Consiliul
Uniunii Europene

Bruxelles, 16 ianuarie 2025
(OR. en)

5426/25

CYBER 21
SAN 15

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	15 ianuarie 2025
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2025) 10 final
Subiect:	COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR Plan de acțiune european privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale.

În anexă, se pune la dispoziția delegațiilor documentul COM(2025) 10 final.

Anexă: COM(2025) 10 final

COMISIA
EUROPEANĂ

Bruxelles, 15.1.2025
COM(2025) 10 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

Plan de acțiune european privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale.

1. Introducere

Mediul de securitate al UE evoluează rapid, înregistrându-se o intensificare a atacurilor hibride și cibernetice care urmăresc să destabilizeze societatea, să provoace diviziuni și perturbări, dar și să genereze profituri din activități de criminalitate informatică. Europa trebuie, așadar, să își consolideze de urgență gradul de pregătire și reziliența în fața acestei noi realități, în toate sectoarele, adoptând o abordare integrată la nivelul întregii societăți și administrații, așa cum se recomandă în raportul dlui Sauli Niinistö, consilierul special al președintei Comisiei Europene.

Sistemele de sănătate sigure și reziliente reprezintă o piatră de temelie a modelului social al UE. Spitalele și sistemele de sănătate se confruntă însă cu amenințări în creștere, în special din partea grupurilor care lansează atacuri de tip *ransomware*. Acestea le vizează pentru câștiguri financiare, fiind atrase de valoarea ridicată a datelor pacienților, inclusiv a dosarelor electronice de sănătate. Sănătatea a devenit într-adevăr cel mai atacat sector din UE în ultimii patru ani, inclusiv în timpul pandemiei de COVID-19, când infrastructura de sănătate a fost ținta unui număr tot mai mare de atacuri cibernetice. Atacurile cibernetice asupra spitalelor și furnizorilor de servicii medicale le provoacă daune directe oamenilor, întârzie procedurile medicale, blochează activitatea serviciilor medicale de urgență și, în cazuri extreme, pot avea drept consecință pierderea de vieți omenești.

Provocările cresc tot mai mult, având în vedere că sectorul traversează o transformare digitală de importanță vitală. Serviciile de sănătate digitală și utilizarea, respectiv, reutilizarea datelor privind sănătatea pot facilita crearea unor modele de îngrijire mai bine adaptate nevoilor și preferințelor oamenilor și pacienților, prin prevenirea apariției bolilor sau prin asigurarea unui tratament mai precoce. Integrarea instrumentelor și a soluțiilor digitale în procesele clinice, precum și utilizarea și reutilizarea datelor privind sănătatea pot sta la baza unor decizii clinice mai bune, pot facilita procesele de automatizare în domeniul sănătății și pot avea ca rezultat o îngrijire mai rapidă și mai bună a pacienților. Instrumentele digitale, utilizarea datelor și dispozitivele medicale – adesea conectate la internet și alimentate de inteligența artificială – sunt, de asemenea, esențiale pentru a aborda provocări precum deficitul de profesioniști din domeniul sănătății.

În același timp, instrumentele digitale măresc și aria potențialelor ținte pentru infractorii cibernetici. În plus, anumiți actori statali nu ezită să vizeze unitățile medicale, astfel cum s-a observat în războiul de agresiune pe care Rusia îl duce în prezent împotriva Ucrainei. Prin urmare, sectorul devine o potențială țintă a atacurilor cibernetice, ca parte a unei campanii hibride mai extinse. Atacurile cibernetice nu numai că pun în pericol siguranța pacienților, ci și erodează încrederea publicului în infrastructura de sănătate și presupun costuri de redresare semnificative. Dincolo de protejarea împotriva atacurilor cibernetice, o infrastructură digitală rezilientă și sigură este, de asemenea, esențială pentru susținerea implementării și punerii în funcțiune pe deplin a spațiului european al datelor privind sănătatea[1].

Prin urmare, este momentul să îmbunătățim și să consolidăm securitatea cibernetică și reziliența spitalelor și a furnizorilor de servicii medicale din Europa, așa cum a subliniat președinta von der Leyen în Orientările sale politice pentru mandatul 2024-2029 al Comisiei[2]. Prezentul plan de acțiune răspunde

[1] https://www.consilium.europa.eu/ro/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_ro

caracterului urgent al situației și amenințărilor unice cu care se confruntă sectorul. Nu există o soluție simplă și miraculoasă la provocările în materie de securitate cibernetică în domeniul asistenței medicale. În schimb, planul de acțiune propune consolidarea măsurilor de prevenire și pregătire, precum și o abordare mai coordonată a solidarității, care să valorifice expertiza din sectorul securității cibernetice din Europa. Ca atare, planul de acțiune reflectă abordarea UE în materie de securitate, care va fi dezvoltată și formalizată în viitoarea strategie europeană de securitate internă, definind un răspuns cuprinzător pentru a face față tuturor amenințărilor la adresa securității interne și concentrându-se pe capacitatea de a anticipa amenințările, de a preveni daunele și de a proteja oamenii, acționând pe toate palierele cu o abordare la nivelul întregii societăți.

Sectorul sănătății include un număr larg de entități și actori, cum ar fi spitalele, clinicile, centrele de îngrijire, centrele de reabilitare și diverși furnizori de servicii medicale, alături de industria farmaceutică, medicală și de biotehnologie, de producătorii de dispozitive medicale și de instituțiile de cercetare medicală. Prezentul plan de acțiune se axează în principal pe securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale, adică orice persoană fizică sau juridică – sau orice altă entitate – care furnizează legal asistență medicală pe teritoriul unui stat membru[3]. Spitalele și furnizorii de servicii medicale se află în interdependență cu alte entități din domeniul sănătății, fiind în prima linie a îngrijirii pacienților. În același timp, măsurile de consolidare a securității cibernetice a spitalelor și a furnizorilor de servicii medicale ar trebui să abordeze și riscurile care afectează lanțul de aprovizionare și ecosistemul, în sens mai larg. Aceste riscuri sunt generate, de exemplu, de entitățile care utilizează date privind sănătatea pentru cercetare și învățare automată sau care produc dispozitive medicale, în special dispozitive cu tehnologie digitală integrată care se conectează la internet sau la alte dispozitive („internetul lucrurilor”).

Deși securizarea sistemelor de sănătate este în primul rând o competență națională, sănătatea este și un sector critic în temeiul Directivei privind măsuri pentru un nivel comun ridicat de securitate cibernetică în UE (NIS 2)[4]. Infractorii cibernetici și alți actori care generează amenințări acționează fără a ține cont de granițe, iar provocările în materie de securitate cibernetică cu care se confruntă organizațiile de asistență medicală sunt, de asemenea, similare în toate statele membre. Cooperarea la nivel european este valoroasă pentru schimbul de bune practici și pentru extinderea folosirii acestor practici de la nivelul UE și de la nivel național. Prin urmare, planul de acțiune propune o coordonare și măsuri la nivelul UE, solicitând în același timp ca statele membre să ia măsuri pentru a aduce o schimbare în ceea ce privește asistența medicală și ecosistemul sanitar în sens larg.

Planul de acțiune se axează în primul rând pe consolidarea capacităților sectorului de **a preveni** incidentele de securitate cibernetică, deoarece a preveni este întotdeauna mai bine decât a repara. În al doilea rând, planul de acțiune detaliază acțiunile de îmbunătățire a schimbului de informații în materie de securitate cibernetică și a capacității de **a detecta** amenințările cibernetice, permițând o reacție mai rapidă. În al treilea rând, planul prevede măsuri pentru **a răspunde** mai adecvat la incidente și pentru a

[3] Articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32011L0024

[4] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

se putea **redresa** în urma acestora. În cele din urmă, planul de acțiune prevede modalități de **a descuraja** actorii care generează amenințări cibernetice să lanseze atacuri împotriva sistemelor de sănătate din Europa.

Planul de acțiune va fi pus în aplicare în strânsă colaborare cu furnizorii de servicii medicale și cu ecosistemul de sănătate în sens larg, cu statele membre și cu comunitatea de securitate cibernetică. O abordare bazată pe colaborare este esențială pentru definirea și perfecționarea în continuare a acțiunilor cu cel mai mare impact, astfel încât toți furnizorii de servicii medicale esențiale din Europa să poată beneficia de acestea. Prin urmare, prezenta comunicare va fi însoțită de lansarea unei consultări cuprinzătoare cu părțile interesate, cu sectorul medical și cu statele membre. Cooperarea internațională este importantă pentru securitatea cibernetică, având în vedere că amenințările cibernetice sunt interconectate și nu se opresc la granițe. Cu amenințări comparabile la adresa securității cibernetice se confruntă și țările implicate în procesul de aderare și țările învecinate, precum și alte țări partenere strategice ale UE. Astfel, în cele din urmă, poate fi pusă în pericol securitatea infrastructurii critice din UE. Prin urmare, va fi important ca lecțiile învățate din punerea în aplicare a planului de acțiune să se reflecte și în cooperarea UE atât cu țările implicate în procesul de aderare, cât și cu alte țări partenere, având în vedere nivelurile de amenințare la care este expusă fiecare dintre acestea.

2. Provocările în materie de securitate cibernetică cu care se confruntă spitalele și furnizorii de servicii medicale

Amenințările cibernetice la adresa sectorului sănătății

Atacurile cibernetice sunt în creștere atât la nivel global, cât și în UE, pe fondul unui ansamblu de amenințări tot mai complex și dinamic. Avansurile înregistrate în domeniul inteligenței artificiale pun la dispoziția infractorilor și a persoanelor rău-intenționate instrumente puternice, care le permit să acționeze cu o precizie și un impact sporite. Aceste avansuri deschid însă și noi perspective pentru apărarea cibernetică, bazate pe acțiuni automate și răspunsuri în timp real la atacurile înregistrate.

