SISTEMELE SI SERVICIILE BANCARE ELECTRONICE DIN ROMANIA ÎN CONTEXTUL RĂZBOIULUI DINTRE UCRAINA ŞI FEDERAŢIA RUSĂ

ELECTRONIC BANKING SYSTEMS AND SERVICES IN ROMANIA IN THE CONTEXT OF THE WAR BETWEEN UKRAINE AND THE RUSSIAN FEDERATION

General de brigadă (r.) prof. univ. dr. Viorel BUŢA*
Dr. Răzvan MANOLIU**

***Rezumat**: Războiul declanşat de către Rusia împotriva Ucrainei a creat implicaţii majore privind afectarea securităţii şi stabilităţii în această ţară, dar şi în regiune şi, într-o anumită măsură, la nivel global. După încheierea Războiului Rece, conflictul ruso-ucrainean a condus la provocări diverse de naturi diferite şi anume: militare, politice, economice, financiare, juridice, informatice şi umanitare.*

***Cuvinte cheie**: conflict, Rusia, Ucraina, financiar.*

***Abstract**: The war launched by Russia against Ukraine has created major implications for affecting security and stability in that country, but also in the region and, to some extent, globally. After the end of the Cold War, the Russian-Ukrainian conflict led to various challenges of different natures, namely: military, political, economic, financial, legal, IT and humanitarian.*

***Keywords:** conflict, Russia, Ukraina, financial.*

Cu toate efectele negative, în actuala situaţie, arhitectura financiară europenă arată că sectorul bancar este rezilient, cu poziţii solide de capital şi lichiditate. Uniunea bancară a contribuit în mod semnificativ la această reziliență.

Sistemele şi serviciile bancare electronice din România au cunoscut o dezvoltare semnificativă în ultimii ani, cu impact pozitiv în economia ţării. Aceste sisteme si servicii au devenit extrem de importante pentru tranzacţiile comerciale şi pentru economia românească în general.

Totuşi, existenţa conflictelor şi tensiunilor învecinate, cum este şi războiul dintre Ucraina si Federaţia Rusa, a permis posibilitatea de a afecta acest sector financiar. În aceste circumstanţe, este important să analizăm situaţia actuală a sistemelor şi serviciilor bancare electronice din România şi să evaluăm impactul războiului dintre Ucraina şi Federaţia Rusa asupra

* membru titular al Academiei Oamenilor de Ştiinţă din România, email: vbuta49@yahoo.com.
** Unicredit Bank Romania, razvanmanoliu@gmail.com

acestora. Desigur că trebuie avute în vedere și tensiunile dintre Rusia și țările din NATO și Uniunea Europeană și nu numai.

Deși sunt luate importante măsuri, România este una dintre țările vulnerabile la atacurile cibernetice din partea Federației Ruse. Unul dintre cele mai expuse sectoare este cel bancar, care a devenit din ce în ce mai dependent de tehnologia informației și s-a digitalizat rapid în ultimii ani. În acest context, hackerii ruși au început să utilizeze tehnici avansate pentru a sparge sistemele de securitate ale băncilor din România. Acest articol are ca scop prezentarea unor aspecte privind atacurile cibernetice asupra băncilor din România, cu accent pe activitățile hackerilor ruși ca o consecință a poziției României față de războiul ruso-ucrainean.

Sistemul bancar, ca și multe alte sectoare, a devenit din ce în ce mai dependent de tehnologie. Digitalizarea operațiunilor bancare a condus la un risc crescut de atacuri cibernetice. Ca urmare a creșterii amenințării cu atacuri cibernetice, băncile au prioritizat măsurile de securitate cibernetică pentru a se proteja de aceste amenințări. România ocupă locul 38 în lume în ceea ce privește activele sistemului bancar, dar sistemul bancar din România rămâne vulnerabil la atacurile cibernetice, în special din partea Federației Ruse. Noi ne-am propus să explorăm în ce măsură sistemul bancar din România este vulnerabil la atacurile cibernetice din partea Rusiei intensificate în condițiile războiului din vecinătatea noastră.

Sistemul bancar din România este supervizat de Banca Națională a României (BNR) și este format din bănci comerciale, bănci de economii și cooperative de credit. Există aproximativ 30 de bănci care activează în România, din care primele 5 bănci dețin aproximativ 70% din cota de piață. Sistemul bancar românesc a suferit schimbări semnificative în ultimii ani, după o perioadă de consolidare și reforme în urma crizei financiare mondiale din 2008-2009.

