1566a/30.09.2026

SENATUL ROMÂNIEI
Senator **RUS Vasile-Ciprian**

Președintele Comisiei de Comunicații, Tehnologia Informației și Inteligență Artificială

Nr. 249/29.09.2026

Adresată:
☑ **Directoratului Național de Securitate Cibernetică**
– în atenția Domnului Director, **Dan CÎMPEAN** –

De către:
☑ **RUS Vasile-Ciprian,** Senator USR; circumscripția electorală nr. 13, Cluj

Obiectul întrebării:

Mecanismul de notificare, urmărire și remediere a vulnerabilităților de securitate cibernetică identificate la nivelul autorităților și instituțiilor publice

Stimate domnule Director,

Incidentele de securitate cibernetică care au afectat în ultimii ani autorități și instituții publice au evidențiat necesitatea consolidării mecanismelor preventive prin care vulnerabilitățile identificate sunt nu doar comunicate instituțiilor afectate, ci urmărite până la remedierea efectivă și verificată.

Ordonanța de urgență a Guvernului nr. 155/2024 instituie obligații privind managementul riscurilor de securitate cibernetică și gestionarea vulnerabilităților și conferă DNSC atribuții de supraveghere, verificare și control.

Totodată, art. 47 din OUG nr. 155/2024 prevede, în cadrul activităților de control, posibilitatea solicitării unui plan de măsuri, asumarea unor termene de remediere și transmiterea documentelor care dovedesc implementarea acestora.

Consider necesară evaluarea modului în care funcționează mecanismul în etapa anterioară producerii unui incident sau declanșării unui control, respectiv atunci când DNSC identifică ori primește informații privind existența unei vulnerabilități și o comunică instituției afectate.

Astfel, în temeiul dispozițiilor art. 34 lit. d) din Legea nr. 96/2006 privind Statutul deputaților și al senatorilor, respectiv potrivit art. 176 alin. (1) din Regulamentul Senatului, formulez prezenta:

ÎNTREBARE

prin care vă rog să îmi transmiteți următoarele informații:

1. În perioada 1 ianuarie 2022 – prezent, câte notificări, informări, avertizări sau alte comunicări privind existența unor vulnerabilități de securitate cibernetică au fost transmise de DNSC către autorități și instituții publice din România? Vă rog să prezentați datele defalcat pe ani și, în măsura în care evidențele DNSC permit, pe niveluri de severitate/risc.

2. Câte autorități și instituții publice distincte au primit astfel de notificări în fiecare dintre anii menționați?

3. Pentru câte dintre vulnerabilitățile comunicate instituțiilor publice DNSC deține în prezent o confirmare sau o dovadă tehnică privind remedierea?

Vă rog să precizați separat, dacă datele sunt disponibile, următoarele aspecte: vulnerabilități remediate, vulnerabilități pentru care au fost implementate doar măsuri compensatorii, vulnerabilități aflate în curs de remediere, vulnerabilități pentru care DNSC nu deține confirmarea remedierii.

4. Pentru vulnerabilitățile pentru care DNSC nu deține confirmarea remedierii, câte au rămas deschise pentru perioade mai mari de: 30 de zile, 60 de zile, 90 de zile, 180 de zile, un an?

Vă rog să prezentați aceste informații exclusiv în formă agregată, fără divulgarea unor date tehnice care ar putea afecta securitatea sistemelor respective.

5. Există în prezent la nivelul DNSC un sistem informatic, registru sau mecanism procedural prin care fiecare vulnerabilitate notificată unei entități poate fi urmărită de la momentul identificării până la remedierea și verificarea acesteia?

În caz afirmativ, vă rog să precizați care sunt principalele stări/statusuri utilizate în acest proces; dacă sunt înregistrate termene de remediere și responsabili; dacă sistemul generează alerte pentru depășirea termenelor;dacă este posibilă raportarea statistică privind durata de remediere.

6. Atunci când DNSC notifică unei autorități sau instituții publice existența unei vulnerabilități, există în prezent termene obligatorii de răspuns și de remediere, diferențiate în funcție de criticitatea vulnerabilității, gradul de expunere sau existența unei exploatări active?

