COMISIA
EUROPEANĂ

Bruxelles, 4.10.2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ANEXĂ

la

COMUNICAREA COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Valorificarea la maximum a NIS – către punerea în aplicare eficace a Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune

CUPRINS

ANEXĂ

1. Introducere

Prezenta anexă urmărește să contribuie la aplicarea, implementarea și asigurarea respectării în mod eficace a Directivei (UE) 2016/1148 privind securitatea rețelelor și a sistemelor informatice în Uniune[1] (denumită în continuare „Directiva NIS" sau „directiva") și să sprijine statele membre să asigure că legislația UE este aplicată în mod eficace. Mai precis, obiectivele sale specifice sunt triple: (a) să ofere mai multă claritate autorităților naționale cu privire la obligațiile prevăzute în directivă care se aplică acestor autorități, (b) să garanteze asigurarea respectării în mod eficace a obligațiilor prevăzute de directivă care se aplică entităților în temeiul obligațiilor privind cerințele de securitate și de notificare a incidentelor, și (c) să contribuie în general la crearea de securitate juridică pentru toți actorii relevanți.

În acest scop, prezenta anexă oferă orientări cu privire la următoarele aspecte, care sunt esențiale pentru a realiza obiectivul Directivei NIS, și anume asigurarea unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în cadrul UE, pe care să se bazeze funcționarea societății și a economiei noastre:

- obligația statelor membre de a adopta o strategie națională privind securitatea rețelelor și a sistemelor informatice (secțiunea 2);
- instituirea de autorități naționale competente, puncte unice de contact și echipe de intervenție în caz de incidente de securitate informatică (secțiunea 3);
- cerințele de securitate și de notificare a incidentelor care se aplică operatorilor de servicii esențiale și furnizorilor de servicii digitale (secțiunea 4) și
- relația dintre Directiva NIS și alte acte legislative (secțiunea 5).

Pentru întocmirea prezentului document de orientare, Comisia a utilizat informații și analize colectate în cursul fazei de elaborare a directivei, precum și contribuții din partea Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și a Grupului de cooperare. De asemenea, Comisia a valorificat experiența anumitor state membre. După caz, Comisia a ținut seama de principiile directoare pentru interpretarea dreptului UE: formularea, contextul și obiectivele Directivei NIS. Dat fiind faptul că directiva nu a fost transpusă, nu s-a pronunțat încă nicio hotărâre a Curții de Justiție a Uniunii Europene (CJUE) sau a instanțelor naționale. Prin urmare, jurisprudența nu oferă orientări.

Compilarea informațiilor într-un document unic poate permite statelor membre să dobândească o bună imagine de ansamblu asupra directivei și să țină seama de aceste informații atunci când își elaborează legislația națională. În același timp, Comisia subliniază

[1] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Directiva a intrat în vigoare la 8 august 2016.

că prezenta anexă nu este obligatorie și nu intenționează să creeze noi norme. Competența finală de a interpreta legislația UE îi revine CJUE.

2. Strategia națională privind securitatea rețelelor și a sistemelor informatice

În temeiul articolului 7 din Directiva NIS, statele membre au obligația de a adopta o strategie națională privind securitatea rețelelor și a sistemelor informatice care poate fi considerată echivalentă cu termenul de strategie națională de securitate cibernetică („SNSC"). Funcția unei strategii naționale este de a defini obiectivele strategice și acțiunile adecvate în materie de politică și reglementare în legătură cu securitatea cibernetică. Conceptul de SNSC este utilizat pe scară largă la nivel internațional și în Europa, în special în contextul activității ENISA desfășurate împreună cu statele membre cu privire la strategiile naționale, ceea ce a condus recent la o actualizare a Ghidului de bune practici SNSC[2].

În această secțiune, Comisia precizează modul în care Directiva NIS îmbunătățește pregătirea statelor membre prin impunerea obligației de a institui strategii naționale solide privind securitatea rețelelor și a sistemelor informatice (articolul 7). Această secțiune abordează aspecte privind: (a) domeniul de aplicare al strategiei și (b) conținutul și procedura de adoptare.

Astfel cum se prezintă în continuare, transpunerea corectă a articolului 7 din Directiva NIS este fundamentală pentru realizarea obiectivelor directivei și necesită alocarea de resurse financiare și umane corespunzătoare în acest scop.

2.1. Domeniul de aplicare al strategiei naționale

Conform formulării articolului 7, obligația de a adopta o strategie SNSC se aplică doar sectoarelor menționate în anexa II (și anume, energie, transport, sectorul bancar, piața financiară, sănătate, furnizarea și distribuirea de apă potabilă și infrastructură digitală) și serviciilor menționate în anexa III (piață online, motor de căutare online și serviciu de cloud computing).

Articolul 3 din directivă prevede în mod expres principiul armonizării minime, în temeiul căruia statele membre pot să adopte sau să mențină dispoziții în vederea obținerii unui nivel mai ridicat de securitate a rețelelor și a sistemelor informatice. Aplicarea acestui principiu în ceea ce privește obligația de a adopta o „SNSC" permite statelor membre să includă mai multe sectoare și servicii decât cele menționate în anexele II și III la directivă.

În opinia Comisiei și având în vedere obiectivul Directivei NIS, și anume de a obține un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune[3], ar fi de dorit să se elaboreze o strategie națională care să cuprindă toate dimensiunile relevante ale societății și

[2] ENISA, *National Cyber-Security Strategy Good Practice* („Bune practici referitoare la strategia națională privind securitatea cibernetică") (2016). Document disponibil la adresa https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[3] A se vedea articolul 1 alineatul (1).

ale economiei, nu numai sectoarele și serviciile digitale menționate în anexa II și, respectiv, în anexa III la Directiva NIS. Acest lucru este în conformitate cu bunele practici internaționale [a se vedea orientările Uniunii Internaționale a Telecomunicațiilor (UIT) și analiza OCDE menționată în continuare] și cu Directiva NIS.

Astfel cum se explică mai jos, acest lucru este valabil în special în ceea ce privește administrațiile publice responsabile de alte sectoare și servicii decât cele enumerate în anexele II și III la directivă. Administrațiile publice pot prelucra informații sensibile, ceea ce justifică necesitatea de a face obiectul unor SNSC și planuri de gestionare care să prevină scurgerile de informații și să asigure o protecție adecvată a acestor informații.

2.2. Conținutul strategiilor naționale și procedura de adoptare a acestora

În temeiul articolului 7 din Directiva NIS, o SNSC trebuie să includă cel puțin următoarele elemente:

i) obiectivele și prioritățile strategiei naționale privind securitatea rețelelor și a sistemelor informatice;
ii) un cadru de guvernanță pentru realizarea obiectivelor și a priorităților strategiei naționale;
iii) identificarea măsurilor referitoare la gradul de pregătire, răspuns și redresare, inclusiv cooperarea între sectorul public și cel privat;
iv) indicarea programelor de instruire, sensibilizare și formare;
v) indicarea planurilor de cercetare și dezvoltare;
vi) un plan de evaluare a riscurilor pentru identificarea riscurilor și
vii) o listă a actorilor implicați în punerea în aplicare a strategiei.

Nici articolul 7, nici considerentul corespunzător 29 nu precizează cerințele pentru adoptarea unei SNSC și nu furnizează mai multe detalii cu privire la conținutul SNSC. În ceea ce privește procesul și elementele suplimentare referitoare la conținutul SNSC, Comisia consideră că abordarea prezentată mai jos este o modalitate adecvată de adoptare a unei strategii SNSC. Aceasta se bazează pe analiza experienței statelor membre și a țărilor terțe cu privire la modul în care statele membre și-au dezvoltat propriile strategii. O resursă suplimentară de informații este instrumentul de formare în materie de SNSC al ENISA, disponibil pe site-ul său web sub formă de videoclipuri și medii care pot fi descărcate[4].

2.3. Procesul și aspectele care trebuie să fie abordate

Procesul de elaborare și adoptare ulterioară a unei strategii naționale este complex și multidimensional, necesitând angajamentul susținut al experților din domeniul securității cibernetice, al societății civile și al proceselor politice naționale pentru a fi eficace și de succes. O condiție *sine qua non* este un sprijin administrativ de înalt nivel, cel puțin la nivel de secretar de stat sau la un nivel echivalent în minister, precum și susținerea politică. Pentru

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

a adopta cu succes o strategie SNSC, poate fi luat în considerare următorul proces în cinci etape (a se vedea figura 1):

Prima etapă – **Instituirea principiilor directoare și a obiectivelor strategice care decurg din strategie**

În primul rând, autoritățile naționale competente ar trebui să definească o serie de elemente-cheie care să fie incluse în SNSC, și anume care sunt rezultatele dorite, în formularea directivei [articolul 7 alineatul (1) litera (a)] *„obiective și priorități”*, modul în care aceste rezultate vin în completarea politicilor sociale și economice naționale și sunt compatibile cu drepturile și obligațiile care îi revin în calitate de stat membru al Uniunii Europene. Obiectivele ar trebui să fie specifice, măsurabile, abordabile, relevante și încadrate în timp (SMART). Un exemplu ilustrativ este următorul: *„Ne vom asigura că această strategie [încadrată în timp] se întemeiază pe o serie riguroasă și cuprinzătoare de indicatori pe baza cărora măsurăm progresele înregistrate în direcția rezultatelor pe care trebuie să le realizăm.”*[5]

Aceasta cuprinde, de asemenea, o evaluare politică menită să stabilească dacă se poate obține un buget semnificativ pentru a finanța punerea în aplicare a strategiei. Aceasta implică, de asemenea, o descriere a domeniului de aplicare preconizat al strategiei și a diverselor categorii de părți interesate din sectorul public și din cel privat care ar trebui să fie implicate în procesul de elaborare a diferitelor obiective și măsuri.

Această primă etapă ar putea fi realizată prin intermediul unor ateliere de lucru specializate cu participarea unor înalți funcționari din cadrul ministerelor și politicieni, moderate de specialiști în domeniul cibernetic cu competențe de comunicare profesională care pot evidenția implicațiile unei securități cibernetice slabe sau inexistente pentru o economie și o societate digitală modernă.

A doua etapă - **Elaborarea conținutului strategiei**

Strategia ar trebui să cuprindă măsuri de sprijin, acțiuni încadrate în timp și indicatori-cheie de performanță pentru evaluarea rezultatelor, rafinare și îmbunătățire după o perioadă definită de punere în aplicare. Aceste măsuri ar trebui să sprijine obiectivele, prioritățile și rezultatele stabilite ca principii directoare. Necesitatea de a include măsuri de sprijin este prevăzută la articolul 7 alineatul (1) litera (c) din Directiva NIS.

Se recomandă instituirea unui grup de coordonare prezidat de ministerul de resort pentru a gestiona procesul de elaborare și pentru a facilita furnizarea de contribuții. Acest lucru ar putea fi realizat prin intermediul unei serii de grupuri de redactare formate din funcționari și experți în materie în jurul unor teme-cheie generice, de exemplu evaluarea riscurilor, planificarea pentru situații de urgență, gestionarea incidentelor, dezvoltarea competențelor, sensibilizarea, cercetarea și dezvoltarea industrială etc. Separat, fiecare sector (de exemplu,

[5] Extras din Strategia națională a Regatului Unit privind securitatea cibernetică pentru perioada 2016-2021, pagina 67.

energie, transport etc.) ar fi invitat, de asemenea, să evalueze implicațiile includerii lor, inclusiv alocarea resurselor, și să implice operatorii de servicii esențiale desemnați și furnizorii de servicii digitale fundamentale desemnați în determinarea priorităților și în prezentarea de propuneri de redactare. Implicarea actorilor sectoriali este esențială, ținând seama și de necesitatea de a asigura o punere în aplicare armonizată a directivei în cadrul diferitelor sectoare, permițând în același timp specificitatea sectorială.

A treia etapă – **Elaborarea unui cadru de guvernanță**

Pentru a fi eficient și eficace, cadrul de guvernanță ar trebui să se bazeze pe principalele părți interesate, pe prioritățile identificate în cadrul procesului de redactare și pe constrângerile și contextul structurilor politice și administrative naționale. Ar fi de dorit să existe o raportare directă la nivel politic, cadrul având o capacitate de luare a deciziilor și de alocare a resurselor, precum și contribuții din partea experților în materie de securitate cibernetică și a părților interesate din sector. Articolul 7 alineatul (1) litera (b) din Directiva NIS face referire la cadrul de guvernanță și impune în mod expres *„responsabilitățile organismelor guvernamentale și ale altor actori relevanți”*.

A patra etapă - **Compilarea și revizuirea proiectului de strategie**

În această etapă, proiectul de strategie ar trebui să fie elaborat și analizat prin utilizarea analizei punctelor forte, a punctelor slabe, a oportunităților și a amenințărilor (SWOT), care ar putea să stabilească dacă ar fi necesară o revizuire a conținutului. În urma analizei interne, ar trebui să aibă loc o consultare cu părțile interesate. Ar fi esențial să se efectueze, de asemenea, o consultare publică pentru a evidenția importanța strategiei propuse pentru public, pentru a primi informații din toate sursele posibile și pentru a solicita sprijin pentru alocarea resurselor necesare în vederea punerii în aplicare ulterioare a strategiei.

A cincea etapă – **Adoptarea formală**

Această etapă finală implică adoptarea formală la nivel politic, cu un buget de sprijin care să reflecte seriozitatea cu care statul membru în cauză abordează securitatea cibernetică. Pentru realizarea obiectivelor Directivei NIS și în comunicarea documentului de strategie națională către Comisie, în temeiul articolului 7 alineatul (3), Comisia încurajează statele membre să furnizeze informații cu privire la buget. Angajamentele privind bugetul și resursele umane necesare sunt absolut esențiale pentru punerea în aplicare eficace a strategiei și a directivei. Întrucât securitatea cibernetică este încă un domeniu de politică publică relativ nou și care se extinde rapid, în majoritatea cazurilor sunt necesare investiții noi, chiar dacă situația globală a finanțelor publice impune reduceri și economii.

Recomandări cu privire la procesul și conținutul strategiilor naționale sunt oferite de diverse surse publice și academice, de exemplu ENISA[6], UIT[7], OCDE[8], Forumul global pentru expertiză informatică și Universitatea Oxford[9].

