



Asociația Națională pentru
Securitatea Sistemelor Informatice



Asociația Națională
pentru
Securitatea
Sistemelor Informatice

Studiul pieței plăților electronice

2013

Cuprins

1. Introducere	3
2. Structura pieței plăților electronice	4
2.1 Evoluții la nivel național	4
2.2 Evoluții la nivelul UE	7
2.3 Piața digitală. Utilizarea internetului în UE: impact, tendințe, preocupări.....	9
3. Inițiative și cadrul de reglementare a pieței plăților electronice.....	14
3.1 Dezvoltarea pieței.....	14
3.2 Cadrul de reglementare la nivel național și european	16
3.3 Recomandări.....	26
3.3.1 Strategii de adresare a riscurilor	26
3.3.2 Recomandări BCE.....	28
3.3.3 Asigurarea securității aplicațiilor de plăți prin intermediul dispozitivelor mobile	29
4. Perspective ale pieței plăților electronice	30
Anexa 1: Tipuri de atacuri informatice asupra dispozitivelor mobile	32
1.1 Dispozitivele mobile.....	33
1.1.1 Atacuri asupra Browser-ului.....	33
1.1.2 Atacuri bazate pe telefon/SMS.....	33
1.1.3 Atacuri asupra aplicațiilor	34
1.1.4 Atacuri asupra sistemului de operare.....	35
1.2 Rețeaua de comunicații	35
1.3 Centrul de Date.....	36
1.3.1 Atacuri asupra serverelor Web.....	36
1.3.2. Atacuri asupra bazelor de date	37
Anexa 2: Statistici plăți	38
2.1 Statistici la nivel național	38
Indicatori privind cardurile și numărul de terminale	39
2.2 Statistici plăți la nivel european	43
Anexa 3: Principalele metode de plată per țară pentru cumpărături online la nivel european.....	46
Anexa 4: Referințe	48

1. Introducere

Acest studiu are în vedere prezentarea pieței plăților electronice în România, la nivel național și în contextul mai larg, european. Evoluția pieței se desprinde din diferitele statistici ai mai multor indicatori din date adunate pe ultimii 5-7 ani.

Pentru a face posibilă determinarea evoluției pieței plăților electronice, e necesară studierea factorilor care țin de adoptarea plăților electronice la nivelul utilizatorilor finali, preocuparea manifestată la utilizare și impactul amenințărilor la adresa acesteia.

Sistemele de plăți electronice joacă un rol din ce în ce mai important în economia modernă, cele mai multe activități economice având nevoie de un sistem de plată și bazându-se pe acestea. Atributele unui sistem de plată în termeni de nivel de acceptare, securitate și cost influențează sănătatea și eficiența unei economii.

Analizele la nivel european arată un cost semnificativ aferent plăților tradiționale (non-electronice), justificând eforturile care ar trebui întreprinse pentru a facilita creșterea în volum a pieței plăților electronice.

Deși Europa este considerată un leader global în adoptarea plăților cu cardul de exemplu, există diferențe foarte mari între țări în ceea ce privește rata de adoptare în rândul populației. Pentru a progresa e necesară o atitudine propice adoptării de măsuri de stimulare a tranziției către plățile electronice la nivelul guvernelor naționale. Și totodată de a asculta și a răspunde dorințelor și așteptărilor consumatorului, pentru a-l educa și atrage către un mijloc modern de plată.

2. Structura pieței plăților electronice

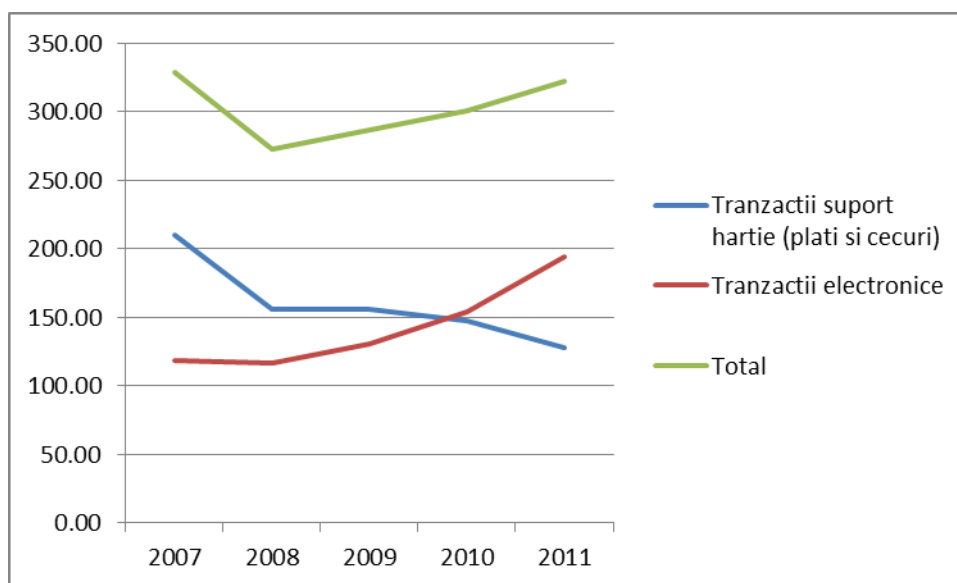
2.1 Evoluții la nivel național

Evoluția plăților electronice raportate la numărul de tranzacții în perioada 2007-2011:

Număr de tranzacții (milioane)	2007	2008	2009	2010	2011
Plăți	258.28	179.09	187.40	185.79	181.38
Plăți suport hârtie	198.78	145.29	146.49	136.38	121.55
Plăți electronice	59.50	33.81	40.91	49.41	59.83
Debite Directe	10.22	6.71	3.60	1.67	3.87
Tranzacții cu carduri	48.47	75.61	86.29	102.52	130.38
CEC-uri	11.43	10.75	9.01	10.79	6.57
Alte instrumente de plată	0.10	0.02	0.01	0.01	0.01
Total general	328.5	272.18	286.31	300.79	322.20

Sursa: ECB Payment Statistics 04.09.2012

Graficul evoluției numărului de tranzacții electronice, pe hârtie și per total:

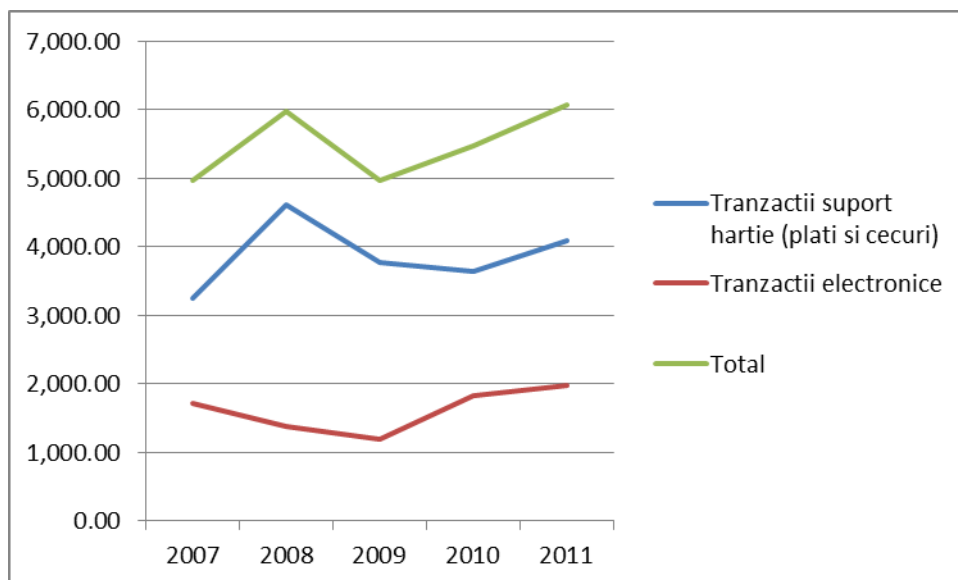


Evoluția plăților electronice raportate la valoarea tranzacțiilor, pe aceeași perioadă:

Valoarea tranzacțiilor (în miliarde RON)	2007	2008	2009	2010	2011
Plăți	4,870.86	5,873.56	4,879.28	5,349.35	5,965.56
Plăți suport hârtie	3,169.90	4,521.23	3,712.44	3,546.40	4,018.15
Plăți electronice	1,700.97	1,352.34	1,166.84	1,802.95	1,947.41
Debite directe	1.27	2.39	3.70	3.42	5.39
Tranzacții cu carduri	8.29	14.36	14.13	16.28	20.43
CEC-uri	75.78	90.46	61.01	91.19	68.13
Alte instrumente de plată	1.62	2.24	0.94	1.70	0.49
Total general	4,957.82	5,983.01	4,959.06	5,461.94	6,060.00

Sursa: ECB Payment Statistics 04.09.2012

Grafic plăți electronice raportate la valoarea tranzacțiilor:

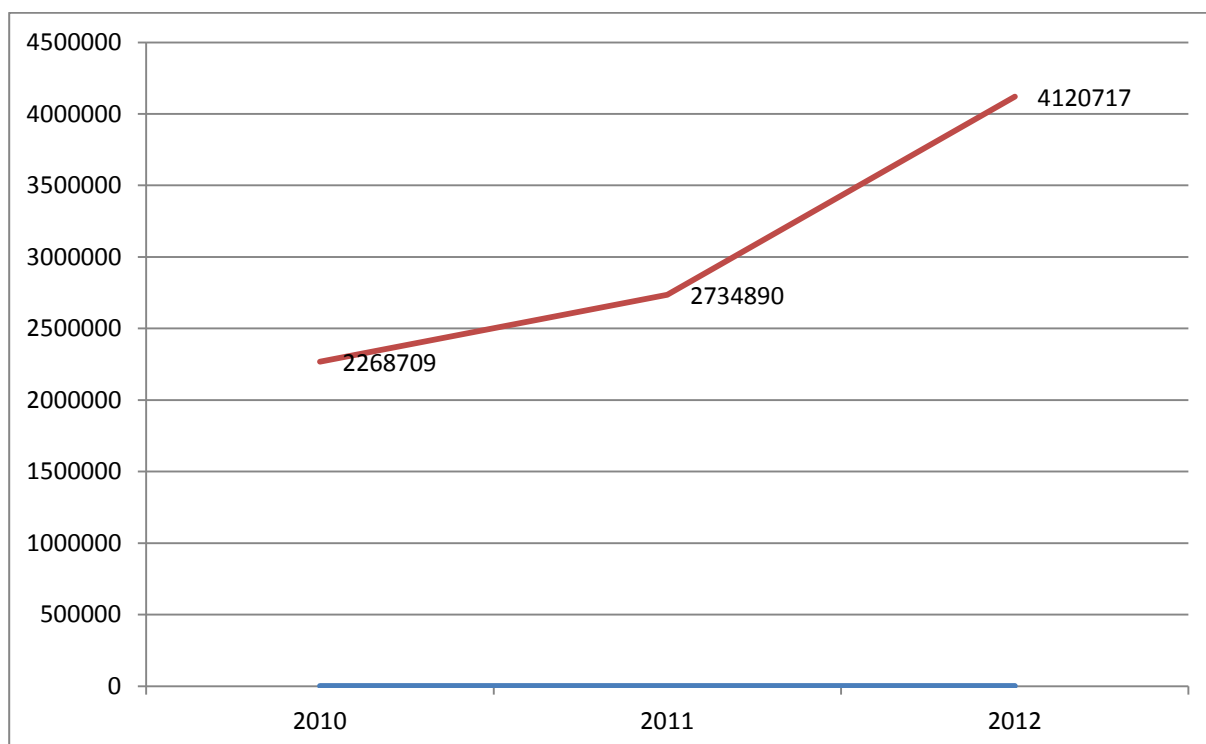


Tranzacții ecommerce procesate de Romcard pentru 9 banci din total 11 banci între 2010-2012:

Anul	Număr tranzacții
2010	2,268,709
2011	2,734,890
2012	4,120,717

Sursa: Romcard

Evoluția tranzacțiilor e-commerce procesate de Romcard pentru 9 banci din total 11:

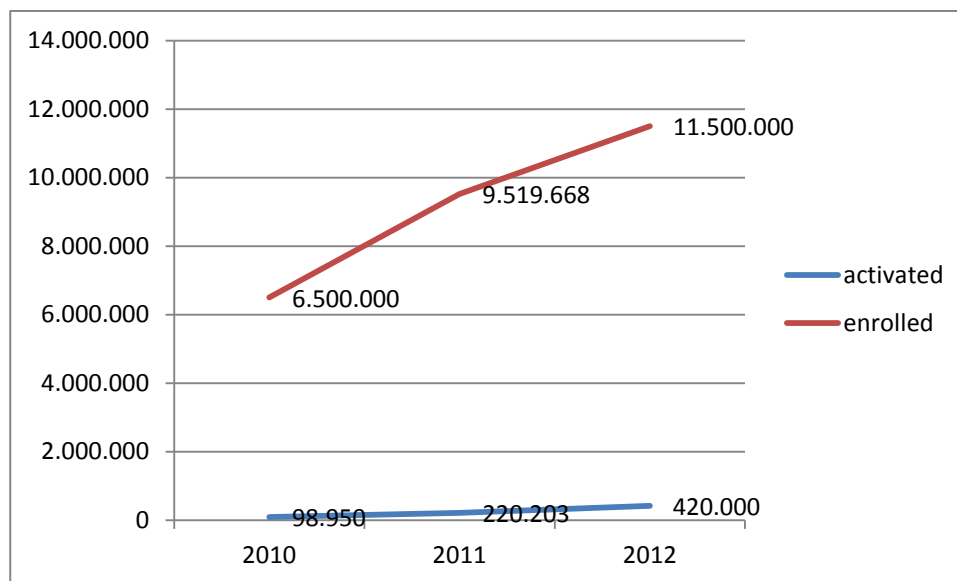


Înrolarea deținătorilor de card în 3DSecure pentru băncile care sunt înrolate în 3DSecure în România (16):

