Cybersecurity
noi cerinte pentru sistemul financiar bancar

Rodica Tuchilă, Director
Asociația Română a Băncilor

CONFERINȚA NAȚIONALĂ DE CYBERSECURITY
14 iunie 2016

Contextul național și european

- Evoluția rapidă a tehnologiei schimbă în mod structural industria serviciilor financiar-bancare
- Au apărut schimbări importante în comportamentul si cerințele consumatorilor de servicii financiar bancare
- Noi oportunități pentru serviciile financiar bancare: servicii prin Internet și mobil, prin rețele sociale, mandate electronice de debitare directă, factura electronică, etc.
- Crearea pieței unice a serviciilor financiar bancare, accesul tuturor cetățenilor la servicii bancare în condiții de siguranță și transparență
- Încurajarea plăților electronice și a serviciilor inițiate și procesate prin canale digitale
- Cerințe complexe de asigurare a securității și de administrare a riscurilor

Inițiative și reglementări

La nivel european

- Strategia de securitate cibernetică a Uniunii Europene – pentru un spațiu cibernetic deschis, sigur și securizat
- Propunere de Directivă privind măsuri de asigurare a unui nivel ridicat de securitate a rețelelor și a informației în UE - 2013/0027
- Recomandările Băncii Centrale Europene și Ghidul Autorității Bancare Europene (EBA) privind securitatea plăților prin Internet
- Directiva revizuita (UE) 2015/2366 privind serviciile de plată în cadrul pieței interne – PSD2

La nivel național

- Proiectul Legii privind securitatea cibernetică

Directiva (UE) 2015/2366

- Payments Services Directive revizuită – PSD2, aplicabilă din luna ianuarie 2018
- Element de noutate: accesul la contul bancar al Third-Party-Provider (TPP) – furnizori din afara sistemului bancar
- Competiție și cooperare între sistemul bancar și alți furnizori – co-opetiție=competiție colaborativă
- Cerințe suplimentare pentru asigurarea securității și confidențialității informațiilor personale și financiare ale clienților
- Autoritatea Bancară Europeană (EBA) și Banca Centrală Europeană (ECB) elaborează standarde tehnice de reglementare (RTS) privind cerințe de autentificare a clienților și comunicatii securizate - termen de publicare ianuarie 2017

Recomandări privind securitatea plăților prin Internet

- Documentul Băncii Centrale Europene *„Recommendations for the security of Internet payments”* se adresează tuturor furnizorilor de servicii de plăți, precum şi autorităților care asigură guvernanța Schemelor de plăți - Scheme de carduri, Scheme de transfer credit, Scheme de debitare directă - din statele membre ale Comunității Europene

- „Ghidul privind securitatea plăților pe Internet” emis de Autoritatea Bancară Europeană stabileşte un set de cerințe minime în domeniul securității plăților pe Internet, bazându-se pe prevederile Directivei 64/2007/CE referitoare la cerințele de informare pentru serviciile de plată și obligațiile prestatorilor de servicii de plată (PSP) în legătură cu prestarea serviciilor de plată

Recomandări privind securitatea plăților prin Internet - obiective

Definește cerințele minime comune pentru serviciile de plăți prin Internet – indiferent de dispozitivul de acces utilizat:

- carduri – execuția plăților cu carduri prin Internet, inclusiv plăți virtuale, exemplu: înregistrarea datelor de plata cu cardul pentru a fi utilizate în soluțiile de tip portofel electronic
- transfer credit – execuția transferurilor credit prin Internet
- e-mandate – emiterea si modificarea mandatelor electronice de debitare directa
- e-money – transferul banilor electronici intre doua conturi e-money prin Internet

Principii de bază (1)

1. Realizarea de **evaluări specifice de riscuri asociate cu furnizarea de servicii prin Internet** - actualizate conform evoluției amenințărilor și mecanismelor de frauda si realizate la intervale regulate de timp

2. Inițierea plăților și accesul la datele sensibile trebuie protejate prin **mecanisme puternice de autentificare a clienților**:

   i) ceva ce doar clientul cunoaște – parola statică, cod, număr personal de identificare

   ii) ceva ce doar clientul are - token, smart card, telefon mobil

   iii) ceva ce doar clientul este – caracteristici biometrice

Principii de bază (2)

3. Implementarea de **procese efective pentru autorizarea tranzacţiilor, monitorizarea tranzacţiilor şi sistemelor, pentru identificarea comportamentelor anormale şi prevenirea fraudelor**

4. Organizarea de **programe de conştientizare şi educare a clienţilor privind problemele de securitate**, astfel încât aceştia sa utilizeze serviciile de plăți prin Internet sigur și eficient

Preocupări

- Crearea unor practici comune la nivelul industriei bancare
- Dialog si colaborare cu specialiști ai instituțiilor cu responsabilități și atribuții în domeniul securității informatice
- Preocupări pentru a contribui la completarea cadrului legislativ în domeniu și pentru crearea unui sistem de tip CERT la nivelul sistemului bancar
- Informarea clienților sistemului bancar, referitor la tipologiile de fraude cele mai des întâlnite
- www.educatiefinanciara.info - informații de bază pentru prevenirea celor mai întâlnite metode de fraudă (Skimming, Phishing, Malware, inginerie socială, etc).