2.4. Măsurile concrete pe care statele membre trebuie să le întreprindă înainte de expirarea termenului de transpunere

Înainte de adoptarea directivei, aproape toate statele membre[10] au publicat deja documente indicate ca SNSC. Secțiunea 6 din prezenta anexă conține strategiile care sunt în prezent în vigoare în fiecare stat membru[11]. Acestea includ, de regulă, principii strategice, orientări, obiective și, în unele cazuri, măsuri specifice pentru atenuarea riscurilor legate de securitatea cibernetică.

Având în vedere că unele dintre respectivele strategii au fost adoptate înainte de adoptarea Directivei NIS, este posibil ca acestea să nu conțină în mod necesar toate elementele prevăzute la articolul 7. Pentru a asigura transpunerea corectă, statele membre vor trebui să realizeze o analiză a lacunelor prin raportarea conținutului propriei SNSC la cele șapte cerințe diferite enumerate la articolul 7 în privința domeniului de aplicare al sectoarelor menționate în anexa II și al serviciilor menționate în anexa III la directivă. Lacunele identificate pot fi abordate ulterior prin intermediul unei revizuiri a SNSC existente sau printr-o decizie de revizuire completă, de la zero, a principiilor strategiei lor naționale privind NIS. Orientările furnizate mai sus cu privire la procesul de adoptare a SNSC sunt relevante și pentru revizuirea și actualizarea unei SNSC existente.

---

[6] ENISA, *National Cyber-Security Strategy Good Practice* („Bune practici referitoare la strategia națională privind securitatea cibernetică") (2016). Document disponibil la adresa https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] UIT, *National Cybersecurity Strategy Guide* („Ghidul privind strategia națională de securitate cibernetică") (2011). Disponibil la adresa http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
În 2017, UIT va publica, de asemenea, un set de instrumente pentru strategia națională de securitate cibernetică (a se vedea prezentarea la adresa http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

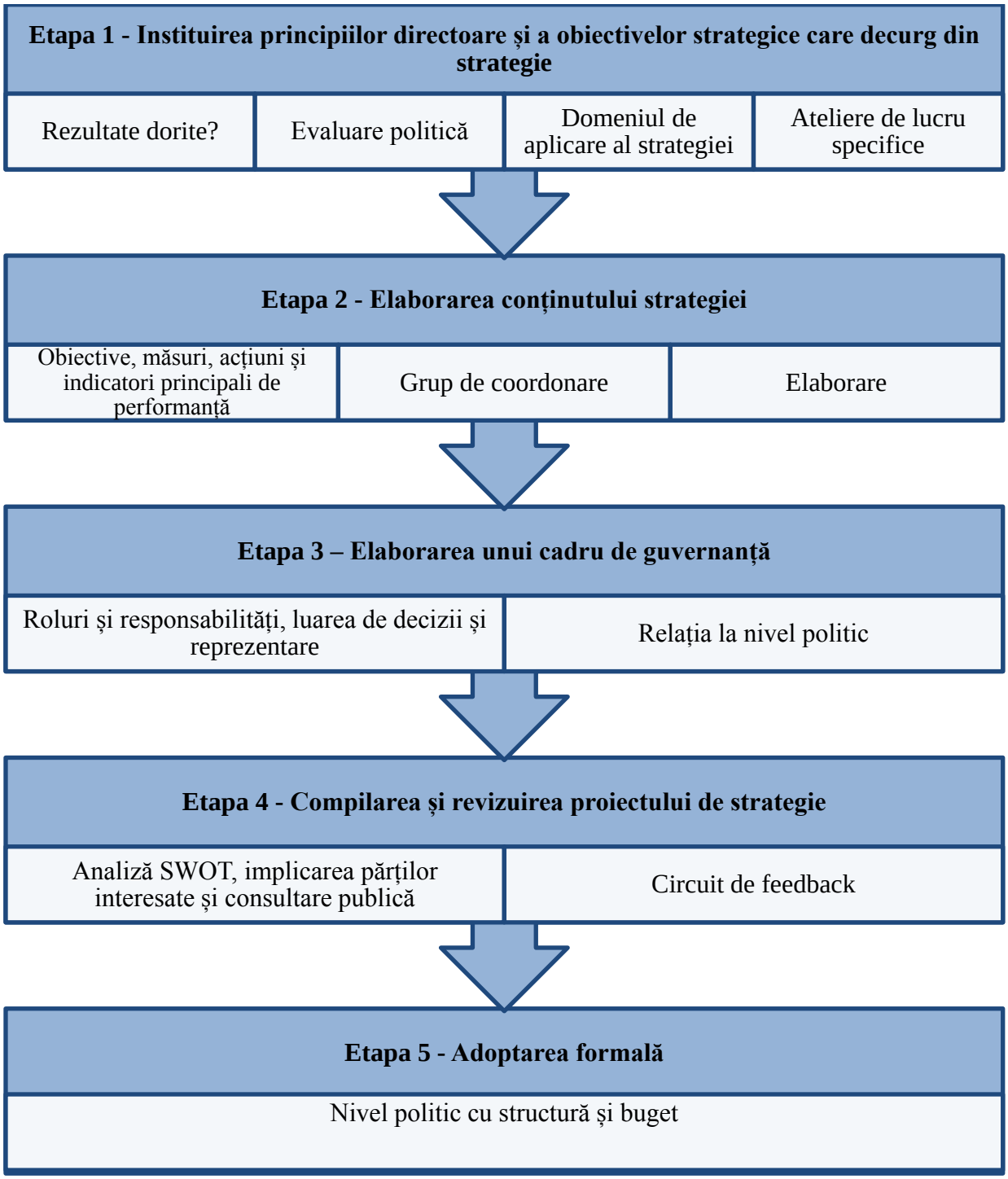
[8] OCDE, *Cybersecurity Policy Making at a Turning Point:Analysing a New Generation of National Cybersecurity Strategies* („Elaborarea de politici de securitate cibernetică, într-un moment de cotitură: analiza unei noi generații de strategii naționale de securitate cibernetică") (2012). Document disponibil la adresa: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Global Cyber Security Capacity Centre și Universitatea Oxford, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* („Model de maturitate a capacității de securitate cibernetică pentru națiuni - Ediție revizuită") (2016). Document disponibil la adresa: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] În afară de Grecia, unde o strategie națională de securitate cibernetică este în curs de elaborare din 2014 (a se vedea https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Aceste informații se bazează pe prezentarea generală a SNSC furnizată de ENISA la adresa https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Figura 1: Cele 5 etape ale procesului de adoptare a SNSC



3. Directiva NIS: autoritățile naționale competente, punctele unice de contact și echipele de intervenție în caz de incidente de securitate informatică (CSIRT)

În temeiul articolului 8 alineatul (1), statele membre au obligația de a desemna una sau mai multe autorități naționale competente, care acoperă cel puțin sectoarele menționate în anexa II și serviciile menționate în anexa III la directivă, cu sarcina de a monitoriza aplicarea directivei. Statele membre pot atribui acest rol uneia sau mai multor autorități existente.

Secțiunea se concentrează asupra modului în care Directiva NIS îmbunătățește nivelul de pregătire al statelor membre prin impunerea obligației de a avea autorități naționale competente eficace și echipe de intervenție în caz de incidente de securitate informatică (CSIRT) eficace. Mai precis, secțiunea abordează obligația de a desemna autoritățile competente naționale, inclusiv rolul punctului unic de contact. Sunt discutate trei teme: (a) posibile structuri naționale de guvernanță (de exemplu, modele centralizate, descentralizate etc.) și alte cerințe, (b) rolul punctului unic de contact și (c) echipe de intervenție în caz de incidente de securitate informatică.

3.1. Tipul de autorități

Articolul 8 din Directiva NIS impune statelor membre obligația de a desemna autorități competente la nivel național privind securitatea rețelelor și a sistemelor informatice, recunoscând, în același timp, în mod explicit posibilitatea de a desemna *„una sau mai multe autorități competente la nivel național”*. Considerentul 30 din directivă explică această opțiune în materie de politică: *„Având în vedere diferențele dintre structurile naționale de guvernanță și pentru a salvgarda acordurile sectoriale sau organismele de supraveghere și de reglementare ale Uniunii deja existente și a evita suprapunerile, statele membre ar trebui să fie capabile să desemneze mai multe autorități naționale competente responsabile cu îndeplinirea atribuțiilor legate de securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale în temeiul prezentei directive”*.

În consecință, statele membre au libertatea de a alege să desemneze o autoritate centrală care să se ocupe de toate sectoarele și serviciile reglementate de directivă sau mai multe autorități, de exemplu în funcție de tipul de sector.

Atunci când decid cu privire la abordare, statele membre se pot baza pe experiența dobândită în urma abordărilor naționale utilizate în contextul legislației existente privind protecția infrastructurilor critice de informații (*Critical Information Infrastructure Protection*, CIIP). Așa cum se arată în tabelul 1, în cazul CIIP, statele membre au decis să adopte o abordare fie centralizată, fie descentralizată în atribuirea competențelor la nivel național. Exemplele naționale sunt utilizate în acest caz numai cu titlu informativ și pentru a aduce în atenția statelor membre cadrele organizatorice existente. Prin urmare, Comisia nu sugerează faptul că modelul utilizat de respectivele țări pentru CIIP ar trebui să fie utilizat în mod necesar în scopul transpunerii Directivei NIS.

Statele membre pot, de asemenea, să opteze pentru diverse mecanisme hibride, care includ elemente atât ale abordărilor centralizate, cât și ale celor descentralizate. Se poate opta pentru alinierea la mecanismele naționale anterioare de guvernanță pentru diversele sectoare și servicii acoperite de directivă sau recent stabilite de autoritățile în cauză, de părțile interesate relevante identificate drept operatori de servicii esențiale și de furnizorii de servicii digitale. Existența cunoștințelor de specialitate privind securitatea cibernetică, considerațiile în materie de finanțare, relațiile dintre părțile interesate și interesele naționale (de exemplu, dezvoltarea economică, siguranța publică etc.) pot fi, de asemenea, factori importanți care să determine opțiunile statelor membre.

3.2 Publicitate și alte aspecte suplimentare relevante

În temeiul articolului 8 alineatul (7), statele membre trebuie să informeze Comisia cu privire la desemnarea autorităților competente și la atribuțiile acestora. Această informare trebuie să fie efectuată până la expirarea termenului de transpunere.

Articolele 15 și 17 din Directiva NIS impune statelor membre obligația de a se asigura că autoritățile competente dispun de competențele și mijloacele specifice pentru îndeplinirea sarcinilor prevăzute la respectivele articole.

În plus, desemnarea unor entități specifice în calitate de autorități naționale competente trebuie să fie făcută publică. Directiva nu precizează modul în care trebuie să se desfășoare această anunțare publică. Dat fiind faptul că obiectivul acestei cerințe este de a atinge un nivel ridicat de sensibilizare în rândul actorilor vizați de NIS și al publicului larg și pe baza experienței din alte sectoare (sectorul telecomunicațiilor, sectorul bancar, sectorul medicamentelor), Comisia consideră că acest lucru ar putea fi realizat, de exemplu, prin intermediul unui portal larg mediatizat.

Articolul 8 alineatul (5) din Directiva NIS prevede obligația ca aceste autorități să dispună de „resurse adecvate” pentru a-și îndeplini atribuțiile încredințate de directivă.

Tabelul 1: Abordări naționale privind protecția infrastructurilor critice de informații (CIIP)

În 2016, ENISA a publicat un studiu[12] cu privire la diferitele abordări pe care statele membre le urmează pentru a-și proteja infrastructurile critice de informații. Sunt prezentate două profiluri în ceea ce privește guvernanța CIIP în statele membre care pot fi utilizate în contextul transpunerii Directivei NIS.

Profilul 1: Abordare descentralizată – multiple autorități sectoriale competente pentru sectoarele și serviciile specifice menționate în anexele II și III la directivă

Abordarea descentralizată se caracterizează prin:

(i) principiul subsidiarității;
(ii) cooperare strânsă între agențiile publice;
(iii)legislație sectorială

Principiul subsidiarității

În loc să stabilească sau să desemneze o singură agenție cu responsabilitate generală, abordarea descentralizată urmează principiul subsidiarității. Aceasta înseamnă că responsabilitatea pentru punerea în aplicare aparține autorităților sectoriale, care înțeleg cel mai bine sectorul local și au deja o relație stabilită cu părțile interesate. În temeiul acestui principiu, deciziile sunt luate de instituțiile aflate cel mai aproape de părțile afectate.

Cooperare strânsă între agențiile publice

Ca urmare a gamei variate de agenții publice implicate în CIIP, multe state membre au dezvoltat scheme de cooperare pentru a coordona activitatea și eforturile depuse de diferitele autorități. Aceste scheme de cooperare pot lua forma unor rețele informale sau a unor foruri sau acorduri mai instituționalizate. Cu toate acestea, schemele de cooperare sunt folosite numai în scopul schimbului de informații și a coordonării între diferitele agenții publice, neavând autoritate asupra acestora.

Legislație sectorială

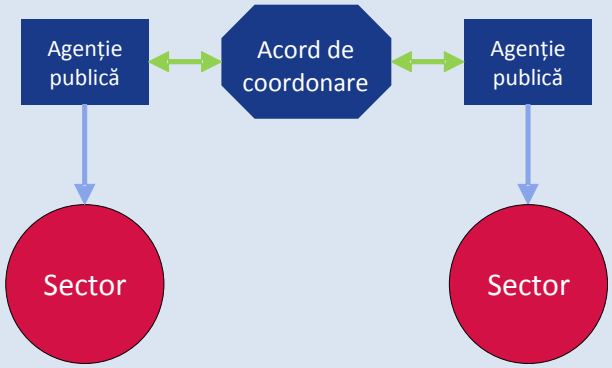
Țările care urmează abordarea descentralizată în sectoarele critice se abțin adesea să legifereze în scopul CIIP. În schimb, adoptarea legilor și a reglementărilor rămâne sectorială și, prin urmare, poate varia în mod semnificativ de la un sector la altul. Această abordare ar avea avantajul alinierii măsurilor legate de NIS la reglementările sectoriale existente pentru a îmbunătăți atât acceptarea de către sector, cât și eficacitatea asigurării respectării legislației de către autoritatea în cauză.