Anul	Carduri activate	Carduri înrolate
2010	98,850	6,500,000
2011	220,203	9,519,668
2012	420,000	11,500,000

Sursa: Romcard

Graficul cu cardurile activate și înrolate în sistemul 3DSecure:



Statistică plăți - Indicatori privind cardurile și numărul de terminale (ATM și POS):

Data	Numărul de carduri emise (inclusiv co-branded și cu funcție de monedă electronică)	Numărul de carduri active (inclusiv co-branded și cu funcție de monedă electronică)	Numărul de ATM existente în țară	Numărul de POS existente în țară	Număr tranzacții de plată cu carduri cu funcție de debit	Număr tranzacții de plată cu carduri cu funcție de debit amanat	Număr tranzacții de plată cu carduri cu funcție de credit
	(unități)	(unități)	(unități)	(unități)	(milioane)	(milioane)	(milioane)
sep. 2012	38.428.169	10.825.307	10.911	125.104	33,46	0,11	7,16
iun. 2012	37.340.006	10.813.509	10.918	123.524	31,47	0,12	6,69
mar. 2012	36.398.213	10.726.281	10.941	122.367	29,44	0,12	5,94
dec. 2011	35.422.029	10.771.042	11.006	124.920	29,31	0,13	6,06
sep. 2011	34.222.327	10.565.662	10.866	123.056	27,52	0,12	5,82
iun. 2011	33.110.220	10.332.299	10.756	120.480	26,31	0,13	5,48
mar. 2011	31.830.447	10.784.964	10.440	115.652	24,31	0,12	5,08
dec. 2010	30.197.848	11.200.867	10.102	107.052	23,81	0,09	4,56
sep. 2010	29.180.019	11.063.229	10.053	103.937	21,98	0,09	4,26
iun. 2010	28.382.843	11.469.807	9.954	101.902	20,77	0,08	3,91

mar. 2010	27.397.927	11.415.451	9.824	99.065	19,34	0,08	3,56
dec. 2009	25.272.697	11.536.052	9.702	98.522	18,94	0,06	4,22
sep. 2009	24.668.255	11.458.510	9.685	96.434	17,81	0,05	4,22
iun. 2009	24.076.767	11.369.278	9.553	98.879	16,97	0,05	4,13
mar. 2009	23.550.058	10.954.430	9.356	94.862	15,95	0,05	3,85
dec. 2008	22.851.795	11.075.764	9.246	90.498	16,33	0,15	4,99
sep. 2008	21.798.303	10.916.452	8.780	84.248	15,38	0,15	4,24
iun. 2008	20.181.404	10.929.270	8.307	80.160	13,55	0,15	3,95
mar. 2008	18.930.445	8.116.776	7.936	80.068	12,36	0,14	4,20

Sursa: Banca Națională a României

2.2 Evoluții la nivelul UE

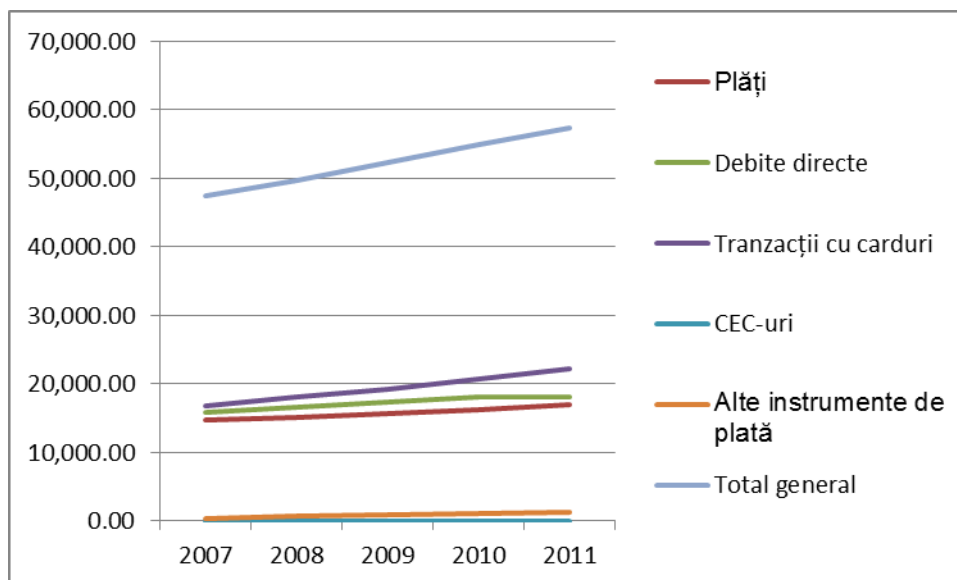
Se așteaptă ca în 2014, mai mult de 40% din europeni să folosească servicii de online banking. Tendințele de creștere în privința folosirii online banking-ului au fost în cea mai mare parte consecvente în Europa, în ultimii câțiva ani, excepții notabile fiind Franța unde adoptarea online banking-ului a crescut cu 11% în 2010 și Marea Britanie unde rata de adoptare a rămas aceeași. Țările nordice conduc în această privință. Consumatorii din Europa de nord – din Islanda până în Estonia – sunt foarte avansați în privința adoptării online banking-lui datorită unei combinații de bunăstare și entuziasm pentru tehnologie. Mobile banking-ul este de asemenea în creștere. Folosirea mobile banking-lui a crescut în Germania și datorită disponibilității telefoanelor inteligente, planurilor tarifare pentru traficul de date și noilor aplicații bancare.

Structura plăților în zona EURO în perioada 2007-2011:

Total tranzacții în Zona EURO (milioane)	2007	2008	2009	2010	2011
Plăți	14,675.99	15,024.58	15,684.61	16,282.00	16,932.79
Debite directe	15,896.78	16,562.89	17,425.11	18,055.91	18,105.08
Tranzacții cu carduri	16,800.29	18,103.18	19,158.74	20,624.60	22,195.31
CEC-uri	8.80	8.01	7.15	6.43	5.83
Alte instrumente de plată	427.97	751.4	857.21	1,025.19	1,266.19
Total general	47,382.89	49,699.61	52,276.38	54,969.61	57,239.70

Sursa: ECB Payment Statistics 04.09.2012

Evoluția tranzacțiilor în zona EURO:

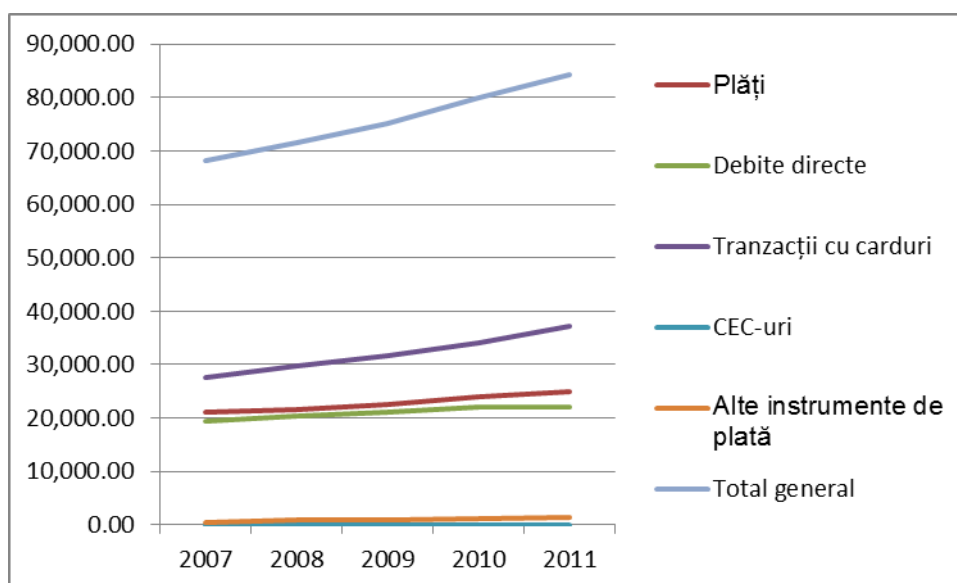


Structura plăților în Uniunea Europeană în perioada 2007-2011:

Total tranzactii UE (milioane)	2007	2008	2009	2010	2011
Plăți	21,176.75	21,659.82	22,428.06	23,857.57	24,897.58
Debite directe	19,469.12	20,255.04	21,124.30	22,019.59	22,166.42
Tranzacții cu carduri	27,483.62	29,717.63	31,657.30	34,178.21	37,154.62
CEC-uri	8.41	7.46	6.64	5.78	5.11
Alte instrumente de plată	488.59	836.93	915.41	1,091.47	1,291.07
Total general	68,138.62	71,640.64	75,216.86	80,061.63	84,224.22

Sursa: ECB Payment Statistics 04.09.2012

Evoluția tranzacțiilor în UE:



Preferințele de plată variază destul de mult în țările din Europa. În Anexa 3 sunt prezentate principalele metode de plată per țară pentru cumpărături online.

2.3 Piața digitală. Utilizarea internetului în UE: impact, tendințe, preocupări

Prin finalizarea Pieței Digitale Unitare, Europa și-ar putea crește PIB-ul cu aproape 500 mld. Euro anual o medie de 1000 Euro per persoană. Este nevoie ca cetățenii să capete încredere în noile tehnologii, inclusiv cele de plăți online, cloud computing, comunicare de tipul machine-to-machine. Un studiu din 2012 al Eurobarometrului (SPECIAL EUROBAROMETER 390 "Cyber security") arată că aproape o treime dintre europeni nu au încredere în abilitatea lor de a folosi internetul pentru tranzacții bancare sau cumpărături. Majoritatea celor intervievați a declarat că evită să-și dea datele personale pe internet, aspectul securității datelor fiind principalul motiv. În UE, mai mult de 1 din 10 utilizatori a fost victima fraudelor informatice.

Impact, tendințe

Mai mult de jumătate din cetățenii UE accesează internetul cel puțin o dată pe zi (53%), deși o minoritate substanțială (29%) spun că nu au acces la internet. Aproape toți utilizatorii de internet (95%), accesează internetul de acasă, în timp ce 39% accesează internetul la locul de muncă, 16% atunci când sunt în mișcare și 11%, la școală sau universitate.

În timp ce proporția de accesare a internetului de pe un computer desktop (63%) ori un laptop computer sau netbook (61%), 24% dintre utilizatorii de internet accesează internetul prin intermediul unui smartphone, și 6 % utilizează un computer tabletă sau touchscreen.

Aproximativ jumătate dintre utilizatorii de Internet din UE afirmă că achiziționează bunuri sau servicii online (53%), utilizează site-uri de rețele sociale (52%), sau fac online banking (48%), în timp ce 20% vând bunuri sau servicii. Există o variație considerabilă în activitățile online, în care respondenții se angajează în diferite țări.

29% din utilizatorii de internet din întreaga UE nu sunt siguri cu privire la capacitatea lor de a utiliza internetul pentru lucruri cum ar fi online banking sau cumpararea de lucruri on-line. 69% spun că sunt destul de sau foarte încrezători.

Preocupări

La utilizarea internetului pentru online banking sau cumpărături, două motive de îngrijorare frecvente sunt atribuirea sau abuzul de date cu caracter personal (menționat de 40% dintre utilizatorii de internet din UE) și securitatea plăților online (38%).

Utilizatorii de Internet și-au schimbat comportamentul, din cauza problemelor de securitate. 37% spun că probabilitatea ca să ofere informații personale pe site-uri e scăzută, în timp ce 43% nu deschid e-mailuri de la oameni care nu-i cunosc. 51% au instalat software anti-virus. Cu toate acestea, mai mult de jumătate (53%) dintre utilizatorii de internet din UE nu au schimbat nici parolele lor on-line pe parcursul anului trecut.

Majoritatea cetățenilor UE spun că au văzut sau auzit ceva despre criminalitatea informatică în ultimele 12 luni (73%), iar acest lucru este cel mai probabil să fi fost de la televizor (59%). Majoritatea cetățenilor UE nu se simt foarte sau deloc bine informați cu privire la riscurile de criminalitate informatică (59%), în timp ce 38% spun că sunt foarte sau destul de bine informați. Există o legătură clară între a fi bine informat și senzația de încredere on-line. Mai mult de jumătate din cei care se simt încredere în capacitatea lor de a face online banking sau cumpararea de lucruri on-line afirmă că se simt bine informați cu privire la criminalitatea informatică (59%).

12% din utilizatorii de internet din întreaga UE au experimentat fraudă online, iar 8% au experimentat furt de identitate. 13% nu au fost în stare să acceseze serviciile online, din cauza atacurilor cibernetice. În plus:

- Mai mult de o treime (38%) spun că au primit un email de escrocherie, inclusiv 10% care spun ca acest lucru este ceva ce li s-a întâmplat de multe ori;
- 15% din utilizatorii de internet spun că au întâlnit accidental materiale care promovează ura rasială sau extremism religios.

