la provocări privind rezolvarea vulnerabilităților descoperite, cum ar fi constrângerile legale sau lipsa de încredere.

Cooperarea dintre instituții, organizații și comunitatea online creată în jurul topicului „securitate cibernetică” poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilității (*CVD - Coordinated Vulnerability Disclosure*) sau divulgarea responsabilă. În esență, aceasta este o formă de cooperare în care un raportor informează proprietarul sistemului informatic, permițându-i acestuia posibilitatea de a diagnostica și remedia vulnerabilitatea înainte ca informațiile trecute cu privire la vulnerabilitate să fie divulgate terților sau publicului larg. [14]

Obiectivele unei politici coordonate privind divulgarea vulnerabilităților includ:

- asigurarea abordării vulnerabilităților identificate;
- minimizarea riscului de securitate provenit de la vulnerabilitățile identificate;
- furnizarea unor informații suficiente pentru evaluarea riscurilor legate de vulnerabilitățile sistemelor;
- stabilirea așteptărilor privind comunicarea și coordonarea pozitivă între părțile implicate.

O politică eficientă de divulgare coordonată a vulnerabilităților poate minimiza șansele ca actorii rău-intenționați să profite de vulnerabilitățile informatice, construi încrederea clienților în ceea ce privește securitatea datelor acestora, aduce informații suplimentare despre noi vulnerabilități relevante și contribui la sporirea nivelului de securitate cibernetică.

Procesul de divulgare a vulnerabilităților implică de obicei următorii pași:

- descoperirea unei vulnerabilități de către un raportor;
- notificarea proprietarului sistemului informatic afectat;
- investigarea vulnerabilității potențiale și a impactului acesteia;
- confirmarea a vulnerabilității (dacă este cazul);
- oferirea de soluții pentru remedierea sau eliminarea vulnerabilității;
- divulgarea publică a informațiilor despre vulnerabilitate.

În practică pot exista multe varietăți ale procesului de divulgare. Descoperirea unei vulnerabilități poate duce la vânzarea acestei informații unei terțe părți sau la dezvăluirea imediată în spațiul public, oferind dezvoltatorilor de software foarte puțin sau deloc timp pentru a rezolva vulnerabilitatea. Între aceste două situații se poate face o divulgare coordonată a vulnerabilității, în care raportorul și producătorii/furnizorii coordonează acțiunile și termenele înainte de divulgare.

În ultimii ani a crescut dorința de a contribui la creșterea nivelului de securitate cibernetică, fiind tot mai frecvent întâlnite raportarea vulnerabilităților descoperite unei terțe părți neutre, precum echipele de tip CERT. În contextul necesităților de a putea procesa semnalări referitoare la vulnerabilitățile informatice identificate, CERT-RO trebuie să asigure un cadru pentru derularea acestei activități. Astfel, cu sprijinul Ministerului de Afaceri Externe, România este parte a inițiativei *Global Forum on Cyber Expertise* (GFCE) [9] de promovare a adopției mecanismelor de divulgare coordonată a vulnerabilităților de către state, guverne, companii și instituții deținătoare sau administratori de servicii, rețele sau sisteme informatice destinate publicului. În formatul GFCE, CERT-RO participă activ la demersuri la nivel național și internațional în vederea creșterii gradului de încredere și cooperare pentru îmbunătățirea climatului de securitate a rețelelor și sistemelor informatice. [15]

Ca parte a inițiativei divulgării coordonate a vulnerabilităților la nivel național, CERT-RO încurajează:

- adoptarea de către companii și instituții a mecanismelor necesare primirii, evaluării și remedierii de vulnerabilități raportate;
- identificarea și adoptarea unui cadru legal adecvat activităților de raportare de vulnerabilități;

- stimularea dezvoltării de comunități de securitate cibernetică, care să aibă ca participanți atât cercetătorii și producătorii/furnizorii de produse și servicii de securitate, cât și companiile și instituțiile publice care pot beneficia de ajutor în securizarea serviciilor, rețelelor și sistemelor informatice pe care le dețin sau le administrează.

În acest scop, Centrul Național de Răspuns la Incidente de Securitate Cibernetică a realizat următoarele demersuri:

- a instituit un proces de intermediere în raportarea vulnerabilităților, care să asigure încredere și un grad minim de protecție pentru părțile implicate;
- elaborează și publică ghiduri și informații utile pentru părțile interesate;
- oferă recunoaștere publică în cazurile în care părțile implicate își doresc acest lucru;
- sprijină și participă la evenimente de promovare a divulgării vulnerabilităților;
- participă la demersurile GFCE la nivel internațional de promovare a divulgării coordonate a vulnerabilităților.

Având în vedere caracterul complex al divulgării coordonate a vulnerabilităților și interesele conflictuale ale părților interesate implicate, există multiple provocări asociate cu dezvăluirea vulnerabilităților:

- raportorii se pot confrunta cu amenințări legale atunci când descoperă o vulnerabilitate (răspundere civilă, răspundere penală sau alte legi);
- pot apare conflicte între părțile interesate implicate, ducând la lipsa de încredere între părțile interesate;
- producătorii / furnizorii și organizațiile de utilizatori pot să nu aibă procese de raportare a vulnerabilităților, putând astfel acționa incorect;
- raportarea în spațiul public a vulnerabilităților descoperite poate introduce noi riscuri pentru organizații, cum ar fi daune de reputație sau litigii;
- utilizatorii ar putea vinde vulnerabilitățile identificate pe piețele negre, în vederea unor câștiguri financiare;
- comunitățile de utilizatori pot fi reticente în a aplica direct patch-urile furnizate pentru vulnerabilitățile raportate, lăsând astfel produsele software-ul nesigure. [9]

Încrederea și cooperarea sunt esențiale pentru divulgarea coordonată a vulnerabilităților cibernetice. În contextul necesității de a primi ajutorul publicului pentru menținerea securității cibernetice, un prim pas pe care toate organizațiile și instituțiile îl pot face este cooperarea prin mecanisme de raportare coordonată și responsabilă a vulnerabilităților sistemelor și serviciilor informatice.

Guvernele au un rol de facilitare în introducerea și punerea în aplicare a unei politici privind divulgarea coordonată a vulnerabilităților. Astfel, ar fi necesară:

- stabilirea unei terțe părți de încredere, ca de exemplu un CSIRT;
- implementarea unui mecanism de armonizare internațională a divulgării coordonate a vulnerabilității și a legislațiilor relevante;
- stimularea unei culturi mai deschise în care vulnerabilitățile sunt acceptate și recunoscute;
- stimularea platformelor on-line de partajare a informațiilor;
- implicarea comunității cercetătorilor de securitate;
- sprijinirea sectorului juridic în identificarea posibilităților și reducerea riscurilor în ceea ce privește divulgarea coordonată responsabilă;
- includerea divulgării coordonate a vulnerabilităților în cerințele de achiziții publice.

Interesul pentru dezvoltarea domeniului divulgării coordonate a vulnerabilităților este demonstrat de diversele programe și abordări în cadrul companiilor producătoare de software și corporațiilor din domeniu (Microsoft Security Response Center [51], Vendor Vulnerability

Reporting and Disclosure Policy – Cisco) [38] și în mediul academic - Software Engineering Institute - Carnegie Mellon University. [2]

3.4. Concluzii

Cooperarea internațională joacă un rol-cheie în acest domeniu, deoarece provocările privind securitatea cibernetică depășesc granițele, extinzându-se până la nivelul sistemelor interconectate la nivel global. Amenințările și vulnerabilitățile cibernetice continuă să evolueze și să se intensifice, ceea ce va necesita o cooperare continuă, mai strânsă, în special în ceea ce privește gestionarea incidentelor de securitate cibernetică transfrontaliere de mare amploare. Colaborarea cu entități europene și internaționale este absolut necesară, fie că este vorba de unități de învățământ, centre de cercetare, companii private sau instituții guvernamentale.

Cooperarea operațională și gestionarea crizelor în domeniul cibernetic ar trebui să se bazeze pe consolidarea capabilităților operaționale de prevenire existente, în special prin modernizarea exercițiilor paneuropene de securitate cibernetică. [46] Este necesară instituirea unei cooperări structurate cu ENISA, CERT-EU, Centrul European de Combatere a Criminalității Informatice (EC3) și cu alte organisme relevante ale U.E.

Cooperarea dintre instituții, organizații și comunitatea de securitate cibernetică poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilităților. O politică eficientă de divulgare coordonată a vulnerabilităților poate minimiza șansele ca actorii rău-intenționați să profite de vulnerabilitățile informatice, construi încrederea clienților în ceea ce privește securitatea datelor acestora, aduce informații suplimentare despre noi vulnerabilități relevante și contribui la sporirea nivelului de securitate cibernetică.

Adoptarea unor politici publice unitare la nivelul statelor membre privind divulgarea coordonată a vulnerabilităților și a unor mecanisme coordonate de acțiune / cooperare trans-sectoriale vor asigura ecosistemul necesar asigurării securității în spațiul comunitar.

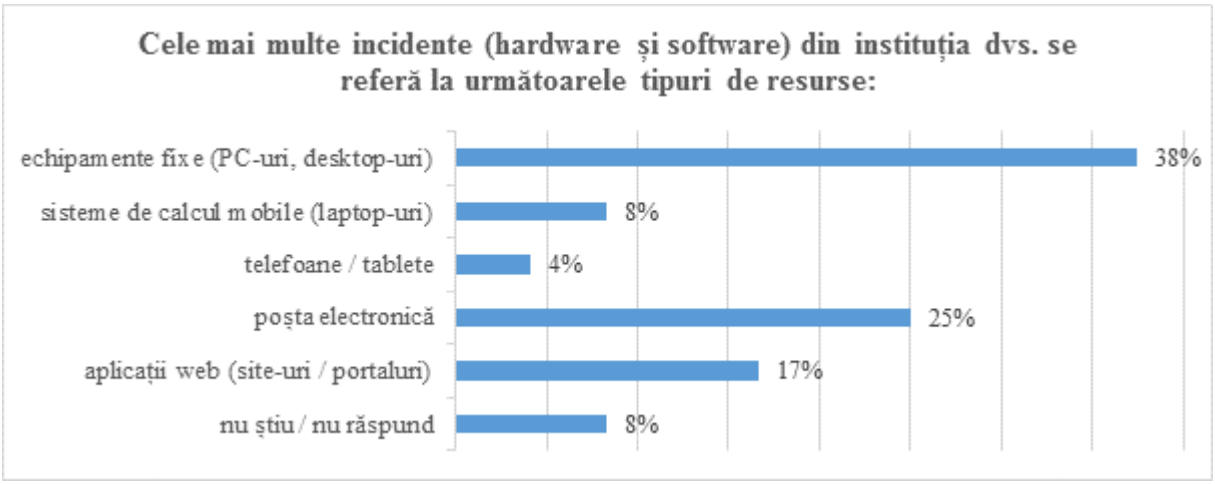
CAPITOLUL IV

RECOMANDĂRI PRIVIND DEZVOLTAREA CULTURII DE SECURITATE CIBERNETICĂ LA NIVEL NAȚIONAL ÎN ACTUALUL CONTEXT EUROPEAN

4.1. Bune practici pentru prevenirea și limitarea efectelor atacurilor cibernetice la nivelul instituțiilor publice din România

Mediul Internet, prin resursele sale hardware și software, este folosit pentru desfășurarea activității și transferul de informații între toate entitățile, de la companii, organizații și agenții guvernamentale până la utilizatorii finali. Potențial vulnerabile la atacuri cibernetice nu sunt doar mediul fizic - echipamente mobile, sisteme informatice, smartphone-uri etc. - ci și cel logic - sisteme de operare, aplicații, poșta electronică, transferurile de informații între companii sau operațiile în cloud.

