Caseta 9. Gestionarea riscurilor de natură cibernetică la adresa sistemelor de plăți

Riscurile cibernetice reprezintă provocări majore la adresa funcționării adecvate a economiilor contemporane, putând indisponibiliza infrastructurile critice din această perspectivă, din rândurile cărora fac parte și sistemele de plăți. În acest context, gestionarea adecvată a acestor riscuri a devenit o preocupare importantă a băncilor centrale.

În cadrul riscurilor operaționale, amenințările cibernetice au un profil tot mai proeminent, ca urmare a atacurilor recente de această natură asupra unor bănci centrale și instituții de credit, cu consecințe foarte grave în plan financiar, reputațional și al disponibilității serviciilor. Aceste atacuri s-au remarcat prin persistență și printr-un nivel foarte avansat de expertiză a inițiatorilor (actori statali și crimă organizată).

În aceste condiții, SWIFT a elaborat un set de recomandări detaliate adresate tuturor instituțiilor financiare conectate (SWIFT *Customer Security Controls Framework*). La rândul său, Banca Centrală Europeană a emis Ghidul *Cyber Resilience Oversight Expectations* (CROE), adresat funcției de monitorizare din cadrul băncilor centrale, și a elaborat o metodologie de testare efectivă a rezilienței cibernetice împotriva noilor amenințări sofisticate și persistente. Denumită *Threat Intelligence Based Ethical Red Teaming* (TIBER-EU), metodologia este adresată tuturor infrastructurilor pieței financiare din UE și participanților la acestea.

Aceste demersuri se înscriu pe linia promovării unui cadru de guvernanță adecvat promovării securității digitale și rezilienței cibernetice, esențial pentru a preveni amenințările de această natură sau pentru a face față cu succes unor astfel de incidente care se produc într-un mediu economic tot mai marcat de digitalizare și interconectare.

La nivelul Sistemului European al Băncilor Centrale se manifestă o preocupare constantă pentru consolidarea în continuare a capacității de reacție și de redresare în cazul unui atac cibernetic, prin perfecționarea planurilor de asigurare a continuității activității și prin testarea modalităților existente de gestionare a incidentelor și a crizelor. De asemenea, se acționează în mod consecvent pentru sporirea gradului de conștientizare cu privire la riscurile cibernetice.

Banca Națională a României acordă o importanță deosebită gestionării riscurilor cibernetice, atât din perspectiva de autoritate națională de monitorizare a sistemelor de plăți, cât și din cea de administrator și operator tehnic al sistemului de plăți ReGIS. În acest context, BNR s-a aliniat la recomandările SWIFT, a efectuat teste comprehensive ale rezilienței cibernetice pentru noua platformă tehnică de operare a ReGIS, a participat direct la procesul de elaborare a CROE și TIBER-EU și implementează cerințele standardului ISO 27001 privind managementul securității informației. Totodată, BNR a adoptat în activitatea de monitorizare Ghidul CROE și a recunoscut oficial cadrul TIBER-EU drept metodologie validă de testare a rezilienței cibernetice.