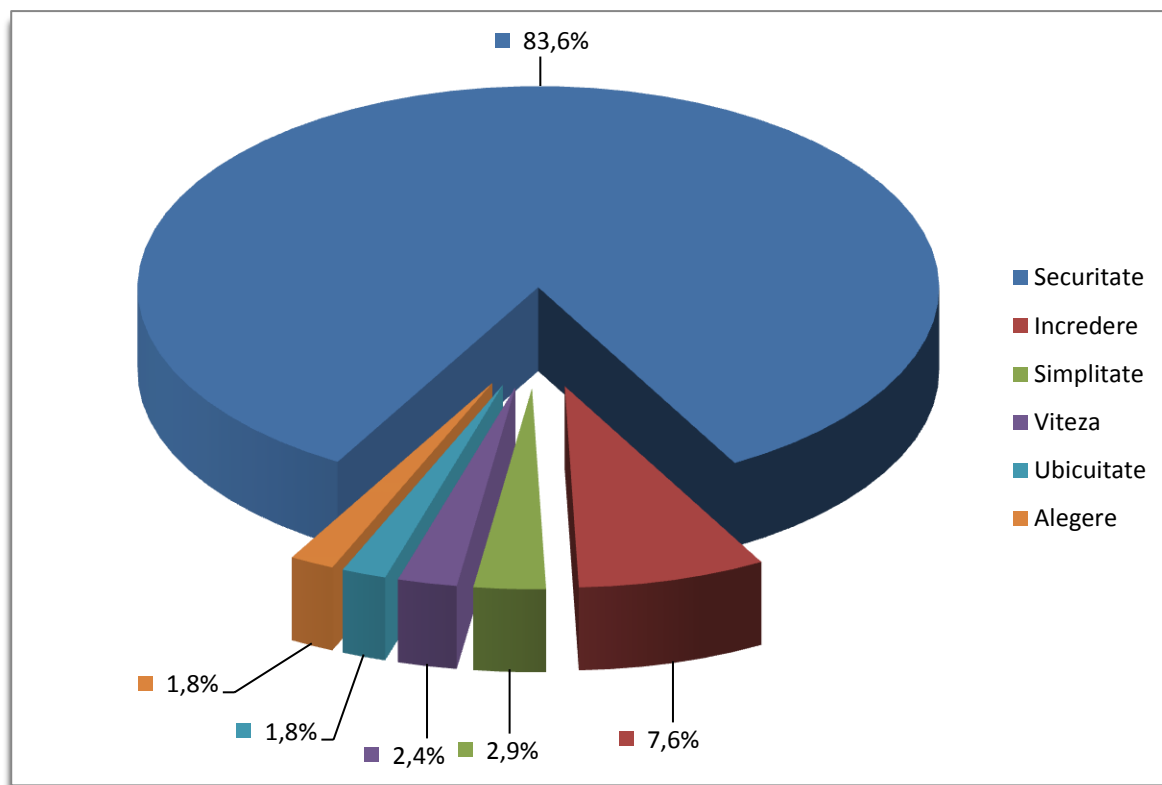
Utilizatorii de Internet Express niveluri ridicate de îngrijorare cu privire la securitatea cibernetică:

- 89% sunt de acord că evita dezvăluirea informațiilor cu caracter personal on-line;
- 74% sunt de acord că riscul de a deveni o victimă a criminalității cibernetice a crescut în ultimul an;
- 72% sunt de acord că sunt îngrijorati de faptul că informațiile personale online nu sunt păstrate în siguranță de către site-uri web;
- 66% sunt de acord că sunt îngrijorati de faptul că informațiile nu sunt păstrate în siguranță de către autoritățile publice.

Majoritatea utilizatorilor internetului în UE (61%) sunt îngrijorați de confruntări cu furtul de identitate. Aproximativ jumătate dintre utilizatorii internetului sunt preocupați de descoperirea accidentală a pornografiei infantile on-line (51%); fraudă on-line (49%) și email-uri frauduloase (48%). În plus, 43% sunt preocupați ca nu vor putea de a accesa servicii on-line din cauza atacurilor cibernetice, iar 41% sunt îngrijorați cu privire la confruntările accidentale cu materiale care promovează ura rasială sau extremismul religios.

Preocupări privind utilizarea comerțului on-line:

Securitatea este cel mai important aspect pentru cumpărători on-line		
Securitate	83.6%	Detaliile cardului și informațiile personale sunt complet sigure
Incredere	7.6%	Procesul de plată va lucra și problemele vor fi rezolvate
Simplitate	2.9%	Procesul de verificare este ușor de utilizat și durează doar câteva click-uri pentru a finaliza tranzacția
Viteza	2.4%	Posibilitatea efectuării rapide a tranzacției
Ubicuitate	1.8%	Utilizarea metodei preferate de plată pe mai multe site-uri
Alegere	1.8%	Site-ul oferă o alegere bună pentru opțiunile de plată



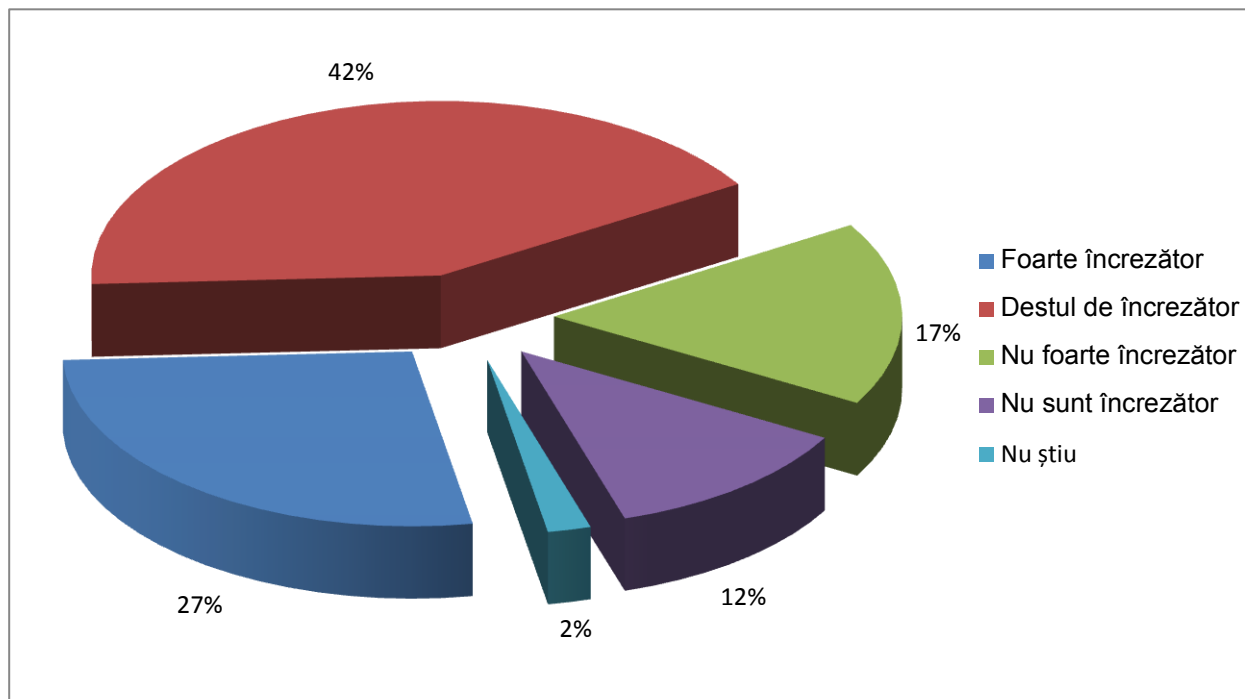
Sursa: Visa Europe

Nivelul de încredere privind tranzacțiile în mediul Internet

În cele ce urmează este prezentat nivelul de încredere a utilizatorilor de internet în utilizarea internetului pentru online banking sau la cumpararea de lucruri on-line, fiind evidențiate preocupările pe care utilizatorii de internet au cu privire la aceste activități și dacă au schimbat comportamentul lor pe internet, ca urmare a anumitor preocupări.

Majoritatea utilizatorilor de internet din întreaga UE (69%) spun că aceștia sunt cel puțin destul de încrezători cu privire la capacitatea lor de a folosi internetul pentru lucruri cum ar fi online banking sau a cumpara lucruri on-line, inclusiv 27% care spun că sunt foarte încrezători. Cu toate acestea, 17% nu sunt foarte încrezători și 12% nu sunt deloc încrezători.

Cât de încrezător sunteți despre capacitatea dumneavoastră de a utiliza Internetul pentru online banking sau cumparaturi on-line?



Sursa: SPECIAL EUROBAROMETER 390 "Cyber security"

Există variații considerabile în funcție de țară, în nivelul de încredere pe care respondenții au în utilizarea internetului pentru lucruri cum ar fi online banking sau cumpararea de lucruri on-line. Aceste variații au tendința de a reflecta nivelul de utilizare efectivă a internetului pentru aceste activități, astfel cum sunt descrise în secțiunea anterioară.

Respondenții din Suedia (91%), Danemarca (90%), Finlanda (88%) și Țările de Jos (86%) sunt cel mai probabil să spun că sunt siguri fac online banking sau cumpararea de lucruri on-line. Danemarca și Suedia arată, de asemenea proporții mari, care sunt foarte încrezători (62% și respectiv 56%). Cele mai scăzute niveluri de încredere sunt observate la Grecia (37%), Bulgaria (38%) și Portugalia (42%).

Încrederea în utilizarea internetului pentru lucruri cum ar fi online banking sau cumpararea de lucruri on-line este mai mare în rândul respondenților care au terminat studiile la vârsta de 20 de ani sau mai mult (78%), decât cei care au terminat studiile cu vârste cuprinse între 16 și 19 (64%) sau terminat de vârsta de 15 ani sau sub (49%). Încrederea este, de asemenea, mai mare în rândul studenților și cele din muncă, în special manageri (85%), decât cei care nu sunt de lucru. Utilizatorii de internet mai în vârstă (55 de ani sau peste) sunt oarecum mai puțin încrezători că respondenții tineri (60% sunt siguri și 38% nu încredere).

În plus, utilizatorii frecvențuale internetului (cei care îl folosesc în fiecare zi) sunt mult mai încrezători decât utilizatorii mai puțin frecvenți (76%, comparativ cu 41%), și în mod similar celor care folosesc dispozitive mai mici, cum ar fi un telefon inteligent (85%) sunt, de asemenea, mai încrezători decât cei care au acces numai la internet de la un computer desktop sau laptop.

Cât de încrezător sunteți despre capacitatea dumneavoastră de a utiliza Internetul pentru online banking sau cumparaturi on-line?

	Total încrezător	Total neîncrezător	Nu știu
UE	69%	29%	2%
Vârsta			
15-24	71%	25%	4%
25-39	74%	24%	2%
40-54	67%	31%	2%
55 +	60%	38%	2%
Educație			
15-	49%	48%	3%
16-19	64%	33%	3%
20*	78%	21%	1%
Studenti	74%	21%	5%
Ocupația respondentului			
PFA	72%	27%	1%
Manageri	85%	14%	1%
Funcționari	72%	27%	1%
Muncitori	65%	32%	3%
Casnici	57%	40%	3%
Șomeri	58%	39%	3%
Pensionari	59%	38%	3%
Studenti	74%	21%	5%
Utilizează Internetul			
Zilnic	76%	22%	2%
Ocazional	41%	55%	4%
Cu ce echipament accesează Internetul			
Calculatoare	69%	29%	2%
Tablete/Telefoane mobile	85%	14%	1%

Sursa: SPECIAL EUROBAROMETER 390 "Cyber security"

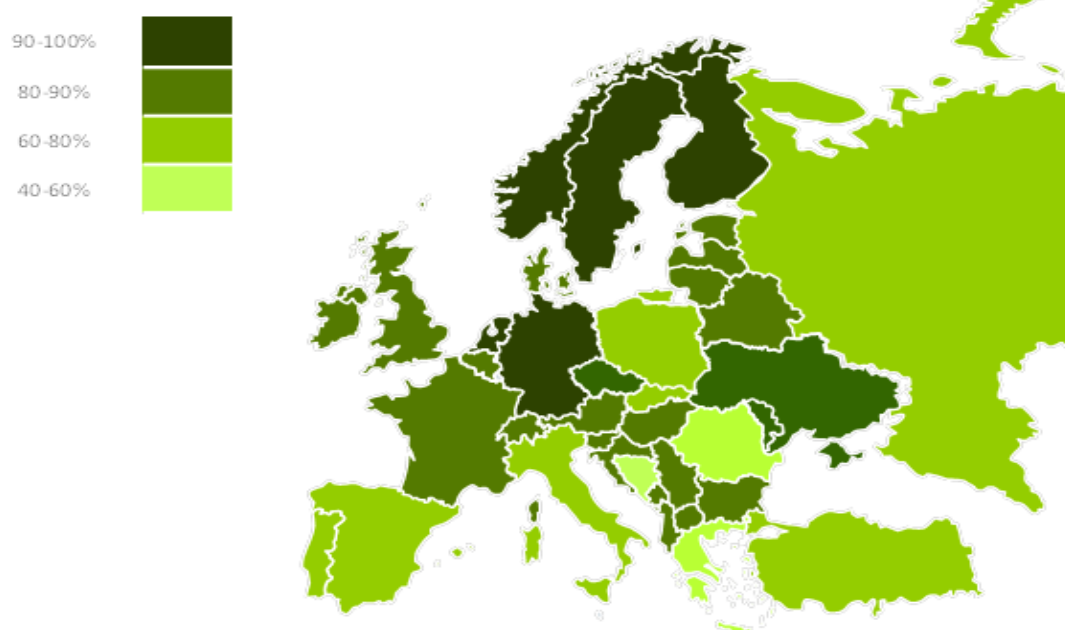
3. Inițiative și cadrul de reglementare a pieței plăților electronice

3.1 Dezvoltarea pieței

Piața e-commerce

În general, europenii sunt printre utilizatorii cei mai entuziaști ai internetului. În martie 2011, numărul total de utilizatori de internet din Europa a ajuns la numai 476.3 milioane, comparativ cu 1.63 miliarde utilizatori din întreaga lume. Mai mult decât atât, până în 2014, este de așteptat ca populația europeană on-line să crească cu aproape 20%, cu țări precum Polonia, Rusia, Ucraina și Turcia, ca principalii promotori pentru această creștere.