Atacurile de tip *ransomware* rămân o provocare critică pentru securitatea cibernetică în UE și la nivel global, iar, potrivit estimărilor unui raport, acestea vor genera, până în 2031, un cost anual de peste 250 de miliarde EUR la nivel mondial[5]. În atacurile de tip *ransomware*, infractorii nu se limitează la blocarea accesului la datele victimelor prin criptare și solicitarea unei răscumpărări pentru decriptare, ci dezvăluie din ce în ce mai des informații sensibile pentru a pune o presiune suplimentară pe victime. O altă provocare importantă o reprezintă vulnerabilitățile legate de software și hardware: potrivit Agenției

[5] Cybersecurity Ventures (1 iunie 2024): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031* (Previziuni: Daunele globale provocate de atacurile de tip *ransomware* vor depăși 265 de miliarde de dolari până în 2031). Disponibil la adresa https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Uniunii Europene pentru Securitate Cibernetică (ENISA)[6], asistența medicală este sectorul care a declarat cele mai multe incidente de securitate legate de astfel de vulnerabilități[7]. Printre alte amenințări în creștere se numără atacurile de blocare distribuită a serviciului (*distributed denial-of-service* – DDoS), care aleg un sistem și îl copleșesc cu un volum masiv de trafic, făcându-l inaccesibil utilizatorilor legitimi[8].

În sectorul sănătății există tendințe similare în ceea ce privește amenințările la adresa securității cibernetice, cu un accent deosebit pe atacurile de tip *ransomware*. Potrivit ENISA, atacurile de tip *ransomware* au reprezentat 54 % din incidentele de securitate cibernetică analizate în sectorul sănătății în perioada 2021-2023. 83 % dintre atacuri au fost motivate financiar, fiind determinate de valoarea ridicată a datelor medicale, în timp ce 10 % dintre atacuri au avut o motivație ideologică[9]. În mod similar, într-un raport din 2024 al Comisiei s-a constatat că 71 % din atacurile care au afectat îngrijirea pacienților, cum ar fi accesul cu întârziere la tratament și diagnosticare și accesul limitat la serviciile de urgență, erau de tip *ransomware*[10]. Atacurile de tip *ransomware* pot perturba într-o măsură foarte mare furnizarea de servicii de asistență medicală, punând în pericol siguranța pacienților. În plus, atacurile de tip *ransomware* sunt adesea însoțite de încălcări ale securității datelor pacienților[11], fiind vorba adesea de date sensibile legate de sănătate, rezultând astfel nerespectarea dreptului fundamental al persoanelor la protecția datelor cu caracter personal.

În același timp, pe măsură ce digitalizarea este din ce în ce mai folosită în sistemul de sănătate, crește și vulnerabilitatea la atacuri. Potrivit raportului „Stadiul evoluției deceniului digital – 2024”, în medie, 79 % dintre cetățenii UE au acces online la dosarele lor electronice de sănătate în cadrul asistenței medicale primare[12]. Dosarele electronice de sănătate, sistemele de informații clinice, sistemele de gestionare a fluxului de lucru în spitale, sistemele informatice pentru rambursarea tratamentelor, sistemele de imagistică medicală și dispozitivele medicale utilizate pentru diagnosticare sau monitorizarea pacienților sunt exemple de instrumente digitale care pot juca un rol esențial în îmbunătățirea eficienței și a performanței sectorului sănătății, dar reprezintă și ținte potențiale pentru atacuri cibernetice. Activitățile medicale specifice, cum ar fi terapia intensivă și imagistica radiologică, dar și domenii medicale precum oncologia și cardiologia, care depind în mare măsură de dispozitive cu

---

[6] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (Regulamentul privind securitatea cibernetică), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

[7] Raportul ENISA privind situația amenințărilor: sectorul sănătății (iulie 2023).

[8] Raportul ENISA privind situația amenințărilor în 2024.

[9] Raportul ENISA privind situația amenințărilor: sectorul sănătății (iulie 2023). Raportul a analizat furnizorii de servicii medicale, dar și alte tipuri de organizații, cum ar fi cele care desfășoară activități de cercetare în domeniul sănătății, fabricanții de produse legate de sănătate, autoritățile din sectorul sănătății, societățile de asigurări de sănătate, centrele rezidențiale de tratament și furnizorii de servicii sociale. Disponibil la adresa https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Comisia Europeană: Centrul Comun de Cercetare (JRC), Reina, V. și Griesinger, C., *Cyber security in the health and medicine sector – A study on available evidence of patient health consequences results from Cyber incident in health settings* (Securitatea cibernetică în sănătate și medicină – Analiză pe bază de dovezi a impactului incidentelor cibernetice asupra sănătății pacienților), Oficiul pentru Publicații al UE, 2024, http//data.europa.eu/doi/10.2760/693487.

[11] Potrivit Raportului ENISA privind situația amenințărilor în sectorul sănătății, în 43 % din incidentele de tip *ransomware* analizate s-a confirmat faptul că au avut loc încălcări ale securității datelor sau furturi de date.

[12] Raportul intitulat „Stadiul evoluției deceniului digital – 2024”.

tehnologie digitală integrată, sunt expuse unui risc sporit de atacuri cibernetice. De asemenea, problemele din lanțul de aprovizionare pot conduce la achiziționarea de dispozitive cu protecție cibernetică insuficientă, amplificând riscurile deja existente.

De exemplu, în timpul pandemiei de COVID-19, un atac de tip *ransomware* a paralizat o mare parte a sistemului de sănătate din Irlanda, ceea ce a dus, în dimineața incidentului, la suspendarea a cel puțin unei părți din serviciile oferite în 31 dintre cele 54 de spitale unde se tratează boli acute[13]. Serviciile medicale au fost nevoite să treacă la utilizarea evidențelor pe hârtie, ceea ce a încetinit considerabil eficiența operațiunilor. Atacul a provenit dintr-un e-mail de tip *phishing* cu un fișier atașat ce conținea *malware*[14]. Incidentul a scos în evidență capacitatea atacurilor cibernetice de a se răspândi în diverse sisteme și, implicit, importanța protejării tuturor zonelor vulnerabile ale unei organizații din domeniul sănătății. Totodată, a subliniat cât de important este să se mențină o igienă cibernetică de bază și să se promoveze o cultură solidă a securității cibernetice în cadrul organizațiilor.

Nivelul de maturitate în materie de securitate cibernetică al spitalelor și al furnizorilor de servicii medicale

Situația asistenței medicale din UE este foarte diversă, spitalele și alți furnizori de servicii medicale variind foarte mult de la un stat membru la altul în ceea ce privește cine le deține și ce structură și dimensiuni au. În unele cazuri, guvernanța în domeniul sănătății urmează o abordare centralizată la nivel național, în timp ce în altele este organizată la nivel regional sau local; furnizorii de servicii medicale pot fi publici sau privați. În plus, pot exista diferențe și în cadrul aceleiași țări, de exemplu acolo unde disparitățile socioeconomice și teritoriale dintre regiuni sunt semnificative, ceea ce contribuie la un peisaj complex. Această situație complexă a asistenței medicale poate fi pusă la încercare de crize sanitare importante, cauzate de boli transmisibile, cum ar fi pandemia de COVID-19, dar și de alte riscuri pentru sănătate, de exemplu cele asociate schimbărilor climatice. Nu în ultimul rând, există o variabilitate și o fragmentare semnificative în ceea ce privește nivelul de digitalizare și de adoptare a tehnologiei de către furnizorii de servicii medicale. Un exemplu al acestei complexități este faptul că indisponibilitatea serviciilor provocată de un incident de securitate cibernetică poate avea consecințe grave pentru pacienți chiar și în unități medicale mici, precum clinici sau servicii medicale de urgență, care oferă servicii esențiale unui număr relativ redus de utilizatori.

Potrivit Raportului ENISA din 2024 privind situația securității cibernetice în Uniune[15], maturitatea în materie de securitate cibernetică a sectorului sănătății din UE este moderată și gradul de maturitate variază puternic în Europa de la o entitate din domeniul sănătății la alta. Se remarcă deficiențe în domenii esențiale, precum disponibilitatea resurselor umane, cunoașterea de către organizații a lanțurilor lor de aprovizionare cu tehnologie a informației și comunicațiilor (TIC) și implementarea în produse a unor

[13] Irish Health Service Executive (2021): Conti cyber attack on the HSE: Independent Post Incident Review (Atacul cibernetic Conti asupra HSE – Analiză independentă a incidentului).
[14] Irish Health Service Executive: *Cyber-attack and HSE response* (Atacuri cibernetice și răspunsul HSE). Disponibil la adresa https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA: Raportul din 2024 privind situația securității cibernetice în Uniune (septembrie 2024). Disponibil la adresa https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

funcții de securitate actualizate. Sectorul întâmpină dificultăți în asigurarea unei igiene cibernetice de bază și în aplicarea măsurilor fundamentale de securitate. Acest lucru este reflectat de faptul că aproape toate organizațiile din domeniul sănătății incluse în raport se confruntă cu provocări atunci când trebuie să realizeze evaluări ale riscurilor în materie de securitate cibernetică, iar aproape jumătate dintre ele nu au efectuat niciodată o astfel de analiză[16].

O altă provocare majoră pentru securitatea cibernetică a spitalelor este intersecția dintre tehnologia informației (TI) și tehnologia operațională (TO), unde se întâlnesc priorități de securitate diferite, precum confidențialitatea, disponibilitatea și fiabilitatea, iar o breșă într-un domeniu poate avea repercusiuni asupra celuilalt domeniu. Raportul ENISA din 2024 privind situația securității cibernetice în Uniune subliniază, de asemenea, că sectorul sănătății nu are rezultate satisfăcătoare în asigurarea securității produselor și proceselor TIC pe care le utilizează, din cauza diversității mari de entități, dispozitive și produse din acest sector.

Această diversitate, combinată cu niveluri diferite de conștientizare cibernetică în rândul personalului și al conducerii spitalelor, generează o provocare complexă în asigurarea securității cibernetice a sistemelor de sănătate. De exemplu, potrivit Eurobarometrului din 2024 privind competențele cibernetice, doar 25 % dintre întreprinderile intervievate din sectoarele sănătății, educației și asistenței sociale au desfășurat activități de formare sau de sensibilizare privind securitatea cibernetică în ultimele 12 luni[17]. Sunt necesare acțiuni pentru a promova o cultură a sensibilizării cu privire la securitatea cibernetică în rândul cadrelor medicale din prima linie. De exemplu, rotația personalului, utilizarea posturilor de lucru comune, gestionarea deficitară a autentificării și utilizarea dispozitivelor de stocare amovibile sunt surse suplimentare de vulnerabilități care afectează securitatea cibernetică a furnizorilor de servicii medicale[18].

