Raport DNSC: Fraudele informatice au crescut în România cu peste 40%, în 2024; atacurile malware, majorare cu 286,8%

Fraudele informatice raportate în România, la nivelul anului 2024, au crescut cu 40,2% fata de anul anterior, în linie cu tendintele globale si ale Uniunii Europene (UE), în timp ce fenomenul malware s-a majorat cu 286,8%, se arata în Raportul anual al Directoratului National pentru Securitate Cibernetic ((DNSC), prezentat miercuri într-o conferinta de presa.

Conform documentului, în ceea ce priveste fraudele, cresterea acestora reprezinta "o consecinta a tehnicilor, tacticilor si protocoalelor tot mai agresive si inovative ale infractorilor, fiind corelata cu intensificarea atacurilor ce utilizeaza tehnici de spoofing telefonic si a schemelor de tip investitii financiare, care exploateaza încrederea victimelor prin oportunitati financiare false promovate agresiv". De asemenea, cresterea numarului de fraude raportate catre Directorat este influentata si de mesajele si demersurile Directoratului în spatiul public încurajând raportarea acestora catre autoritati.

La capitolul malware, raportul de specialitate releva o crestere de 286,8%, în 2024 fata de 2023, în timp ce numarul aplicatiilor compromise a cunoscut un trend ascendent (+125%).

"Acest trend arata o evolutie semnificativa si îngrijoratoare a capabilitatilor si expertizei atacatorilor cibernetici, care au devenit foarte prolifici în crearea de noi varietati de programe malitioase (estimare de ordinul 500.000 programe malware generate zilnic). De asemenea, este o indicatie clara a intentiei atacatorilor de a exploata vulnerabilitatile din lantul de furnizori (prin aplicatiile produse de acestia). De asemenea, trendul indica necesitatea utilizarii cu prioritate a solutiilor antimalware", se mentioneaza în raportul DNSC.

Cresteri ale fenomenului cyber au fost înregistrate în zona Bruteforce (+30.3%) si Cont Compromis (+21%). În acest context, specialisti sustin ca tendinta poate fi explicata de cresterea numarului de atacuri automate, dar si de implementarea slaba a autentificarii cu mai multi factori la nivelul utilizatorilor, coroborata cu o proliferare a activitatii utilizatorului standard pe un numar semnificativ crescut de platforme si aplicatii, cu re-utilizarea prudentialelor de utilizator.

Pe de alta parte, atacurile de tip phishing au consemnat o scadere de 21%, de la un an la altul. "Declinul se datoreaza în principal succesului campaniilor de educare a utilizatorilor dar si a demersurilor efectuate de catre Directorat pentru implementarea de catre organizatii, la scara larga, a masurilor de securizare a serverelor de email (SPF/DKIM/DMARC)", noteaza sursa citata.

De asemenea, la IP-uri infectate s-a raportat o diminuare de 27,8%, ce "poate reflecta o mai buna protectie la nivel de retea si adoptarea unor solutii de securitate mai avansate de catre organizatii".

Alte scaderi s-au înregistrat în zone Defacement (-45.8%), respectiv DDoS (-38.5%). "Aceste scaderi indica o îmbunatatire a monitorizarii serverelor si a protectiei împotriva atacurilor volumetrice la nivel national, organizatiile din sectorul public si privat adoptând din ce în ce mai mult servicii si solutii de protectie cibernetica", se arata în raportul citat.

Potrivit sursei citate, în 2024, DNSC a intervenit conform atributiilor sale legale, în vederea sprijinirii actorilor impactati de o serie de atacuri si incidente cibernetice în: Energie (Rompetrol si Mol România), domeniul bancar (Alpha Bank, Banca Transilvania, Banca Comerciala Româna, Creditcoop, Exim Bank, Edificium, Banca Nationala a României, Banca Româna de Credite si Investitii, Bursa de Valori Bucuresti si Fondul Garantare a

Depozitelor Bancare), infrastructura digitala/telecomunicatii (Orange, Telekom si GTS), Transport (Compania Nationala de Cai Ferate - CFR, Compania Nationala de Administrare a Infrastructurilor Rutiere - CNAIR, Compania Nationala Aeroporturi Bucuresti, Portul Constanta, Astra Trans Carpatica Feroviar, Aeroportul Baneasa si Metrorex) si administratia publica centrala si locala (Guvernul României, Serviciul de Telecomunicatii Speciale, Directoratul National de Securitate Cibernetica, Ministerul Afacerilor Interne, Senatul României, Ministerul Afacerilor Externe, Ministerul Dezvoltarii Lucrarilor Publice si Administratiei, Ministerul Turismului si Primaria Municipiului Bucuresti).

Alte atacuri raportate în cursul anului trecut au vizat: Website defacement (inclusiv, dar fara a se limita la paginile oficiale ale unor partide politice - e.g. Alianta pentru Unirea Românilor), criptare si exfiltrare de date sensibile spre exemplu exfiltrarea de date de la Camera Deputatilor, atacuri de tip brute-force, sens în care mentionam cu titlu exemplificativ atacurile care au vizat infrastructurile Primariei Municipiului Bucuresti, Societatii de Transporturi Bucuresti, Autoritatii Feroviare Române, Universitatii din Bucuresti, având la baza IP-uri sursa gazduite în Rusia.

Totodata, fenomenul ransomware este unul dintre cele mai persistente si grave, iar un numar de 101 astfel de incidente au fost detectate si gestionate, în 2024, de catre DNSC. Printre acestea s-a aflat atacarea informatica a Societatii Romanian Soft Company - dezvoltatorul platformei Hipocrate, care ofera servicii de fluxuri interne catre unitati spitalicesti. În urma atacului, 26 de spitale au fost vizate în mod direct, fiind în imposibilitatea de a-si desfasura activitatea pentru aproximativ o saptamâna.

În plus, alte atacuri de tip ransomware au vizat: societatile din grupul Electrica S.A, cu un impact major asupra serviciilor publice oferite de catre Electrica Furnizare S.A. si Distributie Energie Electrica Romania S.A., cu consecinta afectarii unui numar de peste 800 servere si 4.000 statii de lucru aflate la nivelul sucursalelor Bucuresti, Ploiesti, Brasov si Cluj; Primaria Municipiului Timisoara precum si institutii din subordinea acestora (Directia Fiscala a Municipiului Timisoara si Directia Generala a Politiei Locale Timisoara), fiind afectate aproximativ 112 sisteme; infrastructura proiectului "Sistemul National de Management privind Dizabilitatea", având ca beneficiar Autoritatea Nationala pentru Protectia Drepturilor Persoanelor cu Dizabilitati (ANPDPD); Primaria Sectorului 5 a Municipiului Bucuresti, care a avut un impact major asupra serviciilor puse la dispozitie cetatenilor, fiind afectate serverele de tip Domain Controller, centrala telefonica a Politiei Locale si statii de lucru.

Raportul de activitate DNSC pe anul 2024 a fost aprobat, recent, de catre Consiliul Superior de Aparare a Ţarii (CSAT).