Conform sondajului realizat în cadrul acestui studiu, cele mai multe incidente (hardware și software) din instituțiile publice din România se referă la echipamentele fixe (38%), urmate de poșta electronică (25%) și aplicațiile Web (17%).



Figură 14. Chestionar privind incidentele (hardware și software) întâlnite în cadrul instituțiilor publice din România

Aceste atacuri au crescut exponențial în ceea ce privește atât volumul, cât și gradul de complexitate, conducând la un risc sporit, la costuri suplimentare și pierderi potențiale pentru companii. Instituțiile care operează în special pe piețele financiare și de capital sunt ținte atractive datorită nivelului tranzacțiilor lor financiare și sensibilității datelor vehiculate, cum ar fi informații despre clienți (actuali și potențiali), baze de date (inclusiv informații din istoricul acestora), planul de afaceri și strategiile / investițiile confidențiale, proprietatea intelectuală (de exemplu algoritmi de tranzacționare), portofoliul clienților sau lista de utilizatori și parole.

Progresele în tehnologie au simplificat procesele și procedurile și au permis instituțiilor să adopte noi instrumente care să le permită extinderea mijloacelor de comunicare și să structureze și să pună în aplicare servicii cu viteză crescută și flexibile. Pe de altă parte, utilizarea în creștere a unor astfel de instrumente crește riscul atacurilor cibernetice, ale căror scopuri sunt în principal:

- afectarea funcționării (perturbarea, blocarea), distrugerea sau controlul ilegal al unui sistem de calcul sau infrastructură informațională;
- amenințarea confidențialității, integrității și disponibilității datelor și/sau sistemelor informatice ale instituțiilor;
- afectarea autenticității și non-repudierii datelor sau sustragerea informațiilor cu acces restricționat.

Aceste atacuri sunt efectuate de mai multe tipuri de agenți (organizații criminale, atacatori individuali, autorități guvernamentale, teroriști, angajați nemulțumiți, concurenți etc.) din diverse motive, cele mai importante fiind:

- câștiguri financiare;
- furtul, manipularea sau modificarea informațiilor;
- obținerea unor avantaje competitive și informații confidențiale de la concurenți;
- sabotarea instituției vizate sau expunerea unor date în scopuri de răzbunare;
- promovarea ideilor politice și/sau sociale;
- practicarea terorii, propagarea panicii și a haosului;
- răspunsul la provocări și/sau să stârnească admirația unor hackeri celebri.

Hackerii au la dispoziție mai multe mijloace de atac, dintre care cele mai frecvente sunt enumerate mai jos:

- *programe malware* - instalarea unor programe rău intenționate, concepute să perturbe funcționarea sistemelor de calcul și a rețelelor;
- *ingineria socială* - metodă de manipulare menită să obțină informații confidențiale, cum ar fi parole, date personale și informații ale cardurilor bancare;
- *atacurile DDoS* - concepute pentru a bloca sau întârzia accesul la serviciile sau sistemele unei organizații;
- *botnets* - atacul vine de la o rețea sau un număr mare de computere infectate, utilizate pentru a trimite spam sau viruși sau pentru a inunda rețeaua cu mesaje, ducând la blocarea serviciului;
- *Advanced Persistent Threats (APT)* - atacuri cibernetice sofisticate ce folosesc cunoștințe și instrumente pentru detectarea și exploatarea deficiențelor specifice unei tehnologii.

Orice organizație poate deveni victima unui atac cibernetic. Amenințările cibernetice variază în funcție de natura, vulnerabilitățile și informațiile sau bunurile fiecărei organizații. Consecințele lor pot fi semnificative în ceea ce privește imaginea organizației, daunele financiare sau pierderea avantajului competitiv, în timp ce amploarea impactului depinde de detectarea rapidă și răspunsul după ce atacul a fost identificat.

Câteva dintre cele mai bune practici de securitate cibernetică pentru instituțiile publice din România sunt enumerate în continuare. Aceste bune practici au drept scop stabilirea și menținerea unei conștientizări robuste și bine implementate privind securitatea cibernetică și asigurarea că utilizatorii finali sunt conștienți de importanța protejării informațiilor sensibile și de riscurile de gestionare greșită a informațiilor.

1. Monitorizarea aplicațiilor care au acces la date

Aplicațiile Web oferă unei organizații instrumentele necesare pentru a funcționa și a fi productivă, dar pot pune în pericol datele sensibile. Protejarea informațiilor critice implică, de obicei, instalarea programelor tip firewall și construirea infrastructurii în jurul datelor care trebuie protejate. Configurarea programelor firewall trebuie făcută cu atenție, drepturile de acces fiind acordate doar aplicațiilor îndreptățite să citească sau scrie date confidențiale.

2. Crearea unor controale specifice de acces

Prin crearea unor controale specifice de acces pentru toți utilizatorii se poate limita accesul doar la sistemele de care au nevoie pentru sarcinile de serviciu, limitându-se astfel expunerea datelor sensibile.

3. Colectarea jurnalelor (log-urilor) detaliate

Pentru o înregistrare completă a ceea ce se întâmplă în sistemele din rețeaua companiei - atât pentru asigurarea securității, cât și în scopuri de depanare - trebuie colectate log-uri detaliate și rapoarte complete. Acest lucru este valabil în special pentru aplicațiile care nu au înregistrări interne, astfel încât eventualele breșe de securitate create de aceste aplicații să poată fi identificate și remediate.

4. Actualizarea patch-urilor de securitate

Infractorii cibernetici inventează în mod constant noi tehnici de atac și caută noi vulnerabilități. De aceea, pentru a proteja rețeaua de calculatoare, trebuie instalate cele mai noi semnături sau patch-uri anti-malware.

5. Evitarea ingineriei sociale

Securitatea implementată la nivel tehnic poate fi compromisă de eroarea umană. Tehnica ingineriei sociale a fost utilizată cu succes de zeci de ani pentru a obține informații de conectare și acces la fișiere criptate. Încercările de acest gen pot apărea prin intermediul telefonului, e-mail-ului sau prin alte tipuri de comunicări cu utilizatorii.

6. Educarea și instruirea utilizatorilor

Utilizatorii sunt de obicei veriga cea mai slabă în ceea ce privește asigurarea securității informațiilor, iar acest risc poate fi limitat prin educarea lor permanentă cu privire la cele mai bune practici de securitate cibernetică. Instruirea ar trebui să includă modul de recunoaștere a unui e-mail tip phishing, de creare a parolelor puternice și de evitare a aplicațiilor periculoase, păstrarea informațiilor în interiorul companiei și orice alte riscuri corelate cu securitatea cibernetică.

7. Definirea clară a politicilor de utilizare pentru noii angajați

Pentru a întări și a clarifica educația acordată utilizatorilor, la angajare ar trebui evidențiate în mod clar cerințele și așteptările pe care compania le are în ceea ce privește securitatea IT (contractele de muncă trebuie să prevadă secțiuni care definesc în mod clar aceste cerințe de securitate).

8. Monitorizarea activității utilizatorilor

În timp ce utilizatorii bine pregătiți reprezintă prima linie de securitate, este nevoie de tehnologie ca ultima linie de apărare. Prin monitorizarea activității utilizatorilor se verifică dacă acțiunile lor respectă bunele practici de securitate. Orice activitate suspectă - de exemplu încercarea unui utilizator rău intenționat din exteriorul companiei de a obține acces la datele de conectare sau dacă un utilizator din interior alege să profite de drepturile de acces la sistem - va fi

imediat evidențiată și se vor putea lua măsurile necesare. Cum cele mai multe vulnerabilități apar din cauza factorului uman, o astfel de monitorizare a activității utilizatorilor este foarte importantă.

9. Crearea unui plan de răspuns la breșe de securitate

Indiferent de cât de bine sunt respectate aceste bune practici, incidentele de securitate sunt iminente și inevitabile. De aceea, existența unui plan de răspuns la atacuri cibernetice va permite eliminarea tuturor vulnerabilităților și limitarea pagubelor pe care un atac cibernetic le poate avea.

10. Respectarea standardelor

Dincolo de aceste bune practici, care reprezintă o îndrumare utilă pentru menținerea în siguranță a activității organizației, există standarde (PCI DSS - Payment Card Industry Data Security Standard, seria ISO/IEC 27k etc.) care reglementează aspecte ce țin de securitatea organizației.

4.2. Importanța educației și a cercetării în domeniul securității cibernetice

Satisfacerea cererii tot mai mari de forță de muncă calificată în domeniul tehnologiei informației și securității cibernetice necesită extinderea oportunităților educaționale, creșterea numărului de cadre didactice calificate, oferirea de oportunități de formare pe întregul parcurs al carierei profesionale și alinierea planurilor educaționale cu evoluțiile tehnologiei și cunoștințele avansate în domeniul IT&C și al securității informatice. Planurile de formare în domeniul educației digitale și al forței de muncă ar trebui să fie actuale, diversificate și să includă aspecte cât mai cuprinzătoare.