În multe cazuri, serviciile de TI și TO sunt externalizate cel puțin parțial. Conform Eurobarometrului din 2024, sectoarele sănătății, educației și asistenței sociale înregistrează cea mai mare pondere a societăților care externalizează măcar unele aspecte ale securității cibernetice, 57 % dintre societățile care au participat la eurobarometru recurgând la această practică[19]. În mod similar, migrarea către *cloud computing* devine o tendință puternică, alimentată de nevoia de stocare și gestionare scalabilă a datelor, de eficiența din punctul de vedere al costurilor, de îmbunătățirea colaborării și de sprijinirea tehnologiilor avansate, cum ar fi inteligența artificială și internetul obiectelor medicale. În 2022, 58 % dintre organizațiile din domeniul sănătății utilizau o platformă digitală de sănătate bazată pe *cloud*[20]. Deși poate

[16] Raportul ENISA privind situația amenințărilor: sectorul sănătății (iulie 2023). Disponibil la adresa https://www.enisa.europa.eu/publications/health-threat-landscape.

[17] Sondajul Eurobarometru Flash nr. 547 privind competențele cibernetice (mai 2024). Disponibil la adresa https://europa.eu/eurobarometer/surveys/detail/3176.

[18] *Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres.* (Panacea – Securitate cibernetică centrată pe oameni în domeniul sănătății (2021): Carte albă – Lecții învățate din acțiunea PANACEA privind protecția cibernetică a spitalelor și a centrelor de îngrijire).

[19] Sondajul Eurobarometru Flash nr. 547 privind competențele cibernetice (mai 2024). Disponibil la adresa https://europa.eu/eurobarometer/surveys/detail/3176.

[20] ENISA: Raportul din 2022 privind investițiile în NIS (noiembrie 2022). Disponibil la adresa https://www.enisa.europa.eu/publications/nis-investments-2022.

aduce beneficii semnificative în materie de eficiență, această tranziție vine și cu riscuri, ceea ce impune luarea unor decizii în cunoștință de cauză în privința achizițiilor și a configurării securizate.

Dincolo de toate aceste provocări, problema care se pune este legată de consolidarea capacităților și a finanțării. Securitatea cibernetică în sectorul sănătății a fost subfinanțată, fapt ce rămâne o provocare universală în întreaga UE[21]. În plus, dificultățile de finanțare sunt amplificate de îmbătrânirea populației, un fenomen care, conform estimărilor, va pune presiuni considerabile pe bugetele sistemelor de sănătate europene în deceniile următoare.

Deseori, din cauza problemelor de finanțare, se utilizează în continuare instrumente învechite și sisteme moștenite, nu există resurse suficiente pentru prevenirea sau gestionarea incidentelor, iar nivelul de maturitate în materie de securitate cibernetică prezintă lacune. Spitalele se confruntă constant cu provocarea de a concilia necesitatea unei infrastructuri digitale sigure și actualizate cu alte investiții esențiale pentru îmbunătățirea îngrijirii pacienților, cum ar fi angajarea de medici și alți profesioniști din domeniul sănătății, implementarea unor metode noi de diagnosticare și tratament și achiziția de echipamente. Potrivit ENISA[22], sectorul sănătății se situează pe locul 7 din cele 12 sectoare analizate în ceea ce privește proporția cheltuielilor pentru securitatea informațiilor din totalul cheltuielilor TI, 8,3 % fiind mediana în sectorul sănătății.

3. Centrul european de sprijin pentru securitate cibernetică destinat spitalelor și furnizorilor de servicii medicale

Cadrul de securitate cibernetică al UE oferă o gamă largă de instrumente care ar trebui mobilizate pentru a îmbunătăți securitatea și reziliența spitalelor și a furnizorilor de servicii medicale. Pentru a aborda numeroasele provocări evidențiate anterior, este necesar să se dezvolte o abordare strategică unificată la nivelul UE, care să reunească resursele, expertiza și instrumentele utile pentru a combate în mod eficace amenințările cibernetice. O imagine de ansamblu cuprinzătoare, precum și o mai bună planificare și coordonare sunt esențiale pentru a ajuta furnizorii de servicii medicale din întreaga UE să își consolideze mijloacele de apărare. Pentru a realiza acest obiectiv, ENISA este cea mai în măsură să înființeze, în cadrul organizației sale, un **centru european de sprijin pentru securitate cibernetică destinat spitalelor și furnizorilor de servicii medicale**[23], ca parte a mandatului său[24] de protejare și sprijinire a infrastructurii critice a UE.

Centrul de sprijin ar trebui **să elaboreze** treptat **un catalog cuprinzător de servicii adaptate nevoilor spitalelor și ale furnizorilor de servicii medicale**, evidențiind gama de servicii disponibile pentru

[21] Organizarea și furnizarea de servicii de sănătate și de îngrijire medicală reprezintă o competență națională în temeiul articolului 168 din Tratatul privind funcționarea Uniunii Europene, iar finanțarea sistemelor de sănătate variază de la un stat membru la altul.

[22] ENISA: Raportul din 2022 privind investițiile în NIS (noiembrie 2022). Disponibil la adresa https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] Denumit în prezentul document și „Centrul de sprijin”.

[24] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), JO L 151, 7.6.2019, p. 15.

pregătire, prevenire, detectare și răspuns. În colaborare cu autoritățile statelor membre și pe baza experiențelor spitalelor și ale furnizorilor de servicii medicale, Centrul de sprijin ar trebui să creeze o colecție ușor de utilizat și de accesat, care să includă toate instrumentele disponibile la nivel european, național și regional. Pe parcursul desfășurării activităților sale, centrul ar trebui să asigure o coordonare adecvată cu statele membre și să sprijine prioritizarea și implementarea acțiunilor necesare în timp real.

Ca element esențial pentru elaborarea catalogului de servicii al Centrului de sprijin, Comisia va propune lansarea de proiecte-pilot în întreaga UE pentru a elabora bune practici de evaluare a riscurilor în materie de igienă și securitate cibernetică, precum și pentru a aborda necesitatea monitorizării continue a securității cibernetice, a informațiilor privind amenințările și a răspunsului la incidente, utilizând soluții de securitate cibernetică de ultimă generație. Rezultatele acestor proiecte-pilot, finanțate prin programul „Europa digitală” și implementate de Centrul european de competențe în materie de securitate cibernetică (ECCC), vor sta la baza unor acțiuni suplimentare la nivelul UE, inclusiv a activității Centrului de sprijin.

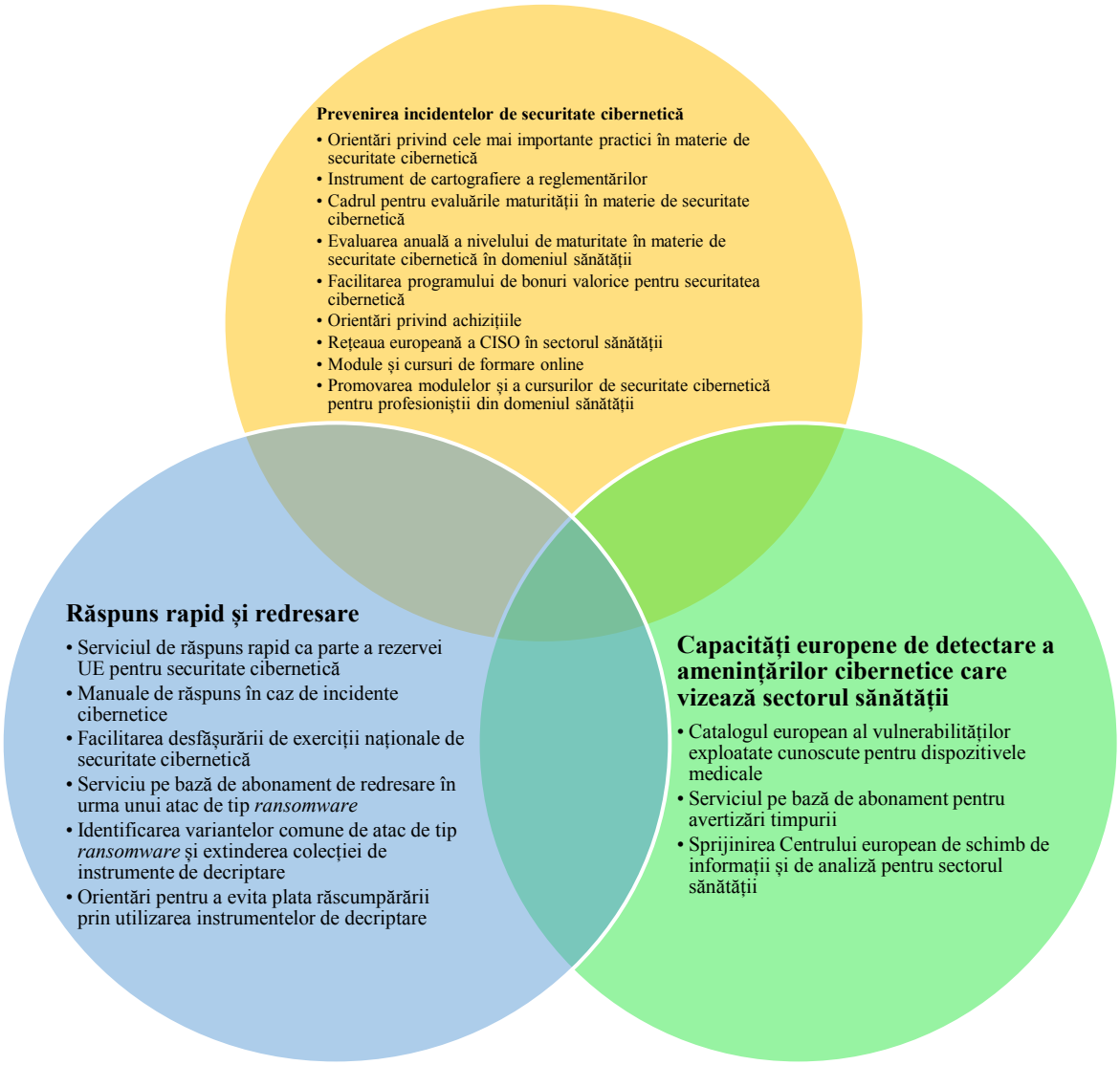

Figura 1: Concepte pentru catalogul de servicii al Centrului de sprijin destinat spitalelor și furnizorilor de servicii medicale

3.1. Prevenirea incidentelor de securitate cibernetică

Acțiuni simple care reduc probabilitatea producerii unui incident cibernetic

Conform unei estimări, măsurile de bază în materie de securitate cibernetică, cum ar fi asigurarea faptului că sistemele sunt actualizate, gestionarea copiilor de rezervă și folosirea autentificării multifactoriale, pot să protejeze organizațiile de până la 98 % din atacuri[25]. Multe dintre măsurile cu cel mai mare impact în materie de igienă cibernetică și de gestionare a riscurilor sunt relativ ușor de adoptat, ceea ce le face să fie o opțiune ușor accesibilă pentru îmbunătățirea securității cibernetice. Unul dintre rolurile esențiale ale Centrului de sprijin ar trebui, prin urmare, să fie **elaborarea unor orientări clare și specifice, care să evidențieze cele mai importante practici în materie de securitate cibernetică și să ajute furnizorii de servicii medicale să le pună în aplicare**. Centrul ar trebui să sprijine nu numai spitalele mari, ci să ofere consiliere personalizată și entităților mai mici, cum ar fi cabinetele medicilor generaliști și clinicile de specialitate de la nivel local, care adesea nu dispun de resursele necesare pentru a avea echipe dedicate pentru asigurarea securității cibernetice, dar sunt la fel de vulnerabile la atacuri. În plus, este necesar să se ia în considerare importanța regională a anumitor entități din domeniul asistenței medicale pentru asigurarea îngrijirii pacienților, de exemplu în zonele slab populate. Institutele de cercetare în domeniul sănătății care gestionează volume mari de date sensibile cu caracter personal ar putea beneficia, de asemenea, de orientări privind măsurile de bază în materie de securitate cibernetică pentru a-și spori reziliența.