Deși este considerat unul dintre cele mai dezvoltate și moderne din Europa, sistemul bancar din România rămâne vulnerabil la atacurile cibernetice. Hackerii ruși au demonstrat, în special în ultimul timp, că sunt capabili să atace băncile din România folosind o combinație de tehnici sofisticate, cum ar fi phishing-ul și atacurile ransomware.

Securitatea cibernetică este una dintre cele mai importante probleme ale prezentului, având în vedere faptul că tehnologia și internetul joacă un rol esențial în economia mondială și în societatea modernă. România, ca și alte țări, se confruntă cu amenințări cibernetice continue, care pot afecta atât sectorul public, cât și cel privat. Pentru a face față acestor amenințări, statul român a dezvoltat o strategie națională de securitate cibernetică pentru perioada 2019 - 2024, în care Asociația Română a Băncilor și TRANSFOND S.A. sunt două instituții fundamentale.

În ultimii ani, România a devenit unul dintre cei mai importanți parteneri ai NATO în ceea ce privește securitatea cibernetică. Centrul de Excelență NATO pentru securitatea cibernetică din România joacă un rol

vital în îmbunătățirea capacității României de a se apăra împotriva amenințărilor cibernetice și în consolidarea colaborării cu organizațiile partenere ale NATO și cu statele membre.

Sistemele și serviciile bancare electronice din România au cunoscut o dezvoltare semnificativă în ultimii ani, în principal datorită creșterii utilizării internetului și a telefoniei mobile. Această creștere a determinat bancile să îmbunătățească serviciile lor prin intermediul sistemelor și serviciilor bancare electronice. Astfel, clienții au acces la o gamă largă de servicii, inclusiv servicii bancare online, e-wallet-uri și aplicații mobile.

Serviciile bancare electronice oferă o serie de avantaje diferite pentru clienți. De exemplu, aceste servicii sunt disponibile 24/7, clienții pot verifica Balanța și tranzacționa online, fără a fi nevoie să viziteze banca, ceea ce economisește timp și bani. De asemenea, aceste servicii sunt sigure și convenabile, permițând clienților să facă tranzacții de orice dimensiune de oriunde din lume.Desigur aceste facilități pot atrage și unele vulnerabilități.

Federația Rusă este renumită pentru capacitățile sale cibernetice, fiind în măsură să efectueze atacuri sofisticate și coordonate. În ultimii ani, în mod deosebit pe timpul războiului ruso-ucrainean, hackerii ruși au început să ia în vizor băncile, din unele țări considerate "neprietenoase". În România, au executat atacuri cibernetice pentru a obține acces la informații sensibile și a bloca operațiunile bancare. Acești hackeri folosesc adesea tehnici avansate de inginerie socială pentru a sparge sistemele de securitate ale băncilor și a încerca să obțină acces la informații sensibile, cum ar fi datele clienților și informațiile financiare.

Federația Rusă a fost acuzată că a efectuat atacuri cibernetice împotriva unor țări din Europa spre exemplu Estonia și Ucraina dată fiind proximitatea celor două țări. România este, de asemenea, considerată a fi expusă riscului de atacuri cibernetice din partea Federației Ruse.

Au existat mai multe cazuri de atacuri cibernetice asupra băncilor care activează în România în ultimii ani. Un astfel de caz a fost în 2017, când Banca Națională a României a fost ținta unui atac de denegare distribuită a serviciului (DDoS). Atacul a dus la indisponibilitatea site-ului băncii timp de câteva ore. În 2020, Banca Transilvania, una dintre cele mai mari bănci din România, a declarat că a fost ținta unui atac ransomware. Deși banca a relatat că a reușit să limiteze atacul, a admis că datele clienților au fost compromise.

Din fericire, până în prezent, războiul dintre Ucraina și Federația Rusă nu a afectat direct sistemele și serviciile bancare electronice din România. Cu toate acestea, există unele probleme legate de riscurile geopolitice și de perspectiva unui conflict mai amplu care ar putea afecta stabilitatea financiară a regiunii.

În primul rând, situația politică instabilă din regiunea noastră poate afecta negativ încrederea clienților în instituțiile financiare și, prin urmare, în serviciile electronice bancare. Deoarece există probabilitatea de a afecta

economia și finanțele regiunii, clienții ar putea fi mai precauți în timp ce investesc sau fac plăți prin intermediul serviciilor bancare electronice.

