

Oficial din Directoratul pentru Securitate Cibernetică: Nu mai e nevoie de cunoștințe avansate pentru a deveni “un mic hacker”. Suntem scanați pentru vulnerabilități în orice secundă

Noile tehnologii permit actorilor malițioși să-și dezvolte tacticile și procedurile de atac, iar în context aceștia nu mai au nevoie de cunoștințe avansate pentru a deveni “un mic hacker” sau o mică structură care poate avea interese financiare, a declarat, miercuri, în cadrul conferinței “Digitalizare și Siguranță Cibernetică”, adjunctul directorului Directoratului Național de Securitate Cibernetică (DNSC), Stelian Cristea.

“Peisajul amenințărilor cibernetice s-a dezvoltat și se dezvoltă permanent. S-au dezvoltat actori malițioși care existau acum cinci ani sau cu mai puțin timp în urmă, care și-au perfecționat tacticile și procedurile. Alți actori malițioși au intrat în rândurile lor, pentru că tehnologia le permite. Nu mai au nevoie de cunoștințe avansate pentru a deveni “un mic hacker” sau o mică structură care poate avea interese financiare sau de altă natură în organizațiile care își desfășoară activitatea în online. În mediul dark web pot fi procurate soluții pentru a fi a deveni un actor malițios cu ușurință. Și atunci iată că numărul actorilor malițioși este în creștere. În sprijinul lor vine tehnologia AI care le permite să devină mult mai eficienți în activitățile pe care le fac”, a explicat Cristea.

Reprezentantul DNSC a punctat faptul că, la ora actuală, toți utilizatorii de Internet sunt scanați de către hackeri la fiecare secundă, transmite Agerpres.

“Un studiu recent preciza că, în fiecare secundă, se întâmplă 36.000 de scanări. Ce înseamnă asta? Că nici măcar nu mai suntem un target. Suntem scanați pentru vulnerabilități în orice minut, în orice secundă. Nu mai avem o problemă de genul: “Nu sunt important pentru actorii malițioși”, ci este o problemă: “De când voi fi în plaja de scanare a atacatorilor”...Evident, numărul vulnerabilităților s-a dezvoltat. Comportamentul utilizatorilor în mediul cibernetic este exploatat din ce în ce mai mult. Același studiu preciza că atacurile de tip “Zero Day” sau care exploatează vulnerabilități încă nedescoperite de producători, dar

descoperite de actorii malițioși și exploatare, au scăzut. Simultan, a crescut numărul atacurilor bazate pe credențiale furate sau credențiale obținute de la furnizori de baze de date, iar cu acele credențiale atacatorii reușind să intre pe culoarele oficiale în structura cibernetică a organizațiilor”, a susținut reprezentantul DNSC.

Agenda de securitate cibernetică a României, modalități de detectare și de contracarare a atacurilor cyber și tendințe în tehnologie și în piața digitală, sunt câteva dintre temele ce vor fi abordate, miercuri, în cadrul conferinței “Digitalizare și Siguranță Cibernetică”, organizată de publicația Bursa.