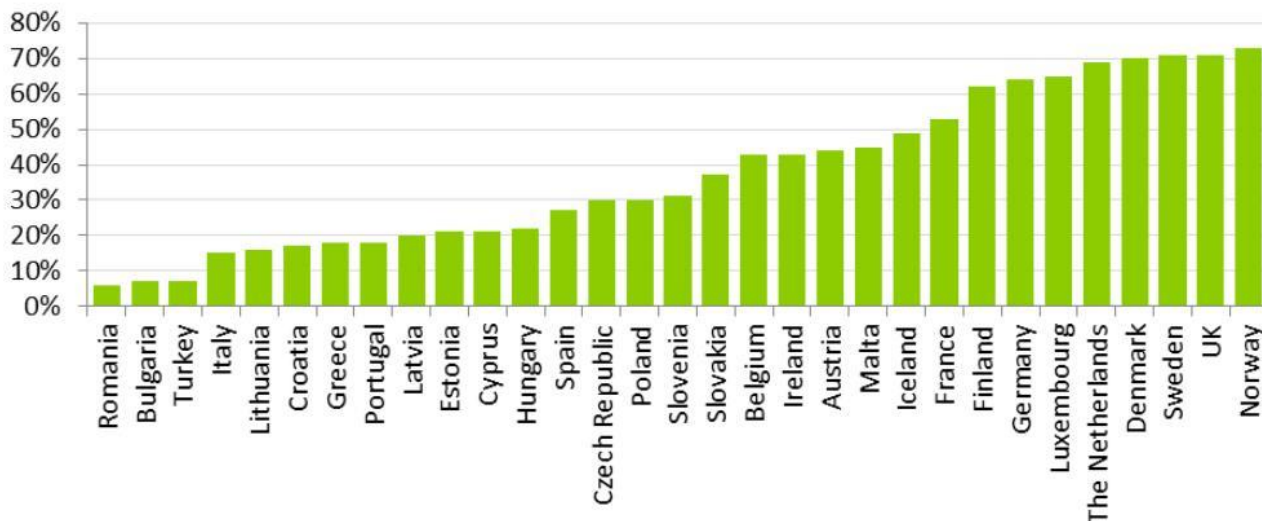
Internet Penetration



Sursa: Online payments 2012 (ECOMMERCE Europe și INNOPAY)

Deși Uniunea Europeană face eforturi spre o piață unică, persistă o mare divizare între maturitatea e-commerce și dezvoltarea sistemelor IT. În general vorbind, țările nordice, Țările de Jos și Regatul Unit sunt cele mai avansate, în timp ce țările din Europa de Sud și Europa de Est recuperează rapid. Accesul la internet în bandă largă a crescut puternic în noile state membre ale UE și proporția consumatorilor care au achiziționat bunuri on-line a crescut în consecință.

European consumers shopping online.



Source: Eurostat, December 2011

Ratele de penetrare în bandă largă sunt foarte diferite de la o țară la alta. Procentul de abonați în bandă largă (DSL, prin cablu și fibră / LAN), în Țările de Jos și Danemarca, este de 37%, în Germania și Franța, aproximativ 30%. Cele mai scăzute rate sunt Republica Cehă și Polonia, cu aproximativ 14%. Spațiul european în domeniul e-commerce nu poate fi considerat ca o piață unică mare în sine, așa cum există diferențe semnificative de la o țară la alta.

O piață matură din Europa de Nord, inclusiv Marea Britanie, Germania și țările nordice, unde între 60% și 80% dintre toți utilizatorii de internet sunt e-cumpărători. Marea Britanie iese în evidență ca țară lider mondial pentru e-commerce. În 2011, cheltuielile online în Marea Britanie a ajuns la 68 miliarde GBP, în creștere cu 16% comparativ cu 2010, în timp ce în 2012, segmentul cheltuielilor on-line este de așteptat să crească cu 13% de la an la an, reprezentând 77 miliarde GBP.

Tendențele pieței plăților electronice prin intermediul dispozitivelor mobile (m-payment) în UE

Plățile mobile în Europa Centrală și de Est au un drum lung de parcurs până când acestea își atingă potențialul maxim. Întrebarea rămâne, totuși, în ce măsură plățile electronice se prezintă ca o oportunitate pentru viitor? Plățile electronice reprezintă în acest moment o oportunitate de care va rămâne întotdeauna în viitor, sau va piata convinge practic toată lumea că plățile electronice reprezintă cea mai bună soluție, în același mod cum și telefonia mobilă a dovedit în ultimul deceniu?

Cu toate acestea, diferențele dintre regiunea CEE și alte zone geografice demonstrează de ce jucătorii de aici nu se pot baza pe aceiași factori care au condus creșterea plăților mobile pe alte piețe. În Asia, de exemplu, creșterea plăților mobile în unele țări a fost determinată de sistemul bancar slab (în special rețeaua de distribuție). Plățile mobile au fost introduse, de fapt, ca un substitut pentru o lipsă de servicii bancare de retail. Opusul este adevărat, însă, în majoritatea țărilor dezvoltate, cum ar fi Japonia sau Coreea, unde creșterea a plăților mobile reflectă nevoile clienților și o piață care cere servicii cu valoare adăugată și alte servicii inovatoare prin intermediul dispozitivelor mobile.

În CEE rețeaua deja bine dezvoltată de retail banking creează o provocare pentru piața tehnologiilor plăților mobile în încercarea de a găsi o oportunitate într-o piață saturată. În același timp, cu penetrarea serviciilor mobile în întreaga regiune ajungând la saturație în ultimii ani, operatorii de rețele mobile - MNO caută noi surse de venit concentrându-se pe mai multe servicii promițătoare în ceea ce privește potențialul de creștere a veniturilor, cum ar fi conținut și mass-media legate de afaceri, consecința naturală a convergenței digitale. Cu toate acestea, ideea de a înlocui portofelul cu telefonul mobil ca opțiune zilnică pentru tranzacțiile de valoare mică este o oportunitate pe care niciun MNO nu va dori să o piardă. În timp ce

valoarea tranzacțiilor mici, în prezent, pare a fi un punct slab al modelului de afaceri al plăților mobile, având potențial de dezvoltare ulterior, aceasta este o piață cu adevărat vastă care cuprinde un procent semnificativ din cheltuielile totale ale consumatorilor, eliminând necesitatea de posibil numerar și în cele din urmă chiar și a cărților de credit.

Cu telefoanele mobile utilizate în mod obișnuit de către majoritatea populației și numărul de terminale POS instalate în regiune într-un ritm foarte rapid de dezvoltare telefoane, partea ofertei arată promițător. În unele țări, inovatoare, furnizori independenți de servicii au observat șansa lor de a lua parte la afacere profitabilă de procesare de plată și au început lansarea inițiativelor competitive de plăți mobile direcționate, nu numai pentru piete locale, dar și pentru alte piețe din CEE (de exemplu, în Polonia m-Pay).

Cautarea de similitudini în tendințele poate conduce, de asemenea, nicăieri. De exemplu, în timp ce în unele piețe subdezvoltarea sectorului bancar a furnizat un declanșator pentru operatorii de telefonie mobilă pentru lansarea de servicii inovatoare de plăți mobile, în timp ce în alte țări, cum ar fi România, nu a fost cazul.

Obiectivul operatorului constă în a dezvolta rețeaua și de a atrage cât mai mulți clienți posibil și, ulterior, de a oferi servicii cu valoare adăugată pentru clienții lor, cum ar fi plățile mobile. Doar recent, astfel cum este piața orientată, în curând va ajunge la rata de penetrare de 100%, a devenit clar faptul că creșterea bazei de clienți nu va mai fi generatorul venitului principal, schimbarea obiectivelor strategice pe termen lung a operatorilor subliniază tot mai mult rolul inovării și serviciilor cu valoare adăugată, ca generatoare viitoare de creștere.

Redefinirea rolului băncilor

În timpul crizei financiare, instituțiile financiare au redus semnificativ expunerea lor la riscurile pe care le-au acumulat în timpul fazelor anterioare de dezvoltare.

Băncile analizează moduri de a rămâne aproape de clienții lor prin diversificarea produselor și accesului la online payments astfel încât să pastreze sau crească gradul de intermediere financiară. De exemplu în Europa băncile din spatele inițiativei MyBank au posibilitatea să-și recâștige o poziție în peisajul de plată on-line.

Determinată de creșterea continuă a comerțului electronic și cota în creștere a comerțului electronic în cheltuielile de vânzare cu amănuntul, băncile ar trebui să depună mai multe eforturi în direcția canalelor on-line, pentru a ține pasul cu cererea consumatorilor pentru confort și securitate. Mulți jucători noi se aliniază să profite de slăbiciunile din modelul bancar tradițional. Băncile au însă o relație puternică și de încredere cu clientul lor. În cazul în care băncile găsesc o modalitate de a construi de la aceste puncte forte, și-ar putea, de asemenea, menține poziția lor dominantă în peisajul plăților on-line.

3.2 Cadrul de reglementare la nivel național și european

Autorități de reglementare

Conform concluziei unui studiu realizat de revista The Economist, utilizarea preponderentă a plăților în numerar poate impacta în mod negativ mecanismele economice din perspectiva costurilor reale ale economiei subterane - în termeni de venituri fiscale pierdute, protecție redusă pentru muncitori, scăderea productivității pentru companii, și în cele din urmă, rate de creștere economică mai lente. În fața climatului economic actual, poziția fiscală slăbită din multe țări oferă un stimulent convingător pentru a lupta cu numerarul care circulă în economia subterană.

Analiza A.T. Kearney arată o corelație puternică între numărul plăților electronice dintr-o țară și mărimea economiei sale subterane.

Corelația între economia subterană și numărul plăților electronice:

Proporția economiei subterane (%)



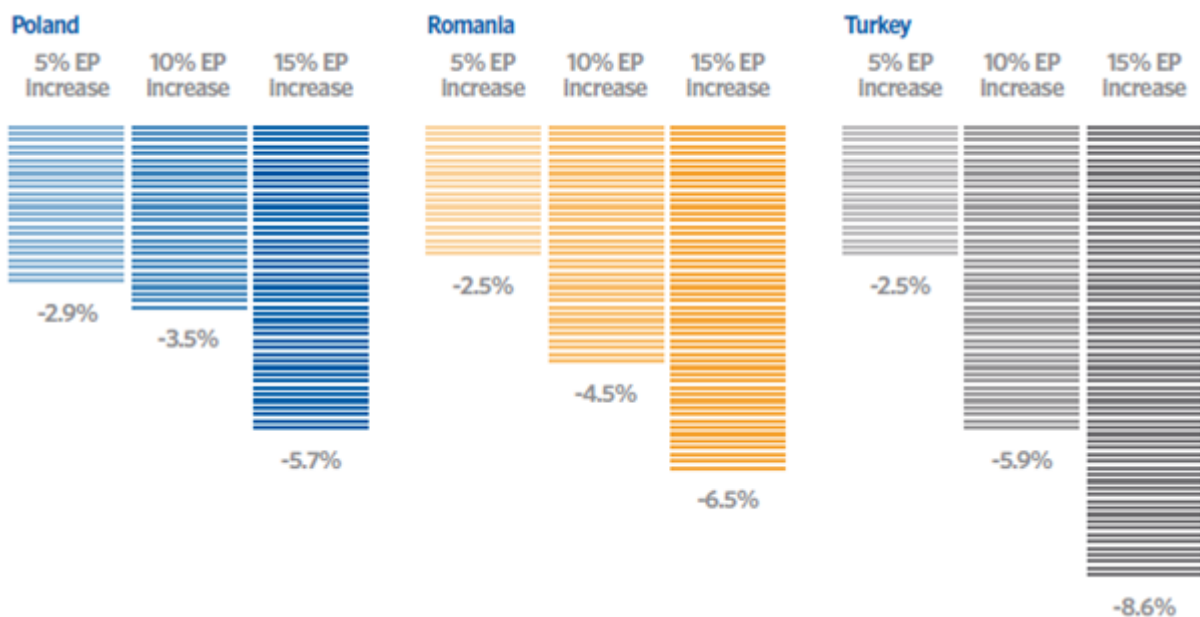
Număr mediu de tranzacții/locuitor/an

Notă: EU-27 (Date indisponibile pentru Cipru, Luxemburg, Malta) + Turcia

Sursa: ECB, Prof. Dr. Schneider, A.T. Kearney

În mod evident, aceste tranzacții pe bază de numerar oferă posibilitatea de a participa la economia subterană. Analiza recentă a profesorului Schneider -Universitatea Johannes Kepler din Linz a cuantificat impactul creșterii plăților electronice asupra economiei subterane în trei țări: Polonia, România și Turcia. Cum este indicat în figura 2, o creștere cu 15 % în asimilarea de plăți electronice poate reduce dimensiunea globală a economiei subterane cu până 6,5 % în cazul României.

Impactul anual mediu al creșterii plăților electronice/locuitor* asupra economiei subterane:



*Simulare pentru următorii 4 ani; sâevoluții medii anuale

Sursa: Prof. Dr. Schneider, 2009

Autoritățile de reglementare au o miză mare în viitorul plăților, un sistem de plăți eficient și dinamic constituind o pre-condiție necesară pentru o economie eficientă și dinamică.

În special, proiectul SEPA și Directiva Serviciilor de Plăți (DSP), deschid calea pentru o piață de plăți competitivă, mai deschisă și dinamică. Există multe motive pentru ca guvernele și autoritățile de reglementare să favorizeze plățile fără numerar și să promoveze în mod activ utilizarea acestora.