Dacă da, vă rog să indicați actul normativ, procedura sau metodologia care stabilește aceste termene și, în măsura în care informațiile sunt publice, valorile sau criteriile aplicate.

7. Care este procedura utilizată de DNSC în situația în care o instituție publică nu răspunde unei notificări de vulnerabilitate; nu transmite un plan de remediere; depășește termenul comunicat sau asumat; declară vulnerabilitatea remediată fără a furniza dovezi tehnice suficiente?

8. În perioada menționată, în câte situații neremedierea sau lipsa unui răspuns la o vulnerabilitate comunicată anterior de DNSC a determinat declanșarea unei verificări; declanșarea unui control; solicitarea unui audit ad-hoc; dispunerea unor măsuri obligatorii; aplicarea unei sancțiuni?

Vă rog să furnizați datele agregat, defalcat anual.

9. În câte cazuri DNSC a retransmis sau reiterat către aceeași instituție o notificare privind aceeași vulnerabilitate ori aceeași categorie de vulnerabilități deoarece problema nu fusese remediată după prima comunicare?

10. În practica actuală a DNSC, simpla identificare și comunicare către o entitate a unei vulnerabilități critice sau exploatate activ permite stabilirea unui termen obligatoriu de remediere și verificarea respectării acestuia, anterior declanșării unei proceduri formale de control?

În cazul în care răspunsul este negativ sau această competență este limitată, vă rog să precizați care sunt principalele limitări procedurale sau normative întâlnite în practică.

11. În ce măsură DNSC primește de la celelalte autorități competente în domeniul securității cibernetice informații referitoare la vulnerabilități identificate în sistemele informatice ale autorităților și instituțiilor publice și există un mecanism prin care DNSC poate urmări ulterior remedierea acestora?

Nu solicit informații clasificate, date privind sursele sau metodele utilizate ori identificarea instituțiilor sau vulnerabilităților concrete, ci exclusiv descrierea mecanismului instituțional și, dacă sunt disponibile, date statistice agregate.

12. DNSC utilizează sau intenționează să utilizeze liste europene ori internaționale privind vulnerabilitățile exploatate activ, informațiile furnizate de producători sau raportările realizate în temeiul Regulamentului (UE) 2024/2847 privind reziliența cibernetică a produselor cu elemente digitale pentru prioritizarea remedierii vulnerabilităților la nivelul entităților din România?

13. Consideră DNSC necesară completarea cadrului normativ astfel încât vulnerabilitățile critice ori exploatate activ, comunicate unei entități, să fie supuse unui mecanism formal care să cuprindă cel puțin desemnarea unui responsabil; aplicarea imediată, după caz, a unor măsuri compensatorii; întocmirea unui plan de remediere; stabilirea unui termen proporțional cu riscul; prezentarea unor dovezi tehnice privind remedierea; retestarea sau verificarea remedierii pentru vulnerabilitățile cu risc ridicat; declanșarea unei proceduri de verificare sau control în cazul depășirii termenului?

În cazul în care DNSC apreciază că sunt necesare modificări legislative sau procedurale pentru funcționarea unui astfel de mecanism, vă rog să indicați punctual aspectele care, în opinia instituției, necesită intervenție.

14. Vă rog să comunicați, pentru perioada analizată, durata mediană de remediere, în măsura în care aceasta poate fi determinată din evidențele existente, separat pentru vulnerabilitățile clasificate ca fiind critice, ridicate și celelalte categorii de risc.

Având în vedere caracterul sensibil al domeniului, precizez că prezenta solicitare nu vizează identificarea instituțiilor afectate, adrese IP, configurații, CVE-uri concrete, vectori de atac, infrastructuri, capabilități, surse sau alte informații a căror divulgare ar putea produce un risc de securitate cibernetică.

Vă rog ca răspunsul să fie transmis în format electronic și la adresa de email iar acolo unde este posibil, informațiile să fie transmise și în format tabelar sau electronic reutilizabil.

29.09.2026

Cu stimă,
Senator **RUS Vasile-Ciprian**