DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Asociația de Acreditare din România

CREȘTEREA CAPACITĂȚII AUTORITĂȚILOR COMPETENTE DIN ROMÂNIA DNSC ȘI RENAR CONFORM REGULAMENTULUI EUROPEAN PRIVIND SECURITATEA CIBERNETICĂ 2019/881 (CYBERSECURITY ACT)

Beneficiari: DNSC, RENAR și EY
Proiect: Creșterea capacității autorităților competente din România DNSC și RENAR conform Regulamentului European privind securitatea cibernetică 2019/881 (Cybersecurity Act)

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Asociația de Acreditare din România

«Studiu privind disponibilitatea pentru a implementa, în România, schema de certificare a securității cibernetice, conform Cybersecurity Act (Regulamentul (UE) 2019/881)»

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Cuprins

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Abrevieri

Acronim	Denumire
DNCS	Directoratul Național de Securitate Cibernetică
RENAR	Asociația de Acreditare din România
EY	Ernst & Young
TIC	Tehnologia informației și telecomunicațiilor
CEF	Mecanismul pentru Interconectarea Europei (*în Engl. Connecting Europe Facility*)
UE	Uniunea Europeană (*în Engl. EU*)
ITSEF	Mecanismul pentru evaluarea securității tehnologiei informației (*în Engl. Information Technology Security Evaluation Facility*)
EUCC	Schema europeană de certificare a securității cibernetice (*în Engl. Common Criteria based European candidate cybersecurity certification scheme*)
EUCS	Schema europeană de certificare a securității cibernetice pentru serviciile de tip cloud (*în Engl. European Cybersecurity Certification Scheme for Cloud Services*)
ENISA	Agenția Uniunii Europene pentru Securitate Cibernetică (*în Engl. European Union Agency for Cybersecurity*)
NCCA	Autoritatea națională de certificare a securității cibernetice (*în Engl. National Cybersecurity Certification Authority*)
OEC (CAB)	Organism de Evaluare a Conformității (*în Engl. Conformity Assessment Bodies)*
SA	Schemă de acreditare
SEC	Schemă de evaluare a conformității

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Sumar executiv

Introducere

Prezentul studiu a fost elaborat în cadrul proiectului „Creșterea capacității autorităților competente din România DNSC și RENAR conform Regulamentului european privind securitatea cibernetică 2019/881 (Cybersecurity Act)". Studiul analizează perspectiva și disponibilitatea de implementare a noilor prevederi ale Cybersecurity Act în rândul entităților din sectorul public și privat din România.

Concluziile acestui studiu contribuie la îndeplinirea obiectivului DNSC și RENAR referitor la identificarea disponibilității de implementare, în România a schemei de certificare a securității cibernetice, conform Cybersecurity Act.

Metodologie

Analiza documentației relevante a condus la identificarea aspectelor de interes pentru elaborarea acestui studiu. Au fost identificate ca idei centrale securitatea cibernetică, considerente financiare și temporale în vederea alinierii la noul cadru al Cybersecurity Act.

În cadrul activității, au fost colectate informații din arii de activitate esențiale din cadrul pieței, precum autoritățile responsabile pentru implementarea Cybersecurity Act Directoratul Național de Securitate Cibernetică (DNSC), Asociația de Acreditare din România (RENAR)), organismele de evaluare a conformității, dezvoltatori de produse, procese și servicii TIC și entități consumatoare (operatori economici privați din sectoare precum cel al energiei, financiar, bancar și instituții din sectorul public).

În cadrul acestui proces au fost contactate treizeci și cinci de entități din cadrul pieței din România, esențiale pentru implementarea cadrului de certificare.

Grupuri țintă vizate de studiu	Interviuri realizate*	Chestionare completate	Entități contactate
DNSC	1	-	1
RENAR	1	-	1
Organismele de evaluare a conformității)	4	2	9

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Grupuri țintă vizate de studiu	Interviuri realizate*	Chestionare completate	Entități contactate
Dezvoltatori de produse, procese și servicii	2	-	6
Entități consumatoare – Instituții publice** și Operatori economici privați	5	2	18

**durata medie a unui interviu a fost de aproximativ o oră*
*** Instituții publice din România altele decât DNSC*

Acest sumar executiv prezintă în continuare rezultatele care decurg din analiza informațiilor colectate pe baza interviurilor online și a chestionarelor.

În urma aplicării metodologiei, din analiza informațiilor colectat au fost constatate următoarele aspecte:

În ceea ce privește strategia de securitate:

- Entitățile participante la discuții manifestă un interes sporit pentru dezvoltarea strategiei de securitate cibernetică. Principalul motiv invocat este dinamica pieței, precum și creșterea semnificativă a amenințărilor de natură cibernetică. O schemă comună de certificare la nivel european este considerată a fi un element care poate susține eforturile de securitate cibernetică ale organizațiilor. Utilizarea produselor certificate simplifică implementarea cerințelor de securitate la nivelul entităților, în vederea minimizării și eliminării riscurilor identificate.

- Reglementarea europeană asigură un context uniform în cadrul pieței interne prin recunoașterea mutuală a produselor certificate. Aceasta reprezintă o oportunitate de dezvoltare a domeniului securității cibernetice. Prin intermediul Cybersecurity Act se stabilesc norme și proceduri comune privind evaluarea nivelului de securitate cibernetică al produselor, serviciilor și proceselor. Acest aspect prezintă oportunități pentru dezvoltatorii de produse pentru extinderea portofoliului de clienți pe piața europeană. Totodată, predictibilitatea procesului de certificare crește nivelul de încredere al consumatorilor de produse, servicii și procese prin asigurarea unei achiziții informate.

În ceea ce privește aspectele financiare

Un alt element esențial identificat în urma studiului este reprezentat de modificarea

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

costurilor produselor, proceselor și serviciilor în urma procesului de certificare. Costul reprezintă un criteriu major de selecție în procesul de achiziție. Așadar, având în vedere că un produs certificat va fi mai scump, achiziționarea lui va implica o analiză mai detaliată din punct de vedere financiar. Este necesară analiza posibilității de achiziție din cadrul companiei, în contextul beneficiilor aduse, a duratei de amortizare a investiției, precum și a gradului de acceptare a pieței.

De asemenea, un element important ce se are în vedere în procesul de achiziție este reprezentat de termenul de valabilitate a certificatelor europene de securitate cibernetică, termen care poate influența semnificativ evaluarea bugetului.

Din perspectiva produselor care pot dezvolta multiple versiuni într-un interval scurt de timp, certificatul produsului permite un patch management în limite rezonabile, decis de Organismul de evaluare a conformității, de la caz la caz. Dacă este o schimbare minoră, nu este necesară o recertificare. Dacă în procesul de evaluare se constată o vulnerabilitate majoră se poate ajunge până la retragerea certificatului.

Organismele de evaluare a conformității și laboratoarele de încercări trebuie să aibă în vedere bugetul, dotarea specifică și pregătirea experților în funcție de nivelul de conformitate în care activează.

- Din perspectiva resurselor umane, s-a menționat existența unei dificultăți în cadrul pieței în a identifica experți cu pregătirea profesională necesară. De asemenea, investiția în pregătirea profesională în această arie, prin training-uri și cursuri de specialitate, poate să reprezinte un risc al companiei, datorită tendinței pronunțate de migrare a resursei umane.

În ceea ce privește aspectele temporale

- Din perspectiva temporală, intervalul de timp considerat oportun pentru achiziționarea și implementarea unor astfel de produse, servicii și procese este de aproximativ 2-3 ani. Strategia de dezvoltare în această direcție are la bază nevoia de analiză aprofundată a produsului certificat, perioada de viață a soluțiilor deja existente, precum și costurile adiționale pentru înlocuire. Considerentul temporal a fost prezentat de către participanți în strânsă legătură cu aspectele privind costurile aferente întregului proces precum și cu cerințele de securitate necesare.

Pe baza constatărilor din cadrul studiului se desprind următoarele concluzii:

- Există un interes sporit privind aspectele legate de securitatea cibernetică.

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

- Contextul european al implementării Cybersecurity Act este perceput ca oportunitate de dezvoltare.
- Costurile unui astfel de produs, proces și serviciu certificat reprezintă un factor decizional important pentru procesul de achiziție.
- Există dificultate în cadrul pieței de identificare a resurselor umane specializate.
- Intervalul de timp reprezintă un factor important în evaluarea procesului de implementare a produselor certificate.

Recomandări în vederea implementării noului cadru european la nivel național:

Armonizarea contextului legislativ

Este necesară o clarificare și o transparență a măsurilor și cerințelor cuprinse în Cybersecurity Act, pentru a facilita implementarea cadrului european în România. De asemenea este esențială identificarea părților interesate în procesul de certificare pentru a stabili nevoia de certificare a unui produs, în funcție de destinația utilizării acestuia. Este important de menționat că certificarea nu este obligatorie, conform Cybersecurity Act. În schimb, în funcție de categoria de consumatori, se poate impune utilizarea unui produs certificat din punct de vedere al securității cibernetice de către operatorii de servicii esențiale și furnizorii de servicii digitale așa cum sunt definiți în Directiva NIS (Legea 362/2018).

Creșterea nivelului de conștientizare

Pentru claritate, se va impune dezvoltarea unor campanii de conștientizare prin care se vor prezenta avantajele utilizării unui produs certificat. Această comunicare va facilita o achiziție mai transparentă și informată pentru companiile din cadrul pieței din România. Pentru o eficiență a procesului de conștientizare se va apela la principalele metode de informare utilizate în cadrul pieței, respectiv conferințe, workshop-uri, comunicate.

Stabilirea costurilor procesului de certificare

Stabilirea costurilor aferente certificării trebuie să țină cont de posibilitatea recuperării investiției într-un interval de timp rezonabil și de capacitatea pieței de a susține aceste costuri (capacitatea dezvoltatorilor de a certifica produsele și a consumatorilor de a achiziționa astfel de produse certificate).

Identificarea și pregătirea resursei umane specializată

Pentru identificarea și pregătirea profesională adecvată a experților implicați în procesul de certificare (NCCA, OEC, ITSEF) se impune dezvoltarea unei curriculum pentru mediul

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

universitar care să adreseze problemele standardizării și certificării. DNSC împreună cu RENAR și alte părți interesate vor colabora în vederea promovării acestui program.

Întrucât migrarea resursei umane este dificil de controlat, este importantă stabilirea unor procese și norme clare în vederea implementării Cybersecurity Act la nivel național.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Executive summary

Introduction

This study was developed within the project "Increasing the capacity of the competent authorities in Romania DNSC and RENAR according to the European Regulation on cybersecurity 2019/881 (Cybersecurity Act)". The study analyzes the perspective and availability of implementation the new requirements of Cybersecurity Act among public and private sector entities in Romania.

The conclusions of this study contribute to the fulfillment of the DNSC and RENAR objective regarding identification of the availability to implement, the cybersecurity certification scheme in Romania, according to the Cybersecurity Ac

Methodology

The analysis of relevant documentation leads to the identification of the main aspects for elaboration of the study. They have been identified as central cybersecurity ideas, considered financial and temporal in order to align with the new framework of the Cybersecurity Act.

The analysis of the relevant documentation led to the identification of the main aspects for elaboration of this study. Cyber Security, financial and time frame considerations for alignment with the new framework of the Cybersecurity Act have been identified as central ideas.