Organizațiile din domeniul sănătății au, la rândul lor, o serie de obligații legate de securitatea cibernetică ce derivă din legislația UE[26]. Deși aceste obligații sunt esențiale pentru asigurarea unui nivel de referință

[25] *Microsoft Digital Defense Report 2022* (Raportul Microsoft privind apărarea în domeniul digital, 2022). Disponibil la https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Cum ar fi Directiva NIS 2; Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale (Regulamentul privind reziliența cibernetică), https://eur-lex.europa.eu/eli/reg/2024/2847/ojhttps://eur-lex.europa.eu/eli/reg/2024/2847/oj; Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, https://eur-lex.europa.eu/eli/reg/2017/745/ojhttps://eur-lex.europa.eu/eli/reg/2017/745/oj (Regulamentul privind dispozitivele medicale), https://eur-lex.europa.eu/eli/reg/2017/745/oj, Regulamentul privind dispozitivele medicale; Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic *in vitro* (Regulamentul privind dispozitivele medicale pentru diagnostic *in vitro*), https://eur-lex.europa.eu/eli/reg/2017/746/ojhttps://eur-lex.europa.eu/eli/reg/2017/746/oj; Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea

comun ridicat în ceea ce privește securitatea cibernetică și securitatea datelor, este crucial să se evite ca, pe parcurs, cadrul de reglementare să devină inutil de complicat și împovărător. Accentul puternic pus pe conformitate nu ar trebui să contravină obiectivului de a promova o cultură puternică a securității cibernetice. Un **instrument de cartografiere a reglementărilor ușor de accesat poate contribui la reducerea la minimum a sarcinii administrative pentru entitățile care fac obiectul mai multor norme de reglementare**. Pe lângă elaborarea de orientări și de seturi de instrumente, Centrul de sprijin ar trebui să colaboreze îndeaproape cu Comisia și cu statele membre pentru a dezvolta și a disemina un astfel de instrument cât mai curând posibil. Prin urmare, Centrul de sprijin ar urma să joace un rol important în facilitarea înțelegerii și a punerii în aplicare a normelor în materie de securitate cibernetică, de exemplu prin furnizarea de orientări privind punerea în aplicare[27] și, după caz, prin promovarea de standarde relevante.

Viitoarele **portofele europene pentru identitatea digitală** constituie un alt instrument menit să faciliteze aplicarea simplă a bunelor practici de igienă cibernetică. Reducerea folosirii soluțiilor de identificare cu un grad scăzut de siguranță, cum ar fi parolele, este esențială pentru a diminua riscurile de acces neautorizat la datele privind sănătatea. Trecerea la soluții sigure de autentificare, bazate pe identificare fiabilă, este esențială. Portofelul european pentru identitatea digitală oferă o abordare armonizată la nivelul UE a identificării electronice pentru profesioniștii din domeniul sănătății, oferind o soluție solidă și unificată ce va fi disponibilă la sfârșitul anului 2026. Pentru toate sistemele online de informații privind sănătatea care trebuie să implementeze autentificarea strictă a utilizatorilor va exista cerința de a accepta acest portofel în scopuri de identificare, începând cu sfârșitul anului 2027[28].

Pregătire și sprijin specific

Testarea pregătirii, care include acțiuni precum testele de penetrare cibernetică, reprezintă un element esențial al unei securități cibernetice eficiente. Comisia a alocat deja finanțare agenției ENISA pentru inițiative-pilot de pregătire, care au evidențiat că sectorul sănătății este unul dintre cele mai solicitate domenii pentru testare și evaluări suplimentare, în vederea identificării lacunelor privind maturitatea în domeniul securității cibernetice. Odată cu intrarea în vigoare a Regulamentului privind solidaritatea cibernetică, aceste eforturi se vor extinde semnificativ, ECCC preluând rolul de lider. Pentru a răspunde acestei nevoi, Comisia va propune, în consultare cu Grupul de cooperare NIS, UE-CyCLONe[29] și

---

datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor), https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016R0679; Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul privind inteligența artificială), https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1689; Propunere de regulament al Parlamentului European și al Consiliului referitor la spațiul european al datelor privind sănătatea, COM(2022)197 final, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52022PC0197. Negocierile s-au încheiat cu un acord politic în primăvara anului 2024 și, după parcurgerea ultimelor etape necesare, se preconizează că actul va fi publicat în Jurnalul Oficial în primăvara anului 2025.

[27] Comitetul european pentru protecția datelor (CEPD) este responsabil cu elaborarea de orientări privind interpretarea Regulamentului general privind protecția datelor (RGPD). Elaborarea orientărilor de către ENISA trebuie să respecte pe deplin prerogativele CEPD.

[28] Articolul 5f alineatele (1) și (2) din Regulamentul (UE) nr. 910/2014.

[29] Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice

ENISA, identificarea sectorului sănătății ca fiind eligibil pentru a primi sprijin în vederea **testării coordonate a nivelului de pregătire**, în conformitate cu prevederile Regulamentului privind solidaritatea cibernetică. În plus, Centrul de sprijin ar trebui să elaboreze **un cadru adaptat pentru evaluările nivelului de maturitate în materie de securitate cibernetică specifice domeniului medical**. Astfel de evaluări ale nivelului de maturitate ar urma să furnizeze entităților informații concrete cu privire la vulnerabilitățile lor, oferindu-le posibilitatea de a demonstra pacienților și părților interesate că sunt pregătite pentru provocările în materie de securitate cibernetică, consolidând astfel încrederea în serviciile oferite. La nivel agregat, Centrul de sprijin ar trebui să efectueze o **evaluare anuală a nivelului de maturitate în materie de securitate cibernetică în domeniul sănătății**, care să stabilească o imagine de ansamblu clară a securității cibernetice a acestui sectorul atât la nivel național, cât și la nivelul UE.

Sectorul sănătății depinde în mare măsură de contractori externi pentru serviciile de securitate cibernetică[30], fapt ce evidențiază necesitatea unui sprijin țintit pentru consolidarea mijloacelor de apărare. Pe baza inițiativelor de succes, precum bonurile valorice ale UE pentru inovare, **statele membre ar trebui să aibă în vedere măsuri specifice, cum ar fi bonurile valorice pentru securitate cibernetică destinate spitalelor și furnizorilor de servicii medicale care sunt microîntreprinderi sau întreprinderi mici și mijlocii**. Aceste bonuri valorice ar urma să ofere asistență financiară pentru a pune în aplicare măsuri specifice de securitate cibernetică. Bonurile valorice ar trebui alocate în funcție de priorități, pe baza rezultatelor testelor de pregătire și ale evaluărilor nivelului de maturitate.

Este esențial să se cunoască situația și contextul de la nivel local pentru derularea eficace a programului de bonuri valorice sau a altor programe de sprijin și pentru asigurarea relevanței și accesibilității acestora. Fondurile UE, cum ar fi Fondul european de dezvoltare regională, sunt deja folosite pentru a sprijini inițiative în materie de securitate cibernetică și sănătate digitală și, prin urmare, ar putea, astfel, să contribuie la dezvoltarea unor scheme specifice pe bază de bonuri valorice pentru securitate cibernetică destinate furnizorilor de servicii medicale. Pentru a impulsiona acest efort, Centrul de sprijin ar urma să colaboreze cu statele membre și cu autoritățile regionale responsabile de programe pentru a susține dezvoltarea unor astfel de scheme regionale de bonuri valorice, valorificând lecțiile învățate din proiectele naționale existente, precum și din acțiunile finanțate în cadrul programului Europa digitală pentru a asigura o aplicare practică și cu impact.

În plus, începând din 2014, programele Orizont au avut un rol esențial în finanțarea unei serii de inițiative de cercetare axate pe consolidarea rezilienței instituțiilor de asistență medicală, cum ar fi spitalele, împotriva amenințărilor cibernetice și pe atenuarea riscurilor asociate utilizării abuzive a tehnologiilor emergente. Printre rezultatele preconizate se numără o serie de instrumente, cadre și sisteme specializate, precum instrumentele de evaluare a riscurilor, platformele de partajare a datelor cu respectarea confidențialității, soluțiile criptografice, programele de formare pentru sensibilizarea cu privire la securitatea cibernetică și sistemele de detectare a amenințărilor în timp real. În special, aceste soluții au fost validate în mod riguros prin implementarea pe teren a unor proiecte-pilot în medii din domeniul

[30] A se vedea Raportul ENISA din 2023 privind investițiile în NIS (noiembrie 2023), care evidențiază importanța sprijinului extern pentru auditul și conformitatea în materie de securitate cibernetică. Disponibil la adresa https://www.enisa.europa.eu/publications/nis-investments-2023.

asistenței medicale, demonstrându-și eficiența și aplicabilitatea practică în protejarea împotriva amenințărilor cibernetice.

