BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Abordarea vulnerabilităților cibernetice în sectoarele critice: sectorul sănătății

On cyber vulnerabilities management in critical sectors: the health sector

Dr. Irina-Delia NEMOIANU*
*Directoratul Național de Securitate Cibernetică
e-mail: irina.nemoianu@dnsc.ro
ORCID: 0009-0000-3276-9656

Abstract

Digitalizarea sectorului sănătății din România a cunoscut o accelerare semnificativă, în special în urma pandemiei de COVID-19, însă această tranziție a amplificat riscurile de securitate cibernetică, expunând infrastructurile critice și datele pacienților la amenințări persistente. Acest studiu analizează vulnerabilitățile tehnice și nontehnice ale sectorului medical, bazându-se atât pe cercetare documentară, cât și pe un sondaj realizat în rândul reprezentanților instituțiilor de sănătate. Rezultatele evidențiază provocări importante, de la utilizarea de software învechit, deficit de personal specializat în securitate cibernetică și variații semnificative în nivelul de maturitate a protecției cibernetice între organizațiile publice și cele private. Având în vedere diversitatea provocărilor identificate, reziliența sectorului medical necesită o strategie integrată de securitate cibernetică, fundamentată pe investiții tehnologice, formare continuă și politici coerente de gestionare a riscurilor.

The digitalisation of the Romanian health sector has accelerated significantly, especially in the aftermath of the COVID-19 pandemic, but this transition has amplified cybersecurity risks, exposing critical infrastructures and patient data to persistent threats. This study analyses the technical and non-technical vulnerabilities of the medical sector, based on both documentary research and a survey conducted among representatives of health institutions. The results highlight important challenges, ranging from the use of outdated software, shortages of specialised cybersecurity staff and significant variations in the level of maturity of cyber protection between public and private organisations. Given the diversity of challenges identified, the resilience of the health sector requires an integrated cybersecurity strategy, underpinned by technological investments, continuous training and coherent risk management policies.

Cuvinte-cheie:
securitate cibernetică; atacuri cibernetice; vulnerabilități; sectorul sănătății; reziliență; factorul uman.

Keywords:
cybersecurity; cyber-attacks; vulnerabilities; the health sector; resilience; the human factor.

Info articol
Primit: 31 martie 2025; Evaluat: 29 aprilie 2025; Acceptat: 6 mai 2025; Disponibil online: ? iunie 2025
Citare: Nemoianu, I.D. 2025. „Abordarea vulnerabilităților cibernetice în sectoarele critice: sectorul sănătății". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(2): 31-40. https://doi.org/10.53477/2065-8281-25-10

© Editura Universității Naționale de Apărare „Carol I"
Articol cu acces deschis distribuit în conformitate cu termenii și condițiile licenței Creative Commons Attribution (CC BY-NC-SA)

Într-un context global marcat de avansul tehnologic, digitalizarea sistemului de sănătate a devenit o prioritate strategică pentru România, vizând îmbunătățirea calității și eficienței serviciilor medicale. Acest demers a fost accelerat de pandemia de COVID-19, care a evidențiat necesitatea adaptării rapide a sectorului medical la noile realități. Cu toate acestea, sectorul se confruntă cu provocări semnificative în ceea ce privește securitatea cibernetică, legate atât de infrastructură, cât și de expertiza resurselor umane.

Creșterea gradului de digitalizare a dus la extinderea suprafeței de atac a amenințărilor cibernetice, fapt evidențiat de creșterea numărului de atacuri cibernetice asupra sistemului de sănătate din România. Proiectul RO-CCH, finanțat de Uniunea Europeană și implementat de Directoratul Național de Securitate Cibernetică (DNSC), a abordat provocările de securitate cibernetică din sectorul sănătății, cu scopul de a reduce riscurile de securitate cibernetică și de a crește gradul de conștientizare în instituțiile de sănătate din România (RO-CCH 2025a).

Pornind de la activitatea desfășurată în cadrul proiectului, acest articol prezintă o analiză a vulnerabilităților de securitate cibernetică ce pot afecta sectorul sănătății din România, evidențiind dimensiunile sociotehnice. Aceste dimensiuni reflectă interacțiunile dintre componentele tehnice – infrastructură hardware, software și de rețea – și factorii sociali – precum comportamentul uman, cultura organizațională, cadrul de reglementare și necesitatea unei abordări integrate pentru obținerea rezilienței sectorului. Studiul integrează, de asemenea, rezultatele unui sondaj, realizat cu reprezentanți ai spitalelor, evidențiind percepția acestora asupra amenințărilor cibernetice și asupra capacității actuale a organizațiilor de a gestiona vulnerabilitățile.