Există un risc substanțial de coerență redusă în ceea ce privește aplicarea directivei la nivelul

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* („Evaluare, analiză și recomandări privind protecția infrastructurilor critice de informații") (2016). Document disponibil la adresa: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

mai multor sectoare și servicii în cazul unei abordări pur descentralizate. În acest caz, directiva prevede un punct unic de contact la nivel național pentru asigurarea legăturii cu privire la chestiuni transfrontaliere, iar această entitate ar putea, de asemenea, să fie însărcinată de statul membru în cauză cu coordonarea internă și cooperarea între multiplele autorități naționale competente, în conformitate cu articolul 10 din directivă.

Figura 2 – Abordare descentralizată



Exemple de abordare descentralizată.

Suedia este un bun exemplu de țară care urmează o abordare descentralizată în materie de CIIP. Această țara utilizează „o perspectivă sistemică", ceea ce înseamnă că sarcinile principale ale CIIP, cum ar fi identificarea serviciilor vitale și a infrastructurilor critice, coordonarea și sprijinul acordat operatorilor, sarcinile de reglementare, precum și măsurile de pregătire pentru situații de urgență sunt în responsabilitatea diferitelor agenții și municipalități. Printre aceste agenții se numără Agenția pentru Urgențe în Materie Civilă din Suedia (MSB), Agenția de Servicii Poștale și Telecomunicații din Suedia (PTS) și mai multe agenții suedeze din sectorul apărării, militar și de asigurare a respectării legii.

În vederea coordonării acțiunilor între diferitele agenții și entități publice, guvernul suedez a creat o rețea de cooperare alcătuită din autorități „cu responsabilități specifice în materie de securitate a informațiilor societale". Acest Grup de cooperare pentru securitatea informațiilor (SAMFI) este format din reprezentanți ai diferitelor autorități și se reunește de mai multe ori pe an pentru a discuta chestiuni legate de securitatea informațiilor la nivel național. Domeniile tematice ale SAMFI se regăsesc în principal în sectoarele politico-strategice și vizează subiecte cum ar fi aspectele tehnice și standardizarea, evoluțiile naționale și internaționale în domeniul securității informațiilor sau gestionarea și prevenirea incidentelor informatice. [Agenția pentru Urgențe în Materie Civilă din Suedia (MSB) 2015].

Suedia nu a publicat o lege centrală în privința CIIP care să fie aplicabilă operatorilor de infrastructuri critice de informații (CII) din toate sectoarele. În schimb, emiterea de acte legislative care să prevadă obligații pentru întreprinderile din sectoare specifice este

responsabilitatea respectivelor autorități publice. De exemplu, MSB are dreptul să emită reglementări pentru autoritățile guvernamentale în domeniul securității informațiilor, în timp ce PTS poate solicita operatorilor să pună în aplicare anumite măsuri tehnice sau organizatorice de securitate pe baza legislației secundare.

Un alt exemplu de țară care prezintă caracteristicile acestui profil este Irlanda. Irlanda urmează o „doctrină a subsidiarității", conform căreia fiecare minister este responsabil de identificarea CII și evaluarea riscurilor din sectorul său. În plus, nu au fost adoptate reglementări specifice pentru CIIP la nivel național. Legislația rămâne sectorială și există în special pentru sectorul energiei și telecomunicațiilor (2015). Alte exemple sunt Austria, Cipru și Finlanda.

Profilul 2: Abordarea centralizată – o autoritate centrală competentă pentru toate sectoarele și serviciile menționate în anexele II și III la directivă

Abordarea centralizată se caracterizează prin:

i) existența unei autorități centrale pentru toate sectoarele;
ii) legislație cuprinzătoare

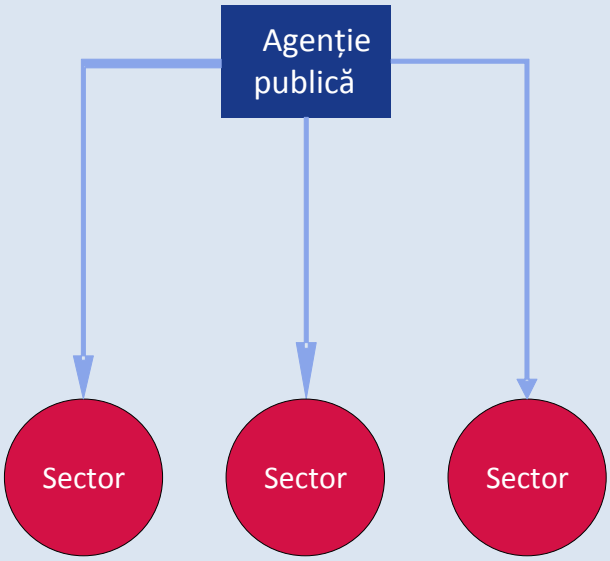
Autoritate centrală pentru toate sectoarele

Statele membre care urmează o abordare centralizată au instituit autorități cu responsabilități și competențe largi în mai multe sectoare critice sau în toate aceste sectoare sau au extins competențele autorităților existente. Aceste autorități principale în materie de CIIP combină mai multe sarcini, cum ar fi planificarea pentru situații de urgență, gestionarea situațiilor de urgență, sarcinile de reglementare și sprijinirea operatorilor privați. În multe cazuri, echipa CSIRT națională sau guvernamentală face parte din autoritatea principală în materie de CIIP. O autoritate centrală este probabil să reunească un nivel mai ridicat al expertizei în domeniul securității cibernetice decât autoritățile sectoriale multiple, dat fiind nivelul general insuficient de competențe în materie de securitate cibernetică.

Legislație cuprinzătoare

O legislație cuprinzătoare creează obligații și cerințe pentru toți operatorii CII din toate sectoarele. Acest lucru poate fi realizat prin noi legi cuprinzătoare sau prin completarea reglementărilor sectoriale existente. Această abordare ar facilita o aplicare coerentă a Directivei NIS la nivelul tuturor sectoarelor și a serviciilor acoperite. S-ar evita riscul unor lacune în materie de punere în aplicare care ar putea apărea în cazul mai multor autorități cu competențe specifice.

Figura 3 – Abordarea centralizată



Exemple de abordare centralizată

Franța este un bun exemplu de stat membru al UE cu o abordare centralizată. În 2011, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) din Franța a fost declarată principala autoritate națională pentru apărarea sistemelor informatice. ANSSI îndeplinește un puternic rol de supraveghere pentru „operatorii de importanță vitală" (OIV): agenția poate dispune ca OIV să respecte măsurile de securitate și este autorizată să efectueze audituri de securitate asupra acestora. În plus, ANSSI este principalul punct unic de contact pentru OIV, care au obligația să raporteze agenției incidentele de securitate.

În caz de incidente de securitate, ANSSI acționează ca agenție de intervenție în materie de CIIP și decide cu privire la măsurile pe care operatorii trebuie să le ia pentru a răspunde crizei. Acțiunile guvernului sunt coordonate în cadrul centrului de operațiuni al ANSSI. Identificarea amenințărilor și reacția în caz de incidente la nivel operațional este asigurată de CERT-FR, care face parte din ANSSI.

Franța a creat un cadru juridic cuprinzător pentru CIIP. În 2006, prim-ministrul a dispus întocmirea unei liste a sectoarelor de infrastructură critică. Pe baza acestei liste, care a identificat douăsprezece sectoare vitale, guvernul a definit circa 250 de OIV. În 2013, a fost promulgată Legea privind programarea militară (LPM)[13]. Aceasta stabilește diferite obligații pentru OIV, cum ar fi raportarea incidentelor sau punerea în aplicare a măsurilor de securitate. Aceste cerințe sunt obligatorii pentru toate OIV din toate sectoarele (Senatul francez, 2013).

[13] La loi de programmation militaire.

3.3. Articolul 9 din Directiva NIS: echipe de intervenție în caz de incidente de securitate informatică (CSIRT)

În temeiul articolului 9, statele membre au obligația de a desemna una sau mai multe echipe CSIRT însărcinate cu gestionarea riscurilor și a incidentelor pentru sectoarele enumerate în anexa II la Directiva NIS și pentru serviciile menționate în anexa III. Ținând seama de cerința de armonizare minimă prevăzută la articolul 3 din directivă, statele membre au libertatea de a folosi echipele CSIRT și pentru alte sectoare care nu sunt acoperite de directivă, cum ar fi administrația publică.

Statele membre pot opta pentru înființarea unei echipe CSIRT în cadrul autorității naționale competente[14].

3.4. Atribuții și cerințe

Atribuțiile echipelor CSIRT desemnate, stabilite în anexa I la Directiva NIS, includ următoarele:

- monitorizarea incidentelor la nivel național;
- asigurarea de avertizări timpurii, alerte, anunțuri și diseminarea de informații privind riscurile și incidentele pentru părțile interesate relevante;
- răspunsul la incidente;
- furnizarea de analize dinamice de risc și de incident și sensibilizare situațională și
- participarea la rețeaua de echipe CSIRT naționale (rețeaua CSIRT) instituită în temeiul articolului 12.

Atribuții suplimentare specifice sunt prevăzute la articolul 14 alineatele (3), (5) și (6) și la articolul 16 alineatele (3), (6) și (7) cu privire la notificările incidentelor în cazul în care un stat membru decide că echipele CSIRT, în plus față de autoritățile naționale competente sau în locul acestora, își pot asuma aceste roluri.

În transpunerea directivei, statele membre au la dispoziție diverse opțiuni pentru rolul echipelor CSIRT în ceea ce privește cerințele de notificare a incidentelor. Este posibilă raportarea obligatorie directă către CSIRT, cu avantajele eficienței administrative; în mod alternativ, statele membre pot opta pentru raportarea directă către autoritățile naționale competente, echipele CSIRT având drept de acces la informațiile raportate. Echipele CSIRT sunt interesate, în ultimă instanță, de soluționarea problemelor în ceea ce privește descurajarea, detectarea și răspunsul la incidente cibernetice și atenuarea impactului acestora (inclusiv a celor care nu sunt esențiale pentru raportarea obligatorie) împreună cu părțile interesate, în timp ce respectarea reglementărilor este o chestiune de care răspund autoritățile naționale competente.

În temeiul articolului 9 alineatul (3) din directivă, statele membre trebuie să se asigure, de asemenea, că aceste echipe CSIRT au acces la o infrastructură TIC sigură și reziliență.

[14] A se vedea articolul 9 alineatul (1) ultima teză.

Articolul 9 alineatul (4) din directivă impune statelor membre obligația de a informa Comisia cu privire la misiunea și principalele elemente ale procedurilor de administrare a incidentelor folosite de echipele CSIRT desemnate.

Cerințele aplicabile echipelor CSIRT desemnate de statele membre sunt prevăzute în anexa I la Directiva NIS. O echipă CSIRT trebuie să asigure o disponibilitate ridicată a serviciilor sale de comunicații. Localurile sale și sistemele informatice de suport sunt situate în amplasamente securizate și garantează continuitatea activităților. În plus, CSIRT ar trebui să aibă posibilitatea să participe la rețele internaționale de cooperare.

3.5. Asistență pentru dezvoltarea CSIRT

Programul Mecanismului pentru interconectarea Europei (MIE) referitor la infrastructurile de servicii digitale pentru securitatea cibernetică (ISD) poate să furnizeze o finanțare semnificativă din partea UE în sprijinul echipelor CSIRT ale statelor membre în vederea îmbunătățirii capacităților și a cooperării acestora prin intermediul unui mecanism de cooperare în materie de schimb de informații. Mecanismul de cooperare în curs de elaborare în cadrul proiectului SMART 2015/1089 este destinat să faciliteze cooperarea operațională rapidă și eficace pe bază voluntară între echipele CSIRT ale statelor membre, și anume în sprijinul sarcinilor atribuite rețelei CSIRT în temeiul articolului 12 din directivă.

Detalii privind cererile de propuneri relevante pentru consolidarea capacităților echipelor CSIRT ale statelor membre sunt disponibile pe site-ul web al Agenției Executive pentru Inovare și Rețele (INEA) a Comisiei Europene[15].

Consiliul de guvernanță ISD pentru securitatea cibernetică a MIE oferă o structură informală pentru furnizarea de orientări și de asistență la nivel de politică echipelor CSIRT ale statelor membre în vederea consolidării capacităților și pentru punerea în aplicare a mecanismului de cooperare voluntară.

O CSIRT nou-înființată sau una desemnată să îndeplinească atribuțiile prevăzute în anexa I la Directiva NIS se poate baza pe consultanța și expertiza ENISA pentru a-și îmbunătăți performanțele și a-și îndeplini cu eficacitate activitatea[16]. În acest sens, este util de subliniat faptul că echipele CSIRT ale statelor membre ar putea lua ca referință unele dintre activitățile efectuate recent de ENISA. În special, astfel cum se menționează în secțiunea 7 din prezenta anexă, agenția a emis o serie de documente și studii care descriu bune practici, recomandări la nivel tehnic, cuprinzând evaluări ale nivelului de maturitate a echipei CSIRT, pentru diversele capacități și servicii ale echipei CSIRT. În plus, rețelele de echipe CSIRT au făcut, de asemenea, schimb de orientări și bune practici atât la nivel mondial (FIRST[17]), cât și la nivel european (Trusted Introducer, TI[18]).

[15] Informații disponibile la adresa: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] A se vedea articolul 9 alineatul (5) din Directiva NIS.
[17] Forumul echipelor de securitate și de intervenție în caz de incidente (https://www.first.org/)
[18] https://www.trusted-introducer.org/

3.6. Rolul punctului unic de contact

În temeiul articolului 8 alineatul (3) din Directiva NIS, fiecare stat membru trebuie să desemneze un punct unic de contact național, care va exercita o funcție de legătură pentru asigurarea cooperării transfrontaliere cu autoritățile relevante din alte state membre, precum și cu Grupul de cooperare și cu rețeaua CSIRT[19], instituite chiar de directivă. Considerentul 31 și articolul 8 alineatul (4) explică motivul care a stat la baza acestei cerințe, și anume facilitarea cooperării și a comunicării transfrontaliere. Acest lucru este deosebit de necesar, având în vedere faptul că statele membre pot decide să aibă mai mult de o autoritate națională. Astfel, existența unui punct unic de contact ar facilita identificarea și cooperarea autorităților din diferite state membre.