Lipsită de scara unei piețe unice cum ar fi SUA, situația europeană stabilește exemplul pentru multe alte regiuni. Europa este o regiune unică în acest context, implicând eforturi de lungă durată și determinate pentru a integra statele membre ale UE într-o piață unică. Implicațiile Directivei privind serviciul de plată (PSD) și SEPA - mai precis, eSEPA, sunt două inițiative publice importante a condus la armonizarea plăților (online), în regiune.

Reglementări pentru plățile europene

Pentru băncile din Europa, plățile sunt cu siguranță în centrul atenției economice actuale - recesiunea a concentrat atenția asupra plăților - în ceea ce privește costurile pe care le consumă, stabilitatea veniturilor pe care le generează, și de asemenea, la rolul pe care îl pot juca în cimentarea relațiilor cu clienții și atragerea de lichidități atât de necesare. Dezvoltările actuale de norme de reglementare (de exemplu, crearea SEPA și punerea în aplicare a PSD) deschid calea pentru mai multă deschidere și dinamism în piața europeană a plăților, pun presiune semnificativă scăderii privind taxele, și permit sectorului nebancar să se stabilească ca instituții de plată.

Reglementari la nivelul Uniunii Europene și cadrul corespunzător în România

	Legislația generală pentru Comerțul electronic	E-money		Protecția consumatorului	
Uniunea Europeană	Directiva 2000/31/EC E-Commerce	Directiva 2000/46/EC privind inițierea, exercitarea și supravegherea prudențială a activității instituțiilor emitente de monedă electronică	Directiva 2000/28/EC de modificare a Directivei 2000/12/CE privind inițierea și exercitarea activității instituțiilor de credit	Directive 97/7/EEC privind protecția consumatorilor cu privire la contractele la distanță	Directive 2002/58/EC asupra confidențialității și comunicațiilor electronice
România	Directiva transpusă prin Legea nr. 365/2002 privind comerțul electronic	Directiva, în general, transpusă prin Ordonanța Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată prin Legea nr. 227/2007	Directiva, în general, transpusă prin Ordonanța Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată prin Legea nr. 227/2007 și prin diverse reglementări emise de Banca Națională din România	Directiva transpusă prin Ordonanța Guvernului nr. 130/2000 privind protecția consumatorilor în ceea ce privește încheierea și executarea contractelor la distanță	Directiva transpusă prin Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor

Următoarele trei directive CE și dezbaterile în jurul furnizează îndrumări influente pentru țările din regiunea CEE:

- Directiva E-Money (EMD) 2000/46/CE se referă în mod specific la e-plăți, și "urmărește să deschidă piața pentru emiterea de monedă electronică pentru instituțiile non-bancare, prin crearea de" instituții emitente de monedă electronică (ELMI), reglementate sub un regim prudential mai ușor decât cel prevăzut de instituțiile de credit ". Până acum, statele membre au exceptat MNOs și mpayments de la licențiere ELMI.

- Directiva privind serviciile de plăți (PSD), 2007/64/CE stabilește nivelurile de acces la informații, obligațiile și datoriile pe procesoare de plată, cum ar fi băncile și societățile de carduri de credit. PSD este parte a acțiunii directe în ajutorul de creare a unei piețe comune a serviciilor de plată.

Scopul directivei este de a asigura ușurința în utilizare, siguranța și eficiența plăților în întreaga Uniune Europeană / Spațiul Economic European, în special pentru transferurile de credit, mandate de debitare directă, plăți de carduri, precum și pentru servicii de transfer de bani. Una din noutățile din PSD a fost sistemul de licențe pentru furnizorii de servicii de plăți (PSP), fiind stabilite cerințele de informare cu privire la serviciile de plată și drepturile și obligațiile atât pentru PSP cât și pentru utilizatori,

La jumătatea anului 2011, existau 341 instituții înregistrate în UE, Marea Britanie este lider clar în ceea ce privește instituțiile de de plăți autorizate, peste 50% din toate instituțiile de plată (PI) și instituțiile emitente de monedă electronică (EMI) fiind înregistrate în această țară.

- Spațiul unic de plată în euro (SEPA), care a fost lansat în ianuarie 2008, deschide serviciile transfrontaliere de credit și carduri de credit la nivelul UE în domeniul concurenței, dar nu și în cazul mpayments. Normele și reglementările care guvernează ELM, inclusiv sistemele de mpayment, au fost amânate până în 2009.

Rata de schimbare în cadrul industriei totale europene de plăți se accelerează acum, programul SEPA fiind aproape de finalizare cu termene limită stabilite pentru anul 2014. În cadrul programului băncile europene încearcă să armonizeze transferurile de credit, debit direct și produse de carduri din 32 de țări europene. Viziunea SEPA este să renunțe la conceptul de plăți transfrontaliere, pentru a trata Europa ca o regiune internă pentru plăți. Fiecare cetățean și organizație ar trebui să aibă acces la aceleași instrumente plată peste tot în Europa, Această viziune a fost parte a Agendei de la Lisabona a Comisiei Europene, în efortul de a face economia Europei mai competitivă,

Relevanța pentru plățile online constă în principal în faptul că SEPA oferă un set de instrumente de plată (și anume transfer de credit și de debit direct) care se aplică în întreaga regiune SEPA. Metodele de plată online, care fac uz de aceste instrumente au, prin definiție, rază de acțiune pan-europeană.

Banca Națională din România a emis un regulament privind plățile efectuate prin instrumente de acces la distanță (cum ar fi mobile banking), care solicita băncilor să obțină o autorizație din partea Ministerului Comunicațiilor și Tehnologiei Informatice (MCTI), în scopul de a fi în măsură să ofere un astfel de instrument pentru clienții lor. În scopul obținerii acestei autorizații de la MCTI, băncile trebuie să efectueze un audit anual de securitate a instrumentului de plată respectiv efectuat de către un auditor independent, specializat.

De asemenea Banca Centrală Europeană a emis în ianuarie 2013 recomandări privind securitatea platilor prin internet și pentru serviciile de accesare a conturilor de plăți, care trebuie implementate de către furnizorii de servicii de plăți până la data de 01 februarie 2015, autoritățile naționale având libertatea să scurteze aceste termene. Stabilirea unor recomandări armonizate la nivel european pentru securitatea platilor electronice are scopul de a contribui la diminuarea fraudelor și la creșterea gradului de încredere a consumatorilor în plățile electronice.

Premisele asigurării securității plăților electronice

Evaluarea caracteristicilor principale ale plăților electronice

Spectrul tehnologiilor mobile de plată			
Recepția și plata facturilor mobile	Persoană la persoană/Emisie internațională	Cumpărături mobile	Echipamente POS/Plăți prin apropiere
Detalii generale: Consumatorul descarcă o aplicație pentru plăți mobile care permite utilizatorilor plata facturilor prin fotografierea unei facturi cu telefonul inteligent, fără setări suplimentare sau emiterea unor cecuri.	Detalii generale: Transferurile persoană la persoană permit consumatorilor să își transfere fonduri utilizând adresa e-mail sau numărul de telefon (fără detalii despre conturile bancare). Pentru a recepționa fondurile, utilizatorii trebuie să se înregistreze și să își valideze identitatea la furnizorul de servicii.	Detalii generale: Consumatorul utilizează aplicațiile web mobile pentru a căuta și achiziționa produse online; experiența este similară cu sistemul clasic de cumpărături online	Detalii generale: Tehnologiile sunt "Arată și plătește" sau "Atinge și pleacă", telefoanele mobile au încorporate echipamente NFC sau atașate astfel de dispozitive prin care se efectuează plăți prin apropierea lor de un terminal NFC aflat la comerciant.
Oferte existente: Majoritatea băncilor oferă o versiune mobilă a sistemului de internet banking de bază.	Oferte existente: Majoritatea băncilor mari au intrat pe această piață cu soluții legate de platforma pentru plăți mobile.	Oferte existente: Comercianții mari din sistemul online oferă variante mobile ale siteurilor. Deși nu este încă implementat, se lucrează la un sistem de recompensare a consumatorilor care utilizează cărțile de credit.	Oferte existente: VISA a încheiat un parteneriat cu DeviceFidelity pentru a oferi dispozitive de plată microSD băncilor partenere. Cardurile microSD pot se introduce în telefonul mobil pentru a permite plățile. De asemenea, sunt disponibile abțibilduri NFC care se lipesc pe carcasa telefoanelor mobile.

Tehnologii de Mobile Banking			
Tehnologia	Utilizare	Avantaje	Dezavantaje
Mesaj text SMS	Răspândit în țările dezvoltate, servicii de atenționare și unele opțiuni de plată.	Pot fi utilizate independent de platforma mobilă sau de furnizorul serviciilor de telecomunicații, cu telefoane clasice sau inteligente, ușor de utilizat și relativ sigure.	Utilizare interzisă în unele regiuni, probleme de securitate, funcționalitate redusă.
Browser mobil	Răspândit în țările dezvoltate, în special de către băncile regionale și mai reduse ca dimensiuni, browserele mobile îi conectează pe utilizatori la un site dezvoltat de internet banking.	Familie pentru clienții de internet banking, integrare facilă cu platformele de internet existente, independent de platforma mobilă sau furnizorul serviciilor de telecomunicații.	Utilizată pe scară largă (nu prezintă avantaj competitiv), presupune mai mulți pași pentru autentificare, adaptare slabă la ecranele cu dimensiuni reduse.
Aplicație dedicată	Câștigă popularitate în țările dezvoltate, utilizare în mobile banking, cupoane și servicii bazate pe locație.	Furnizează o experiență puternică utilizatorului printr-o aplicație dedicată, tinde să fie mai sigură și mai stabilă, menține loialitatea și oferă posibilitatea furnizării de servicii suplimentare.	Probleme de integrarea deoarece aplicația trebuie modificată pentru fiecare platformă mobilă în parte, trebuie să fie instalată de utilizator, poate avea costuri de implementare mai ridicate.

Tehnologii mobile de plată			
Dispozitive dedicate NFC (câmp electromagnetic pe distanțe scurte)	Permit efectuarea plăților fără contact prin apropiere de echipamentele POS ale comercianților, utilizând dispozitive precum abțibilduri, brelocuri și carduri microSD.	Utilizează standardele de utilizare fără contact a cardurilor, permite efectuarea de plăți fără cooperarea furnizorului serviciilor de telecomunicații.	Dispozitivele limitate de obicei la un singur cont bancar, procedură complexă de instalare și activare pentru utilizator, costuri ridicate cu echipamentele și distribuția acestora.
Dispozitive NFC încorporate	Utilizează tehnologia portofelului mobil încorporând un cip NFC pentru a lărgi opțiunile de plată către echipamente aflate la distanțe reduse.	Utilizează standardele de utilizare fără contact a cardurilor, permite accesul la mai multe conturi prin interfața portofelului electronic, asigură un plus de securitate prin cod PIN.	Disponibilitate limitată a echipamentelor, furnizorul serviciilor de telecomunicații controlează inventarul și distribuția dispozitivelor.
Mesaj text SMS	Efectuarea de plăți de la distanță, în special pentru mediul digital.	Utilizare pe scară largă pe majoritatea telefoanelor mobile.	Dimensiunea mesajelor este limitată, costuri ridicate pentru consumator și comerciant, multe jurisdicții nu permit utilizarea mesajelor text pentru efectuarea plăților
Voce	O tehnologie de nișă care furnizează servicii pentru conturi și plăți de facturi, unele sisteme mobile de plată solicită autorizarea prin voce a tranzacțiilor.	Interacțiune personală, oportunități pentru vânzare dinamică de servicii suplimentare.	Costuri ridicate pentru utilizarea operatorilor umani, comunicațiile de date sunt ineficiente.

	Servicii mobile banking de bază	Servicii avansate de mobile banking și plăți mobile	Plăți mobile la POS
Descriere generală	Piața serviciilor mobile banking de bază este alcătuită din instituții financiare concentrate pe dezvoltarea și perfecționarea platformelor proprii de mobile banking.	Piața serviciilor avansate de mobile banking și plăți mobile este alcătuită din instituții care furnizează produse și servicii mature de mobile banking, împreună cu servicii de plăți mobile de bază.	Piața plăților mobile la POS este compusă din entități tradiționale și netradiționale care se luptă pentru veniturile din segmentul de piață al plăților mobile.
Caracteristici semnificative	Includ de obicei servicii de bază, acces la cont, informații despre sold și transferuri interne care se fac prin platforme operate de un vânzător.	Constau de obicei în servicii avansate de mobile banking, depozite bancare, plata facturilor prin fotografiere, și oarecare servicii mobile de plată cum ar fi persoană la persoană.	Caracteristicile și funcționalitatea variază în funcție de entitățile implicate și de regiunea în care sunt lansate soluțiile.
Beneficii	Reputație crescută și servicii oferite clienților	Reduce costurile pentru deservirea clienților și crește capitalul disponibil.	Protejează veniturile actuale din plăți.
	Costuri reduse pentru deservirea clienților (prin urmare mai mult capital flexibil)	Crește eficiența proceselor și reduce intervenția manuală.	Crează noi oportunități de venituri.
	Poate fi implementată direct	Dezvoltă experiența și aptitudinile aganajților interni.	Răspunde cerințelor clienților.
	Ușor de integrat cu serviciile de internet banking	Capitalizează oportunitățile "primului venit pe piață".	
	Demonstrează inovație	Furnizează fluxuri noi de venit.	
	Crează un nivel de referință al confortului consumatorului care utilizează dispozitivele mobile		
	Dezvoltă experiența și aptitudinile aganajților interni		
Impactul asupra clienților	Acces neîngrădit la informațiile bancare și tranzacțiile de bază	Reduce vizitele în agenții și la bancomate.	Convenabil și ușor de utilizat, în special pentru plățile de valori scăzute.
	Convenabil și facil de utilizat	Furnizează clienților flexibilitate crescută.	Securitate și intimitate crescute.
	Perspectivă de ansamblu asupra informațiilor bancare	Sporește încrederea clienților în soluțiile de plată mobile.	Înlocuiește portofelul tradițional sau cardurile de tip portofel electronic.
	Loializarea clienților	Deschide calea plăților prin apropiere fără contact.	
Aspecte importante	Care este strategia băncii privitoare la tehnologia mobilă?	Cine furnizează băncii serviciile mobile și care sunt resursele acestuia?	Cum ar trebui să se pregătească banca pentru îmbunătățirea platformelor mobile de plată?
	Care este strategia băncii privitoare la comerțul mobil?	Care sunt practicile de top în domeniul comerțului mobil?	Cum ar trebui lansată soluția pilot de plăți mobile?
	Care este poziția băncii referitor la plățile mobile?	Cum ar trebui să arate produsul de plăți mobile al băncii?	Care sunt costurile estimate pentru soluția de plăți mobile?
	Care sunt serviciile actuale de mobile banking ale băncii?	Care ar trebui să fie sistemul de împărțire al veniturilor?	