Atacuri cibernetice asupra sistemului de sănătate

Sistemul de sănătate din România se confruntă cu o creștere semnificativă a amenințărilor cibernetice, în special a atacurilor de tip ransomware, care vizează atât infrastructurile IT ale spitalelor, cât și furnizorii de servicii informatice din domeniu. Aceste tendințe sunt în acord cu tendințele europene sau globale (ENISA 2023), unde 8% din atacurile ransomware din 2023-2024 au vizat sectorul sănătății, al treilea cel mai afectat sector (ENISA 2024, 15). În România atacurile au demonstrat existența unor vulnerabilități atât în protecția datelor, cât și în continuitatea operațiunilor medicale, subliniind necesitatea unor măsuri robuste de securitate cibernetică, dar și a unor planuri de recuperare, în caz de incident.

În iulie 2021, Spitalul Clinic nr. 1 Witting din București a fost victima unui atac ransomware cu malware-ul Phobos, care a criptat datele de pe serverele instituției, atacatorii solicitând o răscumpărare pentru decriptare (SRI 2021). Acest ransomware (Cisco Systems Inc. 2023), distribuit prin exploatarea vulnerabilităților Remote Desktop Protocol (RDP) de acces la distanță în sistemele de operare Windows,

funcționează ca o platformă Ransomware-as-a-Service (RaaS). Astfel de platforme permit colaborarea dintre dezvoltatori și afiliați pentru extinderea atacurilor. Caracterul descentralizat al modelului îngreunează identificarea atacatorilor și aplicarea măsurilor de combatere, iar deși Serviciul Român de Informații (SRI) a oferit recomandări pentru securizarea infrastructurii IT, amploarea daunelor nu a fost făcută publică. Un incident similar a avut loc, în 2023, la Spitalul de Recuperare „Sfântul Gheorghe" din Botoșani, unde atacatorii au criptat baza de date a instituției, perturbând grav activitatea și solicitând o răscumpărare de trei bitcoini (aproximativ 50.000 de dolari) (ProTV 2023). Acest atac, intens mediatizat, a evidențiat impactul sever al amenințărilor cibernetice asupra sistemului de sănătate din România.

Cel mai recent atac ransomware de amploare a avut loc între 11 și 12 februarie 2024, afectând Romanian Soft Company, furnizorul platformei informatice Hippocrates, utilizată de numeroase spitale publice din România (DNSC 2024). Incidentul a perturbat grav activitatea a 26 de spitale care depindeau de această platformă pentru gestionarea datelor și coordonarea serviciilor medicale. Malware-ul utilizat a fost Backmydata, o variantă a ransomware-ului Phobos, similar cu cel folosit în atacul asupra Spitalului Clinic nr. 1 Witting, din 2021. La momentul redactării acestui articol, cauza exactă a incidentului nu a fost dezvăluită public, însă DNSC a menționat că nu au fost identificate dovezi de exfiltrare a datelor. Astfel, rămâne incert dacă atacul a exploatat o vulnerabilitate a platformei, o configurație eronată a RDP sau alte erori umane.

Creșterea frecvenței și complexității atacurilor ransomware asupra infrastructurii IT din sectorul medical românesc subliniază riscurile asociate atât deficiențelor în securitatea cibernetică, cât și a vulnerabilităților datorate lanțului de aprovizionare. Atacurile recente evidențiază necesitatea implementării unor strategii de protecție a rețelelor spitalicești, inclusiv implementarea unor politici stricte de backup și de recuperare a datelor pentru a preveni pierderile cauzate de atacurile ransomware, protejarea serviciilor informatice expuse la internet sau conectarea la rețele interne prin conexiuni Virtual Private Network (VPN) securizate. Alte măsuri care asigură reziliența, în caz de atacuri materializate, pot fi creșterea investițiilor în soluții avansate de securitate cibernetică și în planuri de răspuns rapid la incidente cibernetice, precum și instruirea personalului IT și a celui medical pentru a detecta și a preveni amenințările cibernetice comune, începând cu phishingul.