Programe academice în domeniul securității cibernetice

În zona educației universitare au fost identificate programele de Master desfășurate în universități care fac parte din clasamentul întocmit în anul 2016 de Ministerul Educației Naționale pentru a identifica nivelul de vizibilitate al universităților românești în clasamentele internaționale relevante. Astfel, „Exercițiul Național de Metaranking Universitar-2016” [32] sintetizează universitățile (în număr de 20, toate de stat) care au reușit să treacă un prag minimal al vizibilității în clasamentele internaționale ale universităților bazate dominant pe criterii/indicatori academici.

Tabelul următor prezintă programele de Master ce abordează tematica securității cibernetice, în ordinea descrescătoare a pozițiilor universităților în acest clasament. Cele 6 programe de Master identificate se desfășoară în universități din categoria „Universități românești cu potențial de excelență, vizibile și cu impact internațional” (primele 4 universități, în ordinea din clasament: Universitatea din București, Universitatea Politehnica din București, Universitatea „Alexandru Ioan Cuza” din Iași și Universitatea de Vest din Timișoara), respectiv „Universități românești vizibile internațional” (Universitatea Tehnică din Cluj-Napoca și Academia de Studii Economice din București).

Tabel 9. Programe de Master în domeniul securității cibernetice

Program Master	Universitatea	Facultatea	Limba
Securitate și logică aplicată	Universitatea din București	Facultatea Matematică și Informatică	RO
Advanced Cyber Security	Universitatea Politehnica din București	Facultatea de Automatică și Calculatoare	EN
Securitatea informației	Universitatea „Alexandru Ioan Cuza” din Iași	Facultatea de Informatică	RO
Studii de securitate globală	Universitatea de Vest din Timișoara	Facultatea de Științe Politice, Filosofie și Științe ale Comunicării	RO
Securitatea informațiilor și sistemelor de calcul	Universitatea Tehnică din Cluj-Napoca	Facultatea de Automatică și Calculatoare	RO
Securitatea informatică	Academia de Studii Economice din București	Facultatea de Cibernetică, Statistică și Informatică Economică	RO

În domeniul academic militar au fost identificate două programe de Master în problematica securității cibernetice: „Securitatea Tehnologiei Informației” desfășurat la Academia Tehnică Militară din București și „Conducere comunicații, tehnologia informației și apărare cibernetică” de la Facultatea de Securitate și Apărare, Universitatea Națională de Apărare „Carol I” București.

În planurile de învățământ ale multor programe de Master inter-disciplinare au fost identificate cursuri în domeniile: securitate la nivel hardware (sisteme de calcul, rețele de calculatoare) sau software (aplicații, protocoale, arhitecturi, tehnologii Web), telecomunicații, siguranța în funcționare a sistemelor critice, baze de date, audit de securitate sau managementul serviciilor. În continuare enumerăm programe reprezentative de Master inter-disciplinar desfășurate la universități cu vizibilitate internațională:

- „Sisteme distribuite în Internet” (Universitatea Babeș-Bolyai din Cluj-Napoca, Facultatea de Matematică și Informatică);
- „Tehnologii multimedia în aplicații de biometrie și securitatea informației”, „Ingineria calității și siguranței în funcționare în electronică și telecomunicații” (Universitatea Politehnica din București, Facultatea de Electronică, Telecomunicații și Tehnologia Informației);
- „Sisteme distribuite și tehnologii web” (Universitatea Tehnică Gheorghe Asachi din Iași, Facultatea de Automatică și Calculatoare);
- „Tehnologii Informatice” (Universitatea Politehnica din Timișoara, Facultatea de Automatică și Calculatoare);
- „Tehnologii moderne în ingineria sistemelor soft” (Universitatea Transilvania din Brașov, Facultatea de Matematică și Informatică).

Programe educaționale în securitate informatică la nivelul învățământului pre-universitar

Accesul la tehnologie și la comunicațiile online a devenit extrem de facil, însă este în același timp un subiect deosebit de fragil dacă ne referim la vârsta din ce în ce mai mică la care utilizatorii accesează sisteme de calcul conectate online sau echipamente de telecomunicații mobile.

Avantajele indiscutabile aduse de tehnologia actuală trebuie completate cu programe de educație pentru ca fiecare utilizator să cunoască potențialele pericole la care se expune atunci când se află în mediul online și să se poată proteja de posibile atacuri cibernetice.

Este absolut necesar ca programele de învățământ, începând chiar cu ciclul primar, să cuprindă cursuri de securitate cibernetică prin care elevii să învețe să evite capcane întâlnite la tot pasul în poșta electronică sau în platformele de socializare (adrese Internet suspecte, jocuri periculoase sau divulgarea unor date personale). Dezvoltarea unor programe educaționale în securitate cibernetică trebuie să înceapă de la o vârstă rezonabilă în etapa de formare a unui tânăr utilizator, efectul pe termen lung fiind doar unul benefic.

Programe post-universitare și „lifelong learning"

Educația, învățarea și instruirea profesională pe tot parcursul vieții reprezintă nu doar obiectivele unui program propus la nivelul Uniunii Europene, ci scopuri în sine, care îmbunătățesc experiența personală a fiecăruia dintre noi. Prin programul Lifelong Learning (2007 - 2013) inițiat de Parlamentul Uniunii Europene au avut loc schimburi de persoane (elevi, studenți, cadre didactice), conexiuni între instituții și colaborări la nivelul statelor din Uniunea Europeană și Spațiul Economic European în diverse domenii educaționale, pentru toate vârstele și la toate nivelurile profesionale.

Printre cursurile de inițiere sau de specializare în diverse domenii ale tehnologiei informației amintim:

- UTI Academy: cursuri dedicate specialiștilor în IT, implicați în securitatea sistemelor informatice, criminalistică informatică și răspuns la incidente, auditarea securității sistemelor informatice, monitorizarea și detectarea incidentelor de securitate în sistemele informatice și rețele;
- Crystal Mind Academy, InfoAcademy, Telecom Academy, Academia Credis, BIT Academy: cursuri de rețelistică, programare Web, sisteme de operare, baze de date și securitate cibernetică.

Activitatea organizațiilor non-guvernamentale în domeniul securității cibernetice

Activitatea organizațiilor non-guvernamentale constă în participarea sau organizarea unor evenimente corelate domeniului securității cibernetice. Prin implicarea activă în promovarea tehnologiilor, exprimarea publică a punctului de vedere în modificarea legislației și luările de poziție în cadrul unor evenimente, organizațiile non-guvernamentale au un rol bine determinat și contribuie la diseminarea celor mai noi aspecte privind securitatea cibernetică. Printre principalele organizații non-guvernamentale în domeniul securității cibernetice, enumerăm:

- Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI);
- Asociația Română pentru Asigurarea Securității Informației (ARASEC);
- Asociația pentru Dezvoltarea Societății Informaționale (ADSI).

Publicații în domeniul securității cibernetice

Aceste publicații, științifice sau informative, au rolul de a promova în mediul tipărit, dar în special în mediul online, cele mai noi tendințe din sfera securității cibernetice. Principalele publicații identificate în mediul Internet, ce au ca principal obiectiv diseminarea informațiilor privind securitatea informațiilor, sunt:

- „Intelligence" - editată de Serviciul Român de Informații;
- „Infosfera" - editată de Direcția Generală de Informații a Apărării, Ministerul Apărării Naționale;
- „International Journal of Information Security and Cybercrime" - editată de Asociația Română pentru Asigurarea Securității Informației;
- „Cybersecurity Trends" - editată de Agora Group împreună cu Swiss WebAcademy;
- „Revista Română de Studii de Intelligence" - editată de Academia Națională de Informații „Mihai Viteazul" prin Institutul Național de Studii de Intelligence.

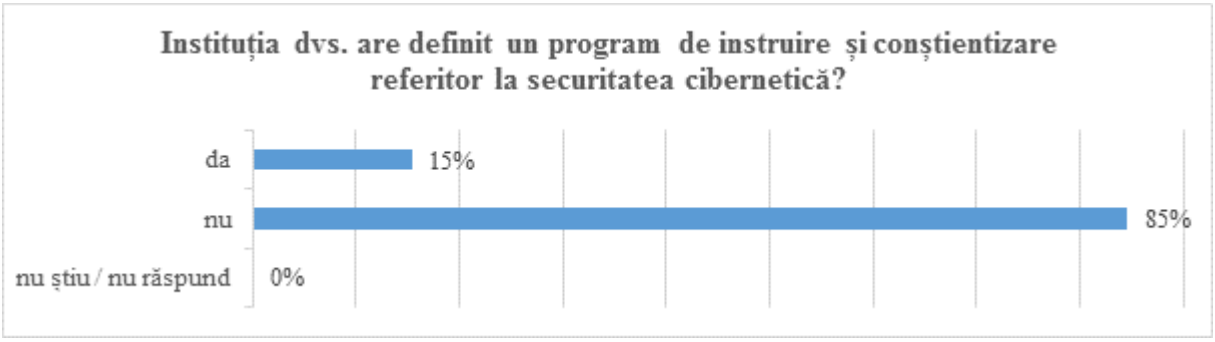
Platforme Web pentru promovarea și conștientizarea securității cibernetice

Portalurile dedicate subiectului securității cibernetice contribuie la promovarea activităților și evenimentelor publice specifice: workshop-uri, conferințe științifice, hackathon-uri și publicații. De asemenea, sunt publicate cele mai recente informații din domeniu (cele mai noi tipuri de atacuri cibernetice, produse și servicii concepute pentru protejarea utilizatorilor sau la nivel business). Rolul acestor portaluri în conștientizarea securității cibernetice este unul activ și deosebit de important, fiind o cale de diseminare a informațiilor către utilizatorii obișnuiți, dar și către companii, organizații și instituții ale statului.

Cu o activitate susținută în peisajul online, se pot menționa următoarele portaluri în domeniul securității și criminalității informatice:

- www.securitatea-informatiilor.ro;
- www.securitatea-cibernetica.ro;
- www.criminalitatea-informatica.ro;
- www.criminalitate.info;
- www.cyberm.ro.

Conștientizarea amenințărilor și a riscurilor prezente în mediul online joacă un rol foarte important în creșterea culturii de securitate cibernetică. Conform sondajului realizat în cadrul acestui studiu, 85% dintre respondenți au precizat că instituțiile în care lucrează nu au definit un program de instruire și conștientizare referitor la securitatea cibernetică.



Figură 15. Chestionar privind definirea unui program de instruire și conștientizare referitor la securitatea cibernetică în cadrul instituțiilor publice din România

Evenimente publice pe subiecte corelate domeniului securității cibernetice

Organizatorii acestor evenimente desfășurate periodic în România provin atât din mediul business sau guvernamental, cât și din lumea academică, financiar-bancară sau a organizațiilor non-profit.