Asigurarea lanțurilor de aprovizionare din domeniul medical

Una dintre principalele provocări pentru organizațiile din domeniul sănătății este gestionarea lanțurilor de aprovizionare cu tehnologii TIC complexe, care includ o gamă variată de produse, precum dispozitive medicale conectate, sistemele de dosare electronice de sănătate și echipamente hardware pentru birouri. Spitalele și furnizorii de servicii medicale au nevoie de sisteme și servicii TIC fiabile și sigure pentru a-și desfășura activitatea. Pentru a contribui la abordarea provocărilor în materie de securitate cibernetică în sectorul sănătății, Grupul de cooperare NIS ar trebui să efectueze **o evaluare coordonată a riscurilor în materie de securitate, analizând atât riscurile tehnice, cât și riscurile strategice legate de lanțurile de aprovizionare cu dispozitive medicale și propunând măsuri de atenuare a riscurilor**[31]**.** După caz, Grupul de cooperare NIS ar trebui să colaboreze cu Grupul de coordonare privind dispozitivele medicale.

Regulamentul privind reziliența cibernetică este un cadru nou și cuprinzător care stabilește cerințe în materie de securitate cibernetică pentru planificarea, proiectarea, dezvoltarea, precum și pentru gestionarea, remedierea și raportarea vulnerabilităților exploatate activ în ceea ce privește aproape toate produsele hardware și software, în fiecare etapă a lanțului valoric[32]. Dispozitivele medicale sunt o categorie de produse utilizate într-unul dintre cele mai sensibile domenii ale societății. Cerințele de securitate cibernetică pentru aceste produse sunt prevăzute în Regulamentul privind dispozitivele medicale și în Regulamentul privind dispozitivele medicale pentru diagnostic *in vitro*[33], aflate deja în vigoare. Evaluarea în curs a acestor regulamente analizează posibilitatea unei mai mari coerențe și sinergii între aceste cadre, pentru a garanta simplificarea și adoptarea celor mai avansate standarde de securitate cibernetică.

În plus, rezultatele evaluării riscurilor ar trebui să ajute organizațiile din domeniul sănătății să își revizuiască practicile de securitate cibernetică din lanțul de aprovizionare, astfel cum se prevede în Directiva NIS 2, și ar putea contribui la elaborarea de noi **orientări privind achizițiile**[34]. Aceste orientări, care ar urma să fie elaborate de ENISA prin intermediul Centrului său de sprijin, ar trebui să reflecte tendințele recente, cum ar fi stocarea în *cloud* a datelor pacienților, inclusiv necesitatea migrării în condiții de siguranță a datelor electronice privind sănătatea în mediile de tip *cloud*. În plus, noile orientări ar trebui să ofere instrumente practice pentru organizații, astfel încât acestea să își poată

[31] În temeiul articolului 22 din Directiva NIS 2.

[32] Într-o primă etapă, începând cu 1 august 2025, categorii largi de echipamente radio care nu intră în domeniul de aplicare al Regulamentului privind dispozitivele medicale și al Regulamentului privind dispozitivele medicale pentru diagnostic *in vitro* vor trebui să respecte cerințele esențiale ale Directivei privind echipamentele radio care se referă la securitatea cibernetică atunci când vor fi introduse pe piața unică. Într-o a doua etapă, Regulamentul privind reziliența cibernetică va începe să se aplice de la 11 decembrie 2027.

[33] În decembrie 2019, Grupul de cooperare privind dispozitivele medicale a emis orientări privind securitatea cibernetică a dispozitivelor medicale, sprijinind producătorii să îndeplinească cerințele din anexa I la cele două regulamente: https://ec.europa.eu/docsroom/documents/41863.

[34] Pe baza Orientărilor ENISA din 2020 privind achizițiile pentru securitatea cibernetică în spitale (februarie 2020). Disponibile la adresa https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

monitoriza lanțurile de aprovizionare, inclusiv furnizorii de servicii de securitate gestionate (*managed security service providers* – MSSP), rapoartele de atestare sau evaluări ale riscurilor generate de terți.

În ceea ce privește utilizarea serviciilor de *cloud*, sunt necesare acțiuni suplimentare pentru a aborda provocările specifice gestionării datelor sensibile din domeniul sănătății, inclusiv riscurile sporite operaționale, de securitate și de confidențialitate. Pentru a consolida măsurile de protecție, experții recomandă integrarea în serviciile de *cloud* a principiului „securitate implicită și de la stadiul conceperii". Această abordare acordă prioritate infrastructurii securizate, gestionării proactive a vulnerabilităților și unei combinații de soluții publice și private de *cloud*. Monitorizarea continuă și atestările specifice furnizorilor – cum ar fi certificările furnizorilor de securitate și auditurile de conformitate cu standardele naționale și internaționale – sunt, de asemenea, esențiale pentru asigurarea unor practici solide în materie de securitate.

Pentru servicii precum infrastructura ca serviciu (*Infrastructure-as-a-Service* – IaaS), platforma ca serviciu (*Platform-as-a-Service* – PaaS) și software-ul ca serviciu (*Software-as-a-Service* – SaaS), responsabilitatea implementării măsurilor de securitate îi revine adesea clientului. Dar multe organizații din domeniul sănătății nu dispun de resursele necesare pentru a îndeplini aceste cerințe în mod independent. Pentru a remedia această situație, **furnizorii de servicii de *cloud* ar trebui încurajați să implementeze măsuri de securitate de bază ca funcționalitate standard**. Aceste măsuri ar reduce riscul configurărilor greșite, ar asigura o protecție uniformă în mediile gestionate de clienți și le-ar oferi o mai mare siguranță utilizatorilor. Stabilirea unui standard de bază de securitate implicită ar avea ca scop găsirea unui echilibru între protecția avansată și ușurința în utilizare, astfel încât să fie accesibil pentru o gamă largă de organizații din domeniul sănătății. Acest demers ar implica o colaborare strânsă între furnizorii de servicii de *cloud* și sectorul sănătății, valorificând cele mai bune practici din industrie pentru a crea soluții eficace și scalabile.

Formare și dezvoltarea competențelor

Dispunerea de personal cu competențe solicitate pe piață este esențială pentru creștere durabilă pe termen lung și competitivitate în Europa, precum și pentru furnizarea de servicii de înaltă calitate, inclusiv de asistență medicală. Lipsa profesioniștilor calificați în securitate cibernetică reprezintă o provocare majoră în întreaga Europă, estimându-se că, pentru a răspunde nevoilor de forță de muncă din UE, ar fi necesari 299 000 de astfel de profesioniști[35]. Potrivit Eurobarometrului din 2024 privind competențele cibernetice[36], 81 % din societăți consideră că dificultățile în ceea ce privește angajarea de personal în domeniul securității cibernetice reprezintă un risc major din perspectiva potențialelor atacuri cibernetice. În sectoarele educației, sănătății și asistenței sociale, 66 % din posturile din domeniul securității cibernetice sunt ocupate de angajați care s-au transferat din alte posturi, fără legătură cu securitatea cibernetică, ceea ce evidențiază nevoia urgentă de recalificare și perfecționare.

[35] Peisajul securității cibernetice în 2024: perspective din studiul ISC2 despre forța de muncă în domeniu | Platforma pentru competențe digitale și locuri de muncă

[36] Sondajul Eurobarometru Flash nr. 547 privind competențele cibernetice.

Pentru a aborda această provocare, Centrul de sprijin ar trebui să colaboreze cu viitorul Consorțiu pentru o infrastructură digitală europeană (*European Digital Infrastructure Consortium* – EDIC) pentru competențe în materie de securitate cibernetică, prevăzut în Comunicarea Comisiei intitulată „Academia de competențe în materie de securitate cibernetică”[37]. Această activitate ar trebui să faciliteze schimburile de experiență dintre profesioniștii în securitate cibernetică din sectorul sănătății, cum ar fi directorii responsabili cu securitatea informațiilor (*Chief Information Security Officers* – CISO). O posibilă acțiune ar fi crearea unei **rețele europene a CISO în sectorul sănătății**, pornind de la un grup de experți care să împărtășească și să dezvolte cele mai bune practici, strategii de păstrare a resurselor umane valoroase și soluții pentru atragerea profesioniștilor în securitate cibernetică în sectorul sănătății. În plus, sub egida Academiei de competențe în materie de securitate cibernetică, ar trebui dezvoltate resurse pentru a consolida forța de muncă specializată în securitate cibernetică în sectorul sănătății, cu sprijinul industriei și al mediului academic. În acest sens, părțile interesate din acest sector ar trebui încurajate să se angajeze să sprijine îmbunătățirea formării în materie de securitate cibernetică.

Eroarea umană continuă să fie un factor major în incidentele de securitate cibernetică în domeniul sănătății, fapt ce subliniază nevoia critică de formare completă a personalului și de sensibilizare în domeniul cibernetic. Având în vedere că profesioniștii din domeniul sănătății utilizează frecvent instrumente digitale, este esențial ca aceștia să aibă cunoștințele necesare privind practicile sigure. Formarea specifică și campaniile de sensibilizare pot reduce în mod semnificativ riscurile. Pentru a aborda acest aspect, Centrul de sprijin ar trebui să colaboreze cu profesioniștii din domeniul sănătății și cu furnizorii de servicii medicale și să coopereze cu furnizorii de educație și formare, cu industria, cu EDIC privind competențele în materie de securitate cibernetică, precum și cu autoritățile statelor membre pentru a crea și a disemina **module și cursuri de formare online extinse și ușor de accesat**.

Integrarea modulelor de competență digitală și securitate cibernetică în programele educaționale este esențială pentru construirea unei baze solide de securitate cibernetică în domeniul sănătății. Aceste module ar trebui să abordeze aspecte sectoriale specifice, precum protecția datelor pacienților și vulnerabilitățile în ceea ce privește securitatea dispozitivelor medicale. Dezvoltarea acestor resurse ar trebui să țină seama de acțiunile anterioare, cum ar fi proiectul BeWell finanțat în cadrul programului Erasmus+[38] și proiectul PANACEA finanțat în cadrul programului Orizont 2020[39].

[37] Comunicarea Comisiei către Parlamentul European și Consiliu: Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE („Academia de competențe în materie de securitate cibernetică”). COM(2023) 207 final.

[38] BeWell – *Blueprint alliance for a future health workforce strategy on digital and green skills* (Alianță pentru o strategie viitoare referitoare la forța de muncă din domeniul sănătății în ceea ce privește competențele digitale și verzi). Disponibil la adresa https://bewell-project.eu/.

[39] PANACEA – *Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people* (Asigurarea protecției și confidențialității infrastructurilor spitalicești și de sănătate prin soluții inteligente de securitate cibernetică și un set de instrumente pentru amenințările cibernetice privind datele și persoanele). Disponibil la adresa https://cordis.europa.eu/project/id/826293.