The information was collected from key areas of activity in the market, such as competent authorities at national level for the implementation of the Cybersecurity Act National Directorate of CyberSecurity (DNSC), Romanian Accreditation Association (RENAR)), conformity assessment bodies, developers of ITC products, processes and services and consumer entities (private economic operators in the sector such as energy, finance, banking and public sector institutions).

During this process, were contacted thirty-five entities from the Romanian market essential for the implementation of the certification framework,.

Target groups of the study	Interviews conducted*	Completed questionnaires	Contacted entities
DNSC	1	-	1

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Target groups of the study	Interviews conducted*	Completed questionnaires	Contacted entities
RENAR	1	-	1
Conformity assessment bodies	4	2	9
Products, processes and services developers	2	-	6
Consumer entities - public institutions** and Private economic operators	5	2	18

** Average duration of an interview was approx. 1 hour*
*** Public institutions in Romania other than DNSC*

This executive summary presents the results of the analysis of the information collected based on online interviews and questionnaires.

Following the application of the methodology, the following aspects were identified from the analysis of the collected information:

Regarding the security strategy

- The entities participating in the discussions show an increased interest for the development of cyber security strategy. The main reason given is the dynamics of the market, as well as the significant increase in cyber threats. A common certification scheme at European level is considered to be an element that can support organizations' cyber security efforts. The use of certified products simplifies the implementation of security requirements at entities level, in order to minimize and eliminate the identified risks

- European regulation ensures an uniform context in the internal market through the mutual recognition of certified products. This is an opportunity to develop the field of cybersecurity. The Cybersecurity Act establishes common rules and procedures for assessing the level of cyber security of products, services and processes. This presents opportunities for product developers to expand their customer portfolio in the European market. At the same time, the predictability of the certification process increases the level of confidence of consumers of products, services and processes by ensuring an informed purchase.

Regarding the financial aspects

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

- Another key element identified from the study is the change in the costs of products, processes and services as a result of the certification process. Cost is a major selection criterion in the procurement process. Therefore, given that a certified product will be more expensive, purchasing it will involve a more detailed analysis from a financial point of view. It is necessary to analyze the possibility of acquisition within the company, in the context of the benefits brought, the return on investment duration, as well as the degree of market acceptance.

  Also, an important element that is taken into account in the procurement process is the term of validity of the European cybersecurity certificates, a term that can significantly influence the evaluation of the budget.

  From the perspective of products that can develop multiple versions in a short period of time, the product certificate allows a patch management within reasonable limits, decided by the Conformity Assessment Body, on a case-by-case basis. If it is a minor change, no recertification is required. If a major vulnerability is found in the evaluation process, the certificate may be withdrawn.

  Conformity assessment bodies and testing laboratories shall take into account the budget, specific equipment and training of experts according to the level of compliance in which they operate.

- From a human resources perspective, it was mentioned that there is a difficulty in the market in identifying experts with the adequate professional knowledge. Also, the investment in the professional training in this area, through specialized courses, can represent a risk of the company, due to the pronounced tendency of migration of the human resource.

Regarding the time frame aspects

- The time frame that is considered appropriate for the purchase and implementation of such products, services and processes is about 2-3 years. The development strategy in this direction is based on the need for in-depth analysis of the certified product, the lifespan of existing solutions, as well as the additional costs for replacement. The time frame was presented by the participants in close connection with the costs aspects of the whole process as well as with the necessary security requirements.

Based on the findings of the study, the following conclusions can be drawn:

◆ There is a growing interest in cybersecurity aspects.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

- The European context of Cybersecurity Act implementation is perceived as an opportunity for development.
- The costs of such certified product, process and service are an important decision factor for the procurement process.
- There is difficulty in the market for identifying specialized human resources.
- Time frame is an important factor in evaluating the implementation process of certified products.

Recommendations for the implementation of new European framework at national level:

Harmonization of the regulatory context

There is a need for clarification and transparency of the measures and requirements contained in Cybersecurity Act, in order to facilitate the implementation of the European framework in Romania. It is also essential to identify the stakeholders in the certification process to determine the need to certify a product, depending on the purpose of its use. It is important to note that certification is not mandatory under the Cybersecurity Act. Instead, depending on the category of consumers, the use of a certified product may be required for essential service operators and digital service providers as defined in the NIS Directive (Law 362/2018).

Raising awareness

For the clarity of the matter, it will be necessary to develop awareness campaigns that will present the benefits of using a certified product. This communication will facilitate a more transparent and informed purchase for companies in the Romanian market. For the efficiency of the awareness process, the main methods of information in the market will be used, such as: conferences, workshops, press releases.

Establishing the costs of the certification process

The determination of certification costs must take into account the ability to recover the investment within a reasonable time frame and the ability of the market to support those costs (the ability of developers to cerifiy the products and the ability of consumers to purchase such certified products).

Identification and training of specialized human resources

In order to identify and adequately train the experts involved in the certification process (NCCA, CAB, ITSEF), it is necessary to develop a curriculum for the university

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

environment that addresses the issues of standardization and certification. DNSC together with RENAR and other stakeholders will work together to promote this program.

As the migration of human resources is difficult to control, it is important to establish clear processes and rules for the implementation of the Cybersecurity Act at the national level.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

1. Introducere

Scopul studiului

Prezentul studiu a fost elaborat în cadrul proiectului „Consolidarea capacității a autorităților competente din România DNSC și RENAR în conformitate cu Regulamentul privind securitatea cibernetică” (Capacity building în line with the Cybersecurity Act for the Romanian competent authorities DNSC and RENAR) în cadrul programului CONNECTING EUROPE FACILITY (CEF) - TELECOMMUNICATIONS SECTOR.

Beneficiarii acestui proiect sunt DNSC și RENAR. Prezentul studiu este elaborat în cadrul Activității 5 „Studiu privind disponibilitatea pentru a implementa, în România, schema de certificare a securității cibernetice, conform Regulamentului privind securitatea cibernetică ("AS IS" assessment and study report on the Romanian readiness for implementing cybersecurity certification schemes în line with the Cybersecurity Act).

Structura raportului este alcătuită din trei secțiuni. În prima parte se prezintă pe scurt documentele de referință și legislația în vigoare relevante pentru domeniul certificării securității cibernetice. În această secțiune, sunt surprinse o serie de aspecte relevante privind procesul de certificare. Următoarea secțiune prezintă principalele aspecte metodologice, inclusiv întrebările de cercetare, metodele de colectare și procesare a datelor, precum și entitățile vizate. Ultima parte pune în valoare aceste date printr-o analiză amănunțită a nivelului de maturitate al pieței din România în vederea implementării acestui Regulament.

Prezentul studiu are la baza analiza pe trei paliere principale, respectiv perspectiva principalelor entități vizate privind strategia de securitate cibernetică, aspectele financiare și temporale aferente procesului de implementare Cybersecurity Act. De asemenea, se va avea în vedere sublinierea aspectelor referitoare la disponibilitatea de aliniere cu prevederile Cybersecurity Act în rândul reprezentanților din cadrul pieței din România.

Concluziile acestui studiu contribuie la îndeplinirea obiectivului DNSC și RENAR referitor la identificarea disponibilității de implementare, în România a schemei de certificare a securității cibernetice, conform Cybersecurity Act.

Context

Uniunea Europeană a lansat în ultimii ani o serie de instrumente pentru protejarea rețelelor electronice de comunicații. Unul dintre acestea este Regulamentul (EU) 2019/881 al Parlamentului și Consiliului European, cunoscut și sub numele de EU Cybersecurity Act, care vizează stabilirea unui cadru european de certificare a securității cibernetice. Acesta va avea scopul armonizării practicilor de securitate cibernetică la nivel

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

european, precum și creșterea nivelului de încredere în produsele TIC.

În acest moment, prin intermediul proiectului din care face parte și prezentul studiu, se urmărește dezvoltarea arhitecturii instituționale naționale și consolidarea capacității autorităților competente responsabile pentru implementarea Cybersecurity Act. Pentru a veni în întâmpinarea nevoilor din cadrul pieței și pentru a înțelege contextul actual în România privind securitatea cibernetică, a fost demarat prezentul studiu în cadrul proiectului, care urmărește analiza maturității pieței. Acest lucru va duce la o mai bună înțelegere a modalității de transpunere a Cybersecurity Act astfel încât aceasta să răspundă nevoilor părților interesate.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

2. Documentele de referință și cerințele relevante pentru certificarea securității cibernetice

Pe baza informațiilor colectate și a documentației relevante certificării securității cibernetice, în cadrul acestui capitol sunt prezentate principalele aspecte relevante procesului de certificare. Aceste aspecte au fost extrase din Cybersecurity Act, schemele de certificare, standardele ISO și legislația națională ce vizează acest domeniu.

2.1 Cybersecurity Act

Cybersecurity Act stabilește reguli la nivelul Uniunii Europene privind certificarea securității cibernetice a produselor, proceselor și serviciilor TIC.

Creșterea gradului de digitalizare a condus inevitabil și la creșterea riscurilor de securitate cibernetică. De asemenea, organizațiile și întreprinderile nu dispun de suficiente resurse sau informații despre caracteristicile de securitate cibernetică ale produselor, serviciilor și proceselor TIC integrate în sistemele interne. Acestea sunt doar câteva dintre considerentele ce au determinat adoptarea Cybersecurity Act. [1]

Cybersecurity Act stabilește cadrul de certificare a securității cibernetice la nivelul UE cu scopul de a asigura o abordare comună în privința certificării securității cibernetice pe piața internă europeană cât și de a îmbunătăți securitatea cibernetică pentru o gamă largă de produse și servicii digitale (de exemplu, IoT). Armonizarea produsă de Cybersecurity Act va conduce la îmbunătățirea condițiilor de piață și la creșterea nivelului de securitate cibernetică.

Cybersecurity Act permite ca certificatele europene de securitate cibernetică și declarațiile UE de conformitate pentru produsele, serviciile sau procesele TIC să fie recunoscute și utilizate în toate statele membre, prin intermediul procesului de trasabilitate și recunoaștere mutuală a certificatelor. Regulamentul va crește nivelul de securitate cibernetică în cadrul statelor membre UE**.** [2]

Regulamentul definește trei niveluri de evaluare a produselor, serviciilor și proceselor TIC din punct de vedere al securității cibernetice după cum urmează: [3]

Nivelul „De bază” – stabilește faptul ca produsele, serviciile și procesele TIC asigură cerințele de securitate pentru minimizarea riscurilor incidentelor și atacurilor cibernetice

[1] Cybersecurity Act (**REGULAMENTUL (UE) 2019/881**) - Recitalul (2), (3), (5), (6)

[2] Cybersecurity Act (REGULAMENTUL (UE) 2019/881) - Articolul 1 - Obiect și domeniu de aplicare

[3] Cybersecurity Act (REGULAMENTUL (UE) 2019/881) - Articolul 52 - Niveluri de asigurare ale sistemelor europene de certificare a securității cibernetice

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

cunoscute.

Nivelul „Substanțial” - stabilește cerințele de securitate pentru minimizarea riscurilor cibernetice cunoscute și desfășurate de actori cu competențe și resurse limitate

Nivelul „Ridicat” - stabilește cerințele de securitate pentru minimizarea riscului de atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse substanțiale.

Aceste niveluri de asigurare sunt prevăzute în funcție de natura riscului asociat scopului utilizării produselor, serviciilor și proceselor TIC, după cum sunt detaliate în cadrul Articolului 52 al Cybersecurity Act**.**

Schemele de certificare a securității cibernetice

O schemă europeană de certificare a securității cibernetice conține un set de reguli, cerințe tehnice, standarde și proceduri, stabilite la nivel European, pentru evaluarea securității cibernetice a unui anumit produs, serviciu sau proces.