Vulnerabilități cibernetice

În securitatea cibernetică, vulnerabilitățile reprezintă deficiențe structurale sau erori în logica computațională, identificate în componente software sau hardware, care, atunci când sunt exploatate, pot compromite confidențialitatea, integritatea și disponibilitatea datelor și sistemelor informatice. Aceste slăbiciuni pot rezulta din deficiențe de proiectare, implementare sau configurare și constituie puncte de acces pentru atacatori.

Atenuarea acestor vulnerabilități implică, de obicei, una sau mai multe dintre următoarele măsuri:

- aplicarea de patch-uri pentru remedierea erorilor din cod;
- modificarea specificațiilor tehnice astfel încât să reducă expunerea la potențiale exploatări;
- deprecierea sau eliminarea completă a funcționalităților sau protocoalelor care prezintă vulnerabilități.

Conform Programului Common Vulnerabilities and Exposures (CVE) (The MITRE Corporation, fără an; SecurityScorecard, fără an), gestionat de MITRE Corporation, fiecare vulnerabilitate este înregistrată sub un CVE ID unic, care permite asocierea acesteia cu versiuni specifice ale software-ului sau ale bibliotecilor partajate, oferind astfel un sistem de referință care să ajute la procesul de gestionare a vulnerabilităților.

Scorul Common Vulnerability Scoring System (CVSS) oferă o metrică pentru evaluarea gravității vulnerabilităților de securitate cibernetică, pe baza mai multor criterii, precum impactul și exploatabilitatea acestora (NIST, fără an). Acesta poate fi transpus într-o reprezentare calitativă (scăzut, mediu, ridicat și critic) pentru a ajuta organizațiile să evalueze și să prioritizeze vulnerabilitățile în cadrul proceselor de management. CVSS este un standard public, dezvoltat de Special Interest Group (SIG) și utilizat pe scară largă de organizații din întreaga lume, cea mai recentă versiune fiind CVSS 4.0.
Sistemele IT din spitale se pot confrunta cu numeroase vulnerabilități cibernetice, multe dintre ele afectând diverse produse hardware, software și de rețea, utilizate pe scară largă și în alte sectoare, care pot compromite securitatea datelor pacienților și funcționarea infrastructurii critice de asistență medicală.

În urma cercetării documentare, dar și din discuțiile cu experți de securitate cibernetică ce colaborează cu entități din domeniul sănătății, printre cele mai frecvente probleme identificate se numără utilizarea software-ului și hardware-ului învechit, expus riscurilor, din cauza lipsei actualizărilor și a suportului tehnic adecvat. De asemenea, protocoalele slabe de securitate a rețelei, configurările defectuoase și măsurile inadecvate de control al accesului pot facilita accesul neautorizat la sistemele informatice. În plus, nivelul insuficient de instruire a personalului medical și a celui administrativ crește vulnerabilitatea instituțiilor sanitare în fața atacurilor de tip phishing, care rămân una dintre principalele metode de compromitere a infrastructurii IT. Aceste deficiențe expun spitalele unor amenințări semnificative, precum încălcări ale securității datelor, atacuri ransomware și acces neautorizat la informații sensibile, subliniind necesitatea implementării unor măsuri eficiente și proactive de securitate cibernetică.

Raportul prezintă o serie de vulnerabilități cibernetice legate de hardware, software, echipamente de rețea sau echipamente de securitate cibernetică, pe care organizațiile din domeniul sănătății pot să le aibă în vedere în strategiile lor de securitate (RO-CCH 2025b). În acest context, anumite vulnerabilități, identificate prin

CVE-urile corespondente, fie istorice, fie recent descoperite, prezintă un scor CVSS ridicat (High) sau critic (Critical), care necesită o abordare urgentă și măsuri de atenuare eficiente, având în vedere potențialul impact asupra continuității serviciilor medicale și asupra protecției infrastructurii critice din sectorul sănătății. În același timp, noi vulnerabilități sunt făcute public frecvent, o strategie adecvată de securitate cibernetică incluzând urmărirea alertelor diverșilor producători sau furnizori, informările diverselor agenții de securitate naționale sau achiziționarea/colaborarea cu organizații pentru obținerea de servicii de tip CERT privind vulnerabilitățile exploatate în mod activ de atacatori.

