

Sectorul energetic din România ramâne cel mai expus la atacuri cibernetice (raport)

Peste 14 milioane de atacuri cibernetice sunt monitorizate, în fiecare luna, de serviciul Business Internet Security (BIS), iar printre cele mai frecvente amenintari se afla ransomware, DDoS si phishing, arata datele centralizate în raportul "Business Internet Security 2025", publicat marti.

Potrivit editiei a 7-a a cercetarii, întocmite de Orange Business, sectorul energetic ramâne cel mai expus, fiind tinta a 31% din atacurile cibernetice înregistrate. Acesta este urmat de administratia publica (27%) si industria IT (25%).

În acelasi timp, Bucuresti este cel mai vizat oras din România, cu peste 1,25 milioane de incidente prevenite, în fiecare luna.

"Astfel, digitalizarea companiilor românesti vine nu doar cu beneficii, ci si cu provocari semnificative în materie de securitate, în contextul în care atacurile devin tot mai sofisticate, iar protectia infrastructurilor informatice devine o prioritate absoluta pentru companii din toate sectoarele (...) Ransomware-ul ramâne principala amenintare, afectând 32% dintre organizatiile monitorizate, în timp ce atacurile de tip DDoS au cunoscut o crestere alarmanta, utilizând dispozitive IoT pentru a genera volume mari de trafic malitios", se mentioneaza în raport.

Predictiile pentru anul 2025, în materie de amenintari cibernetice, vizeaza: cresterea atacurilor personalizate ca urmare a utilizarii Inteligentei Artificiale; extinderea atacurilor asupra infrastructurilor critice, în special prin ransomware; reglementari mai stricte care vor obliga companiile sa investeasca în conformitate; vulnerabilitatea lanturilor de aprovizionare si a dispozitivelor Internet of Things - IoT; automatizarea crescuta a proceselor de securitate, pe fondul lipsei de specialisti.

Orange Business ofera o gama de solutii complete pentru protectia împotriva amenintarilor, precum: Business Internet Security (BIS) - protejeaza datele companiei, ale angajatilor si vizitatorilor împotriva atacurilor cibernetice, Threats & Exposures Management - solutie de securitate bazata pe Inteligenta Artificiala, care detecteaza, evalueaza si raporteaza vulnerabilitatile de securitate în website-uri, aplicatii web si resurse cu IP-uri publice, Security Operations Center (SOC) - protejeaza companiile împotriva riscurilor ce pot afecta informatiile, aplicatiile, bazele de date, serverele, statiile de lucru si sistemele.

Editia din acest an a raportului "Orange Business Internet Security 2025" a fost redactata, pentru prima data, si în limba româna.