3.2. Capacități europene de detectare a amenințărilor cibernetice care vizează sectorul sănătății

Detectarea eficace a amenințărilor cibernetice este esențială pentru a răspunde rapid în caz de incidente. Actorii care generează amenințări pot folosi tehnici care fac intruziunile greu de detectat și astfel beneficiază de un acces neautorizat prelungit într-un sistem[40]. Prin urmare, îmbunătățirea capacităților de detectare a amenințărilor poate contribui la stoparea atacurilor cibernetice din faze incipiente. De exemplu, în atacul de tip *ransomware* împotriva furnizorului finlandez de servicii de psihoterapie Vastaamo, când autorul a șantajat pacienții ale căror dosare confidențiale le furase, intruziunea inițială a avut loc în 2018, dar Vastaamo și-a dat seama de acest lucru abia în 2020[41].

Schimbul eficient de informații și colaborarea sunt esențiale pentru îmbunătățirea detectării amenințărilor și a conștientizării situației în întreaga UE. Echipele de intervenție în caz de incidente de securitate informatică (CSIRT) au un rol vital în primirea rapoartelor privind incidentele, în incidentele evitate la limită și amenințările potențiale, oferind orientări privind măsurile de atenuare la nivel național. Cu toate acestea, **se recomandă insistent ca statele membre să partajeze cu Centrul de sprijin al ENISA și toate notificările de incidente cibernetice pe care le primesc din partea spitalelor și a furnizorilor de asistență medicală, pentru a permite o conștientizare a situației la nivelul UE**. În mod ideal, acest lucru ar trebui să fie însoțit de o descriere detaliată a diferitelor dimensiuni relevante ale incidentelor, inclusiv a vulnerabilităților și a efectelor profunde cunoscute asupra serviciilor de asistență medicală și a evenimentelor adverse ale pacienților. În plus, producătorii de dispozitive medicale și de dispozitive pentru diagnostic *in vitro* sunt încurajați să raporteze în mod voluntar, prin intermediul platformei unice de raportare care urmează să fie instituită și gestionată de ENISA în conformitate cu Regulamentul privind reziliența cibernetică, vulnerabilitățile exploatate activ sau incidentele cibernetice grave care au un impact asupra securității acestor dispozitive, precum și, eventual, alte vulnerabilități, incidente, incidente evitate la limită sau amenințări cibernetice care pot afecta profilul de risc al acestor dispozitive.

În cazul în care informațiile cuprinse în rapoarte nu mai sunt sensibile, Centrul de sprijin ar putea crea un catalog european al vulnerabilităților exploatate cunoscute care să fie sponsorizat de ENISA pentru dispozitivele medicale, sistemele de dosare electronice de sănătate și furnizorii de echipamente și software TIC în domeniul sănătății. Pentru a aborda provocările semnificative legate de detectarea amenințărilor, Centrul de sprijin ar trebui să introducă **un serviciu pe bază de abonament pentru avertizări timpurii la nivelul UE în sectorul sănătății, care să furnizeze alerte în timp aproape real**. Acest serviciu ar urma să se bazeze pe datele prelucrate de echipele de intervenție în caz de incidente de securitate informatică, pe entitățile și producătorii din domeniul asistenței medicale, pe informațiile din surse deschise și pe alți actori relevanți, cum ar fi centrele cibernetice, centrele de schimb de informații și de analiză și autoritățile de aplicare a legii. O cooperare consolidată dintre ENISA și Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) – de exemplu în ceea ce privește modelele de criminalitate informatică împotriva sectorului sănătății – ar contribui la o mai bună conștientizare a situației.

[40] Raportul din 2023 al ENISA privind situația amenințărilor în sectorul sănătății.
[41] Decizia 1150/161/2021 a Ombudsmanului finlandez pentru protecția datelor.

Aceste centre de schimb de informații și de analiză sunt resurse centrale pentru colectarea de informații operative privind amenințările cibernetice, promovând schimbul de informații bidirecțional între sectorul public și cel privat și promovând consolidarea încrederii. Centrul de sprijin ar trebui să intensifice susținerea acordată **Centrului european de schimb de informații și de analiză pentru sectorul sănătății** prin instrumente și schimburi de informații, prin rapoarte sectoriale de conștientizare a situației, precum și prin promovarea unei comunități de încredere pentru colaborarea tactică și strategică. Statele membre ar trebui să încurajeze dezvoltarea la nivel național a unor astfel de centre de schimb de informații și de analiză pentru sectorul sănătății[42]. Aceste centre ar trebui, de asemenea, să fie încurajate să reunească furnizorii de servicii medicale și producătorii pentru a crea o înțelegere comună a amenințărilor la adresa securității cibernetice, inclusiv în lanțul de aprovizionare, și pentru a facilita un dialog cu privire la proiectarea în condiții de siguranță a produselor, care să țină seama cu adevărat de realitățile implementării de pe teren.

3.3.Răspuns rapid și redresare

Având în vedere sensibilitatea ridicată a datelor pacienților privind sănătatea și efectele potențial devastatoare ale atacurilor cibernetice asupra serviciilor de asistență medicală, este esențial să existe un răspuns rapid și eficace la incidentele de securitate cibernetică pentru protejarea siguranței pacienților. Atunci când un spital sau un furnizor de asistență medicală se confruntă cu un atac cibernetic, primul punct de contact este echipa CSIRT națională relevantă[43]. Echipa CSIRT este responsabilă cu furnizarea de sprijin în timp util, în mod ideal în termen de 24 de ore, pentru a ajuta la gestionarea incidentelor semnificative. Cu toate acestea, în cazul în care un incident depășește capacitatea echipei CSIRT, ar trebui să fie disponibil sprijin din partea UE pentru a asigura un răspuns rapid și eficace.

Rezerva UE pentru securitate cibernetică, instituită în temeiul Regulamentului privind solidaritatea cibernetică, oferă servicii de răspuns la incidente din partea unor furnizori de încredere de servicii de securitate gestionate pentru a oferi sprijin în caz de incidente de securitate cibernetică semnificative sau de mare amploare și a ajuta eforturile inițiale de redresare. Această rezervă este menită să completeze eforturile echipelor CSIRT ale statelor membre, permițându-le acestora să solicite sprijin suplimentar în cazurile ce vizează sectoare critice, cum ar fi sănătatea. Pentru a consolida acest sistem, **Comisia și ENISA ar trebui să se asigure că rezerva include un serviciu de răspuns rapid special pentru sectorul sănătății.** În complementaritate cu alte cadre existente, acest serviciu ar urma să trimită experți pentru a gestiona fără întârziere incidentele de securitate cibernetică semnificative sau de mare amploare în domeniul sănătății atunci când sprijinul național este insuficient.

[42] De exemplu, Finlanda are un centru național de schimb de informații și de analiză pentru sectorul asistenței sociale și al asistenței medicale. A se vedea Centrul Național de Securitate Cibernetică din Finlanda: Grupurile de schimb de informații din cadrul centrului, https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] Articolul 23 alineatul (1) din Directiva NIS 2 prevede cerința ca entitățile esențiale și entitățile importante să notifice incidentele semnificative echipei CSIRT relevante sau, după caz, autorității competente.

Pentru a îmbunătăți răspunsul și redresarea, Centrul de sprijin, în colaborare cu Grupul de cooperare NIS, cu rețeaua CSIRT și, după caz, cu Europol, ar trebui să elaboreze **manuale de răspuns în caz de incidente cibernetice adaptate domeniului sănătății**. Aceste manuale ar urma să ofere îndrumări atât echipelor CSIRT, cât și organizațiilor din domeniul sănătății în ceea ce privește răspunsul la amenințările specifice la adresa securității cibernetice, inclusiv la atacurile de tip *ransomware*. Având în vedere importanța unei cooperări eficace între echipele CSIRT și autoritățile de aplicare a legii în ceea ce privește răspunsul în caz de incidente de securitate cibernetică de natură penală și investigarea acestora, manualele ar trebui să includă, printre alte aspecte, orientări clare cu privire la raportarea unor astfel de incidente către autoritățile de aplicare a legii. În plus, Centrul de sprijin ar putea **facilita organizarea pe scară largă de exerciții naționale de securitate cibernetică, pe baza experiențelor dobândite în urma unor exerciții precum exercițiul Cyber Europe din 2022 al ENISA, pentru a testa manualele și a consolida protocoalele de răspuns în caz de incidente**.

Pentru a fundamenta politicile și a evalua eficacitatea măsurilor luate împotriva atacurilor de tip *ransomware*, este necesar să se colecteze date suplimentare. În acest scop, statele membre ar trebui să solicite entităților care intră sub incidența Directivei NIS 2, inclusiv organizațiilor din domeniul sănătății, să raporteze toate plățile de răscumpărare efectuate, precum și plățile de acest tip pe care intenționează să le efectueze, alături de alte informații furnizate în contextul raportării incidentelor semnificative de securitate cibernetică. Astfel se sprijină investigarea eficace a incidentelor de tip *ransomware*, inclusiv urmărirea plăților pe platformele de schimb de criptomonede pentru a se identifica destinatarii.

Viteza de redresare este un factor esențial pentru menținerea rezilienței și a încrederii publicului, în special în domeniul asistenței medicale, în care perioadele de indisponibilitate pot perturba îngrijirea pacienților. Pentru o redresare eficace în urma atacurilor de tip *ransomware*, furnizorii de servicii medicale trebuie să dispună de copii de rezervă sigure, actualizate și izolate, care să poată fi restaurate rapid. Ca parte a catalogului său de servicii, Centrul de sprijin ar putea oferi **un serviciu pe bază de abonament de redresare în urma unui atac de tip *ransomware*, care să ajute spitalele și furnizorii de servicii medicale să elaboreze în prealabil planuri de redresare**. ENISA și Europol ar trebui să colaboreze pentru a identifica cele mai comune tipuri de atac de tip *ransomware* ce vizează organizațiile din domeniul sănătății și pentru **a extinde colecția de instrumente de decriptare** prin intermediul proiectului *No More Ransom*[44]. De asemenea, acestea ar trebui să elaboreze și să promoveze orientări accesibile pentru a ajuta furnizorii de servicii medicale să evite plata de răscumpărări prin utilizarea instrumentelor de decriptare.