Octombrie 2017 a fost *Luna europeană a securității cibernetice*, campanie organizată de ENISA în parteneriat cu Comisia și cu statele membre, aflată la a 5-a ediție. [30] Numeroase evenimente (conferințe, ateliere, sesiuni de formare, reuniuni la nivel înalt, prezentări generale destinate utilizatorilor, campanii online) au avut loc pe parcursul celor 4 teme săptămânale abordate de ediția din acest an:

- securitatea cibernetică la locul de muncă;
- guvernanță, viață privată și protecția datelor;
- securitatea cibernetică la domiciliu;
- competențe în materie de securitate cibernetică.

În România, *Luna europeană a securității cibernetice* a fost marcată de mai multe evenimente, cele mai reprezentative fiind organizate de CERT-RO (*New Global Challenges in Cyber Security*), OWASP (*OWASP Bucharest AppSec Conference*), Concord Communication (*GDPR 2018*), Institutul Bancar Român și certSIGN (*CyberThreats & CyberSecurity Day*) sau CCSIR (*DefCamp 8*). Centrul Național Cyberint a fost implicat în derularea și organizarea de exerciții cibernetice la care au participat numeroase instituții publice, dar și private. Tot Cyberint s-a ocupat și de pregătirea echipei de tineri care participă la *Campionatul European de Securitate Cibernetică*.

Activitatea de cercetare-dezvoltare în cadrul companiilor

Furnizorii de servicii Internet și companiile care activează în domeniul securității datelor investesc permanent în dezvoltarea echipamentelor și a serviciilor în conformitate cu evoluția dinamică a pieței de profil. Astfel, la forumul *We Love Digital* desfășurat în perioada 4 - 5 aprilie 2017 în București, directorul general al Institutului Național de Cercetare-Dezvoltare în Informatică - ICI București, a afirmat intenția institutului de creare a unui centru de cercetare în securitate cibernetică și cooptarea a 6 cercetători în acest domeniu: „În ultima ședință de CA de luna trecută am reușit să demarăm eforturile de a atrage investiții de 5 milioane de dolari prin care ICI, în afară de partea de echipamente și de traineri, să poată să aibă în clădirea unde este cloud-ul, la etajul al doilea, un centru de cyber-security pentru toți cei care activează în zona asta”. [17]

Compania Bitdefender, cel mai valoros brand de tehnologie al României și locul 7 în clasamentul general al celor mai valoroase branduri românești (conform raportului Brand Finance România 50 publicat în august 2017) [50] investește în cercetare și dezvoltare, jumătate dintre cei peste 1 300 de angajați lucrând în centrele R&D din București, Cluj-Napoca, Iași și Timișoara. Este o certitudine faptul că prin parteneriate public-private între universități și companii sunt stimulate atât educația și cercetarea, cât și integrarea mult mai bună a absolvenților în piața muncii. În zona academică, Bitdefender a contribuit la dezvoltarea unor programe de Master în domeniul securității cibernetice la Universitatea Tehnică din Cluj-Napoca și la Universitatea Alexandru Ioan Cuza din Iași, iar începând cu anul universitar 2017 - 2018 a susținut conceperea noului program de Master „Securitate și logică aplicată" la Facultatea Matematică și informatică din cadrul Universității din București. [4]

Sondajul „Security in the Digital World" realizat în perioada martie - aprilie 2017 de PwC și Microsoft România confirmă tendința companiilor de creștere a bugetului alocat investițiilor în securitate cibernetică, impulsionate mai degrabă de reglementările impuse și de creșterea numărului de atacuri cibernetice și mai puțin de conștientizarea amenințărilor cibernetice. [8]

Un alt aspect constă în faptul că organizațiile din România utilizează în general resursele interne, de obicei limitate, în locul unor furnizori specializați de servicii de securitate cibernetică, lucru specific organizațiilor mature din economiile dezvoltate. Luând în considerare această opțiune, organizațiile din România au la dispoziție fie varianta investițiilor în educație (creșterea nivelului de conștientizare în rândul angajaților în privința amenințărilor informatice, inclusiv prin programe de training) și cercetare (pentru formarea și dezvoltarea propriei divizii de securitate cibernetică), fie varianta utilizării serviciilor de cloud.

Studiul citat a mai reliefat faptul că, pentru a îmbunătăți securitatea cibernetică, alți factori importanți ar fi angajarea unor resurse suplimentare (ceea ce denotă o lipsă de personal specializat) sau schimbul de informații și bune practici cu alți parteneri de afaceri (se pot folosi lecțiile învățate și experiența altor organizații). Sunt necesare cercetări finanțate de guvern și coordonarea sectoarelor public și privat, în special în domeniul extinderii noilor arhitecturi de rețele și sisteme de calcul securizate, calcul de înaltă performanță, criptare, integritatea datelor, inteligență artificială, big data, confidențialitate și strategii de management al riscului.

4.3. Politici publice de securitate cibernetică

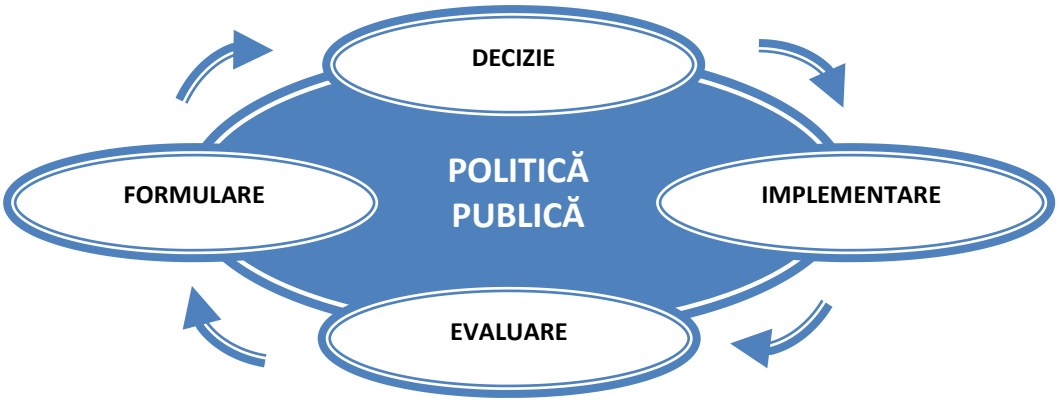
În contextul societății actuale aflate într-o continuă schimbare, a comunicațiilor globale, a conexiunilor accesibile și de mare viteză disponibile pentru diverse categorii de utilizatori și ținând cont de dezvoltarea fără precedent a programelor și aplicațiilor software, securitatea informației a devenit o preocupare majoră.

Actul decizional managerial modern necesită acces la volume mari de informații și un mod de lucru distribuit. Nevoia utilizării și exploatării facilităților oferite de rețelele de comunicații a impus domeniul securității și protecției informațiilor ca o cerință de bază pentru orice sistem, aplicație sau serviciu. Transmiterea datelor între un emițător și un destinatar folosind rețeaua Internet poate tranzita mai multe rețele de comunicații, oferind utilizatorilor din rețelele prin care sunt tranzitate datele posibilitatea de a le intercepta și/sau modifica. De asemenea, printr-un acces neautorizat la resursele sistemului, utilizatori din aceeași rețea cu emițătorul și/sau destinatarul pot modifica și/sau distruge datele și informațiile.

Nevoia de securitate pleacă de la realitatea conform căreia niciun sistem informatic nu poate fi complet securizat, singura modalitate de asigurare a securității fiind reprezentată de dezvoltarea și implementarea unor modele complexe de protecție care fac dificilă, pentru majoritatea utilizatorilor, compromiterea sistemului. Pentru o organizație, din punct de vedere operațional, asigurarea unui mediu securizat prin utilizarea sistemelor informatice reprezintă cerințe obligatorii

ale societății actuale, devenind practic o preocupare intensă și continuă în raport cu riscurile și amenințările posibile.

Fundamentul asigurării securității informației constă în dezvoltarea unor planuri, norme, politici de protecție și acțiune în cazul unor acțiuni care au ca scop compromiterea informațiilor și datelor. Asigurarea securității cibernetice devine un domeniu complex care necesită implicarea pe mai multe niveluri de mecanisme ce pot fi cuprinse la nivelul administrației în politici publice.



Figură 16. Etapele de dezvoltare a unei politici publice

Politicile publice reprezintă „o rețea de decizii legate între ele privind alegerea obiectivelor, a mijloacelor și a resurselor alocate pentru atingerea lor în situații specifice”. [1] Astfel, politicile publice pot fi considerate ca un model aplicat de rezolvare a problemelor la nivelul administrației publice în domeniul securității cibernetice.

Formularea politicilor publice în domeniul securității cibernetice trebuie să aibă la bază o serie de principii, cum ar fi:

- stabilirea unor responsabilități clare referitoare la definirea de strategii și reglementare, coordonare și implementare în vederea fundamentării și coordonării deciziilor strategice;
- promovarea unui ecosistem sigur și de încredere pentru domeniul .ro; [11]
- realizarea unui cadru legal prin care un furnizor de servicii / coduri sursă este obligat contractual să respecte o serie de standarde și norme privind securitatea cibernetică;
- măsuri operaționale privind stabilirea unui plan de răspuns la incidente, facilități de backup și de continuare a activității, precum și testarea periodică împotriva vulnerabilităților.

Din perspectiva particularităților domeniului securității cibernetice, politicile publice prezintă o serie de provocări pentru asigurarea unui mediu virtual sigur și de încredere, cum ar fi:

- realizarea unui studiu de impact la nivelul autorităților publice în vederea fundamentării nevoilor privind securitatea cibernetică pentru sistemele de comunicații și tehnologia informației ca infrastructuri de importanță deosebită;
- colectarea periodică de date (rapoarte, comunicări etc.) în vederea propunerii de noi mijloace / metode reactive și preventive în vederea reducerii la maxim a amenințărilor la adresa administrației;
- structurarea politicilor publice în domeniul securității cibernetice pe modele sectoriale pentru fiecare domeniu de activitate corespunzător instituțiilor din aparatul central al administrației publice din România;

- îmbunătățirea colaborării între autoritățile administrației publice și a cooperării cu diverse instituții europene și internaționale prin suport metodologic, transfer de expertiză și bune practici.