Rolul de legătură al punctului unic de contact este probabil să implice o interacțiune cu secretariatul Grupului de cooperare și cu cel al rețelei CSIRT în cazurile în care punctul unic de contact național nu este nici o echipă CSIRT, nici un membru al Grupului de cooperare. În plus, statele membre trebuie să se asigure că punctul unic de contact este informat cu privire la notificările primite din partea operatorilor de servicii esențiale și a furnizorilor de servicii digitale.[20]

Articolul 8 alineatul (3) din directivă prevede că, în cazul în care un stat membru adoptă o abordare centralizată, și anume desemnează o singură autoritate competentă, autoritatea respectivă va avea, de asemenea, rolul de punct unic de contact. În cazul în care un stat membru optează pentru o abordare descentralizată, acesta ar putea să aleagă una dintre diferitele autorități competente care să acționeze ca punct unic de contact. Indiferent de modelul instituțional ales, ori de câte ori o autoritate competentă, echipa CSIRT și punctul unic de contact sunt entități diferite, statele membre au obligația de a asigura o cooperare eficace între acestea în vederea îndeplinirii obligațiilor prevăzute în directivă[21].

Până la 9 august 2018 și, ulterior, în fiecare an, punctul unic de contact trebuie să prezinte Grupului de cooperare un raport de sinteză privind notificările primite, care include numărul de notificări și natura incidentelor și măsurile luate de autorități, cum ar fi informarea altor state membre afectate cu privire la incident sau furnizarea de informații relevante întreprinderii care a efectuat notificarea, pentru administrarea incidentului[22]. La cererea autorității competente sau a echipei CSIRT, punctul unic de contact are sarcina de a transmite notificările din partea operatorilor de servicii esențiale către punctele unice de contact din alte state membre afectate de incidentele respective[23].

Statele membre trebuie să informeze Comisia cu privire la desemnarea punctului unic de contact și la sarcinile acestuia până la expirarea termenului de transpunere. Desemnarea

[19] O rețea de echipe CSIRT naționale pentru cooperarea operațională dintre statele membre prevăzută la articolul 12.
[20] A se vedea articolul 10 alineatul (3).
[21] A se vedea articolul 10 alineatul (1).
[22] *Idem*.
[23] A se vedea articolul 14 alineatul (5).

punctului unic de contact trebuie să fie făcută publică, la fel ca în cazul autorităților naționale competente. Comisia publică lista punctelor unice de contact desemnate.

3.7. Sancțiuni

Articolul 21 conferă statelor membre o anumită marjă pentru a decide cu privire la tipul și natura sancțiunilor aplicabile, cu condiția ca acestea să fie eficace, proporționale și disuasive. Cu alte cuvinte, statele membre sunt, în principiu, libere să decidă cu privire la cuantumul maxim al sancțiunilor prevăzute în legislația lor națională, dar cuantumul sau procentul ales ar trebui să permită autorităților naționale să impună, în fiecare caz concret, sancțiuni eficace, proporționale și disuasive, luând în considerare diferiți factori precum gravitatea sau frecvența încălcării.

4. Entități care fac obiectul obligațiilor referitoare la cerințele de securitate și de notificare a incidentelor

Entitățile care îndeplinesc un rol important pentru societate și economie menționate la articolul 4 alineatele (4) și (5) din directivă ca operatori de servicii esențiale (OES) și furnizorii de servicii digitale (DSP) au obligația de a adopta măsuri de securitate adecvate și de a notifica incidentele grave autorităților naționale competente. Motivul care a stat la baza acestei cerințe este acela că impactul incidentelor de securitate în cazul unor astfel de servicii poate constitui o amenințare majoră pentru operarea lor care ar putea cauza perturbări majore ale activităților economice și pentru societate în general, care ar putea să submineze încrederea utilizatorilor și să provoace pagube majore economiei Uniunii[24].

Această secțiune prezintă o imagine de ansamblu asupra entităților care sunt incluse în domeniul de aplicare al anexelor II și III la Directiva NIS și enumeră obligațiile care le revin. Identificarea operatorilor de servicii esențiale este acoperită în mod extensiv, având în vedere importanța acestui proces pentru punerea în aplicare armonizată a Directivei NIS în întreaga UE. Aceasta oferă, de asemenea, explicații detaliate pentru definițiile infrastructurilor digitale și ale furnizorilor de servicii digitale. Această secțiune analizează, de asemenea, posibilitatea de a introduce noi sectoare și precizează în continuare abordarea specifică în ceea ce privește furnizorii de servicii digitale.

4.1. Operatorii de servicii esențiale (OES)

Directiva NIS nu definește în mod explicit entitățile specifice care vor fi considerate OES incluse în domeniul său de aplicare. În schimb, aceasta prevede criteriile pe care statele membre vor trebui să le aplice pentru a efectua un proces de identificare care va decide în ultimă instanță ce societăți aparținând tipurilor de entități enumerate în anexa II vor fi considerate operatori de servicii esențiale și, prin urmare, vor face obiectul obligațiilor prevăzute de directivă.

[24] A se vedea considerentul 2.

4.1.1. Tipul de entități enumerate în anexa II la Directiva NIS

Articolul 4 alineatul (4) definește OES ca entități publice sau private de tipul celor enumerate în anexa II din directivă, care îndeplinesc cerințele de la articolul 5 alineatul (2). În anexa II sunt enumerate sectoarele, subsectoarele și tipurile de entități pentru care fiecare stat membru trebuie să efectueze procesul de identificare prevăzut la articolul 5 alineatul (2)[25]. Printre aceste sectoare se numără energia, transporturile, sectorul bancar, infrastructurile pieței financiare, sănătatea, apa și infrastructura digitală.

Pentru cele mai multe dintre entitățile care fac parte din „sectoarele tradiționale", legislația UE conține definiții bine elaborate la care anexa II face trimitere. Acest lucru nu este însă valabil pentru sectorul de infrastructură digitală, menționat la punctul 7 din anexa II, inclusiv IXP (Internet Exchange Points), DNS (Domain Name Systems) și registrele de nume de domenii Top-level. Prin urmare, în scopul de a clarifica aceste definiții, în cele ce urmează se furnizează o explicație detaliată a definițiilor respective.

1) Internet Exchange Point (IXP)

Termenul „Internet Exchange Point" este definit la articolul 4 alineatul (13) și este clarificat în continuare în considerentul 18, putând fi descris ca o facilitate de rețea care permite interconectarea a mai mult de două sisteme independente autonome din punct de vedere tehnic, în primul rând în scopul facilitării schimbului de trafic de internet. Internet Exchange Point poate fi descris, de asemenea, ca o locație fizică în care o serie de rețele pot face schimb de trafic de internet prin intermediul unui comutator. Scopul principal al unui IXP este de a permite rețelelor să se interconecteze în mod direct, prin intermediul schimbului, mai degrabă decât prin intermediul uneia sau mai multor rețele terțe. Furnizorul de IXP nu este responsabil în mod normal pentru rutarea traficului pe internet. Rutarea traficului este efectuată de furnizorii de rețele. Avantajele interconectării directe sunt numeroase, dar principalele motive sunt costul, timpul de așteptare și lățimea de bandă. Traficul care trece printr-un schimb nu este facturat în mod normal de niciuna dintre părțile implicate, fiind facturat traficul către un furnizor de servicii de internet (ISP) din amonte. Interconectarea directă, situată adesea în același oraș ca ambele rețele, evită necesitatea ca datele să parcurgă distanțe lungi pentru a trece de la o rețea la alta, reducând astfel timpul de așteptare.

Ar trebui remarcat faptul că definiția IXP nu acoperă punctele fizice unde se interconectează doar două rețele fizice (și anume, furnizorii de rețele cum ar fi BASE și PROXIMUS). Prin urmare, în transpunerea directivei, statele membre trebuie să facă diferența între operatorii care facilitează schimbul de trafic de internet agregat între mai mulți operatori de rețea și cei care sunt operatori de rețea unică, care își interconectează fizic rețelele pe baza unui acord de interconectare. În cel din urmă caz, furnizorii de rețele nu sunt acoperiți de definiția de la articolul 4 alineatul (13). O clarificare în acest sens este oferită de considerentul 18, care prevede că IXP nu oferă acces la rețea și nici nu acționează ca furnizor sau transportator de

[25] A se vedea secțiunea 4.1.6. pentru mai multe detalii privind procesul de identificare.

tranzit. Ultima categorie de furnizori o reprezintă întreprinderile care furnizează rețele și/sau servicii publice de comunicații care fac obiectul obligațiilor în materie de securitate și de notificare prevăzute la articolul 13a și 13b din Directiva 2002/21/CE și, prin urmare, aceștia sunt excluși din domeniul de aplicare al Directivei NIS[26].

2) Domain Name System (DNS)

Termenul „domain name system" este definit la articolul 4 alineatul (14) ca *„un sistem de atribuire de nume distribuite ierarhic într-o rețea în care se efectuează căutări de nume de domenii"*. Mai exact, DNS poate fi descris ca un sistem de atribuire de nume distribuite ierarhic pentru calculatoare, servicii sau orice altă resursă conectată la internet care permite încodarea numelor de domenii în adrese IP (*Internet Protocol*). Rolul principal al sistemului este de a traduce numele de domenii atribuite în adrese IP. În acest scop, DNS operează o bază de date și utilizează servere de nume și un rezolver pentru a permite acest tip de „traducere" a numelor de domenii în adrese IP operaționale. Deși codificarea numelor de domeniu nu este singura responsabilitate a DNS, aceasta este o sarcină de bază a sistemului. Definiția juridică de la articolul 4 alineatul (14) se axează pe rolul principal al sistemului din punctul de vedere al utilizatorului, fără a intra în mai multe detalii tehnice precum, de exemplu, operarea spațiului pentru numele de domeniu, serverele de nume, rezolverele etc. În fine, articolul 4 alineatul (15) clarifică cine trebuie să fie considerat furnizor de servicii DNS.

3) Registrul de nume de domenii Top-level (Registrul de nume TLD)

Registrul de nume de domenii Top-level este definit la articolul 4 alineatul (16) ca fiind o entitate care administrează și operează înregistrarea de nume de domenii de internet într-un domeniu Top-level (TLD) specific. O astfel de administrare și gestionare a numelor de domenii include codificarea numelor TLD în adrese IP.

Autoritatea responsabilă cu coordonarea funcțiilor internet (*Internet Assigned Numbers Authority*, IANA) răspunde de coordonarea globală a DNS Root, de adresele de protocol internet și de alte resurse ale protocolului de internet. În special, IANA este responsabilă cu alocarea de domenii Top-level generice (gTLD), de exemplu „.com", și domenii Top-level pentru codul de țară (ccTLD), de exemplu „.be", pentru operatori (registre) și întreținerea detaliilor tehnice și administrative ale acestora. IANA ține un registru global al TLD-urilor alocate și joacă un rol în promulgarea acestei liste de utilizatori ai internetului la nivel mondial, precum și în ceea ce privește introducerea de noi TLD-uri.

Un obiectiv important al registrelor este alocarea de nume de nivelul doi așa-numitelor entități înregistrate sub domeniul lor TLD. Aceste entități înregistrate pot, de asemenea, să aloce pe cont propriu, dacă doresc, nume de domenii de nivelul trei. ccTLD-urile sunt desemnate să reprezinte o țară sau un teritoriu pe baza standardului ISO 3166-1. TLD-urile „generice" nu au, în mod normal, o denumire geografică sau de țară.

[26] A se vedea secțiunea 5.2. pentru mai multe detalii privind relația dintre Directiva NIS și Directiva 2002/21/CE.

Ar trebui remarcat faptul că operarea registrului de nume TLD poate include furnizarea de DNS. De exemplu, în conformitate cu normele de delegare ale IANA, entitatea desemnată care se ocupă cu ccTLD trebuie – printre altele – să controleze numele de domeniu și să opereze DNS-ul țării respective[27]. Statele membre trebuie să țină seama de aceste circumstanțe atunci când efectuează procesul de identificare a operatorilor de servicii esențiale prevăzut la articolul 5 alineatul (2).

4.1.2. Identificarea operatorilor de servicii esențiale

În conformitate cu cerințele articolului 5 din directivă, fiecare stat membru are obligația de a efectua un proces de identificare cu privire la toate entitățile de tipul celor enumerate în anexa II care sunt stabilite legal pe teritoriul respectivului stat membru. Ca urmare a acestei evaluări, toate entitățile care îndeplinesc criteriile stabilite la articolul 5 alineatul (2) sunt identificate ca OES și sunt supuse obligațiilor în materie de securitate și notificare prevăzute la articolul 14.

Statele membre au drept termen data de 9 noiembrie 2018 în vederea identificării operatorilor pentru fiecare sector și subsector. Pentru a sprijini statele membre pe parcursul acestui proces, Grupul de cooperare elaborează în prezent un document de orientare cu informații relevante privind măsurile necesare și bunele practici referitoare la identificarea OES.

În plus, în conformitate cu articolul 24 alineatul (2), Grupul de cooperare urmează să discute procesul, substanța și tipul măsurilor naționale care permit identificarea operatorilor de servicii esențiale în sectoare specifice. Înainte de 9 noiembrie 2018, un stat membru poate solicita să discute proiectul său de măsuri naționale care permit identificarea operatorilor de servicii esențiale în cadrul Grupului de cooperare.