Inițiativa internațională de combatere a atacurilor de tip *ransomware*[45] este o arenă valoroasă pentru schimbul de informații cu privire la incidente specifice de tip *ransomware*, precum și pentru consolidarea capacităților țărilor membre de a-și întări cadrele de securitate cibernetică și capacitățile de investigare împotriva actorilor care practică acest tip de atacuri. Comisia, în colaborare cu Înalta Reprezentantă, va continua să promoveze cooperarea în cadrul Inițiativei de combatere a atacurilor de tip ransomware, inclusiv împotriva amenințărilor de acest tip la adresa sectorului sănătății. În plus, Comisia va promova cooperarea în cadrul **Grupului de lucru pentru securitate cibernetică al G7**, pentru a consolida

[44] https://www.nomoreransom.org/en/index.html.
[45] https://www.counter-ransomware.org/

securitatea cibernetică a sectorului sănătății. În special, grupul de lucru ar putea lua în considerare posibilitățile de sprijinire a sectorului sănătății împotriva amenințărilor de genul celor de tip *ransomware*, pe baza unor reflecții precum Declarația comună privind atacurile de tip *ransomware* împotriva structurilor de asistență medicală, din 8 noiembrie 2024, prezentată în cadrul Consiliului de Securitate al Organizației Națiunilor Unite[46].

4. Acțiuni la nivel național

Prezentul plan de acțiune va fi în măsură să genereze îmbunătățirea securității cibernetice în sectorul sănătății doar dacă statele membre se vor implica și angaja activ în acest sens. Pentru a pune în aplicare cu succes planul de acțiune, statele membre ar putea desemna **centre naționale de sprijin pentru securitatea cibernetică dedicate spitalelor și furnizorilor de servicii medicale**. Aceste centre ar urma să acționeze ca puncte principale de contact pentru sectorul sănătății la nivel național, colaborând îndeaproape cu Centrul de sprijin al ENISA. În măsura posibilului și dacă este relevant, statele membre ar trebui să desemneze organismele existente, cum ar fi echipele CSIRT naționale din domeniul sănătății sau autoritățile relevante, drept centre naționale de sprijin pentru securitate cibernetică.

Statele membre sunt totodată încurajate să elaboreze **planuri naționale de acțiune axate pe securitatea cibernetică în sectorul sănătății**. Aceste planuri ar trebui să evidențieze riscurile specifice în materie de securitate cibernetică cu care se confruntă sistemele de sănătate și acțiunile naționale întreprinse pentru a le aborda și să asigure, în același timp, o utilizare eficace a resurselor și a practicilor la nivel european. Centrul de sprijin al ENISA poate contribui la elaborarea acestor planuri, ținând seama de planurile naționale deja existente și de eforturile de coordonare pentru a se asigura că resursele și strategiile fiecărui stat membru se completează reciproc.

Un alt obiectiv esențial pentru statele membre este facilitarea partajării resurselor între furnizorii de servicii medicale, care ar putea fi realizată prin **achiziții comune sau resurse puse în comun** la nivel național, regional sau chiar european. Această abordare ar reduce sarcina financiară asupra fiecărei entități, sporindu-le în același timp puterea acestora de negociere cu furnizorii de servicii de securitate cibernetică.

De exemplu, programul francez CaRE[47] a introdus o serie de măsuri la nivel național și regional pentru a aborda provocările legate de alocarea de resurse: un catalog cibernetic oferă o imagine de ansamblu a soluțiilor și pachetelor cibernetice puse la dispoziția spitalelor prin intermediul agenției naționale pentru securitate cibernetică, al agenției de sănătate digitală, al agențiilor regionale, al organizațiilor naționale de achiziții, precum și al soluțiilor comerciale. Acesta este completat de o finanțare suplimentară pentru ca agențiile regionale să ofere resurse comune.

[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

[47] Agenția franceză de sănătate digitală: *Cybersécurité acceleration et Résilience des Établissements – CaRE*) (Cibersecuritate: accelerare și reziliența entităților). Disponibil la adresa https://esante.gouv.fr/strategie-nationale/cybersecurite.

Statele membre ar trebui, de asemenea, să abordeze nivelurile insuficiente de investiții în securitatea cibernetică existente în sectorul sănătății. Pentru a asigura o finanțare adecvată, statele membre ar trebui să stabilească **criterii de referință fără caracter obligatoriu și să monitorizeze obiectivele de finanțare care vizează în mod specific securitatea cibernetică**, asigurându-se, în același timp, că aceste investiții nu afectează asistența medicală esențială acordată pacienților. Aceste obiective de finanțare ar trebui să vizeze, de asemenea, integrarea considerentelor de securitate în toate investițiile digitale din sectorul sănătății. Statele membre pot face schimb de bune practici și de consiliere cu privire la aceste obiective prin intermediul unor platforme precum rețeaua de e-sănătate[48].

5. Cooperarea dintre sectorul public și cel privat

Cooperarea dintre sectorul public și cel privat și consultarea cu furnizorii de servicii medicale, cu alte entități din sectorul sănătății, precum și cu actorii relevanți din sectorul securității cibernetice sunt esențiale pentru punerea în aplicare cu succes a planului de acțiune. Pentru a contribui în continuare la activitatea Centrului de sprijin, **Comisia, având susținerea ENISA, va institui un Consiliu consultativ comun pentru securitate cibernetică în domeniul sănătății**, cu reprezentanți la nivel înalt din ambele domenii, sănătate și securitate cibernetică, care să poată oferi consiliere Comisiei și Centrului de sprijin cu privire la acțiunile cu impact și să poată discuta despre dezvoltarea în continuare a parteneriatelor public-privat în acest domeniu. Consiliul se va baza pe eforturile existente pentru parteneriatele public-privat, inclusiv pe Centrul european de schimb de informații și de analiză pentru sectorul sănătății.

În plus, Comisia va lansa **un apel la acțiune** pentru ca întreprinderile din domeniul securității cibernetice, fundațiile, instituțiile de învățământ și părțile interesate din industrie **să se angajeze să întreprindă acțiuni pentru a aborda provocările din acest sector**. Bazându-se pe experiența Academiei de competențe în materie de securitate cibernetică, astfel de angajamente ar putea include, de exemplu, promisiuni asumate în cadrul acestei academii pentru a oferi cursuri și materiale de formare axate pe sectorul sănătății destinate profesioniștilor din domeniul securității cibernetice[49]. De asemenea, alte angajamente ar putea viza activități de sensibilizare sau furnizarea, gratuit sau la costuri reduse, de servicii de securitate gestionate pentru entități deosebit de vulnerabile, cu scopul de a le crește gradul de pregătire și reziliența în materie de securitate cibernetică. În plus, aceste angajamente ar putea include schimburi de informații despre amenințările cibernetice cu Centrul de sprijin al ENISA. Centrul de sprijin ar trebui să mențină o evidență clară a angajamentelor asumate în cadrul apelului la acțiune, având ca obiectiv asigurarea coerenței și complementarității acestora.

6. Descurajarea actorilor care generează amenințări cibernetice

Politicile UE în materie de securitate cibernetică, atât interne, cât și externe, ar trebui să sprijine obiectivul de a descuraja actorii care generează amenințări cibernetice să atace sistemele europene de sănătate. Atacurile cibernetice asupra organizațiilor din domeniul sănătății reprezintă o formă absolut

[48] Rețeaua de e-sănătate este o rețea voluntară care conectează autoritățile naționale responsabile de e-sănătate desemnate de statele membre și care a fost instituită în temeiul articolului 14 din Directiva 2011/24/UE.

[49] Academia de competențe în domeniul cibernetic: Implică-te! | Platforma pentru competențe digitale și locuri de muncă

inacceptabilă de activitate cibernetică răuvoitoare, având în vedere potențialul lor de amenințare la adresa siguranței pacienților și a vieților omenești. Prin urmare, UE ar trebui să își utilizeze întreaga capacitate de descurajare în domeniile securității cibernetice și asigurării respectării legii pentru a submina modelul de afaceri al actorilor care generează amenințări cibernetice ce vizează sectorul sănătății și pentru a-i lipsi de câștiguri facile. Acest demers ar implica promovarea investigațiilor transfrontaliere prin intensificarea schimbului de indicatori de compromitere și de alte date relevante, precum și o atenție sporită acordată țintelor de mare valoare și principalilor facilitatori ai infracțiunilor, cum ar fi serviciile de găzduire antiglonț sau cele de mixare a criptomonedelor.

Setul de instrumente pentru diplomația cibernetică oferă un cadru dedicat prevenirii, descurajării și răspunsului la atacurile cibernetice care vizează UE, statele membre și partenerii săi. Înalta Reprezentantă va continua să utilizeze cadrul actual de sancțiuni cibernetice pentru a răspunde amenințărilor ce vizează sistemele de sănătate.

Tragerea la răspundere a autorilor pentru faptele lor reprezintă un factor esențial de descurajare. Prin urmare, statele membre trebuie să se asigure că autoritățile de aplicare a legii sunt pe deplin integrate în planurile naționale de acțiune. În special, acestea ar trebui să valorifice pe deplin prevederile Directivei privind atacurile împotriva sistemelor informatice[50], precum și pe cele ale Convenției de la Budapesta a Consiliului Europei privind criminalitatea informatică, pentru a descuraja atacurile, pentru a aduce infractorii în fața justiției și pentru a demonta infrastructurile infracționale care facilitează atacurile[51]. Punerea în practică cu succes a acestor instrumente ar trebui să garanteze pedepsirea acțiunilor infracționale și răuvoitoare care vizează sectorul sănătății.

7. Punerea în aplicare și monitorizarea planului de acțiune

În cadrul prezentului plan de acțiune se prevăd o serie de sarcini pentru viitorul Centru de sprijin care urmează să fie instituit în cadrul ENISA. Acest lucru asigură o punere în aplicare holistică și coerentă a planului de acțiune, evitând, în același timp, crearea de noi entități care să conducă la potențiale suprapuneri și cheltuieli generale. Comisia intenționează să asigure o alocare de resurse adecvată pentru Centrul de sprijin.

După ce va deveni operațional Centrul de sprijin, ENISA, în consultare cu Comisia, ar trebui să prezinte actualizări periodice privind activitatea centrului către Consiliul de administrație al ENISA, precum și către rețelele relevante ale statelor membre – în special Grupul de cooperare NIS, rețeaua CSIRT, rețeaua de e-sănătate și, dacă este cazul, Comitetul pentru spațiul european al datelor privind sănătatea. În plus, ENISA ar trebui să facă în permanență schimb de opinii cu Consiliul consultativ public-privat pentru securitate cibernetică în domeniul sănătății cu privire la punerea în aplicare a acțiunilor derulate de Centrul de sprijin.

