Studiu EY: Viteza și dimensiunea pieței atrag atenția hacker-ilor, iar aproximativ 10% din fondurile ICO sunt pierdute sau furate

Conform rezultatelor unui studiu lansat de EY în urma analizei a 372 de oferte inițiale de criptovalute (ICO) de la nivel global, investitorii se confruntă cu două riscuri semnificative. Primul ține de zona de reglementare: țări diferite au niveluri diferite de strictețe a reglementărilor pentru ICO-uri, fapt care generează vulnerabilități pe piață. Drept urmare, cei interesați de activități ilegale în cadrul unei oferte ar putea să se îndrepte către jurisdicțiile în care autoritățile au o abordare mai relaxată față de ICO.

Simona Radu, Partener Asociat EY România, evidențiază faptul că „*în acest moment, criptovalutele nu sunt reglementate, așa cum reiese și din studiu. La nivel european sunt însă întreprinse o serie de demersuri pentru reglementarea acestora. Conform unui comunicat al Băncii Centrale Europene, se așteaptă ca regulamentul privind criptovalutele să fie un subiect important pe agenda summit-ului G20 din luna martie a.c. De asemenea, Parlamentul European are în dezbatere proiectul celei de-a cincea Directive privind spălarea banilor, care abordează riscurile valutei virtuale, având în vedere caracterul de volatilitate și anonimatul. Astfel, s-a propus ca platformele de valută virtuală și furnizorii de portofolii virtuale să intre în sfera de aplicare a Directivei, urmând a avea obligații de identificare și verificare a clienților și de control asupra tranzacțiilor, pentru eliminarea suspiciunilor de utilizare a valutei în scopul spălării banilor sau finanțării terorismului*.”

Al doilea risc este legat de furturile prin hacking: peste 10% din fondurile ICO se pierd sau sunt furate de hackeri (aproape 400 milioane USD). Hackerii profită de ireversibilitatea tranzacțiilor bazate pe blockchain și de erorile de codare de bază, elemente care ar putea fi evitate, dacă aceste ICO-uri ar fi revizuite de dezvoltatori experimentați și de analiști de securitate cibernetică.

Fondurile sunt deturnate prin adrese substitut de portofele electronice (phishing, hacking de site), prin accesarea de chei private şi furt de fonduri din portofele, sau prin hacking asupra burselor de schimb și portofelelor. Toate astea se adaugă pierderilor indirecte legate de riscurile reputaţionale ridicate pentru fondatorii proiectelor.

Simona Radu adaugă: *“Pe piață circulă o gamă variată de criptovalute care pot fi utilizate în a disimula fondurile ilicite la tranzacționare. Acestea nu sunt ușor de urmărit pe piață, fiind construite pe baza unor protocoale menite să evite controalele şi având ca scop explicit atât ascunderea valorilor și a destinației fondurilor tranzacționate, cât și a identității celor care tranzacționează. Creativitatea celor implicați în astfel de activități acoperă moduri de operare din ce în ce mai complexe și ingenioase*.”