În al doilea rând, războiul dintre Ucraina și Federația Rusă ar putea duce la măsuri restrictive și embargouri internaționale care ar afecta în mod negativ sectorul financiar. Aceste măsuri ar determina unele instituții financiare să își reducă expunerea către această regiune sau să-și restricționeze serviciile, dacă situația ar deveni din ce în ce mai tensionată.

Pe lângă riscurile geopolitice care îl afectează, sectorul financiar din România poate fi supus și altor amenințări cibernetice. În acest sens, autoritățile române și instituțiile financiare și-au întărit măsurile de securitate cibernetică pentru a proteja sistemele și serviciile bancare electronice.

Acest lucru a implicat consolidarea infrastructurilor digitale prin creșterea nivelului de securitate a serviciilor bancare electronice și a rețelelor de comunicare. În plus, au fost introduse măsuri suplimentare de autentificare a utilizatorilor și verificare a tranzacțiilor pentru a minimiza riscul de fraudă cibernetică.

Au existat mai multe atacuri cibernetice asupra băncilor din România în ultimii ani, iar majoritatea au fost atribuite hackerilor ruși. Singurul scop al acestor atacuri a fost de a obține informații și de a perturba operațiunile bancare. În câteva cazuri, hackerii au reușit să obțină acces la informații sensibile, cum ar fi conturile și parolele clienților, în timp ce în alte cazuri atacurile au fost limitate doar la indisponibilitatea temporară a site-urilor bancare. Mai mult, hackerii ruși au reușit să creeze software-uri malware foarte sofisticate pentru a încerca să spargă sistemele de securitate ale băncilor.

Sistemul bancar românesc a luat diverse măsuri pentru a se proteja împotriva atacurilor cibernetice. BNR a emis directive pentru bănci pentru a-și îmbunătăți postura de securitate cibernetică. Aceste directive includ cerințe pentru bănci de a avea politici și proceduri adecvate de securitate cibernetică, de a efectua evaluări regulate de securitate și de a îi instrui pe angajați în materie de securitate cibernetică. BNR solicită, de asemenea, băncilor să respecte Regulamentul general privind protecția datelor al Uniunii Europene (GDPR).

Băncile individuale care activează în România au investit, de asemenea, în măsuri de securitate cibernetică. De exemplu, Banca Transilvania are un program solid de securitate cibernetică . Banca a stabilit capacități de informații despre amenințări și a implementat un centru de operațiuni de securitate pentru a monitoriza și a răspunde la incidente de securitate. În plus, banca oferă formare permanentă în securitatea cibernetică pentru angajații săi.

Asociația Română a Băncilor (ARB) este una dintre cele mai importante organizații din sistemul bancar românesc, reprezentând interesele și nevoile băncilor membre. În lupta împotriva amenințărilor

cibernetice, ARB joacă un rol esențial prin furnizarea de consultanță și îndrumare pentru bănci, astfel încât acestea să poată să-și îmbunătățească sistemele de securitate cibernetică.

În cadrul strategiei naționale de securitate cibernetică, ARB este implicată în identificarea și evaluarea riscurilor cibernetice pentru bănci, dezvoltarea și implementarea de politici și măsuri de securitate cibernetică și îmbunătățirea cooperării cu autoritățile relevante pentru identificarea și prevenirea activităților ilegale.

TRANSFOND S.A. este o companie aflată în proprietate publică, care administrează sistemul național de plăți electronice din România. Ca o instituție fundamentală, TRANSFOND S.A. joacă un rol important în protejarea infrastructurii critice a sistemului de plăți electronice împotriva amenințărilor cibernetice.TRANSFOND S.A. este responsabilă pentru dezvoltarea și implementarea de politici și măsuri de securitate cibernetică pentru sistemul de plăți electronice din România. Aceste măsuri includ îmbunătățirea securității infrastructurii, detectarea și răspunsul adegvat la incidente de securitate cibernetică și îmbunătățirea pentru gestionarea de incidente.

În cadrul strategiei naționale de securitate cibernetică, colaborarea dintre ARB și TRANSFOND S.A. este esențială astfel încât să se poată proteja instituțiile financiare și infrastructura critică a sistemului de plăți electronice din România.