Un alt aspect care este necesar a fi avut în vedere este dat de componenta financiară a politicilor publice, acestea putând oferi și un cadru coerent și organizat în ceea ce privește costurile și investițiile în domeniul securității cibernetice la nivelul administrației. Lipsa unor previziuni bugetare care să asigure coordonarea dintre obiectivele asumate și fundamentarea deciziilor manageriale reprezintă elementul care de cele mai multe ori conduce la decizii de reducere a cheltuielilor alocate domeniului.

În funcție de sectorul de activitate și de cerințele specifice ale organizației, politicile publice în domeniul securității cibernetice este necesar a fi dezvoltate și aplicate începând de la nivelul decizional, care are misiunea de a autoriza, coordona și impune respectarea acestora, până la nivelul de execuție, responsabil cu implementarea politicilor.

Costurile asociate asigurării securității cibernetice diferă în funcție de particularitățile domeniului respectiv de activitate (complexitatea fluxurilor, dimensiunea sistemelor informatice, număr de utilizatori, public etc.), dar și de importanța și criticitatea infrastructurilor din sectorul respectiv.

Amenințările dinamice pentru sectoarele publice, privat și non-profit continuă să crească, cu potențialul de a provoca perturbări pe scară largă care pot afecta siguranța cetățenilor, dezvoltarea și stabilitatea economică sau securitatea națională. Cooperarea dintre sectorul public, privat și non-profit este necesar a fi reglementată prin înțelegeri / protocoale sectoriale care pot avea la bază politicile publice.

Adoptarea și dezvoltarea politicilor publice în domeniul securității cibernetice și al managementului operațional vor aduce o înțelegere mai bună a provocărilor din domeniu și vor oferi instrumentele necesare pentru a influența modelarea proceselor de management / gestionare a amenințărilor din spațiul cibernetic. De asemenea, oferă posibilitatea unei estimări corecte a eforturilor financiare necesare a fi realizate în vederea implementării măsurilor tehnice și non-tehnice din domeniul securității cibernetice.

4.4. Stabilirea parteneriatelor public-private

În spațiul cibernetic, fiecare este expus riscului de a fi atacat, indiferent dacă este vorba de un stat, o afacere sau un individ. Din ce în ce mai activi în cadrul rețelelor globale, hackerii folosesc așa-numitul fenomen de „salt” de la o rețea neprotejată și vulnerabilă spre alta, modificând astfel proprietarul și, de cele mai multe ori, inclusiv competența juridică. În final, aceste acțiuni permit atacatorilor să-și păstreze anonimatul, activitățile rău intenționate ale acestora fiind imposibil de identificat și respectiv sancționat.

Situația se complică prin faptul că, pe de o parte, niciun guvern, cu mici excepții, nu deține controlul asupra infrastructurii naționale de telecomunicații, iar, pe de altă parte, doar guvernul are autoritatea de a investiga pe deplin incidentele și securitatea cibernetică în scopul de a proteja interesele, drepturile și libertățile cetățenilor săi. Prin urmare, cooperarea dintre instituțiile de stat responsabile și proprietarii de infrastructură de telecomunicații este esențială pentru asigurarea securității cibernetice la nivel național. Succesul unei astfel de colaborări rezidă din identificarea de oferte valoroase , schimb bilateral de informații și sarcini clar definite, în special cu privire la rolul guvernului.

În general, guvernelor le revin o multitudine de funcții în vederea stabilirii proceselor necesare în direcția consolidării cooperării la nivel public și privat. Cu toate acestea, sarcina de bază rămâne definirea strategiei naționale și oferirea cadrului de politici care descrie arhitectura

prin care sunt construite și exploatate eforturile naționale. Ca urmare, guvernul are responsabilitatea de a participa, împreună cu toate părțile interesate, în eforturile de a identifica, analiza și atenua, în același timp, problemele identificate și riscurile majore ce le implică acestea. Guvernul joacă un rol cheie pe arena relațiilor internaționale și a securității cibernetice, în special prin crearea tratatelor referitoare la securitatea cibernetică și armonizarea legislației naționale.

Un rol deosebit în direcția fortificării relațiilor de cooperare revine echipelor naționale și guvernamentale de răspuns la incidente de securitate cibernetică (CSIRT-uri), care se confruntă direct cu problemele de securitate cibernetică. Ele se angajează în mod activ să gestioneze incidentele de securitate cibernetică, să colecteze și să analizeze informațiile cu privire la amenințările emergente și securitatea cibernetică și să acorde asistență clienților săi în vederea diminuării riscurilor existente.

Cooperarea internațională joacă un rol indispensabil în dezvoltarea parteneriatului național public-privat la nivel național. Protejarea spațiului virtual prezintă de fapt o responsabilitate partajată și care poate fi eficient realizată prin colaborarea dintre Guvern și sectorul privat, care de multe ori deține și operează o mare parte a infrastructurii. Pentru a asigura securitatea națională, guvernele trebuie să gestioneze securitatea cibernetică în colaborare cu sectorul privat, ținând cont de faptul că succesul colaborării implică o serie de condiții ce urmează a fi create, cum ar fi încrederea, beneficiile reale și înțelegerea clară a rolurilor reciproce.

În concluzie, este necesară conștientizarea faptului că, pentru a avea rezultate, fiecare actor contează și trebuie integrat în efortul general, chiar dacă a fost de exemplu doar victima unui incident de securitate care nu constituie infracțiune (caz în care statul nu are de ce să intervină).

Deschiderea canalelor de comunicare, crearea de grupuri de lucru și consultare publică, implicarea societății civile și parteneriatul public-privat devin direcții cheie pe care politicile publice trebuie să se axeze. Toate acestea în contextul în care, pe palier administrativ, se creează protocoale de colaborare și se instituie proceduri de lucru comune și de comunicare.

Comisia Europeană a lansat pe 5 iulie 2016 un nou parteneriat public-privat în domeniul securității cibernetice, care se așteaptă să genereze până în 2020 investiții de 1,8 miliarde EUR. Acesta se înscrie într-o serie de noi inițiative destinate să pregătească Europa pentru a face față mai bine atacurilor cibernetice și să consolideze competitivitatea sectorului securității cibernetice.

Conform unui sondaj efectuat de PwC, cel puțin 80% dintre societățile europene s-au confruntat în perioada 2015 - 2016 cu unul sau mai multe incidente din domeniul securității cibernetice, iar numărul incidentelor de securitate din toate sectoarele economice a crescut la nivel mondial cu 38% în 2015. Această situație afectează companiile europene, indiferent de dimensiune, și amenință să submineze încrederea în economia digitală. Ca parte a Strategiei sale privind piața unică digitală pentru Europa, Comisia dorește să consolideze cooperarea transfrontalieră între toate entitățile și toate sectoarele active în domeniul securității cibernetice și să contribuie la dezvoltarea unor tehnologii, produse și servicii inovatoare și sigure în întreaga UE.

Andrus Ansip, vicepreședinte pentru piața unică digitală, a declarat: „În absența încrederii și a securității, nu poate exista o piață unică digitală. Europa trebuie să fie gata să gestioneze atacuri cibernetice care sunt tot mai sofisticate și care nu țin cont de granițe. Astăzi propunem măsuri concrete pentru consolidarea rezistenței Europei la astfel de atacuri și pentru a asigura capacitatea necesară construirii și extinderii economiei noastre digitale." [6]

Günther H. Oettinger, comisar pentru economie digitală și societate digitală, a adăugat: „Europa are nevoie de produse și servicii de securitate cibernetică de calitate, abordabile și interoperabile. Posibilitatea de a concura pe piața globală a securității cibernetice, aflată în creștere rapidă, reprezintă o oportunitate majoră pentru sectorul de profil din UE. Facem apel la statele membre și la toate organismele din domeniul securității cibernetice să își consolideze cooperarea și să își pună în comun cunoștințele, informațiile și competențele de specialitate pentru a face să

crească reziliența cibernetică a Europei. Parteneriatul crucial în materie de securitate cibernetică semnat astăzi cu sectorul de profil reprezintă o evoluție majoră". [6]

Planul de acțiune include lansarea primului parteneriat public-privat european privind securitatea cibernetică. În cadrul programului său de cercetare și inovare Orizont 2020, UE a investit 160 milioane euro în proiecte privind securitatea cibernetică și intenționează să investească încă 450 milioane euro în perioada 2017 - 2020 într-un nou parteneriat public-privat (cPPP - Public-Private Partnership on Cybersecurity). Se preconizează că actorii de pe piața securității cibernetice, reprezentați de Organizația Europeană pentru Securitatea Cibernetică (ECSO - European Cyber Security Organisation), vor investi de trei ori mai mult. Acest parteneriat va include, de asemenea, membri din administrațiile publice, centrele de cercetare și instituțiile universitare naționale, regionale și locale. Obiectivele parteneriatului sunt stimularea cooperării în etapele inițiale ale procesului de cercetare și inovare și dezvoltarea unor soluții de securitate cibernetică pentru diverse sectoare, cum ar fi energia, sănătatea, transporturile și finanțele.

Comisia prezintă, de asemenea, diverse măsuri pentru a aborda fragmentarea pieței securității cibernetice din UE. În prezent, este posibil ca o firmă de TIC să fie nevoită să parcurgă proceduri de certificare diferite pentru a-și vinde produsele și serviciile în mai multe state membre. De aceea, Comisia va examina posibilitatea introducerii unui cadru de certificare la nivel european pentru produsele din domeniul TIC destinate securității.

O multitudine de IMM-uri europene inovatoare au apărut pe diverse piețe de nișă (de exemplu, în domeniul criptografiei), precum și sub formă de noi modele de afaceri pe piețe consacrate (cum ar fi cea a programelor antivirus), dar acestea nu reușesc să își extindă activitatea la o scară mai mare. Comisia dorește să faciliteze accesul la finanțare al întreprinderilor mici care activează în domeniul securității cibernetice și va explora diverse opțiuni în cadrul Planului de investiții al UE.