Certificarea securității cibernetice are un rol important în creșterea încrederii în produsele, serviciile și procesele care, de altfel, sunt esențiale pentru buna funcționare a pieței unice digitale. Având în vedere diversitatea cât și numeroasele utilizări ale produselor, serviciilor și proceselor TIC, cadrul european de certificare a securității cibernetice permite crearea de scheme de certificare adaptate nevoilor actuale, cât și bazate pe riscurile asociate.

Elaborarea schemelor de certificare a securității cibernetice la nivelul UE are ca scop stabilirea unor criterii comune de evaluare a conformității. Acestea vor permite dezvoltarea unor procese comparabile ce va asigura armonizarea practicilor la nivel european. Schemele vor include criterii de verificare a gradului de rezistență la riscuri de securitate cibernetică al produselor, serviciilor și proceselor TIC.

Cadrul european de certificare oferă transparență privind nivelul de rezistență la riscuri de securitate cibernetică a produselor, asigurând astfel conștientizarea privind gradul de rezistență pe care o are un produs, serviciu sau proces. Astfel, consumatorii care le achiziționează, utilizează sau le pun la dispoziție clienților vor cunoaște gradul de protecție împotriva riscurilor.

Certificarea securității cibernetice implică:

- evaluarea formală a produselor, serviciilor și proceselor de către un organism de evaluare a conformității independent și acreditat în conformitate cu un set clar de criterii definit în standarde. Face excepție certificarea la nivelul de bază, unde

acest proces presupune o declarație de conformitate cu un set de cerințe specifice, acțiune pentru care nu este necesar un audit independent.

- emiterea unui certificat care atestă conformitatea și nivelul de asigurare

Schema EUCC – Schema europeană de certificare a securității cibernetice, bazată pe criterii comune (Common Criteria based European candidate cybersecurity certification scheme)

ENISA a elaborat schema de certificare EUCC, considerată a fi succesoarea schemelor existente care funcționează în cadrul SOG-IS MRA.[4]

Schema EUCC prevede efectuarea unei evaluări a vulnerabilităților implementărilor criptografice în funcționalitățile de securitate ale unui produs TIC, în conformitate cu criteriile și metodologia de evaluare definite în cadrul schemei EUCC. Schema EUCC va permite evaluarea produselor pe baza criteriilor ISO/IEC 15408 și Criteriile Comune (Common Criteria CC).[5]

Schema va permite evaluarea la nivelurile de asigurare „substanțial" și „ridicat." Nivelul de evaluare „de bază", va fi abordat în alte scheme de certificare „lightweight" (mai puțin riguroase din perspectiva evaluării documentației) și care acoperă cerințe de securitate mai puțin stricte.

Prin intermediul schemei EUCC, se pot certifica produse dedicate protecției de securitate cibernetică (firewall-uri, dispozitive de criptare, gateway-uri, dispozitive de semnătură electronică, mijloace de identificare precum pașapoarte), precum și a oricărui produs TIC care încorporează o funcționalitate de securitate (de exemplu, routere, smartphone-uri, carduri bancare, servicii medicale, dispozitive, tahografe pentru camioane).[6]

Schema EUCS - Schema europeană de certificare a securității cibernetice pentru serviciile de tip cloud (European Union Cybersecurity Certification Scheme for Cloud Services)

EUCS certifică serviciile cloud la cele trei niveluri de asigurare, „scăzut", „substanțial" și „ridicat". Proiectul de schemă candidat EUCS urmărește evaluarea securității cibernetice pe întregul lanț de aprovizionare din cloud și să formeze o bază solidă pentru schemele

[4] https://www.sogis.eu/

[5] CYBERSECURITY CERTIFICATION EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS – page 9

[6] **CYBERSECURITY CERTIFICATION - EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS V1.1.1 | MAY 2021** - Capitolul 2. PURPOSE OF THE SCHEME

sectoriale ulterioare.

2.2 Standarde ISO

ISO/IEC 15408 Tehnologia informației. Tehnici de securitate. Criterii de evaluare a securității IT.

Partea 1: Introducere și model general (15408-1)

Partea 2: Componente funcționale de securitate (15408-2)

Partea 3: Componente de asigurare a securității (15408-3)

ISO/IEC 18045 Tehnologia informației. Tehnici de securitate. Metodologie pentru evaluarea securității IT

ISO/IEC 17000 Evaluarea conformității. Vocabular și principii generale

ISO/IEC 17065 Evaluarea conformității. Cerințe pentru organisme care certifică produse, procese și servicii

ISO/IEC 17025 Cerințe generale pentru competența laboratoarelor de încercări și etalonări

ISO/IEC 19896-3 Tehnici de securitate IT — Cerințe de competență pentru evaluatorii de securitate a informațiilor — Partea 3: Cerințe privind cunoștințele, abilitățile și eficacitatea evaluatorilor ISO/IEC 15408

ISO/IEC WD TS 23532-1 Tehnici de securitate IT — Cerințe pentru competența laboratoarelor de testare și evaluare a securității informatice — Partea 1: Testare și evaluare pentru ISO/IEC 15408

ISO/IEC 27001 Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației.

ISO/IEC 27002 Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației

ISO/IEC 27005 Tehnologia informației. Tehnici de securitate. Managementul riscului de securitate a informației

ISO/IEC 29147 Tehnologia informației. Tehnici de securitate. Dezvăluirea vulnerabilității

ISO/IEC 30111 Tehnologia informației. Tehnici de securitate. Procese de gestionare a

vulnerabilităților

2.3 Legislație națională

La nivelul României, DNSC este autoritatea națională de certificarea securității cibernetice. Acest rol este introdus prin

- Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică
- Lege 11/2022 pentru aprobarea Ordonanței de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică

RENAR reprezentând Organismului National de Acreditare

- Ordonanța nr. 23/2009 privind activitatea de acreditare a organismelor de evaluare a conformității

2.4 Detalii despre procesul de certificare

Eliberarea certificatelor:

Fiecare stat membru poate emite certificări europene de securitate cibernetică. Autoritățile naționale de certificare a securității cibernetice („NCCA") supraveghează și monitorizează conformitatea acestora cu schemele agreate la nivel european. Certificatele sunt emise de către OEC (Organism de Evaluare a Conformității) acreditate de RENAR (organismul național de acreditare).

Procesul cuprinde următoarele etape:

1. Contractarea ITSEF;

2. Solicitarea aprobării demarării procesului de certificare de către OEC;

3. Furnizarea dovezilor de evaluare de către dezvoltatorul de produse către ITSEF și OEC;

4. ITSEF emite raportul de evaluare și îl trimite către OEC și dezvoltatorul de produs;

5. OEC emite raportul de certificare împreună cu nivelul de asigurare;

Certificatele de securitate cibernetică reprezintă un pas important în conformitatea lor cu cerințele minime de securitate cibernetică.

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Certificatele UE emise de Organismele de Evaluare a Conformității autorizate (OEC care fac parte din țări membre UE) sunt valabile în toate țările UE.

Condițiile de funcționare a OEC:

- Pentru a evalua și certifica în conformitate cu schemele de certificare ale UE, OEC-urile vor trebui să fie acreditate de RENAR, organismul național de acreditare.
- În urma acreditării OEC-ului pentru o schemă europeană de certificare a securității cibernetice, Autoritatea Națională de Certificare a Securității Cibernetice (NCCA) autorizează și transmite Comisiei Europene decizia de funcționare
- Pentru certificare la nivel „înalt" Cybersecurity Act specifică faptul că evaluarea trebuie făcută de un OEC public. Un OEC privat poate funcționa pentru certificarea de nivel „înalt" printr-o derogare de la NCCA.[7]

[7] **REGULAMENTUL (UE) 2019/881** - Articolul 56, punctele 5-6,

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

3. Metodologie de analiza a disponibilității pentru a implementa în România Cybersecurity Act

Studiul privind disponibilitatea pentru a implementa în România Cybersecurity Act a fost demarat la 1 August 2021 și s-a desfășurat pe o perioadă de cinci luni.

Desfășurarea activităților a fost structurată în trei etape principale:

Etapa 1 - Etapa de studiu și analiză a documentației. În cadrul acestei activități au fost identificate documentele de interes și aspectele legislative pentru domeniul reglementat de Cybersecurity Act prezentate în cadrul secțiunii anterioare (capitolului 2.)

Etapa 2 – Desfășurarea interviurilor și completarea chestionarelor. În cadrul acestei etape au fost colectate datele din partea actorilor relevanți privind certificarea securității cibernetice din cadrul pieței

Etapa 3 – Analiza datelor extrase din interviuri și chestionare

3.1 Identificarea aspectelor relevante

Pe baza documentației relevante din prima etapă a desfășurării activității, au fost identificate următoarele aspecte de interes pentru elaborarea acestui studiu:

- Aspecte strategice privind evoluțiile de securitate cibernetică
- Aspecte financiare privind alinierea la noul cadru al Cybersecurity Act.
- Aspecte temporale privind alinierea la noul cadru.

Prin analiza din perspectiva strategiei evoluției securității cibernetice se dorește descoperirea opțiunilor pe care le au companiile în acest moment și proiectele viitoare avute în vederea dezvoltării ariei securității cibernetice.

Din perspectiva aspectelor financiare, se dorește identificarea disponibilității de a investi a companiilor privind dezvoltarea acestei arii a securității cibernetice și a implementării Cybersecurity Act.

Analiza aspectelor temporale are ca scop identificarea unor intervale de timp considerate necesare de către participanți pentru identificarea și asigurarea resurselor necesare implementării Cybersecurity Act.

Colectarea informațiilor în cadrul interviurilor și prin intermediul chestionarelor cu privire la cele trei aspecte, a fost utilizată pentru identificarea atât a nivelului de maturitate și de

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

pregătire privind securitatea cibernetică cât și privind interesul și disponibilitatea din cadrul pieței în vederea implementării cerințelor Cybersecurity Act.

3.2 Identificarea entităților relevante

În vederea elaborării acestui studiu și pentru a capta o imagine de ansamblu în aria certificării securității cibernetice, s-au avut în vedere colectarea de informații din arii de activitate esențiale din cadrul pieței. Așadar au fost identificate următoarele arii de interes în vederea stabilirii sesiunilor de discuții pentru colectarea de informații relevante:

- **Directoratul Național de Securitate Cibernetică (DNSC)** și **Asociația de Acreditare din România (RENAR),** în calitate de autorități publice responsabile pentru implementarea Cybersecurity Act,
- **Organisme de evaluare a conformității** pentru identificarea disponibilității de a introduce în cadrul portofoliilor de activitate acreditarea pentru acest domeniu și care sunt principalele constrângeri la momentul desfășurării studiului în vederea acreditării,
- **Dezvoltatori de produse, procese și servicii TIC** care ar avea capacitatea si resursele necesare parcurgerii procesului de certificare, conform Cybersecurity Act și
- **Consumatorii de produse, procese și servicii TIC** care furnizează servicii esențiale pentru buna funcționare a activităților economice și sociale. Au fost incluse entități din industria de energie și domeniul financiar bancar, precum și din sectorul public. Aceste entități au fost selectate pentru a identifica disponibilitatea de a achiziționa, implementa și utiliza produse, servicii și procese certificate.