4.1.3. Includerea de noi sectoare

Ținând seama de cerința de armonizare minimă prevăzută la articolul 3, statele membre pot să adopte sau să mențină o legislație care să asigure un nivel mai ridicat de securitate a rețelelor și a sistemelor informatice. În această privință, statele membre sunt în general libere să extindă obligațiile în materie de securitate și notificare prevăzute la articolul 14 la entități aparținând altor sectoare și subsectoare decât cele enumerate în anexa II la Directiva NIS. Mai multe state membre au hotărât, sau analizează în prezent în prezent dacă este oportun, să includă unele dintre următoarele sectoare suplimentare:

i) Administrațiile publice

Administrațiile publice pot oferi servicii esențiale menționate în anexa II la directivă care îndeplinesc cerințele de la articolul 5 alineatul (2). În astfel de cazuri, administrațiile publice care oferă astfel de servicii ar face obiectul cerințelor de securitate și al obligațiilor de notificare relevante. Dimpotrivă, în cazul în care administrațiile publice oferă servicii care nu se încadrează în domeniul de aplicare menționat mai sus, aceste servicii nu ar fi vizate de obligațiile relevante.

Administrațiile publice sunt responsabile de furnizarea corespunzătoare a serviciilor publice prestate de organismele guvernamentale, de autoritățile locale și regionale, de agenții și de

[27] Informații disponibile la adresa: https://www.icann.org/resources/pages/delegation-2012-02-25-en

întreprinderile asociate. Aceste servicii implică adesea crearea și gestionarea de date cu caracter personal și date ale întreprinderilor cu privire la persoane și organizații, care pot fi partajate și puse la dispoziția mai multor entități publice. În sens mai larg, un nivel ridicat de securitate a rețelelor și a sistemelor informatice utilizate de administrațiile publice este de un interes major pentru societate și pentru economie în ansamblu. Prin urmare, Comisia este de opinie că ar fi rezonabil ca statele membre să ia în considerare includerea administrației publice în domeniul de aplicare al legislațiilor naționale de transpunere a directivei, dincolo de furnizarea de servicii esențiale, astfel cum se prevede în anexa II și la articolul 5 alineatul (2).

ii) Sectorul poștal

Sectorul poștal cuprinde prestarea de servicii poștale precum colectarea, sortarea, transportul și distribuirea trimiterilor poștale.

iii) Sectorul alimentar

Sectorul alimentar se referă la fabricarea de produse agricole și alte produse alimentare și ar putea include servicii esențiale, cum ar fi furnizarea de servicii de asigurare a securității alimentare și a calității și a siguranței alimentare.

iv) Industria chimică și nucleară

Industria chimică și nucleară se referă în special la depozitarea, producția și prelucrarea de produse chimice și petrochimice sau de materiale nucleare.

v) Sectorul mediului

Activitățile în materie de mediu includ furnizarea de bunuri și servicii necesare pentru protecția mediului și gestionarea resurselor. Prin urmare, activitățile au ca scop prevenirea, reducerea și eliminarea poluării, precum și conservarea rezervelor de resurse naturale disponibile. În cadrul acestui sector, serviciile esențiale ar putea fi monitorizarea și controlul poluării (de exemplu, poluarea aerului și a apei) și fenomenele meteorologice.

vi) Protecția civilă

Obiectivul sectorului de protecție civilă este prevenirea, pregătirea și răspunsul la dezastre naturale și provocate de om. Serviciile furnizate în acest scop pot fi activarea numerelor de urgență și punerea în aplicare a acțiunilor de informare, limitare și reacție în situații de urgență.

4.1.4. Jurisdicție

În temeiul articolului 5 alineatul (1), fiecare stat membru trebuie să identifice OES-urile care au un sediu pe teritoriul său. Dispoziția nu specifică mai detaliat tipul de stabilire legală, dar considerentul 21 clarifică faptul că un astfel de sediu implică exercitarea efectivă și reală a activității prin acorduri stabile, în timp ce forma juridică a acestor acorduri nu ar trebui să fie un factor determinant. Aceasta înseamnă că un stat membru poate avea jurisdicție asupra unui operator de servicii esențiale nu numai în cazurile în care operatorul își are sediul social pe teritoriul său, ci și în cazurile în care operatorul are, de exemplu, o sucursală sau un alt tip de stabilire legală.

Aceasta are drept consecință faptul că mai multe state membre ar putea avea jurisdicție în paralel asupra aceleiași entități.

4.1.5. Informațiile care trebuie prezentate Comisiei

În scopul revizuirii pe care Comisia trebuie să o efectueze în conformitate cu articolul 23 alineatul (1) din Directiva NIS, statele membre au obligația de a transmite Comisiei, până la data de 9 noiembrie 2018 și, ulterior, la fiecare doi ani, următoarele informații:

- măsurile naționale care permit identificarea OES;
- lista de servicii esențiale;
- numărul de OES identificați pentru fiecare sector menționat în anexa II și pertinența acestor operatori pentru sector și
- limitele, atunci când acestea există, utilizate pentru a determina nivelul de furnizare în raport cu numărul de utilizatori care se bazează pe serviciul respectiv, astfel cum se prevede la articolul 6 alineatul (1) litera (a), sau cu importanța entității, în conformitate cu articolul 6 alineatul (1) litera (f).

Revizuirea prevăzută la articolul 23 alineatul (1), care precedă revizuirea amplă a directivei, reflectă importanța pe care colegiuitorii o acordă transpunerii corecte a directivei în ceea ce privește identificarea operatorilor de servicii esențiale pentru a evita fragmentarea pieței.

Pentru derularea acestui proces în cel mai bun mod posibil, Comisia încurajează statele membre să discute acest subiect și să facă schimb de experiențe relevante în cadrul Grupului de cooperare. În plus, Comisia încurajează statele membre să transmită Comisiei - dacă este necesar cu titlu confidențial - listele operatorilor de servicii esențiale identificați (care au fost selectați în cele din urmă), în plus față de toate informațiile pe care statele membre au obligația să le furnizeze Comisiei în temeiul directivei. Disponibilitatea acestor liste ar facilita și ar avea ca rezultat o calitate sporită a evaluării efectuate de Comisie cu privire la coerența procesului de identificare și, de asemenea, ar face posibilă compararea abordărilor între statele membre, conducând astfel la o mai bună realizare a obiectivelor directivei.

4.1.6. Cum se efectuează procesul de identificare?

Astfel cum se arată în figura 4, există șase întrebări-cheie pe care o autoritate națională ar trebui să le examineze atunci când efectuează procesul de identificare cu privire la o anumită entitate. La punctul următor, fiecare întrebare corespunde unei etape care trebuie întreprinsă în conformitate cu articolul 5 coroborat cu articolul 6, luând, de asemenea, în considerare aplicabilitatea articolului 1 alineatul (7).

Etapa 1 – **Aparține entitatea unui sector/subsector și corespunde unui tip acoperit de anexa II la directivă?**

O autoritate națională ar trebui să evalueze dacă o entitate stabilită pe teritoriul său aparține sectoarelor și subsectoarelor enumerate în anexa II la directivă. Anexa II cuprinde diverse

sectoare economice care sunt considerate esențiale pentru a asigura buna funcționare a pieței interne. În special, anexa II se referă la următoarele sectoare și subsectoare:

- energie: electricitate, petrol și gaze naturale;
- transport: transport aerian, feroviar, pe apă și rutier;
- sector bancar: instituții de credit;
- infrastructuri ale pieței financiare: locuri de tranzacționare, contrapartide centrale;
- sănătate: furnizori de servicii medicale (inclusiv spitale și clinici private);
- apă: furnizarea și distribuirea de apă potabilă;
- infrastructură digitală: internet exchange points, furnizori de servicii de „domain name system", registre de nume de domeniu Top-level[28]

Etapa 2 – **Este aplicabilă o *lex specialis*?**

În etapa următoare, autoritatea națională trebuie să evalueze dacă se aplică dispoziția privind *lex specialis* prevăzută la articolul 1 alineatul (7). În special, această dispoziție prevede că, în cazul în care există un act juridic al UE care impune cerințe de securitate și/sau de notificare pentru furnizorii de servicii digitale sau operatorii de servicii esențiale care sunt cel puțin echivalente cu cerințele corespunzătoare din Directiva NIS, ar trebui să se aplice obligațiile prevăzute în legea specială. În plus, considerentul 9 clarifică faptul că, dacă sunt îndeplinite cerințele prevăzute la articolul 1 alineatul (7), statele membre ar trebui să aplice dispozițiile actului sectorial la nivelul UE, inclusiv cele legate de jurisdicție. Dimpotrivă, dispozițiile relevante ale Directivei NIS nu s-ar aplica. În acest caz, autoritatea competentă nu ar trebui să continue procesul de identificare prevăzut la articolul 5 alineatul (2)[29].

Etapa 3 – **Furnizează operatorul un serviciu esențial în sensul directivei?**

În temeiul articolului 5 alineatul (2) litera (a), entitatea care face obiectul identificării trebuie să furnizeze un serviciu care este esențial pentru menținerea unor activități economice și/sau societale de cea mai mare importanță. Atunci când efectuează această evaluare, statele membre ar trebui să ia în considerare faptul că o entitate poate oferi atât servicii esențiale, cât și servicii neesențiale. Acest lucru înseamnă că cerințele de securitate și de notificare prevăzute în Directiva NIS se aplică unui anumit operator doar în măsura în care acesta furnizează servicii esențiale.

În conformitate cu articolul 5 alineatul (3), un stat membru ar trebui să stabilească o listă a tuturor serviciilor esențiale furnizate de OES pe teritoriul său. Această listă va trebui să fie prezentată Comisiei până la 9 noiembrie 2018 și, ulterior, la fiecare doi ani[30].

Etapa 4 - **Depinde serviciul de o rețea și de un sistem informatic?**

[28] Aceste entități sunt explicate mai detaliat în secțiunea 4.1.1.

[29] Mai multe detalii cu privire la aplicabilitatea *lex specialis* sunt furnizate în secțiunea 5.1

[30] A se vedea articolul 5 alineatul (7) litera (b).

În plus, ar trebui să se clarifice dacă acest serviciu îndeplinește cel de al doilea criteriu prevăzut la articolul 5 alineatul (2) litera (b), în special dacă furnizarea serviciului esențial depinde de o rețea și de sisteme informatice, astfel cum sunt definite la articolul 4 alineatul (1).

Etapa 5 – **Un incident de securitate ar putea să aibă un efect perturbator semnificativ?**

Articolul 5 alineatul (2) litera (c) prevede obligația autorității naționale de a evalua dacă un incident ar avea un efect perturbator semnificativ asupra furnizării serviciului. În acest context, articolul 6 alineatul (1) prevede o serie de factori transsectoriali care trebuie luați în considerare în cadrul evaluării. În plus, articolul 6 alineatul (2) prevede că, dacă este cazul, evaluarea ar trebui să ia în considerare, de asemenea, factorii specifici fiecărui sector.

Factorii transsectoriali enumerați la articolul 6 alineatul (1) sunt următorii:

- numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;
- dependența altor sectoare menționate în anexa II de serviciul furnizat de entitatea în cauză;
- impactul pe care l-ar putea avea incidentele, în ceea ce privește intensitatea și durata, asupra activităților economice și societale sau asupra siguranței publice;
- cota de piață a entității în cauză;
- distribuția geografică în ceea ce privește zona care ar putea fi afectată de un incident;
- importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

În ceea ce privește **factorii specifici fiecărui sector**, considerentul 28 oferă o serie de exemple (a se vedea tabelul 4), care ar putea furniza orientări utile pentru autoritățile naționale.

Tabelul 4: Exemple de factori specifici fiecărui sector care trebuie să fie luați în considerare atunci când se stabilește un efect perturbator semnificativ în caz de incident

Sector	Exemple de factori specifici fiecărui sector
Furnizori de energie	volumul sau proporția de energie generată la nivel național
Furnizori de petrol	volumul de petrol furnizat pe zi
Transport aerian (inclusiv aeroporturi și transportatori aerieni) **Transport feroviar** **Porturi maritime**	proporția din volumul de trafic național; numărul de pasageri sau de operațiuni de transport de mărfuri pe an.
Infrastructuri ale piețelor bancare sau financiare	importanța sistemică, pe baza activelor totale; raportul dintre activele totale și PIB
Sectorul sănătății	numărul anual de pacienți aflați în grija furnizorului
Producția, tratarea și	volumul și numărul și tipul de utilizatori (inclusiv, de

furnizarea de apă	exemplu, spitale, organizații de serviciu public sau persoane fizice); existența surselor de apă alternative care să acopere aceeași zonă geografică

