

EXPUNERE DE MOTIVE

Digitalizarea administrației publice a făcut ca furnizarea unor servicii esențiale pentru cetățeni și mediul economic să depindă direct de disponibilitatea și securitatea sistemelor informatice ale statului. Exploatarea unei singure vulnerabilități poate întrerupe servicii publice, poate bloca activitatea unei instituții, poate compromite date și poate genera cheltuieli importante pentru investigarea incidentului, refacerea infrastructurii și reluarea activității. În acest context, existența unor mecanisme eficiente de identificare și remediere timpurie a vulnerabilităților reprezintă o necesitate imediată pentru protejarea interesului public.

Ordonanța de urgență a Guvernului nr. 155/2024 desemnează Directoratul Național de Securitate Cibernetică, denumit în continuare DNSC, drept autoritate competentă la nivel național și coordonator al procesului de divulgare coordonată a vulnerabilităților. DNSC poate primi și evalua raportări, poate verifica vulnerabilități și poate intermedia relația dintre raportor și entitatea afectată. Legea nr. 124/2025 a consolidat obligațiile de raportare și remediere, însă cadrul în vigoare nu conferă DNSC competența expresă de a organiza programe publice de identificare recompensată a vulnerabilităților și nu prevede temeiul bugetar necesar pentru plata recompenselor. În prezent, DNSC poate gestiona o vulnerabilitate care îi este raportată, dar nu poate invita în mod organizat cercetători în securitate cibernetică să testeze, în limite stabilite în prealabil, sisteme informatice publice și să îi recompenseze pentru vulnerabilitățile validate. Această lacună legislativă limitează capacitatea statului de a preveni incidente de securitate înainte ca acestea să producă efecte.

Necesitatea intervenției legislative trebuie analizată și în contextul geopolitic actual. Conflictul armat din proximitatea României a fost însoțit de folosirea atacurilor cibernetice ca instrument de perturbare, presiune și sabotaj. Chiar preambulul OUG nr. 155/2024 menționează atacul asupra rețelei KA-SAT, acțiunile grupării Killnet împotriva unor infrastructuri din România și incidentul care a afectat 26 de spitale prin compromiterea unui furnizor de servicii. Potrivit ENISA Threat Landscape 2025, administrația publică a reprezentat 38,2% dintre incidentele analizate la nivelul Uniunii Europene, fiind sectorul cel mai vizat de atacuri. Persistența acestui nivel ridicat de risc impune adoptarea cu celeritate a unor instrumente suplimentare de prevenție.

Atacul cibernetic asupra ANCPI a scos din funcțiune sistemul e-Terra și serviciile de cadastru, blocând tranzacții imobiliare, credite și activitatea notarială. Pentru un singur cumpărător, amânarea tranzacției înaintea modificării TVA putea genera un cost suplimentar considerabil. Statul a suportat, în paralel, costurile izolării sistemelor, intervenției tehnice, migrării aplicațiilor și reluării serviciilor. Prin comparație, programul „Hack the Pentagon” a

costat 150.000 de dolari și a identificat 138 de vulnerabilități, în timp ce o testare convențională similară fusese estimată la peste un milion de dolari. Un program Bug Bounty are un buget plafonat, dar indisponibilitatea unui sistem public produce costuri în lanț, considerabil mai mari. În lipsa unui cadru legal care să permită organizarea unor astfel de programe, vulnerabilitățile pot rămâne neidentificate până la exploatarea lor de către actori rău intenționați.

Programele de tip Bug Bounty reprezintă mecanisme controlate prin care cercetătorii în securitate cibernetică sunt autorizați să testeze numai sistemele incluse expres în program și pot primi recompense pentru vulnerabilitățile reale, raportate responsabil și validate. Astfel de programe sunt utilizate de autorități publice din Statele Unite ale Americii, Singapore, Franța, Elveția, Olanda, Belgia, Regatul Unit și Coreea de Sud.

Programele propuse nu înlocuiesc auditurile de securitate, testele de penetrare, monitorizarea continuă, copiile de rezervă sau planurile de continuitate. Ele completează aceste măsuri prin implicarea unui număr mai mare și mai divers de specialiști. Recompensa se acordă numai pentru o vulnerabilitate validată, iar valoarea maximă a recompensei și fondul total al programului se stabilesc înaintea lansării. Cheltuiala publică este astfel previzibilă, plafonată și condiționată de rezultat.

Propunerea legislativă conferă DNSC competența de a iniția, organiza și administra programe de identificare și raportare recompensată a vulnerabilităților pentru rețelele și sistemele informatice deținute, administrate ori utilizate de autorități, instituții publice și alte entități de drept public. Pentru sistemele care nu aparțin DNSC, programul va putea fi organizat numai cu acordul prealabil, expres și scris al entității competente. Totodată, se creează temeiul necesar pentru includerea în bugetul DNSC a cheltuielilor privind organizarea programelor și plata recompenselor, în limita creditelor bugetare aprobate cu această destinație în bugetul de venituri și cheltuieli al DNSC.

Activitățile de testare vor fi autorizate numai în prealabil, expres, limitat și condiționat, exclusiv pentru sistemele, perioada și metodele prevăzute de regulile programului. Nu vor putea fi autorizate atacurile brute-force, phishingul, ingineria socială, utilizarea de malware, afectarea disponibilității serviciilor, ștergerea sau modificarea datelor, menținerea accesului ori extinderea acestuia către alte sisteme sau conturi. Depășirea limitelor programului va determina pierderea dreptului la recompensă, fără a înlătura răspunderea civilă, contravențională sau penală.

Detaliile privind inițierea programelor, selectarea sistemelor, condițiile de participare, validarea vulnerabilităților, stabilirea și plata recompenselor, protecția datelor, confidențialitatea, controlul și suspendarea programelor vor fi reglementate prin hotărâre a Guvernului, la propunerea DNSC.

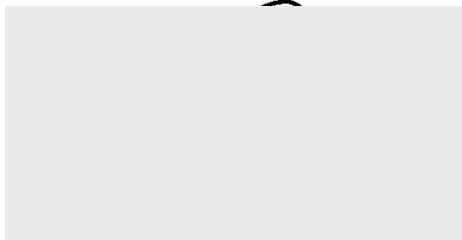
Având în vedere necesitatea consolidării fără întârziere a capacității de prevenire a incidentelor de securitate cibernetică și eliminării vidului normativ existent, adoptarea prezentei propuneri legislative în procedură de urgență este justificată de interesul public major privind asigurarea continuității serviciilor publice și protejarea infrastructurilor digitale ale statului.

Prin această intervenție punctuală, statul român va putea utiliza, într-un cadru legal, controlat și transparent, competențele cercetătorilor în securitate cibernetică pentru a descoperi vulnerabilitățile înainte ca acestea să fie exploatare de actori rău intenționați.

Având în vedere argumentele prezentate mai sus, înaintăm Parlamentului României, spre dezbateră și adoptare, prezenta propunere legislativă, în procedură de urgență.

Pentru inițiatori,

Oprea Octavian, deputat PNL



[illegible]