Prin Directiva privind securitatea rețelelor și a informațiilor se creează deja o rețea a echipelor de intervenție în caz de incidente de securitate cibernetică la nivelul întregii UE, în vederea asigurării unei reacții rapide la amenințările și incidentele cibernetice. Se instituie, de asemenea, un „grup de cooperare" între statele membre, destinat să sprijine și să faciliteze cooperarea strategică și schimbul de informații și să crească încrederea. Comisia face apel la statele membre să valorifice la maxim aceste noi mecanisme și să consolideze coordonarea în momentele și în situațiile în care acest lucru este posibil. Comisia va propune modalități de a consolida cooperarea transfrontalieră în cazul producerii unui incident cibernetic major. Având în vedere ritmul în care evoluează domeniul securității cibernetice, printre măsurile luate de Comisie se va număra și devansarea evaluării Agenției ENISA, prin care se va examina dacă mandatul și capacitățile ENISA sunt în continuare adecvate pentru îndeplinirea misiunii acestei instituții - sprijinirea eforturilor statelor membre ale UE de a-și consolida reziliența cibernetică. Comisia examinează, de asemenea, modalități de consolidare și optimizare a cooperării în materie de securitate cibernetică în diverse sectoare ale economiei, inclusiv în ceea ce privește formarea și educația în domeniul securității cibernetice.

4.5. Mecanisme de cooperare la nivel european

Deoarece statele membre nu pot acționa în mod izolat în fața unui atac informatic major, rețelele în colaborare cu partenerii internaționali sunt esențiale pentru combaterea amenințărilor globale. O industrie dinamică în securitatea cibernetică va contribui la creșterea României ca un centru în cercetare și educație în acest domeniu.

Importanța cooperării la nivel european și internațional este recunoscută de toți actorii implicați (administrație, militar, business), dar, datorită abordărilor naționale și incidentelor cu

care s-au confruntat, au fost convenite doar formal acorduri între state și puține parteneriate public-privat pentru schimbul de date / informații în domeniul securității cibernetice.

Dezvoltarea mecanismelor la nivel european între statele membre și la nivelul industriei de profil necesită adoptarea unor noi direcții care trebuie incluse în strategiile naționale:

- dezvoltarea unor noi modalități de consolidare a cooperării în domeniul securității cibernetice în diferite sectoare ale economiei, inclusiv în formarea profesională și educație prin gestionarea integrată a cunoștințelor, experienței, lecțiilor învățate;
- creșterea cooperării la nivel european: încurajarea utilizării mecanismelor de cooperare și îmbunătățirea modului în care colaborează pentru a se pregăti în cazul unui incident cibernetic (acestea includ dezvoltarea și desfășurarea unor activități privind educația sau formarea profesională și exerciții de securitate cibernetică);
- sprijinirea pieței unice emergente a produselor și serviciilor pentru securitatea cibernetică: dezvoltarea unui cadru de certificare a produselor și serviciilor relevante, adoptarea de măsuri privind creșterea investițiilor în securitatea cibernetică și de sprijinire a IMM-urilor active în domeniu;
- stabilirea unui parteneriat public-privat (PPP) cu industria pentru a stimula capacitățile industriale și inovarea în industria securității cibernetice;
- dezvoltarea unei abordări proactive a incidentelor, ca bază a sistemelor de avertizare timpurie la nivel național și internațional.

Partajarea informațiilor de securitate cibernetică cu partenerii internaționali dezvoltă o înțelegere puternică a amenințărilor colective și îmbunătățește capacitatea României de a preveni, detecta, analiza, răspunde, atenua și recupera în cazul unor amenințări și/sau incidente de securitate cibernetică. Construirea unor rețele de partajare a amenințărilor cibernetice la nivel internațional oferă unei țări și partenerilor acesteia posibilitatea de a rezista cu succes diverselor acțiuni rău-intenționate.

Echipele de răspuns la incidentele de securitate (CSIRT) și centrele de securitate cibernetică din întreaga lume lucrează pentru a proteja și a răspunde la incidentele care afectează infrastructurile și sistemele de interes național. Prin realizarea parteneriatelor se poate dezvolta o comunitate de încredere în care să fie difuzate indicatori de compromis și informații despre amenințări în mod automat, iar membrii acestor rețele de partajare a informațiilor de încredere să poată lua măsurile necesare.

În acest sens, pentru România este necesară realizarea de acorduri bilaterale și multilaterale, memorandum-uri de înțelegere, angajamente între autoritatea competentă și parteneri internaționali strategici din sectorul public, privat și mediul academic. România trebuie să devină lider regional în domeniul securității cibernetice prin Centrul de inovare în domeniul securității cibernetice, realizat în București cu ajutorul Agenției pentru Comerț și Dezvoltare din S.U.A. (USTDA), ca principal mecanism de cooperare la nivelul statelor din Sud-Estul Europei, în vederea consolidării mecanismelor de cooperare zonale.

Dezvoltarea unor capacități regionale de securitate cibernetică va permite:

- membrilor să împărtășească informații despre amenințările în domeniul securității cibernetice;
- oportunități pentru experții tehnici, de a împărtăși instrumente, tehnici și idei;
- să fie un factor de cooperare și colaborare, în special în cazul în care un incident de securitate cibernetică afectează regiunea.

Cooperarea regională va permite dezvoltarea unui sistem eficient de alertă timpurie și aplicarea de măsuri imediate de prevenție privind propagarea unei vulnerabilități.

CONCLUZII FINALE

Atacurile cibernetice au cunoscut o diversificare explozivă în ultima vreme, unele dintre acestea putând fi clasificate drept epidemii globale datorită vitezei mari de răspândire în mediul virtual. Amenințările specifice sistemelor informatice se caracterizează printr-o dinamică accentuată și printr-un caracter global, ceea ce le face dificil de identificat și de contracarat.

Deși există numeroase metode de protecție, din ce în ce mai performante, asigurarea securității informațiilor în mediul cibernetic nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană. De multe ori, incidentele de securitate sunt generate de o organizare necorespunzătoare a politicilor de securitate și mai puțin din cauza unei deficiențe a mecanismelor de securitate. În acest context, este necesară dezvoltarea unor strategii în materie de securitate cibernetică, prin definirea politicilor în acest sens, și a unor campanii de prevenire și combatere a fenomenului de criminalitate informatică la nivel național.

România se află într-un proces continuu de consolidare a securității cibernetice la nivel național, atât din punct de vedere legal, instituțional, cât și procedural, fiind întreprinse, în acest sens, eforturi susținute de către autoritățile cu responsabilități în domeniu.

Din punct de vedere al inițiativelor legislative în domeniul securității cibernetice, un prim pas făcut de România a fost ratificarea, la 15 mai 2004, a *Convenției Consiliului Europei privind criminalitatea informatică,* prin Legea nr. 64/2004. România s-a numărat printre primele state care au ratificat convenția adoptată la Budapesta, la 23 noiembrie 2001.

Guvernul României a aprobat *Strategia de securitate cibernetică a României*, prin Hotărârea nr. 271 din 15 mai 2013, având astfel o abordare comună la nivelul Uniunii Europene, pentru a putea oferi un răspuns prompt la atacurile din spațiul cibernetic. Scopul Strategiei de securitate cibernetică a României este de a defini și menține un spațiu cibernetic sigur, cu un înalt grad de reziliență și de încredere.

La 1 februarie 2014 au intrat în vigoare *Noul Cod Penal* și *Noul Cod de Procedură Penală,* care implementează standardele internaționale existente în domeniul criminalității informatice.

Ministerul Comunicațiilor și Societății Informaționale a lansat în dezbatere publică, în data de 3 octombrie 2017*, Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*. Acest proiect propune adoptarea unui set de norme menite să instituie un cadru național unitar de asigurare a securității cibernetice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale, în conformitate cu cerințele Directivei NIS. În privința autorității competente la nivel național, a punctului unic și a echipei CSIRT naționale, proiectul de lege propune dezvoltarea acestora în cadrul CERT-RO. Pentru definirea domeniului de aplicare, proiectul reglementează operatorii de servicii esențiale și definirea serviciilor esențiale, care vor avea obligativitatea raportării incidentelor cibernetice la CERT-RO.

În contextul implementării în plan național a Directivei NIS, prin Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, se pune problema dacă este necesară adoptarea unei noi strategii de securitate cibernetică, conform prevederilor Directivei, sau este suficientă actualizarea Strategiei de securitate cibernetică a României, prin includerea de obiective clare cu indicatori de monitorizare și evaluare a liniilor strategice din domeniu, definirea de responsabilități pentru instituțiile implicate în asigurarea securității, măsuri privind protecția datelor și proprietatea intelectuală. În vederea consolidării Strategiei de securitate cibernetică a României este necesară o abordare punctuală a indicatorilor, prin lărgirea bazei de colectare a datelor din domeniu și stabilirea unui parcurs în vederea atingerii obiectivelor.

Centrul Național de Răspuns la Incidente de Securitate Cibernetică a colectat și procesat în anul 2016, un număr de 110 194.890 alerte de securitate cibernetică, cu 61,56% mai multe față de anul 2015 și cu 154,89% mai multe față de anul 2013. Pe lângă numărul în creștere de alerte de securitate cibernetică, observăm că cele mai răspândite forme de malware în sistemele informatice din România au fost detectate acum mulți ani și, deși ar fi trebuit să fie eradicate, continuă să infecteze sistemele de operare neactualizate din România.

România este o țară generatoare de incidente de securitate cibernetică și cu rol de tranzit (proxy) pentru atacatori din afara spațiului național, conform rapoartelor anuale ale CERT-RO, însă a devenit în ultima vreme și o țintă a atacurilor cibernetice de tip APT, DDoS sau ransomware.

Regulamentul (UE) 2016/679 privind prelucrarea datelor cu caracter personal și libera circulație a acestor date, care va intra în vigoare începând cu 25 mai 2018, necesită desfășurarea unor acțiuni practice în instituțiile publice pentru sistemele și aplicațiile informatice pe care le dețin, prin realizarea unor modele de auditare și management al riscurilor asociate.

The Global Cybersecurity Index 2017 are ca model de abordare 5 piloni strategici privind securitatea cibernetică și anume: aspectele legale/juridice, tehnice, organizaționale, capabilități și cooperare. Din punct de vedere al index-ului de țară, pentru România se evidențiază necesitatea:

- actualizării cadrului normativ;
- dezvoltării/adoptării de standarde pentru organizații;
- adoptării de metrici de evaluare a stării de securitate;
- îmbunătățirii cadrului legislativ pentru formarea profesională, programe de cercetare și dezvoltare, startup-uri;
- stabilirii de acorduri bilaterale și multilaterale.