Analiza se bazează pe informațiile colectate după cum urmează:

Grupuri țintă vizate de studiu	Interviuri realizate*	Chestionare completate	Entități contactate
DNSC	1	-	1
RENAR	1	-	1
Organismele de evaluare a conformității)	4	2	9

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Grupuri țintă vizate de studiu	Interviuri realizate*	Chestionare completate	Entități contactate
Dezvoltatori de produse, procese și servicii	2	-	6
Entități consumatoare – Instituții publice** și Operatori economici privați	5	2	18

Tabel 1: Participarea la interviurile online și răspunsurile transmise la chestionare de către entitățile participante la studiu

**durata medie a unui interviu a fost de aproximativ o oră*
*** Instituții publice din România altele decât DNSC*

În cadrul sesiunilor de discuții desfășurate pentru acest studiu 33 % dintre aceștia fac parte din categoria Organismelor de evaluare a conformității, 17 % reprezintă dezvoltatorii de produse, servicii și procese TIC, iar 50% din intervievați sunt entități consumatoare a produselor, serviciilor și proceselor TIC, atât din sectorul privat cât și din sectorul public. Valorile prezentate reprezintă procentele confirmărilor de participare ale categoriilor de entități selectate în cadrul studiului, însă nu reflectă proporțiile reale din cadrul pieței.

3.3 Colectarea datelor

Metodele selectate pentru colectare datelor necesare analizei sunt:

Chestionarul (Anexa 2) - a vizat colectarea datelor cantitative privind aspectele de interes cu privire la implementarea cerințelor Cybersecurity Act. Prin intermediul chestionarelor, au fost colectate informațiile din partea participanților la studiu într-o manieră structurată, având scopul prezentării statistice a aspectelor de studiu.

Interviul – a fost organizat într-o manieră semi-structurată cu entitățile identificate. Metoda interviului a servit obținerea de date și informații calitative. Interviul a avut rolul de a complementa informațiile colectate prin intermediul chestionarului, prin consolidarea și completarea informațiilor.

Elaborarea ghidului de interviu a implicat consultarea și **analiza documentelor** relevante certificării securității cibernetice. Drept urmare, analiza prezentată în Capitolul 2 a reprezentat o etapă importantă în elaborarea studiului.

Această triangulare metodologică servește la captarea imaginii de ansamblu a principalelor aspectele din piața din România într-o maniera extinsă și detaliată.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

3.4 Procesarea și analiza datelor colectate

Pentru elaborarea acestui studiu s-au utilizat următoarele metode de procesare și analiză a datelor colectate:

- analiza de documente, prin consultarea legislației europene și naționale în vederea sintetizării principalelor elemente ale cadrului european de certificare a securității cibernetice, precum și captarea unei imagini de ansamblu a cadrului instituțional și legislativ din România,

- analiza statistică a informațiilor colectate prin intermediul chestionarelor completate de către participanții la studiu prezentând astfel într-o manieră structurată principalele aspecte și

- analiza de discurs a mesajelor transmise de participanții la interviu, pentru a capta aspectele privind nivelul de maturitate al pieței din perspectiva principalelor entități implicate în procesul certificării.

Prin procesarea și analiza datelor, precum și prin intermediul instrumentelor utilizate, s-a utilizat o imagine de ansamblu a aspectelor relevante privind nivelul de maturitate și disponibilitatea părților interesate din cadrul pieței din România de a implementa cerințele Cybersecurity Act.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

4. Nivelul de maturitate al pieței și disponibilitatea pentru a implementa în România reglementările Cybersecurity Act

În cadrul acestei secțiuni, este prezentată analiza și sinteza informațiilor colectate, atât în cadrul interviurilor online cât și prin intermediul chestionarelor. Capitolul este structurat în trei sub-secțiuni, menite să ofere informații referitoare la principalele arii de interes abordate în cadrul acestui studiu. Analiza este organizată în jurul aspectelor strategice, financiare și temporale ce influențează nivelul de maturitate al pieței și a disponibilității pentru a implementa în România Cybersecurity Act.

Participanții la studiu, aparțin celor cinci categorii de interes din cadrul pieței, respectiv cele două entități-cheie DNSC și RENAR, organismele de evaluare a conformității (OEC), precum și consumatorii de produse certificate.

4.1 Aspecte strategice privind evoluțiile de securitate cibernetică

În contextul noilor cerințe de reglementare de la nivel european, din perspectiva **strategiei de securitate cibernetică**, **Directoratul Național de Securitate Cibernetică (DNSC)** are în curs de implementare proiectul de creștere a capacității conform Cybersecurity Act, din care face parte și acest studiu. Ulterior dezvoltării nivelului de maturitate instituțională, este prevăzută dezvoltarea unui OEC public un Laborator de Încercare pentru Testarea Produselor, Proceselor și Serviciilor TIC (ITSEF), destinate certificărilor de nivel înalt. Înființarea OEC și ITSEF publice pentru evaluarea nivelului ridicat (”high”) privind securitatea cibernetică sub umbrela DNSC presupune funcționarea lor în mod independent față de Autoritatea Națională de Certificare a Securității Cibernetice, având buget și conducere separată.

Din perspectiva strategiei de securitate, în prezent **RENAR (Asociația de Acreditare din România)** are documentate și implementate schemele de acreditare (SA) relevante pentru acest studiu:

- Schema de acreditare – Acreditarea organismelor de certificare produse – document de referință de nivel 3 - ISO/IEC 17065

- Schema de acreditare – Acreditarea organismelor de certificare sisteme de management – document de referință de nivel 3 - ISO/IEC 17021-1

Pentru a fi posibilă acreditarea în domeniul reglementat de Cybersecurity Act (Regulamentul 881/2019) este necesară modificarea celor două scheme de acreditare precizate anterior prin dezvoltarea a două scheme de evaluare a conformității (SEC) noi.

Este important de menționat faptul că, în conformitate cu prevederile legislației naționale,

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

în situația în care, în aplicarea legislației armonizate la nivel comunitar sau a legislației naționale, o autoritate cu funcție de reglementare (în cazul de față DNSC) decide să utilizeze acreditarea în scopul verificării competenței organismelor de evaluare a conformității și dacă se justifică necesar, RENAR dezvoltă scheme de acreditare specifice, stabilite cu autoritatea respectivă.

Astfel, RENAR a efectuat până în prezent următoarele demersuri, relevante din perspectiva îndeplinirii obiectivelor stabilite prin contractul aferent proiectului:

1. Analiza competenței și resurselor actuale ale RENAR
2. Accesarea și angajarea expertizei necesare modificării SA sau dezvoltării SEC noi
3. Studierea standardelor și documentelor normative aplicabile SA (de nivel 3 și 4)
4. Identificarea documentelor ENISA referitoare la schemele de evaluare a conformității EUCC și EUCS
5. Identificarea legislației specifice, la nivel european și național, aplicabile SA

Într-o primă etapă, în vederea dezvoltării celor două SEC, este necesar ca RENAR să asigure instruirea personalului implicat în managementul SA/SEC.

Toate entitățile participante la studiu au manifestat un interes sporit pentru îmbunătățirea securității cibernetice. Au menționat diverse proiecte ce țin de dezvoltarea acestei arii, în special din perspectiva pieței în continuă evoluție și a riscurilor ce pot apărea pentru produsele, serviciile și procesele TIC. Aceste proiecte sunt menite să creeze și să asigure un nivel de securitate optim pentru desfășurarea activității și să ofere protecție împotriva potențialelor atacuri cibernetice. Luând în considerare evoluția rapidă a tehnologiilor, entitățile participante au menționat că au implementat metodologii de evaluare a riscurilor și procese de analiză periodică pentru identificarea nevoilor de securitate. De asemenea, se depun eforturi constante de aliniere la reglementările în vigoare din acest domeniu, precum și la cerințele pieței.

Strategia de securitate cibernetică este fundamentală pentru **dezvoltatorii de produse.** În primul rând, este esențială pentru desfășurarea activității curente, de a dezvolta produse sigure și de a fi conformi cu reglementările în vigoare. S-a menționat faptul că strategiile ar trebui aliniate cu cerințele regulamentelor naționale și internaționale, iar entitățile ar trebuie să dezvolte și totodată, să întrețină, mecanismele necesare pentru a asigura securitatea cibernetică aferentă serviciilor pe care le prestează. Acest lucru se realizează deseori prin implementarea de sisteme IT de securitate, dar și având în vedere riscurile potențialelor atacuri cibernetice. În plus, elaborarea strategiei de securitate ar trebui considerată atât din perspectiva resurselor tehnice cât și a celor umane.

Din perspectiva **entităților consumatoare de produse, procese și servicii TIC**, atât din sectorul public, cât și cel privat, asigurarea securității cibernetice are o importanță majoră. Aceasta se realizează prin intermediul implementării de soluții, precum hardware

integrate de protecție a rețelelor, firewall, IDS/IPS, soluții Anti-virus, control al aplicațiilor, VPN cât și sisteme pentru Data Loss Prevention. De asemenea, entitățile consumatoare din sectorul public au menționat, că pentru asigurarea măsurilor de securitate cibernetică sunt elaborate politici și proceduri de securitate, care reprezintă un suport pentru menținerea unui cadru optim de desfășurare a activităților în această arie.

Pentru a îndeplini cerințele specifice de securitate, este nevoie de alocarea unui buget adecvat, astfel încât să existe posibilitatea achiziționării de soluții tehnologice cu un nivel de performanță cât mai ridicat, necesare pentru dezvoltarea și furnizarea produselor, proceselor și serviciilor din portofoliu. Bugetul fiind limitat, este nevoie de eficientizarea costurilor. În ceea ce privește fluxul de producție, în ultimii ani, s-au definit roluri și procese specifice, care înglobează cerințele securității cibernetice a produselor și serviciilor. Angajații cu expertiză privind securitatea, dedicați pe proiecte sunt foarte importanți pentru realizarea strategiei dezvoltatorilor de produse și servicii.

Entitățile consumatoare din sectorul privat realizează analize periodice pe aspecte de securitate cibernetică pentru evaluarea nivelului de risc. Există și programe de dezvoltare în acest sens, cu rezultate pe termen mediu și lung. Entitățile intervievate au precizat că strategia de securitate este aliniată cu strategia de business și cu strategia IT. S-au menționat și soluții de SIEM/SOC implementate pentru asigurarea managementului incidentelor de securitate, ținând cont de cerințele legale, reglementările în vigoare, cât și de riscurile identificate în cadrul proceselor interne.

Reprezentanții **DNSC** au specificat că există posibilitatea **introducerii obligativității certificării în contexte bine definite**. S-a precizat faptul că dezvoltarea unui cadru național de certificare va veni și în sprijinul eforturilor de implementare a Directivei NIS (DIRECTIVA (UE) 2016/1148 - privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune), ce menționează posibilitatea folosirii unor produse certificate în echipamentele entităților esențiale. Pentru asigurarea securității se au în vedere certificările pe categorii de produse critice, unde lipsa unor cunoștințe detaliate privind securitate cibernetică conforme poate produce pagube majore. Astfel, pentru operatorii care desfășoară activități critice, există posibilitatea impunerii utilizării de produse certificate. Din această perspectivă se are în vedere intensificarea dialogului cu zona privată, pentru crearea unor reglementări potrivite care să vină în ajutorul tuturor părților relevante din cadrul pieței.