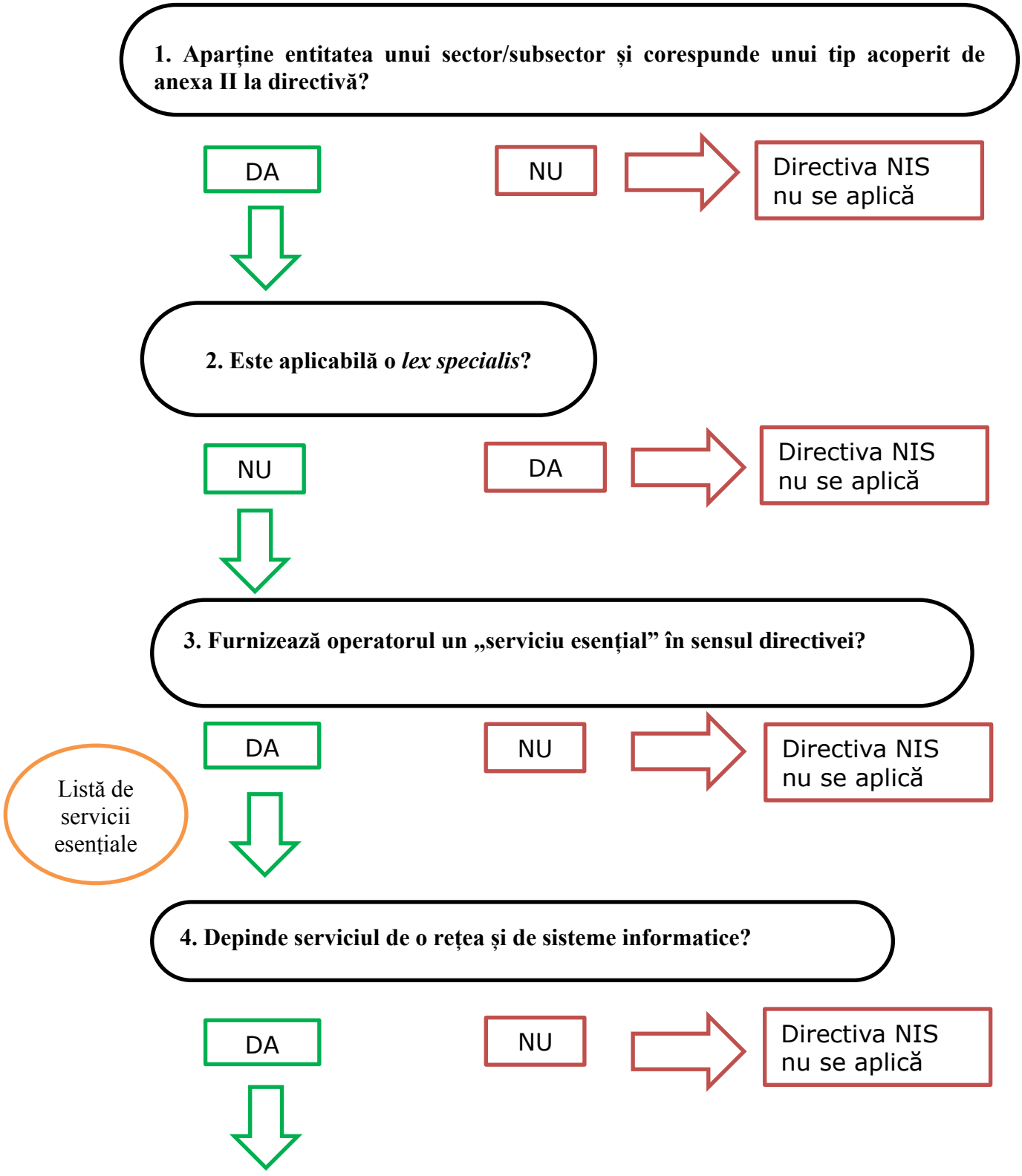
Trebuie precizat faptul că, atunci când efectuează evaluarea prevăzută la articolul 5 alineatul (2), statele membre nu ar trebui să adauge criterii suplimentare, altele decât cele enumerate în dispoziția menționată, deoarece acest lucru ar putea reduce numărul de OES identificați și ar pune în pericol armonizarea minimă pentru OES prevăzută la articolul 3 din directivă.

Etapa 6 - **Furnizează operatorul în cauză servicii esențiale în alte state membre?**

Etapa 6 se referă la cazurile în care operatorul furnizează serviciile sale esențiale în două sau mai multe state membre. Înainte de finalizarea procesului de identificare, articolul 5 alineatul (4) impune statelor membre vizate obligația de a se angaja într-un proces de consultare[31].

[31] Pentru mai multe detalii privind procesul de consultare, a se vedea secțiunea 4.1.7.

Figura 4: Procesul de identificare în 6 etape



5. Un incident de securitate ar avea un efect perturbator semnificativ?

Factori transsectoriali [articolul 6 alineatul (1)]

- **Numărul de utilizatori** care se bazează pe servicii
- **Dependența** altor sectoare esențiale de serviciu
- Impactul pe care l-ar putea avea incidentele asupra **activităților economice și societale** sau a **siguranței publice**
- Posibilă **distribuție geografică**
- Importanța entității pentru menținerea unui **nivel suficient al serviciului**

Factori specifici fiecărui sector (exemple menționate în considerentul 28)

- **Energie**: volumul sau proporția de energie generată la nivel național
- **Transport**: proporția din volumul de trafic național și numărul de operațiuni pe an
- **Sănătate**: numărul anual de pacienți aflați în grija furnizorului

DA

NU → Directiva NIS nu se aplică

6. Furnizează operatorul în cauză servicii esențiale în alte state membre?

DA

NU → Directiva NIS nu se aplică

Consultare obligatorie cu statul membru (statele membre) vizate

Adoptarea măsurilor naționale (de exemplu, lista operatorilor de servicii esențiale, măsuri juridice și de politică)

4.1.7. Procesul de consultare transfrontalieră

În cazul în care un operator furnizează servicii esențiale în două sau mai multe state membre, articolul 5 alineatul (4) prevede obligația statelor membre de a se consulta reciproc înainte de finalizarea procesului de identificare. Scopul acestei consultări este de a facilita evaluarea importanței operatorului din punctul de vedere al impactului transfrontalier.

Rezultatul dorit al consultării este ca autoritățile naționale implicate să facă schimb de argumente și poziții și, în mod ideal, să ajungă la același rezultat în ceea ce privește identificarea operatorului în cauză. Cu toate acestea, Directiva NIS nu împiedică statele membre să ajungă la concluzii divergente cu privire la faptul că o anumită entitate este sau nu identificată ca OES. Considerentul 24 menționează posibilitatea ca statele membre să solicite asistența Grupului de cooperare în această privință.

În opinia Comisiei, statele membre ar trebui să depună eforturi pentru a ajunge la un consens cu privire la aceste aspecte, pentru a se evita o situație în care aceeași întreprindere are un statut juridic diferit în diverse state membre. Diferența ar trebui să fie cu adevărat excepțională, de exemplu atunci când o entitate identificată drept OES într-un stat membru are o activitate marginală și nesemnificativă în alt stat membru.

4.2. Cerințele de securitate

În temeiul articolului 14 alineatul (1), statele membre au obligația să se asigure că OES, ținând seama de cele mai avansate cunoștințe în domeniu, iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care organizațiile le utilizează în furnizarea serviciilor lor. În conformitate cu articolul 14 alineatul (2), măsurile adecvate previn și minimalizează impactul unui incident.

Grupul de cooperare lucrează în prezent la elaborarea de orientări fără caracter obligatoriu privind măsurile de securitate pentru OES[32]. Documentul de orientare urmează să fie finalizat de către grup în al patrulea trimestru din 2017. Comisia încurajează statele membre să urmărească îndeaproape documentul de orientare care urmează să fie elaborat de Grupul de cooperare, astfel încât dispozițiile naționale privind cerințele de securitate să fie aliniate, în măsura în care acest lucru este posibil. Armonizarea acestor cerințe ar facilita în mare măsură conformitatea OES, care adesea furnizează servicii esențiale în mai mult de un stat membru, și sarcinile de supraveghere care revin autorităților naționale competente și CSIRT.

4.3 Cerințele de notificare

În temeiul articolului 14 alineatul (3), statele membre trebuie să se asigure că OES notifică *„orice incident care are un impact semnificativ asupra continuității serviciilor esențiale”*. În

[32] În scopul desfășurării acestei activități, au fost transmise liste de standarde internaționale, bune practici și metodologii pentru evaluarea/gestionarea riscurilor pentru toate sectoarele acoperite de Directiva NIS, care au fost utilizate ca punct de plecare pentru domeniile de securitate și măsurile de securitate propuse.

consecință, OES nu ar trebui să notifice orice incidente minore, ci numai incidentele grave care afectează continuitatea serviciilor esențiale. Articolul 4 alineatul (7) definește incidentul drept *„orice eveniment care are un efect real negativ asupra securității rețelelor și a sistemelor informatice”*. Termenul „securitatea rețelelor și a sistemelor informatice” este definit la articolul 4 alineatul (2) ca fiind *„capacitatea unei rețele de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora”*. Prin urmare, orice eveniment care are un efect negativ nu numai în ceea ce privește disponibilitatea, ci și cu privire la autenticitatea, integritatea sau confidențialitatea datelor sau a serviciilor conexe ar putea să declanșeze obligația de notificare. De fapt, continuitatea serviciului, astfel cum este prevăzută la articolul 14 alineatul (3), poate fi compromisă nu numai în ceea ce privește disponibilitatea fizică, ci și de orice alt incident de securitate care afectează furnizarea corespunzătoare a serviciului[33].

Grupul de cooperare lucrează în prezent la elaborarea de orientări fără caracter obligatoriu referitoare la activitatea de notificare cu privire la circumstanțele în care operatorii de servicii esențiale au obligația de a notifica incidente în temeiul articolului 14 alineatul (7), precum și la formatul și procedura notificărilor la nivel național. Orientările urmează să fie finalizate în al patrulea trimestru din 2017.

Cerințele de notificare naționale diferite pot genera incertitudine juridică, proceduri mai complexe și greoaie și costuri administrative semnificative pentru furnizorii care își desfășoară activitatea la nivel transfrontalier. Prin urmare, Comisia salută activitatea Grupului de cooperare. La fel ca în cazul cerințelor în materie de securitate, Comisia încurajează statele membre să urmărească îndeaproape documentul de orientare care urmează să fie elaborat de Grupul de cooperare, astfel încât dispozițiile naționale privind notificarea incidentelor să fie aliniate, în măsura în care acest lucru este posibil.

4.4. Anexa III la Directiva NIS: furnizorii de servicii digitale

Furnizorii de servicii digitale (DSP) reprezintă a doua categorie de entități incluse în domeniul de aplicare al Directivei NIS. Aceste entități sunt considerate actori economici importanți deoarece sunt utilizate de multe întreprinderi pentru furnizarea propriilor servicii, iar o perturbare a serviciului digital ar putea avea un impact asupra unor activități economice și societale esențiale.

4.4.1. Categoriile de furnizori de servicii digitale

Articolul 4 alineatul (5) care definește serviciul digital face referire la definiția de la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535, prin limitarea domeniului de aplicare la tipurile de servicii enumerate în anexa III. În special, articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 definește aceste servicii ca *„orice serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea*

[33] Același lucru este valabil, de asemenea, pentru furnizorii de servicii digitale.

individuală a beneficiarului serviciului”, iar în anexa III la directivă sunt specificate trei tipuri de servicii: piață online, motor de căutare online și serviciu de cloud computing. Spre deosebire de cazul operatorilor de servicii esențiale, directiva nu impune statelor membre obligația de a-i identifica pe furnizorii de servicii digitale care ar urma să facă ulterior obiectul obligațiilor relevante. Prin urmare, obligațiile relevante prevăzute în directivă, și anume cerințele de securitate și de notificare stabilite la articolul 16, se aplică tuturor furnizorilor de servicii digitale care se încadrează în domeniul său de aplicare.

Următoarele secțiuni oferă explicații suplimentare cu privire la trei tipuri de servicii digitale incluse în domeniul de aplicare al directivei.

1. Furnizori de piață online

Piața online permite ca un număr mare și o gamă largă de întreprinderi să desfășoare activități comerciale destinate consumatorilor și să stabilească relații cu alte întreprinderi. Piața online oferă întreprinderilor infrastructura de bază pentru comerțul electronic și la nivel transfrontalier și îndeplinește un rol important în economie, în special prin asigurarea accesului IMM-urilor la piața unică digitală mai largă a UE. Furnizarea de servicii informatice la distanță care facilitează activitatea economică a clientului, inclusiv prelucrarea operațiunilor și agregarea informațiilor cu privire la cumpărători, furnizori și produse, poate ține, de asemenea, de activitățile unui furnizor de piață online, la fel ca facilitarea căutării de produse adecvate, furnizarea de produse, expertiza de tranzacționare și facilitarea întâlnirii dintre cumpărători și vânzători.

Termenul „piață online” este definit la articolul 4 alineatul (17) și este clarificat în continuare la considerentul 15. Piața online este descrisă ca un serviciu care permite consumatorilor și comercianților să încheie online vânzări sau contracte de servicii cu comercianți și reprezintă destinația finală pentru încheierea acestor contracte. De exemplu, un furnizor precum *E-bay* poate fi considerat drept piață online deoarece permite altora să înființeze magazine pe platforma sa în scopul de a-și pune la dispoziție produsele și serviciile online pentru consumatori sau întreprinderi. De asemenea, magazinele de aplicații online care distribuie aplicații și programe informatice sunt considerate ca încadrându-se în definiția pieței online deoarece permit dezvoltatorilor de aplicații să vândă sau să distribuie servicii către consumatori sau alte întreprinderi. În schimb, intermediarii către serviciile furnizate de terți, precum *Skyscanner* și serviciile de comparare a prețurilor, care îl redirecționează pe utilizator către site-ul web al comerciantului unde este încheiat contractul efectiv pentru un serviciu sau produs, nu intră sub incidența definiției de la articolul 4 alineatul (17).

2. Furnizori de motoare de căutare online

Termenul „motor de căutare online” este definit la articolul 4 alineatul (18) și este clarificat în continuare la considerentul 16. Motorul de căutare online este descris drept un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile web sau în site-urile web într-o anumită limbă pe baza unei interogații privind orice subiect. Nu sunt acoperite funcțiile de căutare limitate la căutarea în site-ul web și pe site-urile web de comparare a prețurilor. De

exemplu, tipul de motor de căutare precum cel furnizat de EUR LEX[34] nu poate fi considerat un motor de căutare în sensul directivei, întrucât funcția sa de căutare este limitată la conținutul respectivului site web.

3. Furnizori de servicii de cloud computing

Articolul 4 alineatul (19) definește serviciul de cloud computing ca „un serviciu digital care permite accesul la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun", iar considerentul 17 oferă clarificări suplimentare cu privire la termenii „resurse informatice" și „bazin redimensionabil și elastic".

Pe scurt, tehnologia de tip cloud computing poate fi descrisă ca un anumit tip de servicii informatice care utilizează resurse comune pentru a prelucra datele la cerere, în cadrul căruia resursele comune se referă la orice tip de componente hardware sau software (de exemplu, rețele, servere sau alte infrastructuri, sisteme de stocare de date, aplicații și servicii) care sunt furnizate la cerere utilizatorilor pentru prelucrarea datelor. Termenul „care pot fi puse în comun" definește resursele informatice în cazul cărora un număr mare de utilizatori folosesc aceeași infrastructură fizică pentru prelucrarea datelor. Resursele informatice pot fi definite ca putând fi puse în comun dacă pachetul de resurse utilizate de furnizor poate fi extins sau redus în orice moment, în funcție de cerințele utilizatorului. Prin urmare, centrele de date sau componentele individuale din cadrul unui centru de date ar putea fi, eventual, adăugate sau eliminate dacă volumul total al capacității de calcul sau de stocare necesită o actualizare. Termenul „bazin elastic" poate fi definit ca implicând modificări ale sarcinii de lucru prin constituirea de provizioane și deconstituirea de provizioane de resurse în mod automat, astfel încât în fiecare moment resursele disponibile să corespundă cererii actuale cât mai exact posibil[35].