Multe dintre sistemele de apărare cibernetică folosite de operatorii de infrastructură critică din România sunt depășite și ineficiente pentru evitarea posibilelor atacuri. În lipsa unor măsuri adecvate și a unei coordonări a eforturilor privind securitatea infrastructurilor critice, aceste sisteme rămân extrem de vulnerabile, persoane neautorizate putând obține controlul asupra unor sisteme vitale pentru funcționarea unui stat. În acest sens, este absolut necesar ca domeniul infrastructurilor critice să fie periodic analizat, monitorizat, evaluat și optimizat, demarându-se un proces de identificare a infrastructurilor critice la nivelul administrației publice. Evoluția rapidă a domeniului și a diverselor componente sectoriale vitale necesită actualizarea strategiei naționale privind protecția infrastructurilor critice, în concordanță cu recomandările europene și internaționale în domeniu.

În contextul general al discuțiilor privind securitatea cibernetică, la nivel național este importantă separarea conceptuală a direcțiilor principale de acțiune: apărare cibernetică, criminalitate informatică, securitate națională, infrastructuri critice și situații de urgență, diplomație cibernetică internațională și guvernanța Internet-ului. Separarea nu reprezintă situația ideală, dar este o realitate, datorită complexității și diversității securității cibernetice în ansamblu. Este nevoie să se stabilească foarte clar rolurile și responsabilitățile fiecărei instituții naționale responsabile în parte.

Un domeniu ce poate fi de interes pe viitor, este dat de asigurările împotriva riscurilor cibernetice, care să acopere riscurile atacurilor care pot afecta serviciile și infrastructurile cibernetice. Existența unor breșe în securitatea cibernetică poate afecta instituțiile și companiile pe mai multe niveluri, atât din punct de vedere financiar, cât și reputațional. O asigurare împotriva riscurilor prezente în spațiul virtual ar putea proteja financiar împotriva pierderilor în cazul unor atacuri cibernetice.

Un alt segment ce necesită a fi dezvoltat este reprezentat de formarea profesională în domeniu și realizarea unor acțiuni de conștientizare/înțelegere a domeniului la nivelul factorilor decizionali din cadrul organizațiilor publice.

Cercetarea și educația în domeniul securității cibernetice trebuie să reprezinte priorități ale politicilor publice. Consolidarea cercetării în domeniul securității informatice, îmbunătățirea educației și dezvoltarea forței de muncă instruite sunt esențiale pentru atingerea obiectivelor generale ale politicii privind securitatea cibernetică. Politicile în cercetare și educație vor fi eficiente doar dacă includ natura multilaterală și multidisciplinară a securității cibernetice ca element fundamental și omniprezent în cultura, abordările, procesele, sistemele și infrastructurile tehnice.

Finanțarea cercetării și dezvoltării în domeniul securității informatice este indispensabilă pentru a aduce inovare și a dezvolta noi tehnologii. Accesul extins la educația privind securitatea cibernetică la toate nivelurile (pre-universitar, universitar și post-universitar) este necesar pentru pregătirea, construirea și îmbunătățirea forței de muncă. Numeroasele posibilități pentru universități, cadre didactice și studenți de la toate ciclurile de studii (licență, master, doctorat) de a se implica în cercetări de ultimă oră, de mare impact, sunt importante pentru dezvoltarea unei puternice comunități științifice.

Cooperarea internațională joacă un rol-cheie în acest domeniu, deoarece provocările privind securitatea cibernetică depășesc granițele, extinzându-se până la nivelul sistemelor interconectate la nivel global. Colaborarea cu entități europene și internaționale este absolut necesară, fie că este vorba de unități de învățământ, centre de cercetare, companii private sau instituții guvernamentale. Cooperarea dintre instituții, organizații și comunitatea de securitate cibernetică poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilităților.

Adoptarea unor politici publice unitare la nivelul statelor membre privind divulgarea coordonată a vulnerabilităților și a unor mecanisme coordonate de acțiune/cooperare trans-sectoriale vor asigura ecosistemul necesar asigurării securității în spațiul comunitar.

Deschiderea canalelor de comunicare, crearea de grupuri de lucru și consultare publică, implicarea societății civile și parteneriatul public-privat devin direcții cheie pe care politicile publice trebuie să se axeze.

Importanța domeniului securității cibernetice în contextul global al securității unui stat, este evidențiată de multitudinea de direcții de dezvoltare a domeniului. Evoluția tehnologică și automatizarea diverselor sectoare de activitate ale unei societăți, califică domeniul securității cibernetice ca fiind o dimensiune prioritară de acțiune în dezvoltarea strategiilor naționale de apărare a statelor.

Securitatea cibernetică necesită un cadru legislativ, adaptat atât la noile amenințări tehnologice, cât și la necesitatea de respectare a drepturilor civile, aliniate ca principii de bază în strategiile naționale de apărare ale statelor. Reglementările legislative existente, precum și gradul de operaționalizare al acestora la nivelul instituțiilor publice din România nu permit, în prezent, prevenirea și contracararea cu maximă eficiență a unor amenințări cibernetice de nivel mediu și ridicat.

Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice reglementează operatorii de servicii esențiale și furnizorii de servicii digitale, dar nu specifică reglementări privind persoanele juridice deținătoare de infrastructuri cibernetice. În perspectiva revizuirii Strategiei europene în domeniul securității cibernetice și a transpunerii Directivei NIS la nivel național, România va trebui să actualizeze cadrul normativ în domeniul securității cibernetice, prin revizuirea Strategiei pentru Securitate Cibernetică a României și dezbaterea unei noi legi pentru securitate cibernetică.

Actualizarea Strategiei de securitate cibernetică a României trebuie să includă obiective clare cu indicatori de monitorizare și evaluare a liniilor strategice din domeniu, definirea de

responsabilități pentru instituțiile implicate în asigurarea securității, măsuri privind protecția datelor și proprietatea intelectuală.

România va asuma în 2019, pentru o perioadă de șase luni, Președinția Consiliului Uniunii Europene, ceea ce presupune consolidarea unei viziuni naționale cu privire la viitorul Uniunii Europene. Piața Internă Digitală, cu importanta dimensiune a securității cibernetice, va reprezenta o prioritate a viitoarei Președinții a României la Consiliul Uniunii Europene. Astfel, consolidarea cadrului legislativ în domeniul securității cibernetice constituie o prioritate națională, pentru a putea fi asigurate condițiile optime de reacție rapidă la incidentele cibernetice.

Concluzionând, adoptarea unei legislații comprehensive și actualizate în domeniul securității cibernetice, care să sprijine dezvoltarea capacităților de apărare ale statului, reprezintă o prioritate națională. Asigurarea unui spațiu cibernetic sigur este responsabilitatea atât a statului, cât și a autorităților competente, a sectorului privat și a societății civile. Pentru dezvoltarea culturii de securitate cibernetică, cele mai importante pârghii sunt educația și cercetarea, parteneriatele public-private și mecanismele de cooperare la nivel european.

BIBLIOGRAFIE

[1] A. Miroiu, *Introducere în analiza politicilor publice*, Editura Punct, 2001.

[2] A.D. Householder, G. Wassermann, A. Manion, C. King, *The CERT Guide to Coordinated Vulnerability Disclosure*, August 2017, CMU/SEI-2017-SR-022.

[3] *Anexă la comunicarea Comisiei către Parlamentul European și Consiliu. Valorificarea la maximum a NIS - către punerea în aplicare eficace a Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, Consiliul Uniunii Europene, 14 septembrie 2017.

[4] *Bitdefender susține masterul de securitate cibernetică al Facultății de Matematică-Informatică din cadrul Universității din București*, 14 septembrie 2017, https://www.bitdefender.ro/news/bitdefender-sustine-masterul-de-securitate-cibernetica-al-facultatii-de-matematica-informatica-din-cadrul-universitatii-din-bucuresti-3358.html

[5] C. Jugastru, „Proceduri și autorități în noul drept european al protecției datelor cu caracter personal", Revista *Universul Juridic* nr. 6, iunie 2017, pp. 112-129.

[6] Comisia Europeană - *Comunicat de presă*, 5 iulie 2016, http://europa.eu/rapid/press-release_IP-16-2321_ro.htm

[7] *Comunicat de presă*, https://politiaromana.ro/ro/comunicate/politia-romana-si-bitdefender-contribuie-la-lupta-globala-impotriva-ransomware

[8] *Comunicat de presă*, https://www.pwc.ro/en/press_room/assets/2017/cybersecurity-report-ro.pdf

[9] *Coordinated Vulnerability Disclosure*, Global Forum on Cyber Expertise (GFCE), www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

[10] *CyberWISER - Cartography of EU cyber security strategies*, www.cyberwiser.eu/cartography

[11] D. Clark, T. Berson, and H.S. Lin, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work, 2014.

[12] *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, Jurnalul Oficial al Uniunii Europene*, 19 iulie 2016.

[13] *Directiva 2008/114/CE - identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora*.

[14] *Divulgarea Coordonată a Vulnerabilităților - componentă esențială a securității cibernetice*, CERT-RO, https://cert.ro/citeste/divulgarea-coordonat-a-vulnerabilit-ilor-component-esen-ial-a-securit-ii-cibernetice

[15] *Divulgarea Coordonată a Vulnerabilităților - CVD*, https://cert.ro/pagini/CVD

[16] E.M. Hutchins, M.J. Cloppert, R.M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin Corporation, 2010.

[17] ECONOMICA.net, http://www.economica.net/ici-vrea-sa-atraga-investitii-de-5-milioane-dolari-pentru-un-centru-de-cercetare-in-cyber-security_135842.html

[18] ENISA, „Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)", Version 1.0, 2006.

