PHCD 66/2025

PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

PROIECT

HOTĂRÂRE
privind adoptarea opiniei referitoare la Comunicarea 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 COM(2025) 10

În temeiul prevederilor art. 67 și ale art. 148 din Constituția României, republicată, ale Legii nr. 373/2013 privind cooperarea dintre Parlament și Guvern în domeniul afacerilor europene și ale art. 165 - 190 din Regulamentul Camerei Deputaților, aprobat prin Hotărârea Camerei Deputaților nr. 8/1994, republicat, cu modificările ulterioare,

Camera Deputaților adoptă prezenta hotărâre.

Articol unic. – Luând în considerare opinia nr. 7c-21/515 adoptată de Comisia pentru afaceri europene, în ședința din 16 septembrie 2025, Camera Deputaților:

1. susține Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Planul de acțiune european privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale;
2. recomandă prevenția ca prim pilon de apărare în lupta cu atacurile cibernetice folosind măsuri de pregătire consolidate, cum ar fi orientări privind punerea în aplicare a practicilor prioritare în materie de securitate cibernetică;
3. subliniază importanța sistemului triunghiular de apărare compus din prevenție, detecție-identificare și răspuns adecvat împotriva eventualelor atacuri cibernetice care pot avea loc fie sub formă materializată (acțiune fizică), fie sub formă dematerializată (software);
4. susține introducerea de vouchere de securitate cibernetică pentru a oferi asistență financiară microîntreprinderilor, spitalelor mici și mijlocii, respectiv furnizorilor de servicii medicale pentru a putea accesa resurse de învățare în materie de securitate cibernetică;
5. recomandă instruirea personalului cu acces direct la infrastructură și informații critice pentru a putea asigura respectarea reglementărilor de confidențialitate privind datele pacienților și condițiile specifice de garantare a dreptului la protecția vieții private, prin asigurarea conformității cu legislația aplicabilă în Uniunea Europeană privind protecția datelor cu caracter personal;
6. consideră că se impune descurajarea tentativelor de atacuri cibernetice prin utilizarea setului de instrumente pentru diplomația cibernetică, un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare;
7. recomandă implementarea de sisteme Firewall duale, de tip IDS/IPS: IDS pentru detecția intruziunilor în sistem și de tip IPS pentru identificarea amenințărilor și luarea măsurilor semiautomatizate, preemptive care sunt impuse de planurile de prevenție și protecție împotriva

amenințărilor cibernetice ale instituțiilor, cu respectarea prevederilor din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;

8. susține folosirea soluțiilor de tip antivirus și software specific de gestiune, precum și întreținerea și menținerea la zi a acestor sisteme de administrare și protecție;

9. subliniază importanța instruirii și formării angajaților în scopul conștientizării riscurilor de securitate cibernetică și a aplicării celor mai bune practici pentru protejarea datelor împotriva celor mai noi metode de atac cibernetic, folosind astfel prevenția ca prim pilon de apărare împotriva unui eventual atac;

10. subliniază importanța realizării de copii de rezervă ale datelor critice atât ale sistemelor medicale, cât și ale pacienților, și depozitarea lor în locuri sigure, care respectă principiile de separare fizică a stocării datelor de avarie, utilizând medii de înregistrare rezistente și conforme cu standardele de confidențialitate, integritate și disponibilitate;

11. recomandă respectarea schemei „3-2-1" de salvare a datelor care impune efectuarea de 3 copii de rezervă, pe cel puțin două medii de stocare diferite, din care cel puțin o copie să fie depozitată într-un spațiu separat;

12. recomandă utilizarea unei scheme de rotație a salvării datelor folosind algoritmi de tip „Turnul Hanoi" care permit 2n-1 rotații ale seturilor de date de recuperare în caz de avarie;

13. atenționează asupra situației creșterii numărului atacurilor de tip ransomware care poate necesita scheme de salvare a datelor mai complexe decât 3-2-1, cum ar fi strategiile de tip 3-2-1-1-0 în care 3 copii de siguranță se stochează pe 2 medii diferite, 1 copie într-un loc extern și 1 copie fără legătură fizică directă de comunicare cu exteriorul, iar datele sunt monitorizate pentru a asigura salvarea lor cu 0 erori;

14. atenționează asupra necesității implementării de planuri centralizate și standardizate la nivel național, de recuperare în caz de atac, prin asigurarea paralelismului și dualității sistemelor critice, de susținere a vieții și de administrare a datelor pacienților pentru recuperare rapidă în cazul unui eveniment cibernetic distructiv;

15. recomandă colaborarea cu Directoratul Național de Securitate Cibernetică (DNSC) pentru securitatea, confidențialitatea, integritatea și disponibilitatea în spațiul cibernetic național, precum și pentru evaluarea impactului noilor tehnologii asupra securității cibernetice și dezvoltarea de programe de instruire și certificare în domeniu;

16. recomandă respectarea principiilor de izolare a rețelelor de comunicații de date ale dispozitivelor medicale critice utilizând tehnici de segregare și de comunicare prin Ethernet unidirecțional (UDE) și rutare unidirecțională (UDRL);

17. atrage atenția asupra importanței calității software-ului și a instruirii personalului cu acces la sistemele de gestionare a aparaturii medicale de monitorizare, de susținere a vieții și de terapie intensivă, cum ar fi: sisteme de anestezie, dializă, ventilare mecanică, pompe de insulină, defibrilatoare, generatoare de ritm cardiac, aparate de radioterapie și chirurgie robotică, precum și sisteme de monitorizare a funcțiilor vitale, electrocardiografie, electroencefalografie, tomografie, rezonanța magnetică nucleară și tomografie PET;

18. susține propunerea Comisiei Europene ca Agenția UE pentru Securitate Cibernetică (ENISA) să înființeze un Centru paneuropean de suport în materie de securitate cibernetică pentru spitale și furnizorii de servicii medicale, oferindu-le orientări, instrumente, servicii și formare;

19. susține lansarea de proiecte-pilot în întreaga Uniune pentru a dezvolta cele mai bune practici pentru igienă cibernetică și evaluarea riscurilor de securitate, precum și abordarea necesității de monitorizare continuă a securității cibernetice, implicând Centrul european de competențe în domeniul securității cibernetice (ECCC);

20. recomandă instruirea personalului din sectorul medical în aplicarea bunelor practici de protecție împotriva atacurilor cibernetice în cadrul zonelor rurale, defavorizate sau cu legături limitate la rețelele informatice de comunicare;

21. subliniază importanța respectării Strategiei de securitate cibernetică a României pentru perioada 2022-2027 pentru actualizarea și dezvoltarea permanentă a cadrului normativ și instituțional pe componenta gestionării amenințărilor cibernetice și asigurării securității cibernetice.

Această hotărâre a fost adoptată de către Camera Deputaților în ședința din _____, cu respectarea prevederilor art. 76 alin. (2) din Constituția României, republicată.

PREȘEDINTELE
CAMEREI DEPUTAȚILOR

SORIN-MIHAI GRINDEANU

București,
Nr.