O abordare tot mai relevantă în managementul vulnerabilităților o reprezintă integrarea soluțiilor de inteligență artificială (IA) în soluțiile existente (AI-driven vulnerability management) prin utilizarea de algoritmi de învățare automată, pentru a îmbunătăți procesele de detecție, de prioritizare și de remediere a vulnerabilităților (Wan și alții 2024). Astfel, soluțiile IA pot analiza în timp real volume mari de date, de la jurnale de sistem și de rețea la fluxuri de threat intelligence, pentru a identifica tipare care sugerează posibile puncte slabe de securitate în infrastructură. Platforme comerciale de management al vulnerabilităților, precum Qualys VMDR, Tenable.io, Rapid7 InsightVM sau Darktrace, au integrat algoritmi de învățare automată pentru a corela vulnerabilitățile cunoscute cu nivelul lor de exploatare activă în mediul real (Tod-Răileanu și alții 2024). Inteligența artificială poate fi utilizată și în predicția vulnerabilităților, prin care se anticipează probabilitatea ca o vulnerabilitate recent descoperită să fie exploatată, pe baza comportamentului istoric al atacatorilor și al vectorilor de atac asociați.

Digitalizarea sectorului sănătății presupune integrarea și a tehnologiilor specifice, a sistemelor și protocoalelor, precum sisteme de gestionare a farmaciilor, a serviciilor de ambulanță și de urgență, sisteme informatice de laborator. Printre cele mai importante, se numără dosarele electronice de sănătate (Electronic Health Records), care integrează istoricul pacienților, folosind standarde, precum HL7 (Health Level 7) pentru schimbul de informații între sisteme, cum ar fi sistemele informatice de radiologie (Radiology Information Systems) și sistemele informatice de laborator (Laboratory Information Systems). Sistemele Picture Archiving and Communication Systems (PACS), de arhivare și comunicare a imaginilor, sunt utilizate pentru stocarea și gestionarea imagisticii medicale, în timp ce standardul Digital Imaging and Communications in Medicine (DICOM) permite interoperabilitatea dintre dispozitivele de imagistică și sistemele de stocare. Aceste tehnologii reprezintă o suprafață suplimentară de atac care trebuie avută în vedere de organizațiile din sectorul medical, atât pentru spitale, clinici, cât și pentru centre de imagistică medicală, laboratoare de analize medicale, cabinete stomatologice.

Vulnerabilități în dispozitive medicale

Dispozitivele medicale moderne, precum monitoarele cardiace, ventilatoarele și pompele de insulină, sunt din ce în ce mai integrate în infrastructura digitală a spitalelor prin Internetul Lucrurilor Medicale (Internet of Medical Things – IoMT).

Această conectivitate permite monitorizarea în timp real a pacienților și transmiterea automată a datelor către sistemele de gestionare a informațiilor clinice, îmbunătățind astfel eficiența actului medical. Dispozitivele comunică utilizând protocoale standard, precum Wi-Fi și Bluetooth, dar și protocoale proprietare, dezvoltate de producătorii de echipamente medicale. Această conectivitate, deși benefică din punct de vedere operațional, ridică provocări în ceea ce privește securitatea cibernetică, în special în protejarea confidențialității, integrității și disponibilității datelor pacienților.

Pentru a asigura securizarea transmisiunilor, peste protocoalele de rețea tradiționale, precum TCP/IP, care permit comunicarea între dispozitive, sunt utilizate și tehnologii de protecție suplimentare, cum ar fi VPN-urile și criptarea TLS/SSL. Aceste mecanisme reduc riscul de interceptare a informațiilor sensibile și protejează împotriva atacurilor cibernetice care vizează infrastructura medicală. Cu toate acestea, numeroase dispozitive IoMT rămân vulnerabile, din cauza configurărilor nesigure, a lipsei actualizărilor software sau a standardelor de securitate care variază între diferiți producători.