Dezvoltatorii de produse au identificat încrederea și transparența ca fiind principalele avantaje în ceea ce privește certificarea produselor, serviciilor și proceselor dezvoltate de către aceștia. Certificarea produselor proprii este văzută ca un mijloc prin care se poate câștiga încrederea clienților. Un produs certificat presupune conformitatea cu anumite standarde, chiar și o interoperabilitate mai bună cu alte sisteme. Scopul unei scheme de certificare este de a crea mai multă transparență între furnizori și consumatori.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

În plus, aceasta poate fi benefică din punct de vedere al protecției împotriva amenințărilor din spațiul cibernetic, impunând anumite cerințe minime de securitate implementate la nivel de design.

Cu toate acestea, **dezvoltatorii de produse** susțin că stabilirea unei certificări obligatorii poate să nu fie cea mai bună cale de urmat, deoarece cerințele de certificare pot restricționa uneori lansarea rapidă a noilor versiuni de produse, menținerea infrastructurilor TIC în parametrii normali, dar și posibilitatea de a face remedieri de securitate rapide. Atunci când există cerințe specifice de reglementare, care ar putea necesita modificări în procesele de dezvoltare, dacă există o interacțiune timpurie între autoritățile de reglementare și companii, aceasta poate fi integrată în proces, mai degrabă decât ajustată ulterior, iar fragmentarea poate fi evitată.

Din perspectiva securității cibernetice, toți participanții la studiu, **entitățile consumatoare atât din sectorul public cât și din sectorul privat** consideră esențială **utilizarea** și implementarea de produse, servicii și procese certificate pentru o bună desfășurare a activității și pentru reducerea și gestionarea expunerii la factorii de risc, preponderent în zone critice de infrastructură, asigurându-se astfel o mai bună protejare a datelor și informațiilor gestionate.

Printre beneficiile utilizării unor astfel de produse a fost evidențiat gradul mai mare de încredere în produse, având în vedere testările și analizele efectuate prin procesul de certificare. De asemenea, pentru astfel de produse se pot primi actualizări de securitate pentru o perioadă de utilizare extinsă ce ar putea proteja utilizatorii din perspectiva unor atacuri indirecte prin țintirea elementelor vulnerabile din lanțul activităților acestora (atacuri de tip supply chain).

Un aspect important menționat în decursul discuțiilor este transparența oferită de un produs certificat, prin identificarea parametrilor ce ar trebui să fie aliniați cu nevoile entităților consumatoare. Produsele certificate ar aduce o valoare și siguranță suplimentară companiilor, dar și clienților sau partenerilor acestora.

Adoptarea Cybersecurity Act este considerată de către **participanții la studiu** a fi o **oportunitate de dezvoltare** din punct de vedere al securității cibernetice. Se au în vedere și posibilități de accesare a fondurilor și sprijinul organizațiilor din aria securității cibernetice pentru a se realiza implementarea și atingerea obiectivelor de dezvoltare a protecției cibernetice. Un cadru european comun de certificare a securității cibernetice, are avantajul de a armoniza reglementările naționale și europene.

Implementarea unei scheme comune de certificare la nivel european, este considerată benefică din perspectiva securității cibernetice pentru **entitățile consumatoare din piață** participante la studiu. Companiile multinaționale deja dispun de un cadru cu cerințe comune, stabilit la nivel de grup, cu instrucțiuni, îndrumări și informații necesare privind

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

dezvoltarea produselor și documentației aferente, pentru asigurarea conformității, securității și confidențialității. Conformitatea cu cerințele de nivel european aduce avantaje competitive și potențiale beneficii financiare pentru dezvoltatori, totodată oferind garanții suplimentare clienților. Totuși, dezvoltatorii trebuie să țină cont de specificul pieței și orientarea clienților către asigurarea costurilor cât mai mici, în detrimentul produselor certificate, de obicei mai scumpe. În acest sens, un nivel mai mare de conștientizare a beneficiilor unor astfel de produse ar ajuta în desfășurarea proceselor de certificare reprezentând un avantaj pentru dezvoltatorii de produse certificate.

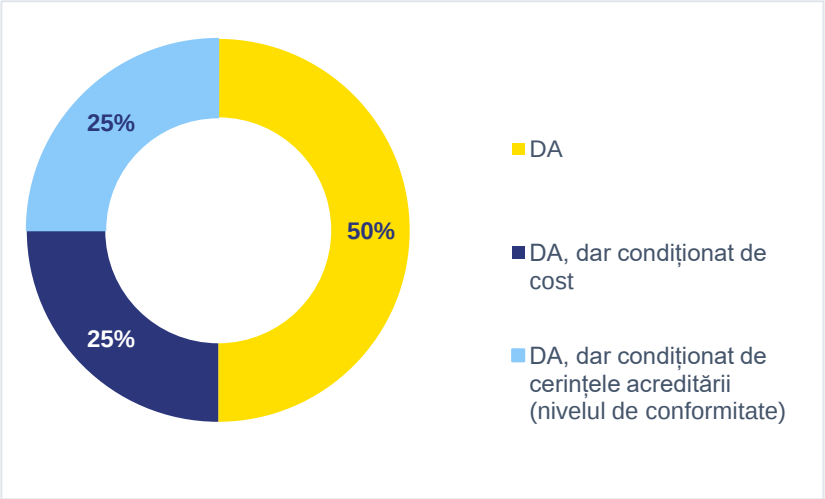
Din perspectiva **Organismelor de evaluare a conformității**, apariția Cybersecurity Act este considerată o oportunitate de dezvoltare din perspectiva asigurării securității cibernetice și dezvoltarea unui cadru care să poată permită realizarea de verificări ale vulnerabilităților produselor, serviciilor și proceselor TIC. Acest aspect este cu atât mai important cu cât riscul unor atacuri cibernetice la nivel mondial este în creștere iar necesitățile de securitate ale beneficiarilor unor produse, servicii și procese TIC este normal să crească și să se diversifice. Acest aspect poate ajuta la diferențierea dezvoltatorilor de produse, servicii și procese TIC certificate față de cele necertificate, facilitând astfel extinderea portofoliului de clienți și accesarea de piețe noi pentru dezvoltatorii produselor certificate. Un alt aspect perceput ca o oportunitate este asigurarea încrederii **entităților consumatoare**, prin utilizarea de produse certificate, asigurându-se astfel creșterea nivelului de securitate cibernetică și transparență.

Din perspectiva **nivelurilor de asigurare** („de bază”, „substanțial” sau „ridicat”) participanții la studiu consideră că primul pas ar trebui sa fie certificarea pe nivelul “de bază”, unde de cele mai multe ori cerințele sunt îndeplinite într-o măsură considerabilă. Apoi, în funcție de cererile din piață, de strategia dezvoltatorului și de costul de certificare, produsele și serviciile se pot plia și pe celelalte niveluri. Cu cât crește mai mult nivelul de asigurare, cu atât ar trebui repetate activitățile care sunt deja efectuate în timpul dezvoltării produsului. Ar trebui luat în calcul și dacă beneficiile aduse de acest proces detaliat de asigurare servesc nevoilor utilizatorilor.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Organismele de evaluare a conformității prezintă un interes ridicat privind introducerea în portofoliul companiei a unei acreditări din aria securității cibernetice. Totuși, aceste entități susțin necesitatea reglementării uniforme a domeniului certificării.



Figură 1: Introducerea în portofoliul Organismelor de evaluare a conformității, a unei acreditări din cadrul acestei arii

În ceea ce privește **categoriile de produse, procese și servicii TIC** ce pot intra sub incidența evaluării conformității securității cibernetice, în cadrul discuțiilor au fost menționate servicii cum ar fi cele de detecție și prevenție, servicii de depunere electronică, servicii de stocare, backup, restaurare centralizată, evaluări de risc si capabilitatea de răspuns a organizațiilor, sisteme de protecție a datelor personale sau critice, servicii tip cloud, echipamente de securitate, furnizori de servicii de management al echipamentelor IT și de securitate.

Reprezentanții **DNSC** au menționat că nu au existat încă solicitări de certificare din piață, deoarece cadrul instituțional necesar acestui proces este în proces de dezvoltare în țara noastră. În plus, domeniul certificării este implementat în exclusivitate în România prin proiectul de față. Totodată, cadrul european în sine este un element de noutate, aflându-se încă în proces de conturare. Prin urmare, este necesară investirea de eforturi în creșterea nivelului de conștientizare în rândul factorilor de decizie politică din perspectiva asigurării securității cibernetice.

Considerând elementul de noutate al Cybersecurity Act, o componentă esențială în vederea transpunerii eficace a Regulamentului în România este creșterea nivelului de **conștientizare** la nivel național. Vor fi făcute cunoscute cerințele și oportunitățile aduse de certificare prin **informarea** entităților interesate **și educarea** publicului cu privire la cadrul european de certificare a securității cibernetice. Se consideră necesară creșterea nivelului de conștientizare cu privire la riscurile ce pot afecta desfășurarea activității companiilor în contextul unor breșe de securitate.

În ceea ce privește strategia de conștientizare a publicului privind noul cadru european de certificare a securității cibernetice, **DNSC** va lua în considerare campanii de promovare pe social media – ex. YouTube, Twitter, LinkedIn, Facebook. Entitățile specializate, interesate de certificare vor fi notificate prin informări oficiale, precum

Cod proiect 2020-RO-IA-0224
Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

newsletter, conferințe și dezvoltarea unor evenimente dedicate acestui subiect. Se intenționează inițierea unui summit al omologilor europeni care se află în proces de dezvoltare instituțională în domeniul certificării. În plus, este luat în calcul pentru conștientizare și o comunicare directă cu organismele de evaluare a conformității și cu producătorii de produse. De asemenea există și o comunicare directă a Directoratului cu operatorii esențiali NIS, care vor fi principalii consumatori de produse certificate.

În rândul **dezvoltatorilor de produse**, metodele de informare preferate sunt comunicarea directă cu instituțiile naționale și internaționale din domeniul securității cibernetice, prezentări ale furnizorilor de soluții de securitate, site-urile de specialitate, colaborarea cu comunitățile de cercetare, dar și cu autoritățile de reglementare.

Din perspectiva **consumatorilor de produse certificate**, cele mai utilizate metode de informare sunt conferințele, site-urile de specialitate, ale instituțiilor din domeniu, bloguri de securitate, cât și întâlniri și prezentări ale furnizorilor de soluții de securitate, precum și newsletter.

Organismele de evaluare a conformității se informează cel mai adesea de pe site-urile de profil și conferințele desfășurate pe subiecte legate de securitatea cibernetică. Schimburile de informații cu privire la incidente de securitate și atacurile cibernetice ce au loc pe teritoriul UE de asemenea reprezintă surse importante. Unii participanți au menționat că realizează și o diseminare ulterioară pentru clienții lor cu privire la aceste aspecte, prin postarea pe site-ul companiei a informațiilor referitoare la posibile incidente

4.2 Aspecte financiare privind alinierea la noul cadru al Cybersecurity Act

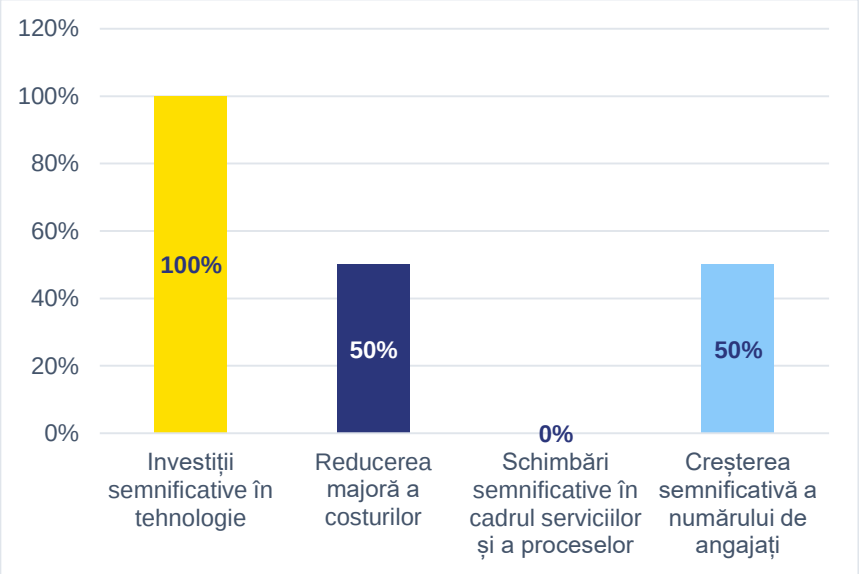
Resursele financiare necesare dezvoltării cadrului instituțional în vederea implementării Regulamentului reprezintă un factor important. În acest sens este necesară identificarea surselor de finanțare pentru dezvoltarea structurilor necesare, inclusiv de la bugetul de stat, cât și surse externe, precum finanțarea europeană.