Preocupările legate de infracțiunile informatice specifice

În ultimii ani s-a constatat că lumea digitală, pe lângă beneficiile enorme pe care le creează, este în egală măsură extrem de vulnerabilă. Incidentele de securitate cibernetică la măsurile și acțiunile de siguranță care pot fi luate pentru a proteja domeniul informatic, atât în mediul militar cât și civil, de acele amenințări care sunt asociate sau care pot aduce prejudicii rețelelor independente și infrastructurii informatice ale acestuia. Prin securitate cibernetică rețelele și infrastructura, precum și confidențialitatea informațiilor pe care le conțin, sunt păstrate în parametri optimi de disponibilitate și integritate, indiferent dacă sunt premeditate sau accidentale, sunt într-o creștere alarmantă și ar putea duce la întreruperea furnizării unor servicii esențiale, precum apa, electricitatea, serviciile medicale și cele de telefonie mobilă. Amenințările pot avea la bază atacuri criminale, atacuri motivate politic, atacuri teroriste sau comandate de alte state, precum și dezastre naturale sau erori comise fără intenție.

Economia UE este deja afectată de fenomenul infracționalității cibernetice. Infracțiunea cibernetică se referă la o arie largă de diverse activități infracționale în care sunt implicate computere sau sisteme informatice ca și instrument primar sau țintă primară. Infracțiunile cibernetice includ infracțiunile tradiționale (de ex. fraudă, falsul, furtul de identitate), infracțiunile de conținut (de ex. distribuirea de pornografie infantilă sau incitarea la ură rasială) și infracțiunile specifice computerelor și sistemelor informatice (de ex. atacuri împotriva sistemelor informatice, atacuri de tipul denial of service și malware), astfel de acțiuni vizând sectorul privat și cetățenii. Infractorii recurg la metode tot mai sofisticate de penetrare a sistemelor informatice și sustrag date critice sau cer răscumpărare de la diverse companii. Intensificarea spionajului economic și a activităților finanțate de state în spațiul cibernetic reprezintă o nouă categorie de amenințare la adresa guvernelor UE și a companiilor.

Utilizarea abuzivă a datelor cu caracter personal și securitatea plăților online sunt cele mai mari două probleme - Utilizatorii de Internet au fost întrebați ce privește utilizarea care le-au despre Internet pentru lucruri cum ar fi online banking sau cumpararea de lucruri on-line.

Cele două preocupări cu privire la cele mai frecvente sunt utilizarea sau abuzeazărea de date cu caracter personal (menționat de 40%) și de securitate a plăților online (38%). Unii respondenți exprimă, de asemenea, o preferință pentru efectuarea tranzacțiilor în persoană (24%), în timp ce 19% sunt preocupați neprimirea bunurilor sau serviciilor pe care le cumpara on-line. O cincime din utilizatorii de internet (21%) spun ca nu au probleme cu privire la utilizarea internetului pentru lucruri cum ar fi online banking sau cumpara de lucruri on-line.

Preocupările ale utilizatorilor de internet variază în funcție de țară. În general, preocupările legate de securitatea datelor cu caracter personal și au tendința de a fi mai puternice în UE15, în decăt NMS12. În medie, în UE15, 43% sunt îngrijorați cu privire la cineva care ar putea lua sau abuza de date cu caracter personal, în comparație cu 28% în NMS12; și în UE15, 40% sunt preocupați de securitatea plăților online, comparativ 27% în NMS12.

Preocupările legate de cineva care ar putea lua sau abuza de date cu caracter personal sunt mai raspandite in Germania (59%), Luxemburg (54%), Cipru (51%) și Slovenia (50%), în timp ce respondenții din Marea Britanie (56%) și Franța (50%) sunt cie mai preocupati de securitatea plăților online.

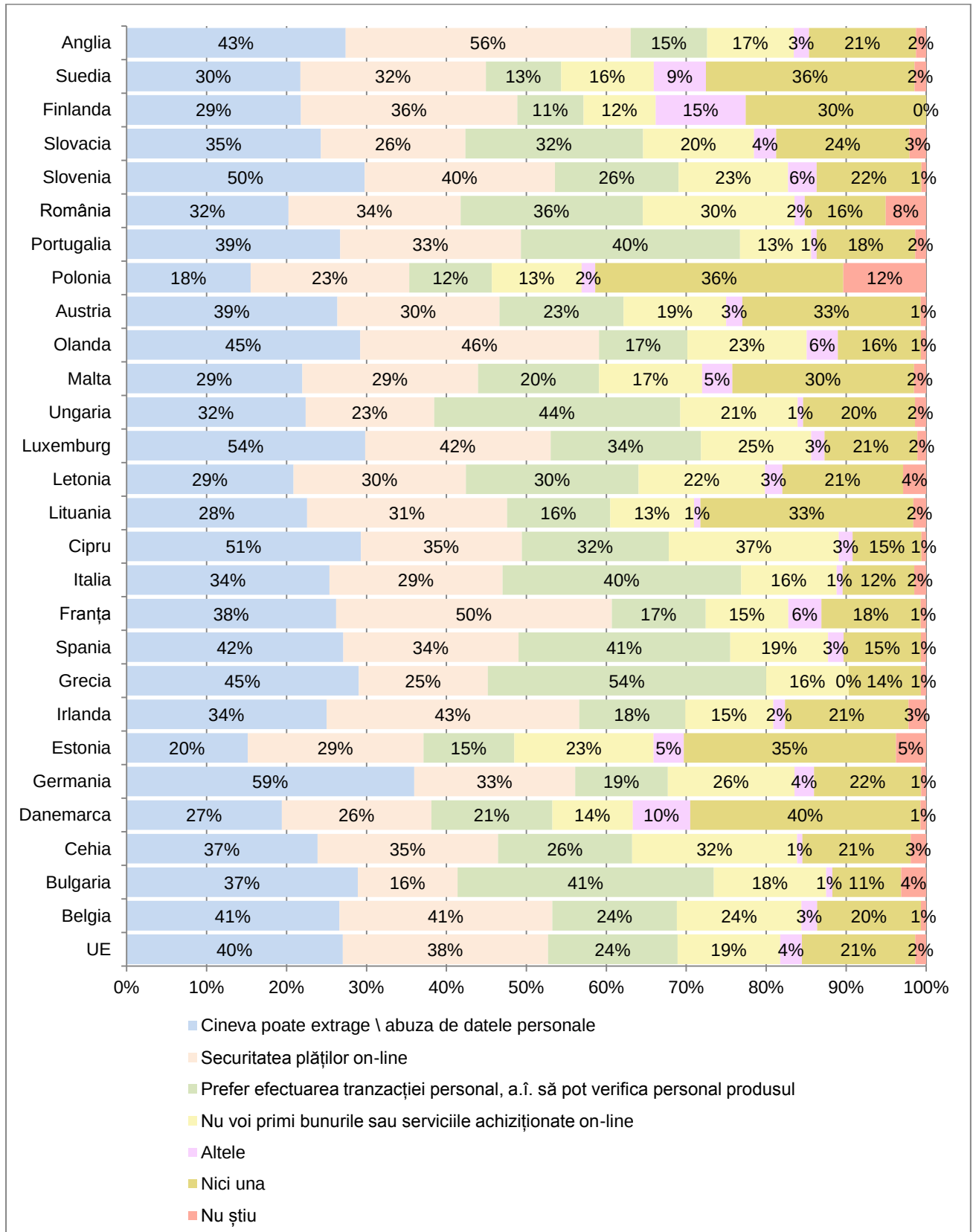
Preferința unei tranzacții personale este mai puternică în Grecia (54%), Ungaria (44%), Bulgaria (41%), Spania (41%), Italia (40%) și Portugalia (40%), în timp ce respondenții cel mai preocupat de neprimirea bunurilor sau serviciilor în Cipru (37%), Republica Cehă (32%) și România (30%).

În unele țări, o proporție relativ mare de utilizatori de internet nu au preocupări cu privire la online banking sau cumpara de lucruri on-line: Danemarca (40%), Suedia (36%), Polonia (36%), Estonia (35%), Austria (33%) și Letonia (33%).

Preocupările exprimate de respondenți sunt foarte consecvente în grupuri socio-demografice. Utilizatorii de Internet care nu au încredere în capacitatea lor de a folosi internetul pentru lucruri cum ar fi online

banking sau cumpararea de lucruri on-line sunt mult mai susceptibile de a avea probleme, în special, ele sunt mult mai probabil să-și exprime o preferință pentru efectuarea tranzacțiilor în persoană (44%) decât cei care sunt increzatori in utilizarea internetului pentru aceste activități (16%).

Ce preocupări aveți despre utilizarea internetului pentru online banking sau cumparaturi on-line?

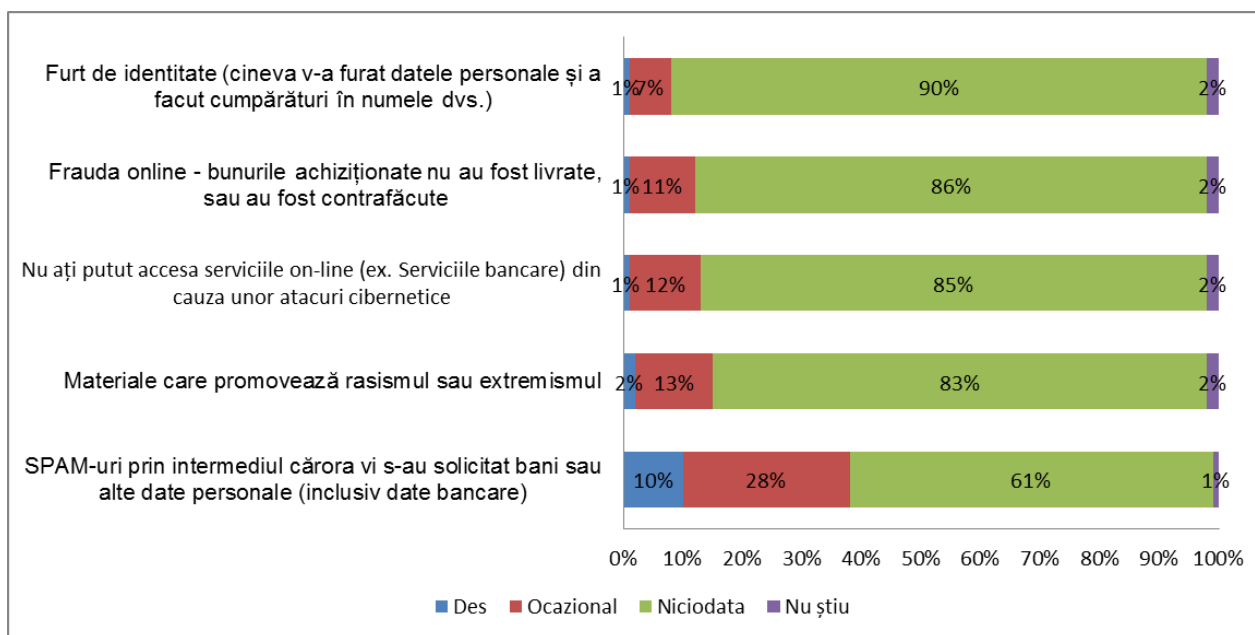


Sursa: SPECIAL EUROBAROMETER 390 "Cyber security"

Mai mult de o treime din utilizatorii de internet din întreaga UE (38%) spun că au primit e-mailuri în mod fraudulos care solicită bani sau detalii personale. Acest lucru este de departe cel mai comun tip de criminalitate informatică experimentat de către respondenți. În total, 10% dintre utilizatorii de internet spun că acest lucru sa întâmplat de multe ori să-i, în timp ce 28% spun că sa întâmplat ocazional.

În plus, 15% dintre utilizatorii de internet spun că au întâlnit accidental materiale care promovează ura rasială sau extremismul religios, în timp ce 13% nu au fost în măsură pentru a accesa servicii online, din cauza unor atacuri informatice, iar 12% au experimentat fraudă on-line (în cazul în care mărfurile nu sunt livrate, contrafăcut sau nu ca publicitate). Pe întreg teritoriul UE, 8% dintre utilizatorii de internet spun ca au experimentat furt de identitate.

Cât de des v-ați confruntat sau ați fost victimele următoarelor infracțiuni informatice?