În prezent există trei tipuri principale de modele de servicii de cloud pe care le poate oferi un furnizor:

- infrastructura ca serviciu (IaaS): o categorie de serviciu de cloud în care capacitățile de tip cloud furnizate clientului constituie o infrastructură. Acest serviciu include furnizarea virtuală de resurse informatice sub formă de hardware, crearea de rețele și serviciile de stocare de date. IaaS alimentează servere, sisteme de stocare de date, rețele și sisteme de operare. IaaS oferă întreprinderilor o infrastructură în cadrul căreia își pot stoca datele și pot utiliza aplicațiile necesare pentru desfășurarea activității lor zilnice;

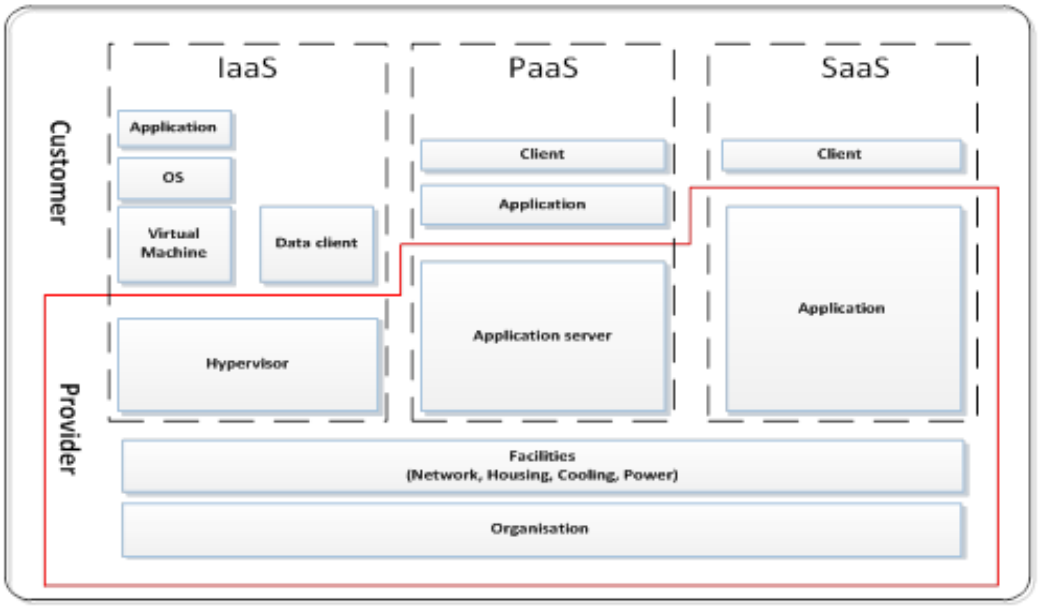
- platforma ca serviciu (PaaS): o categorie de serviciu de cloud în care capacitățile de tip cloud furnizate clientului constituie o platformă. Acest serviciu include platforme online care permit întreprinderilor să ruleze aplicațiile existente sau să dezvolte și să testeze aplicații noi;

[34] Disponibil la adresa: http://eur-lex.europa.eu/homepage.html

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Institutul Tehnologic din Karlsruhe, *Elasticity in Cloud Computing: What It Is, and What It Is Not* („Elasticitatea în cloud computing: ce este și ce nu este aceasta"). Document disponibil la adresa: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. A se vedea, de asemenea, paginile 2-5 din COM(2012) 529.

- software-ul ca serviciu (SaaS): o categorie de serviciu de cloud în care capacitățile de tip cloud furnizate clientului constituie o aplicație sau un program informatic instalat pe internet. Acest tip de servicii de cloud elimină necesitatea ca utilizatorul final să achiziționeze, să instaleze și să gestioneze programe informatice și are avantajul de a pune la dispoziție programele informatice din orice loc cu ajutorul unei conexiuni la internet.

Figura 5: Modele de servicii și active în tehnologia de tip cloud computing



ENISA a furnizat orientări cuprinzătoare cu privire la subiecte specifice din domeniul tehnologiei cloud[36] și un document de orientare cu privire la noțiunile de bază ale tehnologiei de tip cloud computing[37].

4.4.2. Cerințele de securitate

În temeiul articolului 16 alineatul (1), statele membre au obligația de a se asigura că furnizorii de servicii digitale iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care întreprinderile le utilizează în furnizarea serviciilor lor. Măsurile de securitate ar trebui să ia în considerare cele mai avansate cunoștințe în domeniu și următoarele cinci elemente: i) securitatea sistemelor și a instalațiilor; ii) gestionarea incidentelor; iii) gestionarea continuității activității; iv) monitorizarea, auditarea și testarea; v) conformitatea cu standardele internaționale.

[36] Disponibile la adresa: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* („Ghid de securitate în materie de cloud pentru IMM-uri") (2015). Document disponibil la adresa: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

În această privință, Comisia este împuternicită, în temeiul articolului 16 alineatul (8), să adopte acte de punere în aplicare care precizează elementele respective și asigură un nivel ridicat de armonizare pentru acești furnizori de servicii. Se preconizează că actul de punere în aplicare va fi adoptat de către Comisie în toamna anului 2017. În plus, statele membre au obligația de a se asigura că furnizorii de servicii digitale iau măsurile necesare de prevenire și de minimalizare a impactului incidentelor în vederea asigurării continuității serviciilor lor.

4.4.3. Cerințele de notificare

Furnizorii de servicii digitale ar trebui să aibă obligația de a notifica incidentele grave către autoritățile competente sau CSIRT. În conformitate cu articolul 16 alineatul (3) din Directiva NIS, cerința de notificare pentru furnizorii de servicii digitale va fi activată în cazurile în care incidentul de securitate are un impact substanțial asupra furnizării serviciului. Pentru determinarea impactului, articolul 16 alineatul (4) enumeră în special cinci parametri care trebuie să fie luați în considerare de către furnizorii de servicii digitale. În această privință, Comisia este împuternicită, în temeiul articolului 16 alineatul (8), să adopte acte de punere în aplicare care furnizează descrieri mai detaliate ale parametrilor. Specificarea mai detaliată a acestor parametri va face parte din actul de punere în aplicare care precizează elementele de securitate menționate la punctul 4.4.2, pe care Comisia intenționează să îl adopte în toamnă.

4.4.4. Abordare de reglementare bazată pe riscuri

Articolul 17 prevede că furnizorii de servicii digitale fac obiectul unei supravegheri *ex post* exercitate de către autoritățile naționale competente. Statele membre trebuie să se asigure că autoritățile competente iau măsuri, atunci când primesc dovezi conform cărora un furnizor de servicii digitale nu îndeplinește cerințele de la articolul 16 din directivă.

În plus, în temeiul articolului 16 alineatele (8) și (9), Comisia este împuternicită să adopte acte de punere în aplicare în ceea ce privește cerințele de securitate și de notificare care vor spori nivelul de armonizare pentru furnizorii de servicii digitale. În plus, în temeiul articolului 16 alineatul (10), statele membre nu sunt autorizate să impună alte cerințe suplimentare de securitate și de notificare pentru furnizorii de servicii digitale decât cele prevăzute de directivă, cu excepția cazurilor în care astfel de măsuri sunt necesare pentru a garanta funcțiile esențiale ale statului, în special pentru a proteja securitatea națională și pentru a permite investigarea, detectarea și urmărirea penală a infracțiunilor.

În fine, ținând seama de caracterul transfrontalier al furnizorilor de servicii digitale, directiva nu urmează modelul unor jurisdicții multiple paralele, ci o abordare bazată pe criteriul sediului principal al întreprinderii în UE[38]. Această abordare permite ca un set unic de norme să fie aplicat furnizorilor de servicii digitale de către o autoritate competentă responsabilă de supraveghere, ceea ce este deosebit de important deoarece un număr mare de furnizori de servicii digitale își oferă serviciile în mai multe state membre în același timp. Aplicarea acestei abordări reduce la minimum sarcina de conformare pentru furnizorii de servicii digitale și asigură buna funcționare a pieței unice digitale.

[38] A se vedea, în special, articolul 18 din directivă.

4.4.5. Jurisdicție

Astfel cum s-a explicat mai sus, în temeiul articolului 18 alineatul (1) din Directiva NIS, statul membru în care furnizorul de servicii digitale își are sediul principal are jurisdicție asupra întreprinderii. În cazurile în care furnizorul concret de servicii digitale oferă servicii în UE, dar nu este stabilit pe teritoriul UE, articolul 18 alineatul (2) impune furnizorului de servicii digitale obligația de a desemna un reprezentant în Uniune. În acest caz, statul membru în care este stabilit reprezentantul va avea jurisdicție asupra întreprinderii. În cazurile în care un furnizor de servicii digitale prestează servicii într-un stat membru, dar nu a desemnat un reprezentant pe teritoriul UE, statul membru poate, în principiu, să ia măsuri împotriva furnizorului de servicii digitale, întrucât acesta își încalcă obligațiile care decurg din directivă.

4.4.6. Exceptarea furnizorilor de servicii digitale de dimensiune redusă din domeniul de aplicare al cerințelor de securitate și de notificare

În temeiul articolului 16 alineatul (11), furnizorii de servicii digitale care sunt microîntreprinderi sau întreprinderi mici, în sensul Recomandării Comisiei 2003/361/CE39, sunt excluși din domeniul de aplicare al cerințelor de securitate și de notificare prevăzute la articolul 16. Acest lucru înseamnă că întreprinderile care au sub 50 de angajați și a căror cifră de afaceri și/sau al căror bilanț anual total nu depășește suma de 10 milioane EUR nu trebuie să se supună acestor cerințe. Atunci când se stabilește dimensiunea entității, nu este relevant dacă întreprinderea respectivă oferă doar servicii digitale în sensul Directivei NIS sau și alte servicii.

5. Relația dintre Directiva NIS și alte acte legislative

Această secțiune se axează pe dispozițiile privind *lex specialis* prevăzute în Directiva NIS la articolul 1 alineatul (7), care ilustrează trei exemple de *lex specialis* evaluate până în prezent de către Comisie și clarifică cerințele privind securitatea și notificarea aplicabile furnizorilor de servici de telecomunicații și de servicii de încredere.

5.1. Articolul 1 alineatul (7) din Directiva NIS: dispoziția privind *lex specialis*

În temeiul articolului 1 alineatul (7) din Directiva NIS, dispozițiile referitoare la cerințele de securitate și/sau de notificare pentru furnizorii de servicii digitale sau operatorii de servicii esențiale în temeiul prezentei directive nu sunt aplicabile în cazul în care legislația sectorială a UE prevede cerințe de securitate și/sau de notificare care sunt cel puțin echivalente ca efect cu obligațiile corespunzătoare din Directiva NIS. Statele membre trebuie să aibă în vedere articolul 1 alineatul (7) în transpunerea globală a acestei directive și să furnizeze Comisiei informații privind aplicarea dispozițiilor *lex specialis*.

Metodologia

Atunci când se evaluează echivalența unui act legislativ sectorial al UE cu dispozițiile relevante ale Directivei NIS, ar trebui acordată o importanță deosebită stabilirii faptului dacă

[39] JO L 24, 20.5.2003, p. 36.

obligațiile în materie de securitate prevăzute în legislația sectorială cuprind măsuri care asigură securitatea rețelelor și a sistemelor informatice, astfel cum sunt definite la articolul 4 alineatul (2) din directivă.

În ceea ce privește cerințele de notificare, articolul 14 alineatul (3) și articolul 16 alineatul (3) din Directiva NIS prevăd că operatorii de servicii esențiale și furnizorii de servicii digitale trebuie să informeze fără întârziere autoritățile competente sau CSIRT cu privire la orice incident care are un impact semnificativ/substanțial asupra furnizării serviciului. În acest context, o atenție specială trebuie acordată obligațiilor operatorului/furnizorului de servicii digitale de a include în notificare informații care să permită autorității competente sau echipelor CSIRT să stabilească orice impact transfrontalier al incidentului de securitate.

În prezent, nu există nicio legislație sectorială pentru categoria de furnizori de servicii digitale care să prevadă cerințe de securitate și de notificare comparabile cu cele prevăzute la articolul 16 din Directiva NIS și care să poate fi luată în considerare în aplicarea articolului 1 alineatul (7) din Directiva NIS[40].

În ceea ce privește operatorii de servicii esențiale, sectorul financiar și, în special, sectoarele infrastructurilor bancare și pieței financiare, astfel cum se prevede la punctele 3 și 4 din anexa II, fac în prezent obiectul unor notificări de securitate și/sau cerințe care decurg din legislația sectorială a UE. Acest lucru se datorează faptului că securitatea și soliditatea tehnologiei informației și a rețelelor și a sistemelor informatice utilizate de instituțiile financiare reprezintă o parte esențială a cerințelor privind riscul operațional impuse de legislația UE instituțiilor financiare.

Exemple

i) Directiva privind serviciile de plată 2

În cazul sectorului bancar, în special în ceea ce privește furnizarea de servicii de plată de către instituțiile de credit, astfel cum sunt definite la articolul 4 punctul (1) din Regulamentul (UE) nr. 575/2013, așa-numita Directivă privind serviciile de plată 2 (DSP2)[41] prevede cerințe de securitate și de notificare, care sunt stabilite la articolele 95 și 96 din directivă.

