g4media.ro

Oficial din Directoratul pentru Securitate Cibernetică: Nu mai e nevoie de cunoştinţe avansate pentru a deveni „un mic hackeraş”. Suntem scanaţi pentru vulnerabilităţi în orice secundă

Noile tehnologii permit actorilor maliţioşi să-şi dezvolte tacticile şi procedurile de atac, iar în context aceştia nu mai au nevoie de cunoştinţe avansate pentru a deveni „un mic hackeraş” sau o mică structură care poate avea interese financiare, a declarat, miercuri, în cadrul conferinţei „Digitalizare şi Siguranţă Cibernetică”, adjunctul directorului Directoratului Naţional de Securitate Cibernetică (DNSC), Stelian Cristea.

„Peisajul ameninţărilor cibernetice s-a dezvoltat şi se dezvoltă permanent. S-au dezvoltat actori maliţioşi care existau acum cinci ani sau cu mai puţin timp în urmă, care şi-au perfecţionat tacticile şi procedurile. Alţi actori maliţioşi au intrat în rândurile lor, pentru că tehnologia le permite. Nu mai au nevoie de cunoştinţe avansate pentru a deveni „un mic hackeraş” sau o mică structură care poate avea interese financiare sau de altă natură în organizaţiile care îşi desfăşoară activitatea în online. În mediul dark web pot fi procurate soluţii pentru a fi a deveni un actor maliţios cu uşurinţă. Şi atunci iată că numărul actorilor maliţioşi este în creştere. În sprijinul lor vine tehnologia AI care le permite să devină mult mai eficienţi în activităţile pe care le fac”, a explicat Cristea.

Reprezentantul DNSC a punctat faptul că, la ora actuală, toţi utilizatorii de Internet sunt scanaţi 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 scanaţi pentru vulnerabilităţi în orice minut, în orice secundă. Nu mai avem o problemă de genul: „Nu sunt important pentru actorii maliţioşi”, ci este o problemă: „De când voi fi în plaja de scanare a atacatorilor”…Evident, numărul vulnerabilităţilor s-a dezvoltat. Comportamentul utilizatorilor în mediul cibernetic este exploatat din ce în ce mai mult. Acelaşi studiu preciza că atacurile de tip „Zero Day” sau care exploatează vulnerabilităţi încă nedescoperite de producători, dar descoperite de actorii maliţioşi şi exploatate, au scăzut. Simultan, a

crescut numărul atacurilor bazate pe credenţiale furate sau credenţiale obţinute de la furnizori de baze de date, iar cu acele credenţiale atacatorii reuşind să intre pe culoarele oficiale în structura cibernetică a organizaţiilor”, a susţinut reprezentantul DNSC.

Agenda de securitate cibernetică a României, modalităţi de detectare şi de contracarare a atacurilor cyber şi tendinţe în tehnologie şi în piaţa digitală, sunt câteva dintre temele ce vor fi abordate, miercuri, în cadrul conferinţei „Digitalizare şi Siguranţă Cibernetică”, organizată de publicaţia Bursa.