[19] *ENISA's Position on the NIS Directive*, ENISA, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-position-on-the-nis-directive

[20] G. Alexandru, G. Văduva, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare, București, 2006.
[21] *Ghid orientativ de aplicare a Regulamentului General privind Protecția Datelor destinat operatorilor*, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, http://www.dataprotection.ro
[22] *Hotărârea 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*, Guvernul României, Monitorul Oficial, Partea I nr. 296 din 23.05.2013, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf
[23] I.C. Mihai, G. Petrică, C. Ciuchi, L. Giurea, P*rovocări și strategii de securitate cibernetică*, Editura Sitech, 2015.
[24] I.C. Mihai, G. Petrică, *Securitatea informațiilor*. Ediția a II-a, îmbunătățită și adăugită, Editura Sitech, 2014.
[25] I.C. Mihai, L. Giurea, *Criminalitatea informatică*. Ediția a II-a, îmbunătățită și adăugită, Editura Sitech, 2014.
[26] *International Strategy of Cooperation on Cyberspace issued by the Ministry of Foreign Affairs of the People's Republic of China* on March 1, 2017, http://www.scio.gov.cn/32618/Document/1543874/1543874.htm
[27] *International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity* - October 2, 2013, Information Security Policy Council, Japan
[28] L. Vasiu, I. Vasiu, „Riscul de atac electronic asupra sistemelor de informații", capitol în *Fenomene și procese cu risc major la scară națională*, Editura Academiei Române, București, pag. 145-165, 2004.
[29] „Legile pământești ale lumii virtuale", Revista *Intelligence*, http://intelligence.sri.ro/legile-pamantesti-ale-lumii-virtuale/
[30] *Luna europeană a securității cibernetice*, https://www.enisa.europa.eu/news/enisa-news/cybersecmonth-2017/2017-10-02%20ENISA%20Press%20Release%20-%20European%20Cyber%20Security%20Month_RO.pdf
[31] M. Troutt, „IT Security Issues: The Need for End User Oriented Research", *Journal of End User Computing*, pp. 48-49, 2002.
[32] Metarankingul universitar 2016, https://www.edu.ro
[33] Ministerul Afacerilor Interne, Centrul de Coordonare a Protecției Infrastructurilor Critice, http://ccpic.mai.gov.ro/legislatie.html
[34] National Institute of Standards and Technology (NIST), „Special Publication 800-30: Risk Management Guide for Information Technology Systems", July 2002.
[35] No More Ransom, https://www.nomoreransom.org/ro/
[36] OECD Digital Economy Outlook 2017, ISBN 9789264276284, October 11, 2017, OECD Publishing, https://books.google.ro/books?id=PIQ5DwAAQBAJ
[37] *Pan-European Status of the NIS Directive*, https://geistwert.at/en/status-der-nis-richtlinie-in-den-eu-mitgliedstaaten/
[38] *Politica de raportare a vulnerabilităților*, www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html
[39] *Privacy and Data Protection by Design - from policy to engineering*, ENISA, January 12, 2015.
[40] *Proiectul de Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, Ministerul Comunicațiilor și Societății Informaționale, http://www.comunicatii.gov.ro/wp-content/uploads/2017/10/Proiect-lege-NIS-20171002.pdf

[41] *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, COM (2013) 48.
[42] R. G. Wilsher, and H. Kurth, „Security Assurance in Information Systems", Sokratis K. Katsikas and Dimitris Gritzalis (Eds.), *Information Systems Security: Facing the information society of the 21st century*, Chapman and Hall, 1996.
[43] *Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016*, CERT-RO, 2016, https://cert.ro/vezi/document/raport-alerte-cert-ro-2016
[44] *Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2015*, CERT-RO, 2015, https://cert.ro/vezi/document/raport-alerte-cert-ro-2015
[45] *Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2014*, CERT-RO, 2014, https://cert.ro/vezi/document/raport-alerte-cert-ro-2014
[46] Regulament al Parlamentului European şi al Consiliului privind ENISA, „Agenția UE pentru securitate cibernetică", de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică")
[47] Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).
[48] „Război hibrid și atacuri cibernetice", Revista Intelligence , http://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/
[49] Rezoluția Consiliului din 18 decembrie 2009 privind o abordare europeană a securității rețelelor și a informațiilor bazată pe colaborare (2009/C 321/01).
[50] *ROMÂNIA 50, Raportul anual privind cele mai valoroase branduri româneşti*, 2017, http://brandfinance.com/images/upload/bf_romania_50_2017_romanian_locked.pdf
[51] Security Updates, https://technet.microsoft.com/en-us/security/dn440717.aspx
[52] Serviciul de Combatere a Criminalității Informatice, http://www.efrauda.ro/
[53] *Transpunerea Directivei UE privind securitatea rețelelor și a sistemelor informatice (NIS)*, Digital Europe, 2016.
[54] United Nations Security Council resolution 2341, *Physical protection of critical infrastructure against terrorist attacks*, 2017, https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf
[55] V. Spiridon, *Tendințe în criminalitatea informatică*, Cybersecurity Trends, 1/2015.
[56] V.V. Patriciu, M.E. Pietrosanu, I. Bica, J. Priescu, *Semnături electronice și securitate informatică*, Editura All, 2006.
[57] V. Vlad, *Strategia de dezvoltare a României în următorii 20 de ani*, vol. II și III, Editura Academiei Române, 2016, http://www.acad.ro/strategiaAR/strategiaAR.htm

ANEXĂ

CHESTIONAR PRIVIND SECURITATEA CIBERNETICĂ

Prezentul chestionar își propune să trateze stadiul de maturitate a proceselor din domeniul securității cibernetice la nivelul instituțiilor din administrația publică din România. În vederea determinării nivelului de maturitate a domeniului au fost avute în vedere următoarele direcții:

- responsabilități și sarcini în domeniul securității cibernetice;
- managementul riscului de securitate (politici, planuri și proceduri);
- instrumente și automatisme la nivelul infrastructurii;
- cadrul privind stabilirea obiectivelor, indicatorilor și a mecanismelor de cooperare;
- cultura organizațională (dezvoltarea de expertiză la nivelul organizației prin programe de instruire, conștientizare și comunicare).

1. **Considerați că instituția dvs. acordă suficientă importanță securității cibernetice?**
   a. da;
   b. nu;
   c. nu știu / nu răspund.

2. **La nivelul instituției dvs. există un cadru intern / capabilități (norme interne, personal, infrastructură) privind gestionarea incidentelor de securitate cibernetică?**
   a. este definită o politică de securitate cibernetică la nivelul instituției;
   b. este definită o politică de management al incidentelor (clasificare / colectare / detecție / analiză și evaluare);
   c. sunt definite proceduri operaționale privind răspunsul la incidente (identificare / tratare a vulnerabilităților / raportare);
   d. există angajați cu atribuții (fișa postului) în domeniul securității cibernetice;
   e. infrastructura organizației are implementate soluții de securitate;
   f. nu știu / nu răspund.

3. **Cadrul legislativ național și de reglementare în domeniul securității cibernetice este clar definit și suficient pentru asigurarea unor obiective precise la nivelul instituțiilor publice?**
   a. da;
   b. nu;
   c. nu știu / nu răspund.

4. **Utilizați standarde / recomandări / ghiduri sau alte documente de standardizare europene și/sau internaționale în cadrul instituției dvs., pentru implementarea de măsuri în domeniul securității cibernetice?**
   a. da;
   b. nu;
   c. nu știu / nu răspund.

5. **Considerați utilă o uniformizare a cadrului organizațional privind securitatea cibernetică la nivelul instituțiilor publice din România în următoarele direcții:**

a. adoptarea de standarde / modele de securitate unitare;
b. politici, proceduri și planuri comune;
c. diseminarea frecventă a cazurilor de bună practică;
d. programe de instruire și conștientizare;
e. nu știu / nu răspund.

6. Instituția dvs. are definit un program de instruire și conștientizare referitor la securitatea cibernetică?
a. da;
b. nu;
c. nu știu / nu răspund.

7. Când a participat un reprezentant / angajat al instituției dvs. la un program / curs de instruire în domeniul securității cibernetice?
a. anul acesta;
b. anul trecut;
c. în urmă cu 2 ani sau mai mult;
d. nu a participat vreodată;
e. nu știu / nu răspund.

8. Când a fost revizuită ultima oară politica de securitate în cadrul instituției dvs.?
a. anul acesta;
b. anul trecut;
c. în urmă cu 2 ani sau mai mult;
d. nu s-a revizuit vreodată;
e. nu știu / nu răspund.

9. Referitor la managementul incidentelor, care sunt etapele în care vă confruntați cu dificultăți la nivelul instituției dvs.?
a. detectarea și raportarea evenimentelor / incidentelor / vulnerabilităților;
b. analiza, evaluarea și prioritizarea incidentelor;
c. răspunsul la incidente, inclusiv raportarea;
d. colectarea informațiilor despre incidente și păstrarea evidenței acestora;
e. comunicarea informațiilor despre incidente către entități externe;
f. alte probleme (vă rugăm să le specificați): ……
g. nu știu / nu răspund.

10. Care dintre etapele managementului incidentelor sunt implementate la nivelul instituției dvs.?
a. detectarea și raportarea evenimentelor / incidentelor / vulnerabilităților;
b. analiza, evaluarea și prioritizarea incidentelor;
c. răspunsul la incidente, inclusiv raportarea;
d. colectarea informațiilor despre incidente și păstrarea evidenței acestora;
e. comunicarea informațiilor despre incidente către entități externe;
f. alte probleme (vă rugăm să le specificați): ……
g. nu știu / nu răspund.

11. **Instituția dvs. a colaborat / cooperat în tratarea incidentelor cu:**
    a. instituții abilitate;
    b. companii specializate, private;
    c. furnizori de soluții de securitate;
    d. nu știu / nu răspund.

12. **Cele mai multe incidente (hardware și software) din instituția dvs. se referă la următoarele tipuri de resurse:**

Tip resursă	Top *
echipamente fixe (PC-uri, desktop-uri)	....
sisteme de calcul mobile (laptop-uri)	....
telefoane / tablete	....
poșta electronică	....
aplicații Web (site-uri / portaluri)	....
nu știu / nu răspund	....

** - se introduc cifre de la 1 (cele mai multe incidente) la 5 (cele mai puține incidente) sau „x" pentru ultima linie*

13. **În instituția dvs. există sisteme de protecție împotriva atacurilor cibernetice?**
    a. antivirus / antimalware;
    b. firewall;
    c. IDS/IPS (Intrusion Detection Systems / Intrusion Prevention Systems);
    d. SIEM (Security Information and Event Management);
    e. nu știu / nu răspund.

14. **Cum apreciați nivelul de importanță acordat domeniului securității cibernetice de instituția dvs.?**

	Foarte bun	Bun	Suficient	Insuficient	Deloc	Nu știu / nu răspund
Protecția la malware	☐	☐	☐	☐	☐	☐
Protecția rețelei locale (firewall)	☐	☐	☐	☐	☐	☐
Accesul la distanță și utilizarea dispozitivelor mobile	☐	☐	☐	☐	☐	☐

	Foarte bun	**Bun**	**Suficient**	**Insuficient**	**Deloc**	**Nu știu / nu răspund**
Controlul echipamentelor mobile de stocare a datelor (USB flash drive, HDD etc.)	☐	☐	☐	☐	☐	☐
Sisteme de management al evenimentelor (SIEM)	☐	☐	☐	☐	☐	☐
Gestiunea riscurilor de securitate	☐	☐	☐	☐	☐	☐

15. Comentarii, sugestii, observații: ……