Un studiu asupra dispozitivelor medicale (Cynerio 2023) a analizat securitatea dispozitivelor medicale din 14 trusturi NHS (organizații din sistemul de sănătate din Regatul Unit), reprezentând 6,4% din totalul trusturilor NHS. Aceste instituții au fost selectate pentru a reflecta diversitatea spitalelor din punctul de vedere al dimensiunii, numărului de paturi și nivelului de finanțare. Studiul a utilizat un instrument de analiză anonimizată pentru a identifica principalele riscuri, vulnerabilități și amenințări active, asociate dispozitivelor IoMT. Constatările au evidențiat probleme critice, inclusiv posibilitatea exploatării vulnerabilităților nepatch-uite în peste 40% din dispozitive, configurații de rețea nesigure sau risc de acces neautorizat. În același timp, peste 36,7% dintre dispozitive s-ar confrunta cu riscuri reduse prin implementarea unei microsegmentări adecvate la nivel de rețea.

Factorul uman în securitatea cibernetică

Sistemele informatice din cadrul unităților medicale sunt susceptibile la o serie de vulnerabilități care au ca origine factorul uman. Aceste deficiențe, deși nu se corelează întotdeauna cu vulnerabilități și expuneri comune sau CVE-uri specifice, reprezintă un vector critic în evaluarea riscului cibernetic. Analiza acestor vulnerabilități impune o abordare contextuală, având în vedere fluxurile de lucru și interacțiunile umane din domeniul medical.

Vectori de atac și erori umane în contextul spitalicesc – unul dintre vectorii de atac predominanți îl reprezintă campaniile de tip phishing, prin care personalul este indus în eroare prin intermediul unor mesaje electronice care imită surse legitime. Această manipulare are ca rezultat compromiterea datelor de autentificare sau instalarea de software malițios. În paralel, practicile deficitare de gestionare a credențialelor, cum ar fi utilizarea unor parole slab configurate sau reutilizarea acestora pe multiple platforme, facilitează accesul neautorizat.

Amenințări interne și ingineria socială – amenințările interne, provenind din partea angajaților cu intenții răuvoitoare sau nemulțumiri, reprezintă un risc semnificativ, aceștia putând abuza de privilegiile de acces pentru a exfiltra date sensibile sau a perturba operațiunile. În plus, tehnicile de inginerie socială, care manipulează personalul pentru a divulga informații confidențiale sau pentru a efectua acțiuni care compromit securitatea, subliniază importanța conștientizării și formării continue.

Gestionarea inadecvată a datelor și deficiențe în formarea personalului – manipularea necorespunzătoare a datelor sensibile prin transmiterea accidentală a informațiilor pacientului prin canale nesecurizate sau expunerea neintenționată a acestora reprezintă o altă categorie de risc. Deficiențele în programele de formare în domeniul securității cibernetice contribuie la această vulnerabilitate, personalul nefiind adesea familiarizat cu cele mai recente amenințări și practici de securitate.

Deficiențe în controlul accesului și nerespectarea protocoalelor de securitate – o gestionare deficitară a accesului utilizatorilor, manifestată prin neactualizarea drepturilor de acces, în urma modificării rolurilor sau părăsirii organizației, creează puncte de intrare pentru atacatori. Nerespectarea protocoalelor de securitate, precum ignorarea actualizărilor software sau ocolirea rețelelor private virtuale (VPN), expune suplimentar sistemele la vulnerabilități cunoscute.

Riscuri asociate dispozitivelor mobile și divulgării neintenționate – pierderea sau furtul dispozitivelor mobile care conțin date sensibile reprezintă un risc considerabil de exfiltrare a informațiilor. De asemenea, divulgarea neintenționată a datelor prin transmiterea eronată sau lăsarea ecranelor nesupravegheate reprezintă riscuri suplimentare, care pot fi atenuate prin implementarea unei culturi organizaționale, orientate spre securitate.

Percepția reprezentanților din sector asupra nivelului de securitate cibernetică

În ultimii ani, pe lângă atacurile cu ransomware care au afectat activitatea unităților spitalicești din România, organizațiile au fost expuse unei varietăți de atacuri cibernetice, evidențiind un peisaj de amenințări din ce în ce mai sofisticat. Unul dintre sondajele realizate în cadrul proiectului cu reprezentanți IT și din managementul a 30 de organizații cu profil medical din România a generat date care oferă indicii cu privire la nivelul de pregătire al acestor organizații în fața amenințărilor cibernetice, precum și la percepția subiecților asupra stadiului actual al securității cibernetice în sector.