ARB are un rol important de consultanță pentru bănci, în timp ce TRANSFOND S.A. este responsabilă pentru securitatea infrastructurii critice a sistemului de plăți electronice. Colaborarea între cele două instituții este esențială pentru a îmbunătăți securitatea sistemului financiar și pentru a preveni atacurile cibernetice din ce în ce mai sofisticate.

ARB și TRANSFOND S.A. sunt două instituții cheie în strategia națională de securitate cibernetică, jucând un rol esențial în protejarea instituțiilor financiare și a infrastructurii critice a sistemului de plăți electronice. Împreună cu alte instituții și sectorul privat, acestea trebuie să continue să ia măsuri proactive pentru a identifica și preveni amenințările cibernetice și pentru a îmbunătăți securitatea cibernetică a României și în special a sectorului bancar.

Pe lângă ARB și TRANSFOND S.A., mai multe instituții sunt implicate în strategia națională de securitate cibernetică, cum ar fi Guvernul României, Ministerul Afacerilor Interne, Ministerul Apărării Naționale și Consiliul Național pentru Securitatea Cibernetică.

Aceste instituții au fiecare un rol important în abordarea amenințărilor cibernetice din România, prin evaluarea riscurilor, dezvoltarea și implementarea de politici și măsuri de securitate cibernetică și îmbunătățirea cooperării între sectoare.

Pentru a se proteja împotriva atacurilor cibernetice, băncile din România au început să ia măsuri, cum ar fi să investească în tehnologii de

securitate, politici și proceduri de securitate cibernetică îmbunătățite și procese mai stricte de verificare și autentificare a utilizatorilor. În plus, Banca Națională a României a emis directive stricte cu privire la securitatea cibernetică a băncilor, care trebuie respectate de către toate instituțiile financiare din țară. Lucrând împreună și luând măsuri proactive de securitate cibernetică, băncile din România au prevenit multe din atacurile cibernetice care au avut loc până acum și pot limita pierderile lor financiare și reputaționale.

Atacurile cibernetice din partea hackerilor ruși reprezintă o amenințare majoră pentru băncile din România. Aceste atacuri pot cauza pierderi semnificative de date și informații, precum și pierderi financiare importante. În ciuda acestor amenințări, băncile din România au început să ia măsuri proactive în materie de securitate cibernetică pentru a se proteja împotriva atacurilor. Este foarte important ca băncile din România să continue să îmbunătățească și să actualizeze sistemele lor de securitate și politici și să colaboreze cu autoritățile relevante pentru a identifica și a preveni posibilele amenințări cibernetice.

În timp ce sistemul bancar românesc este vulnerabil la atacurile cibernetice, există măsuri de protecție împotriva unor astfel de atacuri. Cu toate acestea, amenințarea de atacuri cibernetice din partea Federației Ruse rămâne, dar este esențial ca România să continue să acorde prioritate securității cibernetice pentru a se proteja sistemul bancar.

Centrul de Excelență NATO pentru securitatea cibernetică a fost înființat în anul 2010, ca parte a unui efort pentru a spori capacitatea NATO și a statelor membre în protecția infrastructurilor naționale și a altor sisteme critice împotriva amenințărilor cibernetice.

România a fost selecționată pentru a găzdui acest centru, datorită poziționării sale geografice strategice și a capacității sale de a dezvolta competențe avansate în domeniul tehnologiei informației și comunicațiilor.

Centrul de Excelență NATO pentru securitatea cibernetică are ca obiectiv îmbunătățirea capacității de apărare cibernetică a României și a altor țări partenere din cadrul NATO, prin cooperarea și colaborarea în domeniul securității cibernetice.

În realizarea obiectivului său, Centrul de Excelență NATO pentru securitatea cibernetică a dezvoltat o serie de proiecte și activități, care includ:

- Organizarea de cursuri de formare în domeniul securității cibernetice pentru personalul militar și civil din NATO și din statele partenere;
- Elaborarea și dezvoltarea de protocoale și proceduri în domeniul securității cibernetice;
- Participarea la exerciții de simulare a atacurilor cibernetice în cadrul NATO și la nivel național;

- Furnizarea de consultanță și sprijin tehnic în domeniul securității cibernetice pentru autoritățile naționale și pentru organizațiile din sectorul privat;
- Dezvoltarea de instrumente și tehnologii avansate de monitorizare și detectare a amenințărilor cibernetice.