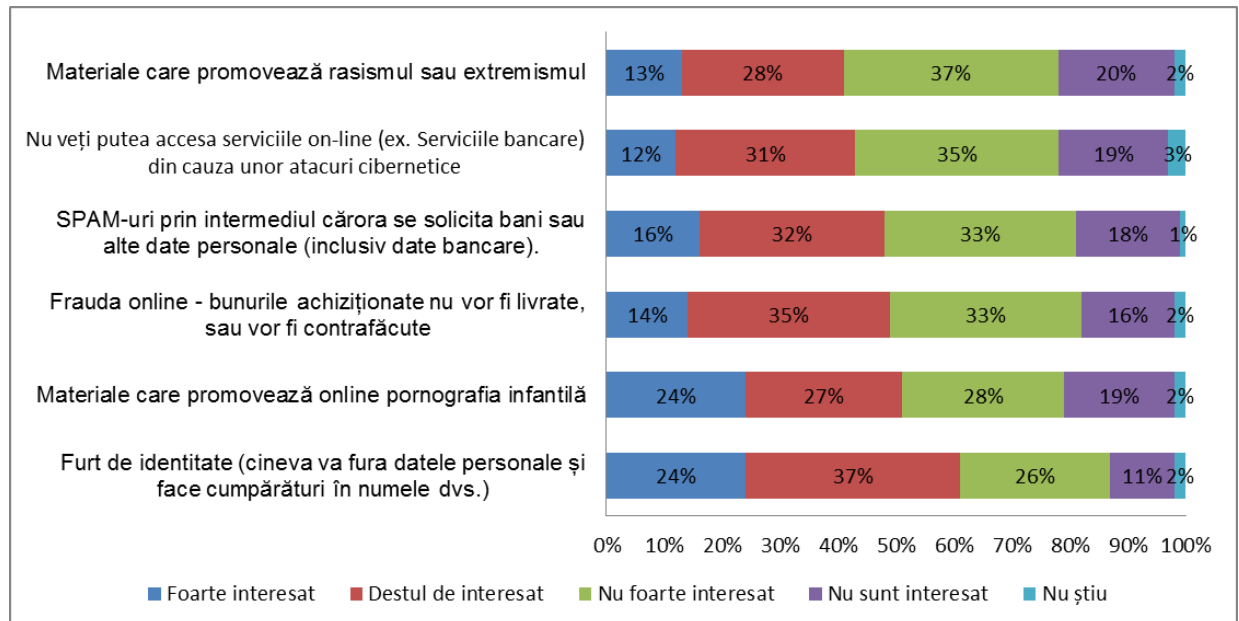
Sursa: SPECIAL EUROBAROMETER 390 "Cyber security"

Fiind întrebați cât de interesați sunt despre experimentarea sau de a fi o victimă a diferitelor tipuri de criminalitate informatică, utilizatorii de internet sunt cel mai probabil să afirme că sunt îngrijorați cu privire la furtul de identitate. Majoritatea respondenților (61%) sunt îngrijorați de acest lucru, inclusiv 24% care sunt foarte îngrijorați.

Aproximativ jumătate dintre utilizatorii de internet sunt preocupați întâmpină următoarele tipuri de criminalitate informatică: descoperirea accidental on-line a pornografiei infantile (51%), în cazul în care fraudă online bunurilor achiziționate nu sunt livrate, sunt contrafacute sau sunt astfel cum au fost promovate (49%) și e-mailurile primite în mod fraudulos solicitând bani sau detalii personale (48%).

În proporții ușor mai scăzute sunt preocupați de a nu fi capabili să accesa servicii online, din cauza unor atacuri informatice (43%) și se confruntă accidental cu materiale care promovează ura rasială sau extremismul religios (41%).

Cât de interesat sunteți de faptul că vă puteți confrunta sau puteți deveni victimele următoarelor infracțiuni informatice?



Sursa: SPECIAL EUROBAROMETER 390 "Cyber security"

3.3 Recomandări

3.3.1 Strategii de adresare a riscurilor

Plățile mobile aduc noi oportunități și riscuri noi. Operațiunile de plăți mobile pot fi mult mai expuse la risc, deoarece mai multe părți sunt implicate în efectuarea de servicii de plată în comun. Acest lucru se poate agrava dacă serviciile importante sunt externalizate pentru părțile terțe posibil nereglementate, fără linii clare de responsabilitate și supraveghere, sau care se află în străinătate. Acest mediu tranzacție multipartit este propice exploatarei de către infractori care folosesc atacuri atât tehnologice cât și sociologice în cazul în care mecanismele adecvate de protecție și controalele de responsabilizare nu sunt stabilite de-a lungul ecosistemului de plată mobil. Cu o planificare atentă, care include toate părțile interesate, procesele și tehnologiile implicate, există posibilitatea de a face securitatea un element intrinsec al tuturor sistemelor de plăți mobile.

Piața financiară, precum și furnizorii de servicii de rețea (FSP - Financial service providers, PSP - Payment service providers, NSP - Network service providers) ar trebui să pună în aplicare măsurile de siguranță corespunzătoare și de confidențialitate precum și a programelor de guvernare a securității. Lipsa unor reglementări clare, nu ar trebui să fie utilizată de către o organizație ca o scuză pentru a nu fi proactivă. Fiecare organizație implicată în lanțul de date despre tranzacții ar trebui să pună în aplicare controale puternice pozitive pentru a proteja astfel de date în timp ce se afla în custodia sa.

O preocupare centrală este asigurarea ca tranzacția este realizată de persoana autorizată sau înregistrată să o efectueze. În cazul băncilor orientate pe tranzacțiile NFC, protecția tranzacțiilor care provin de la utilizatori neautorizați sau telefoane mobile fictive poate fi realizată prin utilizarea de valori dinamice de

verificare (CVVs). Telefoanele mobile NFC cip-enabled suporta CVV dinamice în comparație cu CVV statice utilizate pe carduri cu bandă magnetică. Astfel, în cazul în care un telefon mobil fals este ulterior utilizat, acesta va prezenta CVV greșit și tranzacția nu va trece, protejând astfel atât furnizorul de servicii cât și consumatorul și comerciantul. În mod similar, același tip de asigurare pentru consumator ar trebui să fie stabilită la partea de comerciant.

Aceste puncte sunt reprezentative pentru un set mai mare de probleme în ceea ce privește onestitatea identităților și credentials atât pentru plățile mobile cât și pentru comerțul mobil, în general. Un alt factor important este luarea în considerare a clasificării datelor pe parcursul transmiterii și stocării datelor în noduri diferite. Organizațiile ar trebui să identifice datele care sunt considerate personale și sensibile și ar trebui să se asigure că există mecanisme corespunzătoare implementate. De asemenea, în cazul datelor financiare, un aspect foarte important (în afară de criptare) este problema integrității datelor. În cazul în care datele de plată mobile vor fi utilizate pentru servicii de marketing, organizația ar putea fi declarată răspunzătoare pentru practicile de afaceri neloiale cazul în care utilizează datele clienților pentru scopuri care nu sunt incluse în anunțurile clienților.

La fel de important să se considere sunt sistemele POS, în cazul plăților de proximitate. Organizațiile ar trebui să se asigure că părțile terțe cu care acestea interacționează au proiecte robuste de securitate de guvernare în vigoare. În plus, de asemenea, o atenție specială ar trebui acordată TSM (Trusted Service Manager – este un terț care potențial poate fi utilizat pentru administrarea implementării de aplicații mobile), care acționează în calitate de entitate care "personalizează" cip-urile TSM-compatibile pe dispozitivul mobil furnizat de vendor. Într-un astfel de mediu de colaborare cross-platform, programul de control al riscului ar trebui să aibă un puternic accent pe gestionarea serviciilor terțelor părți.

Producatorii de dispozitive mobile nu ar trebui să colaboreze numai cu industria de plata pentru dezvoltarea unor platforme care să asigure un mediu sigur pentru efectuarea tranzacțiilor mobile, cât și interoperabilitatea între diferite modele de smartphone-uri astfel cum utilizatorii au tendința de a modifica sau actualiza frecvent telefoanele lor mobile. Furnizarea continuă a serviciilor de securitate interoperabile este de o importanță critică pentru succesul plăților mobile.

În cele din urmă, la fel cum un lanț este la fel de puternic ca cea mai slabă verigă a sa, o atenție specială ar trebui acordată la punctul de originare a unei tranzacții mobile - dispozitivul clientului și utilizator. Utilizatorii ar trebui să fie educați să înțeleagă riscul corespunzător. Fără asigurarea că schimbul de informații sigure și în condiții de siguranță a tranzacțiilor financiare electronice prin intermediul rețelelor de telefonie mobilă se poate face, proceduri diferite de securitate pentru platile mobile și metode de plată au fost sugerate și puse în aplicare pentru plățile mobile.

Un sistem securizat de plată pentru platile mobile trebuie să conțină următoarele caracteristici:

- Confidențialitatea - informațiile confidențiale trebuie să fie asigurate împotriva accesului de către o persoană neautorizată, proces sau dispozitiv.
- Autentificare - asigură părților accesul la o tranzacție și care sunt de încredere. Acesta se obține de obicei prin utilizarea de protocoale de rețea pe bază de autentificare.
- Integritate - sistemele de informare și nu au fost modificate sau corupte de către părțile din afara.
- Autorizare - verificarea faptului că utilizatorului se permite să facă tranzacția solicitată.
- Disponibilitate - sistemul trebuie să fie accesibil pentru utilizatorii autorizați în orice moment.
- Non-repudiare - asigură faptul că utilizatorul nu trebuie să nege că el / ea a efectuat o tranzacție și trebuie să furnizeze dovezi în cazul în care o astfel de situație apare.

3.3.2 Recomadări BCE

Măsuri generale de control și securitate

Datorită specificului sistemelor de plăți mobile, riscurile asociate acestora ridică probleme pentru toți actorii implicați. Pentru a veni în sprijinul diminuării acestor riscuri prezente pentru plățile mobile, Banca Centrală Europeană a emis în ianuarie 2013 documentul „Recommendations for the security of internet payments” care recomandă măsurile ce trebuie implementate pentru cele trei categorii astfel:

- 3.3.2.1** *Măsuri de control general și mediul de securitate privind platformele de servicii de plată de internet. Recomandările fac referire la identificarea riscurilor de guvernare, evaluare, monitorizare, raportare și control al riscurilor.*
- 3.3.2.2** *Măsuri specifice de control și măsurile de securitate pentru plăți pe internet. Recomandările din a doua categorie acoperă toate etapele procesare a tranzacțiilor de plată, de la accesul la servicii (informații despre clienți, înscriere, soluții de autentificare) pentru inițierea de plată, monitorizare și autorizare, precum și protecția datelor cu caracter sensibil.*
- 3.3.2.3** *Măsuri de conștientizare a clienților, educare și comunicare. Recomandările din a treia categorie includ protecția clienților, modul de utilizare a serviciilor de plată pe internet în condiții de siguranță și modul în care clienții pot verifica faptul că tranzacția a fost inițiată și executată.*

Măsuri de control general și mediul de securitate

3.3.2.4 Guvernanța

PSP-urile și sistemele de plată ar trebui să pună în aplicare și în mod regulat revizuiască o politică formală de securitate pentru serviciile de plăți prin Internet.

3.3.2.5 Evaluarea riscurilor

PSP-urile și sistemele de plată ar trebui să efectueze și să documenteze evaluări detaliate a riscurilor în ceea ce privește securitatea plăților pe internet și serviciile conexe, atât înainte de înființarea serviciului (lor) și în mod regulat după aceea.

3.3.2.6 Monitorizarea și raportarea incidentelor

PSP-urile și schemele de plată ar trebui să asigure coerentă și integrată monitorizarea, manipularea și follow-up a incidentelor de securitate, inclusiv plângeri ale clienților legate de securitate. PSP-urile și schemele de plată ar trebui să stabilească o procedură pentru raportarea unor astfel de incidente către management și, în caz de incidente majore de securitate de plată, autoritățile competente.

3.3.2.7 Controlul și diminuarea riscurilor

PSP-urile și schemele de plată ar trebui să pună în aplicare măsuri de securitate, în conformitate cu politicile lor de securitate, în scopul de a reduce riscurile identificate. Aceste măsuri ar trebui să includă mai multe niveluri de securitate, în care, eșecul din o linie de apărare este capturat de către următoarea linie de apărare ("apărare în adâncime").

3.3.2.8 Trasabilitatea

PSP-urile ar trebui să aibă loc în procesele pentru a garanta că toate tranzacțiile, precum și fluxul procesului de e-mandat, sunt urmărite în mod corespunzător.

Măsurile specifice de control și de securitate

Referitor la măsurile specifice de control și măsurile de securitate pentru plăți pe internet, recomandările BCE vizează următoarele:

3.3.2.9 Identificarea clienților inițiali, informații

Clienții ar trebui să fie identificați în mod corespunzător, în conformitate cu legislația europeană privind combaterea spălării banilor și confirmă disponibilitatea lor de a face plăți pe internet prin intermediul serviciilor înainte de a fi acordat accesul la astfel de servicii. PSP ar trebui să ofere "înainte", "regulat", sau, după caz, "ad-hoc" informații adecvate clienților cu privire la cerințele necesare (de exemplu, echipamente, proceduri) pentru efectuarea operațiunilor de plată sigure de internet și a riscurilor inerente.

3.3.2.10 Autentificarea sigură a clienților

Inițierea plăților pe internet, precum și accesul la date sensibile de plată, ar trebui să fie protejate de autentificarea puternică a clienților.

3.3.2.11 Înscrierea pentru și furnizarea de instrumente de autentificare și / sau software-ul livrat clientului

PSP ar trebui să se asigure că înscrierea clientului pentru și furnizarea inițială a instrumentelor de autentificare necesare pentru a utiliza serviciul de plată internet și / sau livrarea software-ului legat de plată clienților se realizează într-un mod securizat.

3.3.2.12 Incercări de conectare, timpul sesiunii, valabilitatea autentificării

PSP ar trebui să limiteze numărul de conectări sau tentative de autentificare, să definească reguli de time-out pentru sesiunile de servicii pentru plată și să stabilească limitele de valabilitate a autentificării.