[50] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.

[51] Convenția privind criminalitatea informatică (Convenția de la Budapesta, ETS nr. 185) și protocoalele la aceasta: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Rapoartele periodice ale ENISA, precum Raportul privind situația securității cibernetice în Uniune, care oferă o evaluare agregată a nivelului de maturitate al capacităților și resurselor de securitate cibernetică în întreaga UE, inclusiv în sectorul sănătății, ar trebui să fie prilejuri pentru publicarea unor date relevante, sprijinind astfel monitorizarea planului de acțiune. De asemenea, indicele de securitate cibernetică al UE[52], elaborat de ENISA, poate furniza date cantitative și calitative, ce pot servi ca bază solidă de dovezi pentru evaluarea nivelului de criticalitate și de maturitate al sectorului sănătății.

8. Etapele următoare

Prezenta comunicare propune o agendă ambițioasă pentru un sector al sănătății mai sigur din punct de vedere cibernetic în UE. Odată cu înființarea, în cadrul ENISA, a Centrului de sprijin pentru securitate cibernetică dedicat spitalelor și furnizorilor de servicii medicale, planul de acțiune deschide calea unei abordări europene coerente și comune în fața provocărilor de securitate cibernetică din acest sector.

Prezenta comunicare ar trebui considerată ca punctul de plecare al unui proces menit să îmbunătățească securitatea cibernetică în sectorul sănătății. Prin urmare, adoptarea planului de acțiune va fi însoțită de lansarea unor consultări cuprinzătoare cu părțile interesate și de continuarea schimburilor cu statele membre și cu rețelele relevante pentru colectarea de informații. Pe baza rezultatelor consultărilor, Comisia intenționează să prezinte recomandări în al patrulea trimestru al anului 2025 pentru a rafina în continuare planul de acțiune.

Comisia invită statele membre și toate părțile interesate să colaboreze pentru a realiza obiectivele ambițioase ale planului de acțiune.

[52] ENISA, Indicele de securitate cibernetică al UE, cadrul și nota metodologică (2024). Disponibil la adresa https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

ANEXĂ – Prezentare generală a acțiunilor propuse

Comisia

ENISA – Centrul european de sprijin pentru securitate cibernetică destinat spitalelor și furnizorilor de servicii medicale	
Asigurarea resurselor adecvate pentru funcționarea Centrului de sprijin pentru securitate cibernetică Colaborarea cu ECCC pentru a lansa proiecte-pilot în urma cărora să se dezvolte cele mai bune practici de evaluare a riscurilor în domeniul igienei și securității cibernetice și să se răspundă necesității de a asigura o monitorizare continuă din perspectiva securității cibernetice, colectarea de informații despre amenințări și răspunsul în caz de incidente, utilizând soluții de securitate cibernetică de ultimă generație, astfel încât să contribuie la elaborarea catalogului de servicii al Centrului european de sprijin pentru securitate cibernetică	2025
Prevenirea incidentelor de securitate cibernetică	
În consultare cu Grupul de cooperare NIS, UE-CyCLONe și ENISA, explorarea posibilității de a identifica sectorul sănătății ca fiind eligibil pentru a primi sprijin în vederea testării coordonate a nivelului de pregătire, în conformitate cu prevederile Regulamentului privind solidaritatea cibernetică	T1 2025
Răspuns rapid și redresare	
Împreună cu ENISA, asigurarea faptului că rezerva UE pentru securitate cibernetică include un serviciu de răspuns rapid specific pentru sectorul sănătății	T4 2025
Cooperarea dintre sectorul public și cel privat	
Cu sprijinul ENISA, instituirea Consiliului consultativ comun pentru securitate cibernetică în domeniul sănătății	T1 2025
Lansarea unui apel la acțiune pentru ca întreprinderile din domeniul securității cibernetice, fundațiile, instituțiile de învățământ și părțile interesate din industrie să se angajeze să întreprindă acțiuni pentru a aborda provocările din sectorul sănătății	T2 2025

Descurajarea actorilor care generează amenințări cibernetice	
Împreună cu Înalta Reprezentantă, explorarea ipotezei de a utiliza măsurile din setul de instrumente pentru diplomația cibernetică pentru a preveni, a descuraja, a disuada și a răspunde la activitățile răuvoitoare împotriva sistemelor de sănătate	2025
Promovarea cooperării internaționale împotriva actorilor care sunt responsabili de atacuri de tip *ransomware*, în special în cadrul Inițiativei internaționale de combatere a atacurilor de tip *ransomware*, în colaborare cu Înalta Reprezentantă	2025-2026
Promovarea cooperării în cadrul Grupului de lucru pentru securitate cibernetică al G7 în vederea consolidării securității cibernetice a sectorului sănătății	2025-2026
Etapele următoare	
Lansarea unor consultări extinse cu părțile interesate	T1 2025
Adoptarea de recomandări pentru îmbunătățirea suplimentară a planului de acțiune	T4 2025

ENISA

Centrul UE de sprijin pentru securitate cibernetică destinat spitalelor și furnizorilor de servicii medicale	
Demararea activităților de înființare a Centrului european de sprijin pentru securitate cibernetică destinat spitalelor și furnizorilor de servicii medicale	T2 2025
Elaborarea unui catalog cuprinzător de servicii care să fie furnizate de Centrul de sprijin pentru securitatea cibernetică	Din T4 2025
Prevenirea incidentelor de securitate cibernetică	
Emiterea de orientări care să sublinieze cele mai importante practici în domeniul securității cibernetice și să sprijine furnizorii de servicii medicale în aplicarea acestora	T3 2025
Elaborarea, în strânsă colaborare cu Comisia și statele membre, a unui instrument de cartografiere a reglementărilor	T1 2025

Dezvoltarea unui cadru pentru evaluarea nivelului de maturitate în materie de securitate cibernetică care să fie specific asistenței medicale	T3 2025
Realizarea unei evaluări anuale a nivelului de maturitate în materie de securitate cibernetică a sectorului sănătății	2025-2026
Colaborarea cu statele membre și autoritățile regionale responsabile de programe pentru a crea programe-model de bonuri valorice pentru securitatea cibernetică	2025-2026
Elaborarea de noi orientări privind achizițiile în domeniul securității cibernetice a spitalelor și a furnizorilor de servicii medicale	T3 2025
Crearea Rețelei europene a CISO în sectorul sănătății	T1 2026
Proiectarea și promovarea de module și cursuri de formare destinate profesioniștilor din sectorul sănătății	T1 2026
Capacități europene de detectare a amenințărilor cibernetice care vizează sectorul sănătății	
Crearea unui catalog european al vulnerabilităților exploatate cunoscute pentru dispozitive medicale, sisteme de dosare electronice de sănătate și furnizori de echipamente și software TIC în sectorul sănătății	T4 2025
Introducerea la nivelul UE a unui serviciu pe bază de abonament pentru avertizări timpurii în sectorul sănătății	Începând cu 2026
Sprijinirea Centrului european de schimb de informații și de analiză pentru sectorul sănătății prin instrumente și schimb de informații	2025-2026
Răspuns rapid și redresare	
Împreună cu Comisia, asigurarea faptului că rezerva UE pentru securitate cibernetică include un serviciu de răspuns rapid specific pentru sectorul sănătății	T4 2025
În colaborare cu rețeaua CSIRT, elaborarea unor manuale de răspuns în caz de incidente cibernetice adaptate pentru sectorul sănătății	T3 2025
Facilitarea organizării pe scară largă de exerciții naționale de securitate cibernetică pentru a testa	Începând cu T4 2025

manualele și pentru a consolida protocoalele de răspuns în caz de incidente	
Oferirea unui serviciu pe bază de abonament de redresare în urma unui atac de tip *ransomware*	Începând cu 2026
Împreună cu Europol, identificarea celor mai comune tipuri de atac de tip *ransomware* care vizează organizațiile din domeniul sănătății și extinderea colecției de instrumente de decriptare prin intermediul proiectului *No More Ransom*.	T4 2025
Împreună cu Europol, elaborarea de orientări accesibile pentru a ajuta furnizorii de servicii medicale să evite plata răscumpărărilor	T3 2025
Acțiuni la nivel național	
Sprijinirea statelor membre să elaboreze planuri naționale de acțiune	2025
Coordonarea eforturilor pentru a asigura complementaritatea resurselor și a strategiilor fiecărui stat membru	2025-2026
Punerea în aplicare și monitorizarea planului de acțiune	
În consultare cu Comisia, furnizarea periodică către rețelele relevante ale statelor membre de actualizări privind activitatea Centrului de sprijin pentru securitate cibernetică	2025-2026
Menținerea unui schimb continuu de informații cu Consiliul consultativ pentru securitate cibernetică în domeniul sănătății	2025-2026

Statele membre

Capacități europene de detectare a amenințărilor cibernetice care vizează sectorul sănătății	
Partajarea cu Centrul european de sprijin pentru securitate cibernetică a notificărilor privind incidentele pe cale le transmit spitalele și furnizorii de servicii medicale în cadrul NIS 2	Începând cu T4 2025
Încurajarea dezvoltării de centre naționale de schimb de informații și de analiză pentru sectorul sănătății	2025-2026
Prevenirea incidentelor de securitate cibernetică	

Efectuarea, în cadrul Grupului de cooperare NIS, a unei evaluări coordonate a riscurilor de securitate, care să includă atât riscuri tehnice, cât și strategice, legate de lanțurile de aprovizionare cu dispozitive medicale	T4 2025
Răspuns rapid și redresare	
Organizarea de exerciții naționale de securitate cibernetică pentru a testa manualele și pentru a consolida protocoalele de răspuns în caz de incidente	Începând cu 2026
Acțiuni la nivel național	
Desemnarea centrelor naționale de sprijin pentru securitate cibernetică destinate spitalelor și furnizorilor de servicii medicale	T2 2025
Elaborarea de planuri naționale de acțiune axate pe securitatea cibernetică în sectorul sănătății	T4 2025
Facilitarea partajării resurselor între furnizorii de servicii medicale	2025-2026
Stabilirea unor criterii de referință fără caracter obligatoriu și monitorizarea obiectivelor de finanțare dedicate securității cibernetice	T4 2025
Solicitarea ca organizațiile din domeniul sănătății și alte entități care intră sub incidența Directivei NIS 2 să raporteze intențiile de a plăti răscumpărări	T4 2025