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

O mare pare din reglementarile cu care vine Directiva europeana privind rezilienta operationala digitala (DORA) sunt prinse într-un fel sau altul în legislatia românească, dar va trebui sa vedem unde sunt golurile si cum le acoperim, a afirmat miercuri Adrian Codirlasu, vicepresedinte CFA România, într-o conferinta de specialitate.

"Riscul cibernetic si riscul aferent furnizorilor terti sunt riscuri operationale. Prin urmare, DORA se refera la o componenta a riscului operational. Însa daca ne uitam, sa zicem, la tipurile de evenimente de risc operational prevazute de legislatie, începând cu Basel II, sunt sapte tipuri de evenimente si as spune ca DORA se refera la patru dintre ele. Poate chiar la cinci. Practic, la ce ne poate duce neluarea în considerare a acestui risc aferent utilizarii de echipamente IT? La fraude ne poate conduce, în cazul în care sistemele nu sunt corect setate si avem asemenea evenimente si ne mai poate conduce la întreruperi ale activitatii într-o institutie financiara. De asemenea, când nu sunt corect implementate sau corect calibrate pentru activitatea pe care o avem, ne poate duce la erori în relatia cu clientii si chiar cu reglementatorii atunci când avem de raportat anumite lucruri facute de sisteme si nu reusim sa raportam. Deci, vedem ca merge catre o mare parte din riscurile operationale. De asemenea, trebuie sa ne uitam si la relatia cu tertii", a explicat Adrian Codirlasu, la conferinta "DORA - Strategy, Regulation, Resilience" organizata de Oxygen Events si Model Tree.

El a adaugat ca în legislatia românească pe partea de sistem bancar exista regulamentul BNR, care se refera la conditiile de externalizare semnificativa, unde trebuie expres aprobarea Bancii Nationale, lucru care este mai strict reglementat decât de Directiva DORA.

Adrian Codirlasu a afirmat ca si pe partea de piata financiara nebancara, România are norme ASF care reglementeaza riscul cibernetic si relatiile cu tertii, însa Directiva DORA vine cu ceva suplimentar.

"Pâna acum în legislatia aveam doar partea de externalizari, dar mai putem avea relatii cu tertii care nu sunt externalizari, sunt de exemplu contracte pe o perioada limitata. Însa, asemenea relatii implica institutia financiara. Daca se întâmpla o frauda la furnizorul tert sau scurgere de informatii la furnizorii terti, noua ne vine ca institutie financiara amenda de la reglementator. Deci, noi raspundem pentru ceea ce face teretul. Şi în contextul acesta vine DORA cu niste cerinte care trebuie puse pe furnizorii de asemenea servicii pentru a gestiona tocmai riscurile operationale aferente sistemelor IT din aceste institutii terte", a explicat Adrian Codirlasu.

Potrivit acestuia, Directiva vine cu cerinte privind teste de penetrare a sistemelor, inclusiv pentru companiile terte, fapt care va creste costul furnizarii de asemenea servicii.

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

Guvernul a aprobat, în septembrie, un proiect de lege care transpune în legislatia nationala Directiva DORA, pentru consolidarea securitatii cibernetice a entitatilor financiare si, implicit, o mai buna protejare a informatiilor clientilor de servicii financiare, a declarat atunci purtatorul de cuvânt al Executivului, Mihai Constantin.

"Începând cu 17 ianuarie 2025, anul viitor asadar, vor fi aplicate în România noi reglementari 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.