Din perspectiva **dezvoltatorilor de produse** există disponibilitatea de a investi, pentru certificarea produselor dezvoltate. O investiție de acest fel poate duce și la simplificarea unor procese de audit. În cadrul unui proces de audit anumite aspecte privind securitatea cibernetică a produsului pot fi validate mai facil, dacă produsul a trecut prin procesul de certificare si este conform cu prevederile Cybersecurity Act. Bugetele anuale ar trebui să

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

prevadă alocarea de resurse pentru investiții legate de certificarea securității cibernetice a produselor. Pentru realizarea priorităților strategice, **dezvoltatorii de produse și servicii prevăd** investiții semnificative în tehnologie, reducerea majoră a costurilor, schimbări semnificative în cadrul serviciilor și a proceselor, dar și creșterea semnificativă a numărului de angajați cu focus pe noile capabilități și evoluția continuă din domeniul IT.



Figură 2: Prioritățile strategice ale dezvoltatorilor de produse, procese și servicii

În rândul **Organismelor de evaluare a conformității**, aspectele de ordin financiar sunt considerate esențiale de către majoritatea participanților la studiu menționându-se aici costurile aferente procesului de introducere în portofoliu și gradul de acceptare al pieței de a suporta aceste costuri. Pentru a suplimenta fondurile, în situația în care va fi necesar, doar 50% din respondenți au menționat ca ar putea accesa instrumente precum CEF Telecom, Orizont Europa și alte programe europene.

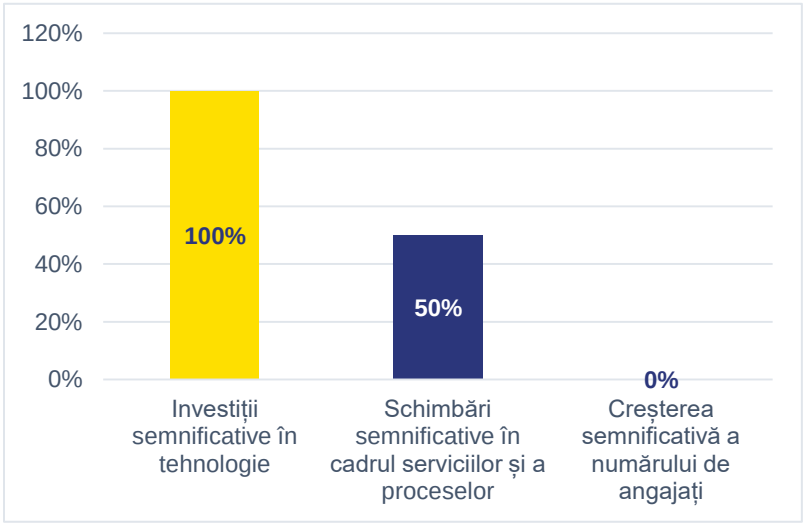
În ultimul timp, este tot mai evidentă necesitatea creșterii investițiilor în domeniul securității, inclusiv prin **achiziționarea de produse certificate**. Respondenții din aria **dezvoltatorilor de produse** au menționat drept factori declanșatori răspunsul la situații de criză, introducerea sau modificarea reglementărilor legislative și necesitatea reducerii riscurilor cibernetice. Chiar dacă ultimele atacuri la nivel global au afectat multe companii generând situații de criză, sectorul ITC a dispus de măsurile necesare pentru evitarea unor pagube majore. Au fost identificate rapid produsele afectate, iar vulnerabilitățile au fost remediate. Situațiile de acest gen duc la o mai bună înțelegere a importanței managementului vulnerabilităților, care în final implică reducerea riscului.

Autoritățile de reglementare locale pot folosi standardele existente la nivel internațional, ceea ce ar permite certificarea de produse care pot fi utilizate apoi la nivel global. Există situații însă în care cerințele de reglementare specifice se adoptă târziu și nu țin cont de evoluția tehnologică, ceea ce ar putea îngreuna procesul de certificare. Dar și în astfel de cazuri, din punct de vedere al industriei ITC, dacă toate cerințele sunt îndeplinite, certificarea aduce beneficii și siguranță atât industriei, cât și utilizatorilor de produse

Cod proiect 2020-RO-IA-0224
Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

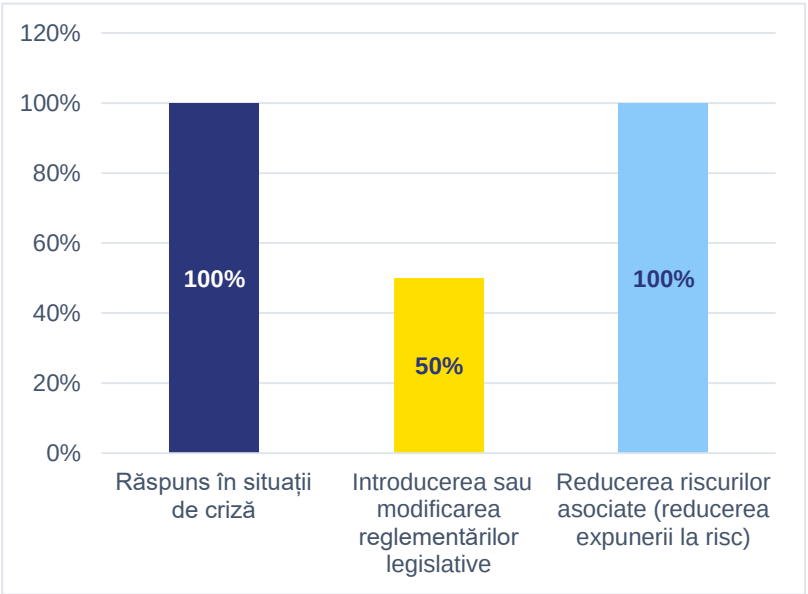
certificate.

În cadrul **entităților consumatoare din sectorul public**, există disponibilitate de a investi în achiziția, implementarea și utilizarea de produse, servicii și procese certificate. De asemenea, se fac permanent eforturi de aliniere cu cerințele pieței și se urmărește achiziționarea de soluții cât mai sigure și tehnologii cât mai noi, în funcție de bugetele alocate pentru acestea. Luând în considerare limitările de buget alocat pentru astfel de investiții, și necesitatea de a se alinia cu cerințele de securitate, nu se pot achiziționa de fiecare data soluțiile dorite din cauza costurilor ridicate. Cu toate acestea, se fac demersuri pentru menținerea nivelului minim necesar de securitate cibernetică.



Figură 3: Prioritățile strategice aliniate cu strategia, misiunea sau valorile instituției în cadrul entităților consumatoare din sectorul public

Investițiile în tehnologie și schimbările tehnologice sunt cuprinse în prioritățile strategice ale **entităților consumatoare din sectorul public**. Aspectul financiar reprezentă o constrângere în procesul de aliniere la noul context privind securitatea cibernetică. Acest proces este îngreunat de procedurile de achiziție specifice sectorului public.



Figură 4: Principalul motiv ce determină o creștere a investițiilor în domeniul securității cibernetice în cadrul entităților consumatoare din sectorul public

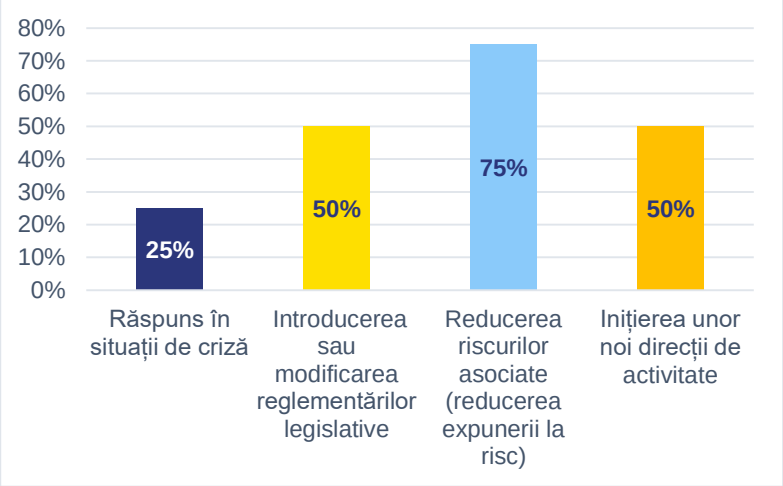
Entitățile consumatoare din sectorul public întreprind acțiuni în vederea reducerii riscurilor la care sunt expuși și demersurile periodice de conștientizare și informare pe care le efectuează pentru a preîntâmpina o situație de

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

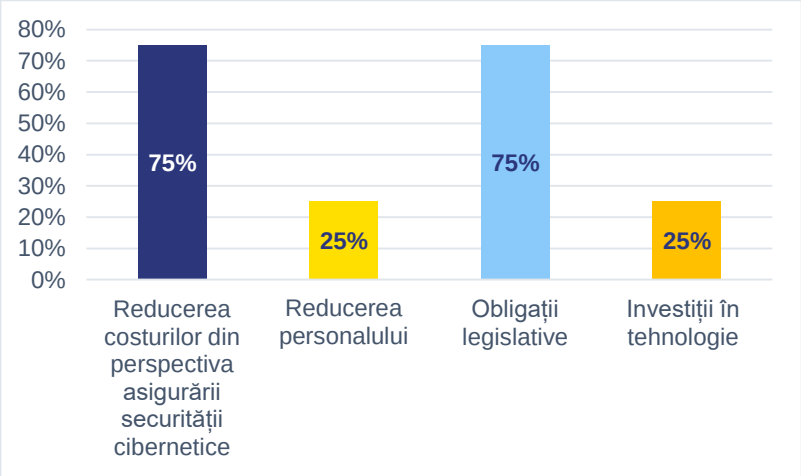
criză. În acest sens, se practică raportări periodice privind securitatea cibernetică, reprezentând astfel factori declanșatori privind creșterea investițiilor. Din perspectiva introducerii sau modificării reglementărilor legislative se consideră esențial ca acestea să se facă într-o manieră uniformă, pentru a ușura implementarea în cadrul organizațiilor.

Din perspectiva investițiilor în domeniul securității cibernetice, **entitățile private consumatoare de produse** și-au exprimat deschiderea de a crește pe viitor ponderea acestora. Obiectivul principal al companiilor de reducere a riscurilor cibernetice a fost menționat de către 75% dintre participanți, urmat de inițierea unor noi direcții de activitate, introducerea sau modificarea reglementărilor legislative, și răspunsul în situații de criză. Totodată, identificarea anumitor riscuri în urma unui proces de audit poate declanșa o creștere a investițiilor pentru remedierea deficiențelor raportate.