Conform răspunsurilor obținute de la reprezentanți din sector, în ultimii trei ani phishingul și spear-phishingul au constituit cea mai mare parte a incidentelor raportate, fiind urmate de atacurile de tip Distributed Denial of Service (DDoS) care vizează indisponibilizarea infrastructurilor IT, și de atacurile de tip brute force, folosite pentru compromiterea credențialelor de acces. De asemenea, o categorie semnificativă

de amenințări a fost reprezentată de distribuirea de malware și spyware, indicând o diversificare a metodelor utilizate de atacatori. Această ierarhizare a incidentelor subliniază natura dinamică și adaptabilă a amenințărilor cibernetice, precum și necesitatea implementării unor măsuri de securitate multilaterale. În mod particular, prevalența atacurilor de tip phishing justifică necesitatea considerării vulnerabilităților umane ca un vector de exploatare în cadrul sistemelor de securitate cibernetică.

În ceea ce privește evaluarea și prioritizarea vulnerabilităților cibernetice în cadrul organizațiilor, participanții au oferit răspunsuri variate privind existența unor cadre sau metodologii specifice utilizate pentru determinarea nivelului de risc asociat fiecărei vulnerabilități. Dintre cei 30 de respondenți, 12 au declarat că nu dispun de un astfel de program structurat pentru gestionarea vulnerabilităților. Cu toate acestea, aproximativ jumătate dintre participanți folosesc instrumente de scanare a vulnerabilităților, sisteme de detectare a intruziunilor (IDS) sau alte instrumente automatizate, menite să identifice riscurile și amenințările. Aceste rezultate indică o abordare eterogenă a securității cibernetice în sector, în care, deși există eforturi pentru monitorizarea amenințărilor, un număr semnificativ de organizații nu implementează încă un proces formalizat de evaluare și gestionare a vulnerabilităților.

Nivelul scăzut de securitate cibernetică și capacitatea redusă de gestionare a incidentelor în cadrul organizațiilor sunt atribuite unei combinații de factori tehnici, organizaționali și umani. Conform datelor obținute, 28 din 30 de respondenți au indicat drept cauze principale utilizarea unor sisteme informatice învechite sau nesigure, implementarea controalelor de securitate inadecvate și resursele limitate alocate pentru protecția infrastructurii IT. Acești factori nu doar că sporesc riscul de compromitere a datelor și infrastructurilor critice, dar și îngreunează implementarea unor măsuri proactive de securitate.

Un aspect secundar, dar semnificativ, identificat în cadrul analizei, este lipsa de conștientizare, în rândul angajaților, a problemei privind securitatea cibernetică, ceea ce contribuie la vulnerabilități suplimentare în fața atacurilor bazate pe inginerie socială, cum ar fi phishingul. Aceste deficiențe reflectă probleme sistemice mai profunde, în special subfinanțarea și investițiile insuficiente în infrastructura de securitate cibernetică. În plus, acestea sunt amplificate de factori umani, inclusiv de deficitul de personal specializat, care limitează capacitatea organizațiilor de a detecta, de a preveni și de a răspunde eficient la incidente cibernetice. De asemenea, lipsa unui angajament strategic pentru dezvoltarea unei culturi organizaționale orientate spre securitate agravează și mai mult riscurile, subliniind necesitatea unor măsuri urgente pentru consolidarea rezilienței cibernetice la nivel instituțional.

Concluzii

România a făcut progrese semnificative în digitalizarea sectorului de sănătate, accelerate de pandemia de COVID-19, însă această transformare a crescut riscurile

cibernetice, expunând rețelele informatice și datele pacienților la amenințări. În acest articol, am evidențiat vulnerabilitățile tehnice și nontehnice ale sectorului, obținute atât din cercetare documentară, cât și din chestionarele cu reprezentanți din sector. Problemele evidențiate ale sectorului, de la utilizarea de software învechit la lipsa personalului instruit în securitate cibernetică atât din sectorul public, cât și din cel privat subliniază necesitatea unor măsuri mai stricte pentru protejarea infrastructurii IT din sănătate împotriva amenințărilor în creștere.

Pentru a proteja infrastructura critică din sănătate și datele pacienților, este necesară o gestionare eficientă a vulnerabilităților, actualizarea software-ului și modernizarea infrastructurilor IT. Date fiind nivelurile diferite de maturitate a securității cibernetice ale organizațiilor din sistem, reziliența sistemului de sănătate necesită o strategie națională coerentă, bazată pe investiții în tehnologie, pe formare în domeniul securității cibernetice și pe politici eficiente de gestionare a riscurilor.