Mai precis, articolul 95 alineatul (1) prevede obligația prestatorilor de servicii de plată să adopte măsuri de atenuare și mecanisme de control adecvate care să permită gestionarea riscurilor operaționale și de securitate legate de serviciile de plată pe care le furnizează. Aceste măsuri ar trebui să includă stabilirea și menținerea unor proceduri eficace de gestionare a incidentelor, inclusiv pentru detectarea și clasificarea incidentelor operaționale și de securitate majore. Considerentele 95 și 96 din DSP 2 clarifică în continuare natura acestor măsuri de securitate. Din aceste dispoziții rezultă că măsurile prevăzute vizează gestionarea

[40] Acest lucru nu aduce atingere notificării autorității de supraveghere în cazul încălcării securității datelor cu caracter personal, care intră sub incidența articolului 33 din Regulamentul general privind protecția datelor.
[41] Directiva (UE) 2015/2366, JO L 337, 23.12.2015, p. 35.

riscurilor legate de securitatea rețelelor și a sistemelor informatice care sunt utilizate pentru prestarea de servicii de plată. Prin urmare, aceste cerințe de securitate pot fi considerate cel puțin echivalente ca efect cu dispoziția corespunzătoare de la articolul 14 alineatele (1) și (2) din Directiva NIS.

În ceea ce privește cerințele în materie de notificare, articolul 96 alineatul (1) din DSP 2 prevede obligația prestatorilor de servicii de plată de a raporta, fără întârzieri nejustificate, incidentele grave de securitate către autoritatea competentă. În plus, comparabil cu articolul 14 alineatul (5) din Directiva NIS, articolul 96 alineatul (2) din DSP 2 prevede obligația autorității competente de a informa autoritățile competente ale altor state membre în cazul în care un incident este relevant pentru acestea. Această obligație implică, în același timp, faptul că raportarea incidentelor de securitate trebuie să includă informații care permit autorităților să evalueze impactul transfrontalier al unui incident. Articolul 96 alineatul (3) litera (a) din DSP 2 împuternicește în acest sens ABE, în cooperare cu BCE, să elaboreze orientări referitoare la conținutul și formatul exact al notificării.

În consecință, se poate concluziona că, în temeiul articolului 1 alineatul (7) din Directiva NIS, atât cerințele de securitate, cât și cele de notificare prevăzute la articolele 95 și 96 din DSP 2 ar trebui să se aplice în locul dispozițiilor corespunzătoare ale articolului 14 din Directiva NIS în ceea ce privește furnizarea de servicii de plată de către instituții de credit.

ii) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții

În ceea ce privește infrastructura pieței financiare, Regulamentul (UE) nr. 648/2012, coroborat cu Regulamentul delegat al Comisiei (UE) nr. 153/2013, conține dispoziții referitoare la cerințele de securitate pentru contrapărțile centrale (CPC) care pot fi considerate *lex specialis.* În special, actele juridice prevăd măsuri tehnice și organizaționale referitoare la securitatea rețelelor și a sistemelor informatice, care, în termeni de detaliere, depășesc chiar și cerințele de la articolul 14 alineatele (1) și (2) din Directiva NIS și, prin urmare, se poate considera că îndeplinesc cerințele de la articolul 1 alineatul (7) din Directiva NIS în ceea ce privește cerințele de securitate respective.

Mai precis, articolul 26 alineatul (1) din Regulamentul (UE) nr. 648/2012 prevede că entitatea în cauză ar trebui să aibă *„un sistem robust de guvernanță, care include o structură organizatorică clară, cu responsabilități bine definite, transparente și coerente, procese eficace de identificare, gestionare, monitorizare și raportare a riscurilor la care sunt sau pot fi expuse, precum și mecanisme adecvate de control intern, inclusiv proceduri administrative și contabile solide”.* Articolul 26 alineatul (3) prevede că structura organizatorică trebuie să asigure continuitatea și buna funcționare a serviciilor și activităților utilizând sisteme, resurse și proceduri adecvate și proporționale.

În plus, articolul 26 alineatul (6) clarifică faptul că o CPC trebuie să mențină *„sisteme informatice adecvate pentru a face față complexității, diversității și tipului de servicii prestate și activități desfășurate, astfel încât să asigure standarde ridicate de siguranță și integritatea*

și confidențialitatea informațiilor păstrate". În plus, articolul 34 alineatul (1) impune stabilirea, punerea în aplicare și menținerea unei politici adecvate de continuitate a activității și a unui plan de redresare în caz de dezastru, care ar trebui să asigure reluarea rapidă a operațiunilor.

Aceste obligații sunt detaliate în Regulamentul delegat (UE) nr. 153/2013 al Comisiei din 19 decembrie 2012 de completare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare privind cerințele pentru contrapărțile centrale[42]. În special articolul 4 impune CPC obligația de a elabora instrumente adecvate de gestionare a riscurilor care să permită gestionarea și raportarea cu privire la toate riscurile relevante și precizează mai detaliat tipul de măsuri (de exemplu, utilizarea de informații fiabile și sisteme de control, disponibilitatea resurselor, expertiza și accesul la toate informațiile relevante pentru funcția de gestionare a riscurilor, disponibilitatea unor mecanisme adecvate de control intern, cum ar fi procedurile contabile și administrative sigure pentru a asista Consiliul de administrație al CPC în monitorizarea și accesarea caracterului adecvat și a eficacității politicilor, procedurilor și sistemelor de gestionare a riscurilor).

În plus, articolul 9 se referă în mod explicit la securitatea sistemelor informatice și impune măsuri tehnice și organizatorice concrete legate de menținerea unui cadru solid de siguranță a informațiilor pentru gestionarea riscurilor în materie de siguranță a informațiilor. Aceste măsuri ar trebui să includă mecanisme și proceduri care să asigure disponibilitatea serviciilor și protecția autenticității, integrității și confidențialității datelor.

(iii) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE[43]

În ceea ce privește locurile de tranzacționare, articolul 48 alineatul (1) din Directiva 2014/65/UE impune operatorilor obligația de a asigura continuitatea serviciilor în cazul în care survine o defecțiune a sistemului lor de tranzacționare. Această obligație generală a fost recent precizată mai clar și completată prin Regulamentul delegat (UE) 2017/584 al Comisiei[44] din 14 iulie 2016 de completare a Directivei 2014/65/UE a Parlamentului European și a Consiliului în ceea ce privește standardele tehnice de reglementare în care sunt precizate cerințele organizatorice pentru locurile de tranzacționare[45]. În special, articolul 23 alineatul (1) din regulamentul menționat prevede că locurile de tranzacționare instituie proceduri și mecanisme de securitate fizică și electronică, concepute pentru a proteja sistemele împotriva accesului neautorizat sau abuziv și pentru a asigura integritatea datelor. Aceste măsuri ar trebui să permită prevenirea sau reducerea la minimum a riscurilor de atacuri împotriva sistemelor informatice.

[42] JO L 52, 23.2.2013, p. 41.
[43] JO L 173, 12.6.2014, p. 349.
[44] JO L 87, 31.3.2017, p. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

Articolul 23 alineatul (2) prevede, de asemenea, că măsurile și mecanismele instituite de către operatori ar trebui să permită identificarea și gestionarea promptă a riscurilor legate de orice acces neautorizat, intervenții în sistem care afectează semnificativ sau întrerup funcționarea sistemelor de informații și intervenții asupra datelor care compromit disponibilitatea, integritatea sau autenticitatea datelor. În plus, articolul 15 din regulament impune obligația ca locurile de tranzacționare să dispună de mecanisme eficace privind continuitatea activității pentru a garanta stabilitatea suficientă a sistemului și pentru a face față incidentelor perturbatoare. În special, aceste măsuri ar trebui să permită operatorului să își reia tranzacționarea în interval de două ore sau de aproape două ore și, în același timp, să asigure că volumul de date pierdute este aproape egal cu zero.

Articolul 16 prevede, de asemenea, că măsurile identificate pentru abordarea și gestionarea incidentelor perturbatoare ar trebui să facă parte din planul de continuitate a activității al locurilor de tranzacționare și prevede în special elementele care trebuie luate în considerare de către operator în momentul adoptării planului de continuitate a activității (de exemplu, instituirea unei echipe speciale pentru operațiuni de securitate, efectuarea unei evaluări a impactului pentru identificarea riscurilor, care este revizuită periodic).

Având în vedere conținutul respectivelor măsuri de securitate, se pare că acestea au scopul de a gestiona și a preveni riscurile legate de disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor sau a serviciilor furnizate și, prin urmare, se poate concluziona că legislația sectorială a UE menționată mai sus conține obligații în materie de securitate care au un efect cel puțin echivalent cu obligațiile corespunzătoare prevăzute la articolul 14 alineatele (1) și (2) din Directiva NIS.

5.2 Articolul 1 alineatul (3) din Directiva NIS: furnizorii de servicii de telecomunicații și furnizorii de servicii de încredere

În temeiul articolului 1 alineatul (3), cerințele de securitate și de notificare prevăzute de directivă nu se aplică furnizorilor care fac obiectul cerințelor de la articolul 13a și 13b din Directiva 2002/21/CE. Articolul 13a și 13b din Directiva 2002/21/CE se aplică întreprinderilor care furnizează rețele publice de comunicații sau servicii de comunicații electronice accesibile publicului. În consecință, în ceea ce privește furnizarea de rețele publice de comunicații sau de servicii de comunicații electronice accesibile publicului, întreprinderea trebuie să respecte cerințele de securitate și de notificare prevăzute de Directiva 2002/21/CE.

Cu toate acestea, în cazul în care aceeași întreprindere oferă și alte servicii, cum ar fi serviciile digitale (de exemplu, tehnologie de tip cloud computing sau piață online) enumerate în anexa III la Directiva NIS, cum ar fi DNS sau IXP, în temeiul punctului 7 din anexa II la Directiva NIS, întreprinderea va face obiectul cerințelor de securitate și de notificare prevăzute în Directiva NIS pentru furnizarea acestor servicii. Trebuie precizat faptul că, întrucât furnizorii de servicii enumerate la punctul 7 din anexa II se încadrează în categoria operatorilor de servicii esențiale, statele membre au obligația de a efectua procesul de identificare prevăzut la articolul 5 alineatul (2) și de a-i identifica pe furnizorii de servicii DNS, IXP sau TLD care ar trebui să respecte cerințele Directivei NIS. Aceasta înseamnă că, în urma evaluării respective, numai furnizorii DNS, IXP sau TLD care îndeplinesc criteriile prevăzute la articolul 5

alineatul (2) din Directiva NIS vor avea obligația să respecte cerințele prevăzute de Directiva NIS.

Articolul 1 alineatul (3) prevede, de asemenea, că cerințele de securitate și de notificare stabilite în directivă nu se aplică nici furnizorilor de servicii de încredere care fac obiectul unor cerințe similare în temeiul articolului 19 din Regulamentul (UE) nr. 910/2014.

6. Documente publicate privind Strategia națională de securitate cibernetică

	Stat membru	Denumirea strategiei și linkuri disponibile
1	Austria	*Strategia de securitate cibernetică din Austria* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgia	*Protejarea spațiului cibernetic* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulgaria	*Bulgaria rezilientă cibernetic 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Croația	*Strategia națională de securitate cibernetică a Republicii Croația* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Republica Cehă	*Strategia națională de securitate cibernetică a Republicii Cehe pentru perioada 2015-2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Cipru	*Strategia de securitate cibernetică a Republicii Cipru* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Danemarca	*Strategia de securitate cibernetică și a informațiilor a Danemarcei* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estonia	*Strategia de securitate cibernetică* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finlanda	*Strategia de securitate cibernetică a Finlandei* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Franța	*Strategia națională de securitate digitală a Franței* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)

11	Irlanda	*Strategia națională de securitate cibernetică 2015-2017* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Italia	*Cadrul strategic național pentru securitatea spațiului cibernetic* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Germania	*Strategia de securitate cibernetică a Germaniei* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Ungaria	*Strategia națională de securitate cibernetică a Ungariei* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Letonia	*Strategia de securitate cibernetică a Letoniei 2014-2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Lituania	*Programul pentru dezvoltarea securității informațiilor electronice (securitate cibernetică) pentru perioada 2011-2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxemburg	*Strategia națională de securitate cibernetică II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*Cartea verde „Strategia națională de securitate cibernetică”* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Țările de Jos	*Strategia națională de securitate cibernetică 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polonia	*Politica de protecție a spațiului cibernetic a Republicii Polone* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	România	*Strategia de securitate cibernetică a României* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)

22	Portugalia	*Strategia națională de securitate cibernetică* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Republica Slovacă	*Conceptul de securitate cibernetică al Republicii Slovace pentru perioada 2015-2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovenia	*Strategia de securitate cibernetică de stabilire a unui sistem menit să asigure un nivel ridicat de securitate cibernetică* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Spania	*Strategia națională de securitate cibernetică* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Suedia	*Strategia națională de securitate cibernetică a Suediei* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Regatul Unit	*Strategia națională de securitate cibernetică (2016-2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Lista de bune practici și recomandări emise de ENISA

Pentru răspunsul în caz de incidente

- ✓ Strategii de răspuns în caz de incidente și de cooperare în caz de criză cibernetică[46]

Pentru gestionarea incidentelor

- ✓ Proiect de automatizare a gestionării incidentelor[47]
- ✓ Ghid de bune practici pentru gestionarea incidentelor[48]

Pentru clasificarea și taxonomia incidentelor

- ✓ Prezentarea generală a taxonomiilor existente[49]
- ✓ Ghid de bune practici privind utilizarea taxonomiilor în prevenirea și detectarea incidentelor[50]

Pentru maturitatea CSIRT

- ✓ Provocări pentru echipele CSIRT naționale în Europa în 2016: studiu privind maturitatea CSIRT[51]
- ✓ Studiu privind maturitatea CSIRT – procesul de evaluare[52]
- ✓ Orientări pentru echipele CSIRT naționale și guvernamentale cu privire la modul de evaluare a maturității[53]

Pentru formarea și consolidarea capacităților CSIRT

- ✓ Ghid de bune practici cu privire la metodologiile de formare[54]

Pentru a găsi informații despre echipele CSIRT existente în Europa - Prezentare generală a echipelor CSIRT defalcate pe țări[55]

---

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). Document disponibil la adresa:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Mai multe informații sunt disponibile la adresa: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[47] Mai multe informații sunt disponibile la adresa: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010). Document disponibil la adresa:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Mai multe informații sunt disponibile la adresa: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). Document disponibil la adresa:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). Document disponibil la adresa:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). Document disponibil la adresa:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). Document disponibil la adresa: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014). Document disponibil la adresa:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
[55] Mai multe informații sunt disponibile la adresa: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map