Figură 5: Principalul motiv ce determină o creștere a investițiilor în domeniul securității cibernetice în cadrul entităților consumatoare din sectorul privat

Entități consumatoare din sectorul privat au evidențiat un interes ridicat pentru achiziționarea de produse certificate, în vederea conformării cu măsurile de diminuare a riscurilor de securitate prin revizuirea periodică și alinierea la reglementările actuale. În cadrul entităților sunt implementate procese și metodologii de analiză a riscurilor care se face periodic in funcție de importanța și nivelul critic al sistemelor și a aplicațiilor. Pentru eficientizarea procesului este menținut și un registru al riscurilor, actualizat constant pentru o monitorizare adecvată a mediului IT, dar și implementarea de măsuri care țin de prevenție și detecție. În ceea ce privește



Figură 6: Motivul achiziției de produse, servicii și procese certificate în cadrul entităților consumatoare din sectorul privat

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

managementul riscului se apelează la audituri interne sau externe, cât și din partea autorității din domeniu.

75% dintre **consumatorii de produse din sectorul privat** au răspuns afirmativ în privința disponibilității de a investi în achiziția, implementarea și utilizarea de produse, servicii și procese certificate. Există însă și constrângeri, pentru că un produs certificat va fi mai scump. Astfel decizia de achiziție se va baza pe o analiză detaliată a informațiilor suplimentare despre beneficiile aduse, inclusiv modalitatea de recuperare a investiției. Interesul **entităților consumatoare din sectorul privat** de a achiziționa produse certificate rezidă în asigurarea suplimentară prin evaluarea lor, actualizarea de securitate ulterioară și conformitatea cu legislația națională și internațională.

Achiziționarea unui produs, serviciu sau proces certificat este preferată, chiar și la un cost mai mare. Însă decizia ar trebui luată în baza unei analize de risc, având în vedere destinația utilizării acelui produs, dar și cerințelor de business.

În contextul încheierii unui contract de colaborare, subcontractare de servicii sau furnizare de produse, procese și servicii, cu o parte terță, în vederea achiziționării de produse, procese și servicii toți participanții la studiu au menționat că în mod obligatoriu se au în vedere și aspecte legate de securitatea cibernetică.

Aspectele privind securitatea cibernetică a produselor, proceselor și serviciilor sunt incluse în caietele de sarcini aferente procesului de achiziții din sectorul public, pentru stabilirea și validarea aspectelor de securitate în relațiile de colaborare cu terții încă din faza de achiziție.

În sectorul privat sunt implementate proceduri speciale prin care aspectele de securitate sunt incluse în analiza relației cu partenerii, atât la încheierea contractelor cât și pe durata desfășurării acestora, pentru a se asigura nivelul de securitate dorit. De asemenea, dacă se consideră necesar se efectuează și teste de penetrare pentru validarea nivelului de securitate.

În cadrul discuțiilor, criteriile achiziționării de produse includ elemente precum firewall necesare, elemente de optimizare a software-ului, mecanisme de criptare, elemente de parolare, modalități de autentificare autorizată, respectarea standardelor naționale sau internaționale în domeniu, includerea de servicii de mentenanță și suport, posibilitatea ca tehnologia să fie integrabilă cu cea existentă, dar și criterii adaptate, definite în dependență de specificul organizației sau companiei.

Din perspectiva **resurselor umane și tehnice**, **DNSC** consideră resursa umană ca fiind una din principalele provocări în transpunerea cadrului european de certificare a securității cibernetice. Pe de o parte, resursa umană este fluctuantă, fiind necesară dezvoltarea de strategii de retenție a experților. Pe de altă parte, fiind un domeniu nou în

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

România, există și un deficit de expertiză la nivel național în domeniul certificării. Cu toate acestea, cunoștințele tehnice din domeniul securității cibernetice pot deveni transferabile prin livrarea de training-uri specializate. Este prevăzută explorarea intersectorială pentru identificarea experților cu aptitudini transferabile din domenii tangențiale.

Este prevăzut la nivelul Directoratului pregătirea unui nucleu de specialiști, experți care ulterior să poată dezvolta și finaliza procesul de certificare, inclusiv cu aspectele referitoare la acreditarea unor organisme de evaluare a conformității și laboratoare de încercare. Se dorește ca până la sfârșitul anului 2022 să se poată efectua pași importanți în desfășurarea acestui proces, prin crearea unor astfel de nuclee, care ulterior să poată fi perfecționate și să poată la rândul lor să furnizeze expertiză în domeniul certificării, ținând cont de nivelul de specializare existent și de aspectele din cadrul pieței.

Din punct de vedere al strategiei de dezvoltare, DNSC manifestă un interes sporit pentru pregătirea personalului în vederea dezvoltării structurii instituționale de certificare. Organigrama întregului Directorat va include și structurile competente în domeniul certificării securității cibernetice.

În ceea ce privește alinierea cu noul context european, prima etapă este pregătirea personalului și crearea nucleelor care ulterior pot promova procedeele de certificare, urmând ca apoi să se efectueze evaluarea resurselor financiare atât din zona publică cât și privată pentru a putea crea procedurile necesare procesului de certificare a produselor, proceselor și serviciilor TIC.

Pentru asigurarea condițiilor optime de desfășurare a activității aferente programelor de instruire din proiect **RENAR**:

- va aloca resursele umane necesare pentru efectuarea instruirilor specifice schemelor de evaluare a conformității EUCC și EUCS,

- va aloca resursele umane necesare pentru a participa la instruirile specifice schemelor de evaluare a conformității EUCC și EUCS,

- vor fi elaborate proiectele fișelor de competențe pentru personalul evaluator (evaluator șef, evaluator, evaluator tehnic și expert tehnic) implicat în efectuarea evaluărilor în cadrul schemelor EUCC și EUCS.

Organismele de evaluare a conformității au confirmat disponibilitatea resurselor tehnice necesare pentru desfășurarea activităților de evaluare a conformității unor produse, servicii și procese la nivel substanțial, din perspectiva cerințelor de securitate cibernetică. Există însă anumite arii asupra cărora sunt necesare îmbunătățiri, dar acestea sunt deja avute în vedere pentru remediere, în proiecte viitoare. Din perspectiva resurselor umane, **peste 70% din participanți au menționat că există o dificultate în**

a identifica persoane cu nivel de expertiză înalt pentru o astfel de specializare în cadrul pieței. Pentru asigurarea nivelului necesar de competențe a personalului pentru efectuarea activităților de certificare, sunt necesare investiții în pregătirea profesională în această arie, prin training-uri și cursuri de specialitate. Aceste activități trebuie să țină cont de tendința de migrare a resursei umane.

4.3 Aspecte temporale privind alinierea la Cybersecurity Act

Aspectele temporale privind durata de transpunere a Cybersecurity Act sunt considerate de **DNSC** un impediment care poate afecta procesul de înființare OEC public, precum și eforturile de creștere a capacității umane și achiziția infrastructurii necesare.

D**ezvoltatorii de produse și servicii** au menționat că o parte din produse sunt dezvoltate din start implementând conceptul “security by design”, ceea ce ar scurta durata procesului de certificare. Pentru produsele „legacy”, un demers de certificare poate să aducă constrângeri temporale semnificative. Astfel, obligativitatea utilizării de produse certificate nu ar trebui impusă cu restricții temporale, oferindu-le companiilor interesate suficient timp la dispoziție pentru a lua decizii și a parcurge toți pașii necesari.

Participanții din cadrul **entităților consumatoare din sectorul public**, au menționat că intervalul de timp oportun pentru a achiziționa astfel de produse, servicii și procese certificate a fost estimat în cadrul interviurilor între unul și doi ani. Se consideră a fi oricând oportună achiziția de astfel de produse, însă aceste achiziții sunt corelate cu bugetele alocate și aprobările necesare și sunt bazate pe procese de durată.

Entitățile consumatoare din sectorul privat susțin în proporție de 50% că prevăd un interval de timp de aproximativ doi-trei ani, invocând nevoia de analiză aprofundată a produsului respectiv, luând în calcul perioada de viață a soluțiilor existente, cât și costurile adiționale pentru înlocuire. S-a menționat și posibilitatea ca unele produse să fie certificate din momentul punerii lor în vânzare pe piață, pentru a scurta timpul de achiziție.

Organismele de evaluare a conformității prevăd demararea acreditării într-o perioadă de peste un an, până la doi ani. Principalele constrângeri menționate cu privire la acest aspect sunt cerințele privind acreditarea (care pot avea efecte de timp), contextul legislativ, măsurile legislative secundare, precum și norme ce contribuie la implementarea noului cadru european.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

5. Concluzii și recomandări

În urma analizei la nivel național privind disponibilitatea de a implementa schema de certificare a securității cibernetice, conform Cybersecurity Act (Regulamentului (UE) 2019/881), prezentul studiu ridică o serie de observații și recomandări.

Concluzii:

Există un interes sporit privind aspectele legate de securitatea cibernetică

Entitățile participante la discuții manifestă un interes sporit pentru dezvoltarea strategiei de securitate cibernetică. Principalul motiv invocat este dinamica pieței, precum și creșterea semnificativă a amenințărilor de natură cibernetică. O schemă comună de certificare la nivel european este considerată a fi un element care poate susține eforturile de securitate cibernetică ale organizațiilor. Utilizarea produselor certificate simplifică implementarea cerințelor de securitate la nivelul entităților, în vederea minimizării și eliminării riscurilor identificate.

Contextul european al implementării Cybersecurity Act este perceput ca oportunitate de dezvoltare.

Reglementarea europeană asigură un context uniform în cadrul pieței interne prin recunoașterea mutuală a produselor certificate. Aceasta reprezintă o oportunitate de dezvoltare a domeniului securității cibernetice. Prin intermediul Cybersecurity Act se stabilesc norme și proceduri comune privind evaluarea nivelului de securitate cibernetică al produselor, serviciilor și proceselor. Acest aspect prezintă oportunități pentru dezvoltatorii de produse pentru extinderea portofoliului de clienți pe piața europeană. Totodată, predictibilitatea procesului de certificare crește nivelul de încredere al consumatorilor de produse, servicii și procese prin asigurarea unei achiziții informate.

Costurile unui astfel de produs, proces și serviciu certificat reprezintă un factor decizional important pentru procesul de achiziție

Un alt element esențial identificat în urma studiului este reprezentat de modificarea costurilor produselor, proceselor și serviciilor în urma procesului de certificare. Costul reprezintă un criteriu major de selecție în procesul de achiziție. Așadar, având în vedere că un produs certificat va fi mai scump, achiziționarea lui va implica o analiză mai detaliată din punct de vedere financiar. Este necesară analiza posibilității de achiziție din cadrul companiei, în contextul beneficiilor aduse, a duratei de amortizare a investiției, precum și a gradului de acceptare a pieței.

De asemenea, un element important ce se are în vedere în procesul de achiziție este

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

reprezentat de termenul de valabilitate a certificatelor europene de securitate cibernetică, termen care poate influența semnificativ evaluarea bugetului.

Din perspectiva produselor care pot dezvolta multiple versiuni într-un interval scurt de timp, certificatul produsului permite un patch management în limite rezonabile, decis de Organismul de evaluare a conformității, de la caz la caz. Dacă este o schimbare minoră, nu este necesară o recertificare. Dacă în procesul de evaluare se constată o vulnerabilitate majoră se poate ajunge până la retragerea certificatului.