Pe măsură ce tehnologia avansează, integrarea inteligenței artificiale ar putea avea un rol decisiv în abordarea proactivă a riscurilor cibernetice atât în sectorul sănătății, cât și în alte sectoare critice. Prin automatizarea proceselor de identificare a riscurilor și amenințărilor, de prioritizare a vulnerabilităților, soluțiile bazate pe IA pot îmbunătăți considerabil capacitatea de reacție și eficiența operațională. Adoptarea unei strategii naționale care să includă astfel de tehnologii ar putea reprezenta un atu pentru România în protejarea infrastructurilor critice și în creșterea rezilienței cibernetice la nivel național.

Referințe

Cisco Systems Inc. 2023. ”Understanding the Phobos affiliate structure and activity.” https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/.

Cynerio. 2023. ”The State of NHS Trust IoT Device Security 2023.” https://www.cynerio.com/nhs-trusts-iot-security-report-cynerio-only.

DNSC. 2024. ”Backmydata Ransomware (Alert).” https://www.dnsc.ro/vezi/document/alert-backmydata-ransomware-eng-pdf.

ENISA. 2023. ”Enisa Threat Landscape: Health Sector.” https://www.enisa.europa.eu/publications/health-threat-landscape.

___. 2024. ”ENISA Threat Landscape 2024.” doi:10.2824/0710888.

NIST. fără an. ”CVSS – Vulnerability Metrics.” Accesat decembrie 2024. https://nvd.nist.gov/vuln-metrics/cvss.

ProTV. 2023. „Spital din Botoșani, atacat de hackeri. Le-au criptat baza de date și cer 50.000 de dolari răscumpărare.” https://stirileprotv.ro/stiri/ilikeit/spital-din-botosani-atacat-de-hackeri-le-au-criptat-baza-de-date-si-cer-50-000-de-dolari-rascumparare.html.

RO-CCH. 2025a. ”About RO=CCH.” https://rocch.ro/en/about-ro-cch.

___. 2025b. ”Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1).” https://rocch.ro/en/dissemination/deliverables/d2-1/download.

SecurityScorecard. fără an. ”CVE Details.” Accesat decembrie 2024. https://www.cvedetails.com/.

SRI. 2021. „Atac ransomware asupra Spitalului Clinic Witting din București.” https://www.sri.ro/articole/atac-ransomware-asupra-Spitalului-Clinic-Witting-din-Bucuresti.html.

The MITRE Corporation. fără an. ”CVE® Program Mission.” Accesat decembrie 2024. https://www.cve.org/.

Tod-Răileanu, Gabriela, Ana-Maria Dincă, Sabina-Daniela Axinte și Ioan C. Bacivarov. 2024. ”Enhancing Vulnerability Management with Artificial Intelligence Algorithms.” *International Conference on Cybersecurity and Cybercrime.* 96–101. doi:10.19107/CYBERCON.2024.13.

Wan, Shengye, Joshua Saxe, Craig Gomes, Sahana Chennabasappa, Avilash Rath, Kun Sun și Xinda Wang. 2024. ”Bridging the Gap: A Study of AI-based Vulnerability Management between Industry and Academia.” *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S).* IEEE Computer Society. 80-87.

INFORMAȚII PRIVIND FINANȚAREA

Această cercetare a fost posibilă parțial prin sprijinul proiectului RO-CCH, care a furnizat date directe despre managementul vulnerabilităților cibernetice în instituțiile medicale din România, prin raportul *Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1)*. Autorul își exprimă aprecierea față de organizațiile din domeniul sănătății și față de experții care au contribuit prin participare la sondaje și prin furnizarea de perspective valoroase.

Direcția Națională de Securitate Cibernetică Română (DNSC) este beneficiarul unei finanțări nerambursabile pentru implementarea proiectului „Romanian Cyber Care Health - RO-CCH”, în temeiul acordului de grant nr. 101101522. Proiectul este finanțat prin autoritatea de finanțare: CNECT.H – Digital Society, Trust, and Cybersecurity, în cadrul apelului DIGITAL-2022-CYBER-02-SUPPORTHEALTH.

DECLARAȚIE PRIVIND CONFLICTUL DE INTERESE

Autorul declară că nu există potențiale conflicte de interese cu privire la cercetarea, paternitatea și/sau publicarea acestui articol.