DNSC confirma ca persoane fizice si persoane juridice au fost afectate de atacul hackerilor asupra Orange România

Institutii guvernamentale, primarii, unitati de învatamânt, autoritati publice, unitati spitalicesti, institutii financiar-bancare si asiguratori, companii de transport si energie sunt printre persoanele juridice care au fost afectate de incidentul de securitate cibernetica care a afectat operatorul de telecomunicatii Orange România, în data de 23 februarie 2025, informeaza Directoratul National de Securitate Cibernetica (DNSC), într-un comunicat transmis, marti, AGERPRES.

"Urmare a incidentului de securitate cibernetica care a afectat operatorul de telecomunicatii Orange România (Orange RO) din data de 23 februarie 2025 si mediatizat la data de 25 februarie 2025, Directoratul National de Securitate Cibernetica (DNSC sau Directoratul), în calitate de autoritate nationala cu atributii în asigurarea securitatii spatiului cibernetic national civil (cf. OUG 104/2021), a demarat o actiune de analiza a incidentului cibernetic mentionat. DNSC este în contact cu Orange România privind incidentul, iar din concluziile preliminare ale analizei mentionam ca, pe lânga persoane fizice, au fost identificate si persoane juridice inclusiv institutii guvernamentale, primarii, unitati de învatamânt, autoritati publice, unitati spitalicesti, institutii financiar-bancare si asiguratori, companii de transport si energie", noteaza institutia.

În context, DNSC considera important de avut în vedere urmatoarele riscuri si amenintari subsecvente atacului ca fiind cele mai relevante pentru urmatoare perioada pentru entitatile si utilizatorii impactati: cresterea riscului de campanii de tip phishing, riscul de atacuri subsecvente în special asupra sectorului telecomunicatiilor, riscuri de frauda si furt de identitate, riscul de inginerie sociala si escaladarea accesului si riscul de frauda comerciala prin emiterea de documente false.

Totodata, expertii în securitate cibernetica vin cu o serie de recomandari pentru utilizatori, precum: sa fie vigilenti cu privire la viitoare apeluri, emailuri sau mesaje primite din partea persoanelor ce sustin ca ar fi angajati ai companiei Orange România; atentie sporita cu privire la apeluri, emailuri sau mesaje suspecte legate de actualizare factura, date, sau alte tipuri de cereri ce par a veni din partea companiei Orange România; orice astfel de solicitari sa fie tratate cu suspiciune si verificate prin canalele oficiale Orange România; raportarea catre Directorat a oricarei tentative suspecte prin platforma PNRISC (https://pnrisc.dnsc.ro/), sporirea masurilor de securitate asupra conturilor de utilizator/client asociate aplicatiilor administrate de Orange România, inclusiv prin schimbarea parolelor, re-instalarea aplicatiilor respective pe telefoanele mobile sau tablete, precum si prin activarea sau implementarea de autentificare cu mai multi factori (MFA/2FA).

De asemenea, este nevoie de atentie cu privire la accesarea linkurilor catre pagini de web ce au elemente grafice similare cu ale Orange România, prin verificarea veridicitatii domeniului pe care îl acceseaza, precum si utilizarea instrumentelor de tip https://www.scamadviser.com/, dar si monitorizarea tranzactiilor efectuate pe cardurile bancare asociate contractelor cu Orange România si activarea, daca este posibila a notificarilor pentru aceste tranzactii; la primele indicii este necesara contactarea bancii emitente, pentru blocarea conturilor si/sau tranzactiilor.

Mass media au relatat, saptamâna trecuta, ca un hacker din grupul HellCat a furat si publicat 380.000 de adrese de e-mail si documente interne ale Orange România, iar diverse date confidentiale, inclusiv detalii partiale de carduri de credit si informatii angajati, au fost divulgate.

Ulterior, compania a confirmat bresa într-o aplicatie non-critica si a anuntat ca investigheaza incidentul pentru a minimiza efectele atacului.