Organismele de evaluare a conformității și laboratoarele de încercări trebuie să aibă în vedere bugetul, dotarea specifică și pregătirea experților în funcție de nivelul de conformitate în care activează.

Există dificultate în cadrul pieței de identificare a resurselor umane specializate

Din perspectiva resurselor umane, s-a menționat existența unei dificultăți în cadrul pieței în a identifica experți cu pregătirea profesională necesară. De asemenea, investiția în pregătirea profesională în această arie, prin training-uri și cursuri de specialitate, poate să reprezinte un risc al companiei, datorită tendinței pronunțate de migrare a resursei umane.

Intervalul de timp reprezintă un factor important în evaluarea procesului de implementare a produselor certificate

Din perspectiva temporală, intervalul de timp considerat oportun pentru achiziționarea și implementarea unor astfel de produse, servicii și procese este de aproximativ 2-3 ani. Strategia de dezvoltare în această direcție are la bază nevoia de analiză aprofundată a produsului certificat, perioada de viață a soluțiilor deja existente, precum și costurile adiționale pentru înlocuire. Considerentul temporal a fost prezentat de către participanți în strânsă legătură cu aspectele privind costurile aferente întregului proces precum și cu cerințele de securitate necesare.

Recomandări în vederea implementării noului cadru european la nivel național:

Armonizarea contextului legislativ

Este necesară o clarificare și o transparență a măsurilor și cerințelor cuprinse în Cybersecurity Act, pentru a facilita implementarea cadrului european în România. De asemenea este esențială identificarea părților interesate în procesul de certificare pentru a stabili nevoia de certificare a unui produs, în funcție de destinația utilizării acestuia. Este important de menționat că certificarea nu este obligatorie, conform Cybersecurity Act. În schimb, în funcție de categoria de consumatori, se poate impune utilizarea unui produs certificat din punct de vedere al securității cibernetice de către operatorii de servicii

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

esențiale și furnizorii de servicii digitale așa cum sunt definiți în Directiva NIS (Legea 362/2018).

Creșterea nivelului de conștientizare

Pentru claritate, se va impune dezvoltarea unor campanii de conștientizare prin care se vor prezenta avantajele utilizării unui produs certificat. Această comunicare va facilita o achiziție mai transparentă și informată pentru companiile din cadrul pieței din România. Pentru o eficiență a procesului de conștientizare se va apela la principalele metode de informare utilizate în cadrul pieței, respectiv conferințe, workshop-uri, comunicate.

Stabilirea costurilor procesului de certificare

Stabilirea costurilor aferente certificării trebuie să țină cont de posibilitatea recuperării investiției într-un interval de timp rezonabil și de capacitatea pieței de a susține aceste costuri (capacitatea dezvoltatorilor de a certifica produsele și a consumatorilor de a achiziționa astfel de produse certificate).

Identificarea și pregătirea resursei umane specializată

Pentru identificarea și pregătirea profesională adecvată a experților implicați în procesul de certificare (NCCA, OEC, ITSEF) se impune dezvoltarea unei curriculum pentru mediul universitar care să adreseze problemele standardizării și certificării. DNSC împreună cu RENAR și alte părți interesate vor colabora în vederea promovării acestui program.

Întrucât migrarea resursei umane este dificil de controlat, este importantă stabilirea unor procese și norme clare în vederea implementării Cybersecurity Act la nivel național.

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Anexe

Anexa 1 - Agenda întâlnirilor

Anexa 2 – Template chestionar

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Anexa 1 - Agenda întâlnirilor

Nr. Crt.	Subiect
01	**Introducere cu privire la prevederile Cybersecurity Act**
02	**Scopul proiectului**
03	**Aspecte privind strategia securității cibernetice**
04	**Considerente financiare și temporale**
05	**Întrebări și răspunsuri**

Anexa 2 - Template chestionar

Studiu privind disponibilitatea pentru a implementa, în România, schema de certificare a securității cibernetice, conform Cybersecurity Act (Regulamentului (UE) 2019/881) privind ENISA și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor

Strategia companiei privind securitatea cibernetică

Nr. Crt.	Întrebare	Răspuns
1	Care este strategia de securitate cibernetică a organizației dumneavoastră?	Deschis
2	Care este strategia de dezvoltare a organizației dumneavoastră din perspectiva securității cibernetice? (dezvoltatori, Organisme de evaluare a conformității)și entități consumatoare din mediul privat)	Deschis
3	Care sunt măsurile de securitate cibernetică ale organizației dumneavoastră? (entități consumatoare din sectorul public și privat)	Deschis
4	Care sunt modalitățile pentru asigurarea măsurilor de securitate cibernetică în cadrul instituției? (entități consumatoare din sectorul public)	Deschis
5	Care dintre prioritățile strategice de mai jos sunt aliniate cu strategia organizației dumneavoastră? a. Investiții semnificative în tehnologie a. Reducere majoră a costurilor b. Schimbări semnificative în cadrul produse, servicii și procese c. Creșterea semnificativă a numărului de angajați Vă rugăm să detaliați alegerea făcută. (dezvoltatori și entități consumatoare din	Deschis

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Nr. Crt.	Întrebare	Răspuns
	sectorul public)	
6	Sunt măsurile de diminuare a riscurilor din cadrul organizației dumneavoastră, revizuite și aliniate (adecvate sau conforme) la reglementările actuale? (entități consumatoare din sectorul public și privat)	Deschis
7	Care este principalul motiv, din cele menționate mai jos, care ar putea determina o creștere a investițiilor în domeniul securității cibernetice în cadrul organizației dumneavoastră? a. Inițierea unor noi direcții de activitate b. Răspuns în situații de criza c. Introducerea sau modificarea reglementărilor legislative d. Reducerea riscurilor asociate (reducerea expunerii la risc) Vă rugăm să detaliați alegerea făcută.	Deschis
8	Care ar fi motivul, din cele menționate mai jos, pentru care ați achiziționa produse, servicii și procese certificate a. Reducerea costurilor din perspectiva asigurării securității cibernetice b. Reducerea personalului c. Obligațiile legislative d. Investiții în tehnologie Vă rugăm să detaliați alegerea făcută. (entități consumatoare din mediul privat)	Deschis
9	În contextului noului Regulament european cu privire la măsurile de securitate cibernetică vi se pare oportună inserarea în portofoliul companiei dumneavoastră a unei acreditări din cadrul acestei arii? (Organismele de evaluare a conformității)	Deschis
10	In viziunea dumneavoastră, care sunt categoriile de produse, servicii și procese pe care doriți să le evaluați în vederea stabilirii conformității? (Organismele de evaluare a conformității)	Deschis
11	Au existat solicitări din partea clienților dumneavoastră cu privire la certificarea de produse, servicii și procese din domeniul securității cibernetice? (Organismele de evaluare a conformității))	Deschis
12	Din punct de vedere al securității cibernetice, care considerați că sunt avantajele pe care le poate aduce certificarea de produse, servicii și procese? (dezvoltatori)	Deschis
13	În ce măsură considerați că apariția acestui regulament va duce la o dezvoltare a activității de certificare în cadrul companiei dumneavoastră, în contextul unei abordări unitare ce are drept scop stabilirea unui cadru comun european de certificare a securității cibernetice care să se permită recunoașterea și utilizarea în toate statele membre a certificatelor europene de securitate cibernetică pentru produse, servicii și procese TIC?	Deschis
14	Considerați că este importantă utilizarea sau implementării de produse, servicii și procese certificate din punct de vedere al securității cibernetice? Ce beneficii considerați că ar putea aduce? (entități consumatoare din sectorul public și privat)	Deschis
15	Care sunt metodele de informare pe care le utilizați referitor la noutățile tehnologice și a măsurilor de securitate cibernetica? (atacuri, tools, information exchange, etc.) Care ar fi metoda preferată de comunicare? (ex: newsletter, etc.)	Deschis

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Nr. Crt.	Întrebare	Răspuns
16	În acest moment, organizația dumneavoastră, atunci când încheie contracte de colaborare sau subcontractare are in vedere si aspecte legate de securitatea cibernetică? (entități consumatoare din sectorul public și privat)	Deschis
17	Care sunt criteriile avute în vedere la momentul achiziționării unui produs din punct de vedere al securității cibernetice? (Standarde ISO, etc.) (entități consumatoare din sectorul public și privat)	Deschis
18	Până în acest moment au fost achiziționate produse, servicii și procese pentru care a fost stabilită conformitatea cu prevederile Cybersecurity Act (Regulamentul 2019/881)? (entități consumatoare din sectorul public și privat)	Deschis
19	Considerați că dispuneți de suficiente resurse tehnice și umane în vederea evaluării conformității unor produse, servicii și procese la nivel substanțial/ ridicat, din perspectiva cerințelor de securitate cibernetică? (Organismele de evaluare a conformității))	Deschis
20	Care sunt nivelurile de asigurare („de bază”, „substanțial” sau „ridicat”) pentru care intenționați să certificați produse, servicii și procese? (dezvoltatori)	Deschis

Cod proiect
2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene

Considerente financiare

Nr. Crt.	Întrebare	Răspuns
21	Există disponibilitate de a investi, la nivelul organizației dumneavoastră, pentru obținerea unei astfel de certificări în domeniul securității cibernetice? (dezvoltatori)	Deschis
22	Există disponibilitate de a investi, la nivelul organizației dumneavoastră, pentru achiziția, implementarea și utilizarea de produse, servicii și procese certificate din punct de vedere al securității cibernetice? (entități consumatoare din sectorul public și privat)	Deschis
23	Există disponibilitatea de a investi în consolidarea capacității organizaționale, cum ar fi formarea profesionala a personalului, necesitatea suplimentării personalului din cadrul echipelor de certificare, investiții în echipamente? (Organismele de evaluare a conformității))	Deschis
24	Există impedimente de ordin financiar care ar îngreuna obținerea unei astfel de acreditări în domeniul securității cibernetice? (Organismele de evaluare a conformității))	Da/Nu
25	Daca da, ce instrumente puteți utiliza în acest sens (CEF Telecom, HORIZON, etc). (Organismele de evaluare a conformității))	Deschis

Considerente temporale

Nr. Crt.	Întrebare	Răspuns
26	Care este orizontul de timp pe care îl luați în calcul în vederea certificării produsului ? Care sunt, în viziunea dumneavoastră, principalele constrângeri ce trebuie avute în vedere într-un astfel de proces de certificare? (dezvoltatori)	Deschis
27	Care este orizontul de timp pe care îl luați în calcul în vederea acreditării organizației dumneavoastră în acest domeniu? Care sunt, în viziunea dumneavoastră, principalele constrângeri ce trebuie avute în vedere într-un astfel de proces de acreditare? (Organismele de evaluare a conformității))	Deschis
28	Care este orizontul de timp pe care îl estimați în vederea începerii procesului de certificare al produselor, serviciilor și proceselor? (Organismele de evaluare a conformității))	Deschis
29	Care e orizontul de timp pe care îl considerați oportun pentru a achiziționa astfel de produse, servicii și procese certificate? (entități consumatoare din sectorul public și privat)	Deschis
30	Care sunt, în viziunea dumneavoastră, principalele constrângeri ce trebuie avute în vederea achiziționării și implementării de produse, servicii și procese certificare? (entități consumatoare din sectorul public și privat)	Deschis

Cod proiect 2020-RO-IA-0224

Cofinanțat de Mecanismul pentru Interconectarea Europei al Uniunii Europene