**Ecosistemul financiar, înainte și după implementarea cadrului TIBER-EU în România.**

**Care sunt provocările?**

*Articol de opinie de Andrei Ionescu, Partener coordonator, Consultanță și Managementul Riscului, și Adrian Ifrim, Senior Manager, Managementul Riscului, Deloitte România*

Atacurile cibernetice reprezintă o amenințare pentru fiecare dintre noi, iar evenimentele din ultima perioadă ne-au demonstrat că perturbările produse pot fi considerabile. Riscurile provocate de aceste perturbări trebuie luate în considerare și de către bănci și alți actori ai domeniului financiar, deoarece pot avea un impact nu numai asupra fiecărei organizații în parte, ci și asupra stabilității întregului ecosistem financiar. Riscul atacurilor cibernetice este accentuat și de folosirea tehnologiilor digitale de către sistemul financiar și de provocările generate de viteza cu care evoluează amenințările cibernetice.

Banca Națională a României (BNR) a considerat, așadar, că este esențial ca băncile, alte instituții financiare sau infrastructurile pieței financiare aflate sub supravegherea sa să își asigure un nivel adecvat de rezistență cibernetică pentru a se proteja atât pe ele însele, cât și întregul ecosistem. În luna mai 2022, BNR a transpus la nivel local cadrul TIBER-EU (*Threat Intelligence-based Ethical Red Teaming*), un standard de desfășurare a testelor pentru determinarea gradului de reziliență cibernetică elaborat de Banca Centrală Europeană și celelalte bănci centrale din Uniunea Europeană.

[Cadrul TIBER-RO](https://www2.deloitte.com/ro/en/pages/risk/solutions/tiber-ro-framework.html?nc=42), publicat în Monitorul Oficial nr. 432/03.05.2022, se aplică instituțiilor financiare aflate sub supravegherea Băncii Naționale a României, care vor fi nevoite să-și testeze rezistența cibernetică la fiecare trei ani, spre deosebire de alți actori ai ecosistemului financiar, care nu vor avea obligativitatea aplicării acestui cadru.

Înainte de introducerea cadrului TIBER-RO, testarea rezistenței cibernetice se realiza fragmentat, prin verificări izolate sau separate asupra aplicațiilor folosite în cadrul organizațiilor, în medii controlate, demers care nu oferea o imagine de ansamblu a riscurilor la care băncile erau supuse din acest punct de vedere.

Derularea unui test care să evidențieze capacitatea de ansamblu a unei organizații de a se apăra de atacurile cibernetice este un exercițiu complex, care necesită coordonarea mai multor echipe, nu doar a celor dedicate securității cibernetice, ci și a celor de IT și management. În contextul implementării TIBER-RO, membrii consiliilor de administrație, directorii și responsabilii în domeniul cibernetic sau IT vor fi nevoiți să planifice din timp acest tip de exerciții, dar și să implementeze metode de management al riscului cibernetic, în vederea atingerii unui punct maxim de eficiență.

În primul rând, organizațiile trebuie să conștientizeze faptul că o testare conformă cu cadrul TIBER-RO va evidenția atât plusurile, cât și minusurile practicilor de securitate cibernetică pe care le au implementate. De această dată, companiile vor fi nevoite să facă față unui atac care are loc în condiții identice cu cele ale unui incident real, neanunțat, în mediul de producție, în timp real, la finalul căruia vor putea aplica măsurile necesare pentru a-și îmbunătăți nivelul de securitate cibernetică.

Din punctul de vedere al infrastructurii, aplicarea unui test TIBER-RO poate avea un impact semnificativ asupra unei organizații, de la transformări asupra culturii organizaționale, până la procesele companiei sau chiar capitalul uman. În funcție de rezultatul testului, companiile vor lua în considerare o serie de măsuri care presupun investiții pentru actualizarea sistemelor informatice, instruirea specialiștilor în securitate cibernetică sau chiar pregătirea unor campanii de conștientizare în rândul angajaților privind amenințările din spațiul virtual.

O altă provocare privind implementarea cadrului TIBER-RO o reprezintă și componența echipelor interne de specialiști în securitate cibernetică. Securitatea cibernetică este un domeniu care se confruntă cu un deficit de experți. Deși numărul lor a crescut în ultima perioadă, avansul înregistrat nu este suficient pentru a răspunde nevoilor din piață. Pentru derularea unui exercițiu care stabilește nivelul de rezistență cibernetică a unei organizații, aceasta trebuie să ia în considerarea formarea sau consolidarea echipelor interne de securitate cibernetică.

Procesul de testare în urma căruia este stabilit nivelul de eficiență a practicilor de management al riscului cibernetic din cadrul unei organizații trebuie să fie unul continuu, iar, pentru îmbunătățirea sa, companiile trebuie să ia în considerare o serie de acțiuni care ar putea avea un impact direct semnificativ asupra întregii organizații. Activitățile efectuate în cadrul unui exercițiu bazat pe TIBER-RO trebuie executate de către echipe ai căror membri au atât certificările necesare, cât și experiență în domeniul securității cibernetice conform cerințelor din regulamentul BNR. În plus, exercițiile se desfășoară pe parcursul mai multor luni, aspect care necesită o planificare detaliată și o supraveghere constantă a fiecărei etape.