

Codirlasu (CFA România): O mare parte din reglementarile DORA sunt prinse în legislația românească

O mare parte din reglementarile cu care vine Directiva europeană privind reziliența operațională digitală (DORA) sunt prinse într-un fel sau altul în legislația românească, dar va trebui să vedem unde sunt golurile și cum le acoperim, a afirmat miercuri Adrian Codirlasu, vicepreședinte CFA România, într-o conferință de specialitate.

"Riscul cibernetic și riscul aferent furnizorilor terți sunt riscuri operaționale. Prin urmare, DORA se referă la o componentă a riscului operațional. Însă dacă ne uităm, să zicem, la tipurile de evenimente de risc operațional prevăzute de legislație, începând cu Basel II, sunt șapte tipuri de evenimente și așa spune că DORA se referă la patru dintre ele. Poate chiar la cinci. Practic, la ce ne poate duce neluarea în considerare a acestui risc aferent utilizării de echipamente IT? La fraude ne poate conduce, în cazul în care sistemele nu sunt corect setate și avem asemenea evenimente și ne mai poate conduce la întreruperi ale activității într-o instituție financiară. De asemenea, când nu sunt corect implementate sau corect calibrate pentru activitatea pe care o avem, ne poate duce la erori în relația cu clienții și chiar cu reglementatorii atunci când avem de raportat anumite lucruri făcute de sisteme și nu reușim să raportăm. Deci, vedem că merge către o mare parte din riscurile operaționale. De asemenea, trebuie să ne uităm și la relația cu terții", a explicat Adrian Codirlasu, la conferința "DORA - Strategy, Regulation, Resilience" organizată de Oxygen Events și Model Tree.

El a adăugat că în legislația românească pe partea de sistem bancar există regulamentul BNR, care se referă la condițiile de externalizare semnificativă, unde trebuie expres aprobarea Bancii Naționale, lucru care este mai strict reglementat decât de Directiva DORA.

Adrian Codirlasu a afirmat că și pe partea de piața financiară nebankară, România are norme ASF care reglementează riscul cibernetic și relațiile cu terții, însă Directiva DORA vine cu ceva suplimentar.

"Până acum în legislația aveam doar partea de externalizări, dar mai putem avea relații cu terții care nu sunt externalizări, sunt de exemplu contracte pe o perioadă limitată. Însă, asemenea relații implică instituția financiară. Dacă se întâmplă o fraudă la furnizorul terț sau scurgere de informații la furnizorii terți, noua ne vine ca instituție financiară amenda de la reglementator. Deci, noi răspundem pentru ceea ce face teretul. Și în contextul acesta vine DORA cu niste cerințe care trebuie puse pe furnizorii de asemenea servicii pentru a gestiona tocmai riscurile operaționale aferente sistemelor IT din aceste instituții terțe", a explicat Adrian Codirlasu.

Potrivit acestuia, Directiva vine cu cerințe privind teste de penetrare a sistemelor, inclusiv pentru companiile terțe, fapt care va crește costul furnizării de asemenea servicii.

"În concluzie, o mare parte dintre componentele riscului operațional sunt acoperite de DORA. În legislația românească aveam o mare parte dintre ele, deci avem pe ce construi. E adevărat, trebuie să punem într-un anumit framework toate lucrurile acestea, însă nu pornim de la zero. O mare parte din aceste reglementări sunt cumva într-un fel sau altul prinse în legislația românească. Altele erau să zicem implicite, nu prevăzute expres însă va trebui să existe un proces de a vedea unde sunt gap-urile și de a le acoperi", a mai spus Adrian Codirlasu.

Guvernul a aprobat, în septembrie, un proiect de lege care transpune în legislația națională Directiva DORA, pentru consolidarea securității cibernetice a entităților financiare și, implicit, o mai bună protecție a informațiilor clienților de servicii financiare, a declarat atunci purtătorul de cuvânt al Executivului, Mihai Constantin.

"Începând cu 17 ianuarie 2025, anul viitor asadar, vor fi aplicate în România noi reglementări pentru consolidarea

securitatii cibernetice a entitatilor financiare si, implicit, o mai buna protejare a informatiilor clientilor de servicii financiare. Este vorba despre transpunerea în legislatia nationala a Directivei DORA printr-un proiect de lege aprobat astazi de catre Guvern si care urmeaza sa fie transmis, tot în procedura de urgenta, Parlamentului. Directiva DORA se va aplica începând, asa cum am anuntat, cu 17 ianuarie anul viitor, împreuna cu Regulamentul 2554 pe 2022 al Uniunii Europene privind rezilienta operationala digitala pentru sectorul financiar, care este de directa aplicare si nu necesita transpunere în dreptul intern. Ambele aceste documente, regulamentul si proiectul de lege, au scopul sa sprijine si sa faciliteze consolidarea securitatii cibernetice în domeniul serviciilor financiare", a precizat Mihai Constantin.

Acesta a dat si exemple de aplicabilitate a reglementarilor europene mentionate.

"De exemplu, Banca Nationala a României va fi informata cu privire la orice incident operational sau de securitate major. De asemenea, potrivit regulamentului DORA, care se va aplica în mod direct, se mentioneaza ca în cazul în care are loc un incident major legat de tehnologia informatiilor, atunci asupra intereselor financiare ale clientilor, entitatile financiare îi informeaza pe acestia, fara întârzieri nejustificate, de îndata ce afla despre acest incident major. De asemenea, informeaza pe clientii afectati cu privire la eventualele masuri de protectie luate pentru a preveni aceste atacuri sau pentru a combate un atac deja precizat", a aratat purtatorul de cuvânt al Guvernului.