Pe lângă activitățile proprii, Centrul de Excelență NATO pentru securitatea cibernetică colaborează strâns cu alte organizații NATO și cu statele membre, în scopul de a îmbunătăți sinergia și de a dezvolta capacități avansate în domeniul securității cibernetice. Exemple de astfel de colaborări includ:
- Participarea la proiecte și activități organizate de alte Centre de Excelență NATO, precum și de către Alianța Nord-Atlantică;
- Coordonarea activităților cu Centrele naționale de Excelență din statele membre NATO;
- Cooperarea cu organizațiile UE și cu statele care fac parte din aceasta, în ceea ce privește securitatea cibernetică;
- Furnizarea de sprijin și consultanță pentru autoritățile naționale și pentru organizațiile din sectorul privat din statele partenere.

Centrul de Excelență NATO pentru securitatea cibernetică a avut un impact semnificativ asupra capacității de apărare cibernetică a României, în special în ceea ce privește pregătirea și formarea specialiștilor în domeniu. În plus, Centrul de Excelență NATO pentru securitatea cibernetică a deschis noi oportunități pentru sectorul IT românesc pentru a se dezvolta și a-și extinde valoarea în ceea ce privește securitatea cibernetică.

Centrul de Excelență NATO pentru securitatea cibernetică din România este un parteneriat strategic vital pentru NATO și pentru statele membre, în ceea ce privește protejarea infrastructurii naționale și a altor sisteme critice împotriva amenințărilor cibernetice. Activitățile Centrului sunt esențiale pentru dezvoltarea de capacități avansate și pentru consolidarea colaborării între națiuni în domeniul securității cibernetice. Este important să se mențină și să se dezvolte această colaborare, pentru a proteja securitatea națională și a promova o lume digitală sigură și prosperă.

Ca urmare a războiului declanșat de Federația Rusă împotriva Ucrainei, Uniunea Europeană (UE) a adoptat printre altele și următoarele măsuri:

-a interzis **tranzacțiile** cu Banca Centrală a Rusiei;
-a interzis **accesul la SWIFT** pentru șapte bănci rusești;
-a interzis furnizarea de **bancnote euro** spre Rusia.

De asemenea și alte țări, din afara UE, au întreprins sancțiuni pe linia financiar-bancară. Spre exemplu Elveția, stat neutru, a înghețat activele oligarhilor ruși în valoare de 7,5 miliarde de franci elvețieni.

În concluzie, sistemele și serviciile bancare electronice din România au avut o dezvoltare semnificativă în ultimii ani, fiind esențiale pentru

economia țării și, în general, pentru realizarea tranzacțiilor comerciale. Cu toate acestea, există riscuri geopolitice care ar putea afecta stabilitatea financiară a regiunii, în special în contextul războiului dintre Ucraina și Federația Rusa.

Cu toate acestea, autoritățile financiare din România și instituțiile financiare au luat măsuri pentru a proteja sistemele și serviciile bancare electronice prin consolidarea infrastructurii și îmbunătățirea securității cibernetice. Astfel, România este pregătită să facă față amenințărilor sau riscurilor, pe măsură ce acestea apar.

BIBLIOGRAFIE

„Șase bănci din România, între care și cele mai mari, au fost ținta unui atac cibernetic din partea hackerilor ruși", disponibil la HotNews.ro, 6 mai 2021;

„Riscuri cibernetice pentru sectoarele financiare și bancare din România", disponibil la CERT-RO, 24 ianuarie 2018;

„Guvernul a adoptat strategia națională de securitate cibernetică 2019-2024", Ministerul Comunicațiilor și Societății Informaționale, 18 iunie 2019;

„Recomandări de securitate pentru serviciile bancare și financiare online", disponibil la CERT-RO, 30 ianuarie 2020;

„România în contextul securității cibernetice europene", Institutul de Studii Politice și Relații Internaționale, Universitatea din București, 2018;

„Sistemul bancar din România, vulnerabil la atacurile cibernetice", Bloomberg Businessweek România, 23 aprilie 2019;

„NATO lansează un centru de excelență pentru securitatea cibernetică la București", NATO, 18 septembrie 2018;

„Băncile românești, în alertă! Hackerii ruși au atacat sistemele informatice ale mai multor instituții financiare din România", Antena 3, 6 mai 2021;

„Securitatea cibernetică, o prioritate pentru BNR", Banca Națională a României, 17 octombrie 2019;

„Băncile trebuie să-și protejeze clienții și să ia măsuri de securitate cibernetică", disponibil la Wall-Street.ro, 19 ianuarie 2021.