3.3.2.13 Monitorizarea tranzacțiilor

Mecanisme de monitorizare a tranzacțiilor destinate a preveni, detecta și bloca tranzacțiile frauduloase de plată ar trebui să fie operate înainte de autorizarea finală PSP; tranzacții suspecte sau de risc ridicat trebuie să facă obiectul unei examinări și procedura de evaluare. Mecanisme echivalente de autorizare și de monitorizare de securitate trebuie să fie, de asemenea, implementate pentru emiterea mandatelor electronice.

3.3.2.14 Protecția datelor de plată cu caracter sensibil

Datele de plată sensibile ar trebui să fie protejate atunci când sunt depozitate, procesate sau transmise.

Măsuri de conștientizare a clienților, educare și comunicare

3.3.2.15 Educarea clienților și comunicarea

PSP ar trebui să ofere asistență și consiliere clienților, acolo unde este necesar, cu privire la utilizarea sigură a serviciilor de plată pe internet. PSP ar trebui să comunice cu clienții lor, astfel încât să le asigure autenticitatea mesajelor primite.

3.3.2.16 Notificări, stabilirea limitărilor

PSP ar trebui să stabilească limitările pentru serviciile de plată prin internet ar putea oferi clienților lor opțiuni pentru limitarea riscului în cadrul acestor limite. Ele pot oferi, de asemenea, alertări și servicii de management de profil ale clienților.

3.3.2.17 Accesul clienților la informații cu privire la statutul inițierii și execuției plății

PSP ar trebui să confirme clienților lor inițierea și să ofere clienților în timp util cu informațiile necesare pentru a verifica dacă o operațiune de plată a fost corect inițiată și / sau executată.

3.3.3 Asigurarea securității aplicațiilor de plăți prin intermediul dispozitivelor mobile

Asigurarea securității aplicațiilor mobile presupune o abordare amplă care să cuprindă măsuri de protecție împotriva diferitelor metode de atac existente. O formă unică și impenetrabilă de securizare a aplicațiilor nu există. Pașii necesari pentru asigurarea nivelului dorit de securitatea al unei aplicații trebuie

implementați înainte ca aceasta să fie distribuită utilizatorilor. Principalele măsuri care asigură securitatea aplicațiilor sunt:

- Stocarea securizată a datelor sensibile sau evitarea stocării acestora
- Managementul responsabil al sesiunilor și mijloacelor de autentificare
- Proiectarea și programarea aplicațiilor pentru utilizarea corectă a instrumentelor de securitate și criptare
- Evitarea scurgerilor neintenționate de informații
- Rezistența la atacurile asupra perioadei de utilizare a procesorului
- Implementarea de măsuri care să prevină ingineria inversă a aplicațiilor și sistemelor de securizare, complexitate și metode anti-manipularea codului

Aceste măsuri se implementează respectând normele comune de bune practici pentru a respinge orice atacuri care ar putea duce la cedarea controlului către un atacator sau la periclitarea confidențialității, integrității și autenticității datelor procesate pe dispozitivele mobile.

4. Perspective ale pieței plăților electronice

Oportunități

În ciuda nivelului ridicat al inovării și creșterea interesului consumatorilor și societăților, platile mobile în Europa Centrală și de Est reprezintă încă o piață tânără. Având în vedere că la sfârșitul anilor '90 de mai multe sisteme mobile de plată au fost lansate într-o varietate de țări europene, inclusiv în unele sisteme disponibile la nivel național. Cu toate acestea, alegerile rămân la fel de uimitoare ca înainte. În scopul de a crește ponderea de plăți mobile este nevoie de o soluție cuprinzătoare.

Plățile mobile sunt de o importanță strategică ca parte a unei tendințe generale față de utilizarea de monedă electronică și limitarea utilizării de numerar, care implică costuri ridicate pentru bănci.

Atunci când piața devine saturată, operatorii de telefonie mobilă vor trebui să caute atât surse de venit cat și instrumente noi de retenție ale clienților. Furnizorii de servicii independenți, pe de altă parte, vor fi în căutarea pentru șansa lor de a castiga o parte din piața cash și non-cash de plăți mobile, servita în mod tradițional de către instituțiile financiare (emitenți, bănci, etc).

Până în prezent, cu toate acestea, piața s-a confruntat cu câteva provocări-cheie care vor trebui să fie abordate în viitorul apropiat, dacă plățile mobile vor să ajungă la potențialul lor în regiune:

- gama limitată de oportunități de plată rezultate ca urmare a ofertei limitate (infrastructură insuficientă) sau cererii limitate (clienți insuficienti);
- dificultăți în îndeplinirea așteptărilor tuturor părților în lanțul de valori, prin urmare, și obținerea rezultatelor scontate financiare, ceea ce duce la afaceri nesustenabile pe termen lung;
- lipsa de unei propuneri de valoare clară și convingătoare pentru utilizatorul final (de exemplu, în cazul în care serviciul a fost prea complicat de utilizat în comparație cu soluțiile tradiționale).

În acest ecosistem complex de operatori, bănci și alți furnizori terți, fiecare parte are interese financiare uneori diferite de a participa la piața plăților mobile.

Indiferent de soluțiile de plată mobilă luate în considerare, exemplele din sondajul nostru sugerează că prima condiție necesară pentru ca inițiativele de plăți mobile să aibă succes colaborarea reciproc avantajoasă a tuturor părților interesate - incluzând atât jucătorii tradiționali în lanțul valoric, cât și ca inovatori.

Provocări

Au fost identificați următorii factori critici de succes pentru implementarea cu succes de soluțiilor de plăți mobile :

- Piața va trebui să atingă etapa critică, atât prin saturarea penetrării telefoniei mobile, precum și prin maturitatea instituțiilor financiare, pentru a crea un mediu care să stimuleze toate părțile interesate, în scopul de a lansa agresiv soluții mobile de plăți mobile.

- Inițiativa trebuie să se bazeze pe un model de afaceri win-win, în cazul în care toate părțile implicate doresc să realizeze beneficii clare într-un domeniu de aplicare definit. După cum noile tehnologii de plăți mobile continuă să combine elemente din ambele industrii - financiar și telecomunicații, un obiectiv central pentru viitor este de a identifica competențele esențiale, rolurile naturale, modelele de afaceri, și strategii pe care diferiții jucători ar putea să le abordeze în lanțul valoric de plăți mobile.

- Soluția propusă de plăți mobile trebuie să ofere o îmbunătățire față de soluțiile existente în termeni de confort, siguranță și cost pentru toate părțile, în special pentru clienți, dar și pentru comercianții și furnizorii de servicii.

- Inițiativa trebuie să obțină adoptarea largă a comerciantului și, astfel, să devină o metodă de plată atractivă pentru un număr mare de consumatori. Cu toate acestea, ne putem imagina că comercianții vor fi reticenți să investească în noua metodă de plată înainte ca acestea să aibă suficientă încredere că m-payments va fi acceptat pe scară largă și, prin urmare, va aduce venituri suplimentare.

Anexa 1: Tipuri de atacuri informatice asupra dispozitivelor mobile

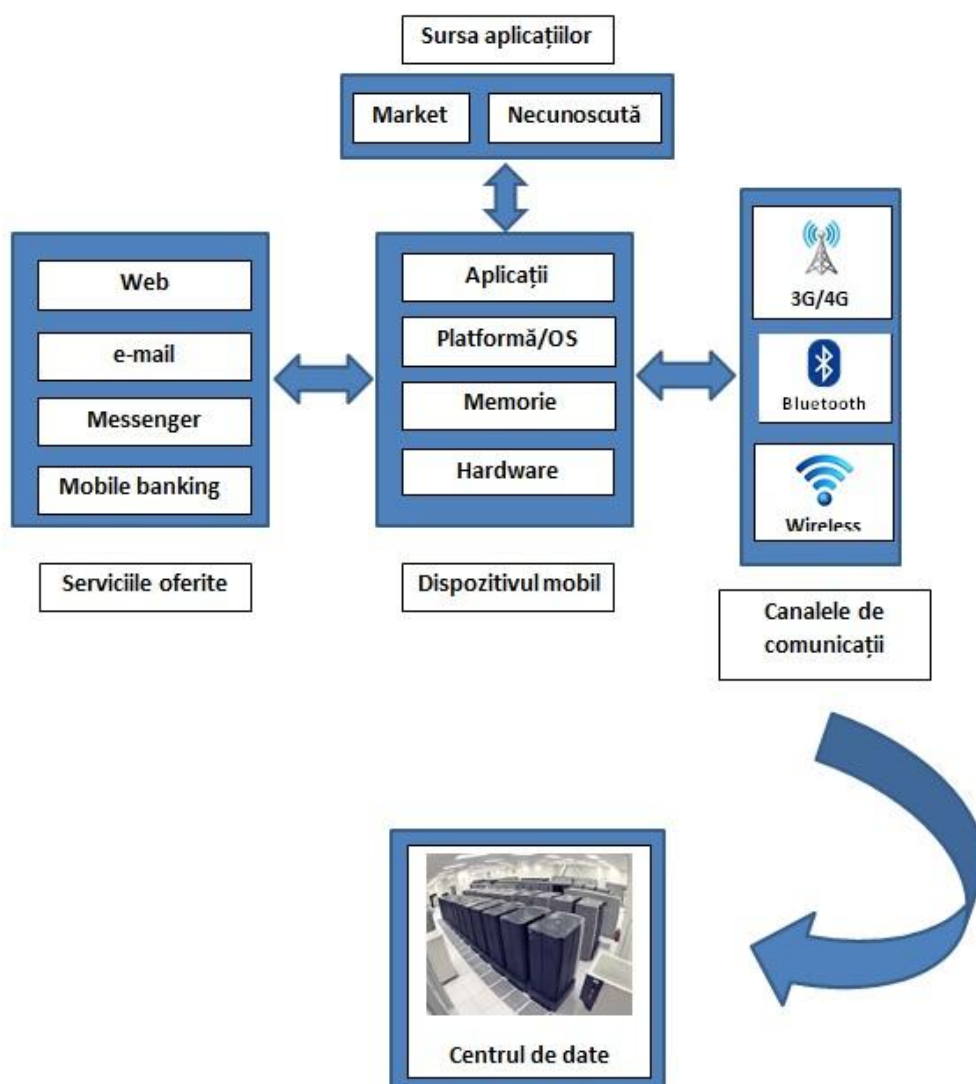
Dispozitivele mobile încorporează tehnologii și funcționalități similare cu un computer. Serviciile oferite de acestea se diversifică pe măsură ce furnizorii de servicii încearcă să rămână permanent în contact cu utilizatorii. Odată cu multitudinea de servicii transferate către dispozitivele mobile se transferă și vulnerabilitățile sistemelor informatice clasice. Atacatorii cibernetici vizează obținerea ilicită de date personale și informații financiare prin exploatarea lipsei de pregătire de securitate a utilizatorilor sau a vulnerabilităților dispozitivelor mobile, rețelelor de comunicații și centrelor de date.

Vectori de atac

Există trei puncte în lanțul tehnologiei mobile unde părțile rău intenționate pot căuta și exploata vulnerabilități pentru a lansa atacuri malițioase:

- Dispozitivul
- Rețeaua de comunicații
- Centrul de date

Acestea sunt prezentate în imaginea de mai jos:



1.1 Dispozitivele mobile

Dispozitivele mobile prezintă riscuri semnificative pentru informațiile sensibile corporative, principalele riscuri includ pierderi de date și compromiterea securității rețelelor interne prin exploatarea dispozitivelor mobile în scopul infectării stațiilor de lucru sau serverelor. Sistemele de operare ale telefoanelor inteligente, iPhone, Android sau altele, oferă atacatorilor o varietate de oportunități prin care pot penetra securitatea dispozitivelor:

- Browser, e-mail
- Telefon / SMS
- Aplicații
- Sistem de operare

1.1.1 Atacuri asupra Browser-ului

Modalitățile de atac asupra Browser-ului includ:

Phishing - Presupune dobândirea ilicită de informații personale, date de autentificare, detalii de carduri bancare, sau utilizarea ilicită a conturilor de e-mail pentru transmiterea de mesaje către potențiale victime. Statisticile arată că utilizatorii de telefoane mobile inteligente sunt de trei ori mai expuși la acest tip de atac, decât utilizatorii sistemelor clasice, iar serviciile financiare reprezintă peste 90% din totalul atacurilor de acest tip. Utilizatorii dispozitivelor mobile prezintă vulnerabilitate ridicată la acest tip de atac datorită dimensiunilor reduse, adresele site-urilor web nu sunt afișate integral și mesajele de alertă pot fi ușor ignorate.

Framing – Implică livrarea unui site Web / WAP într-un iframe (o pagină inclusă în altă pagină), care deschide calea pentru alte tipuri de atacuri, cel mai frecvent și periculos fiind clickjacking.

Clickjacking - Cunoscut și sub numele de UI redressing (redirecționarea interfeței utilizator), clickjacking vizează utilizarea click-urilor/acțiunilor efectuate de utilizatori în interesul atacatorului, divulgarea de date confidențiale, plasarea de comenzi sau preluarea controlului dispozitivului. Clickjacking utilizează o pagină transparentă preîncărcată peste pagina dorită de utilizator sau cod încorporat care se execută fără știrea utilizatorului când acesta face click pe diferite link-uri invizibile. Clickjacking a fost exploatat pe site-uri des utilizate (inclusiv Facebook) pentru a fura informații sau pentru a direcționa utilizatorii către site-uri care plasează cod malițios pe dispozitivele mobile.

Drive-by Download – Atacatorul descarcă un conținut malițios fără știrea utilizatorului, prin inițierea descărcării în momentul accesării unei pagini web sau prin inducerea în eroare a utilizatorului. Sistemul de operare Android, este vulnerabil la acest atac pentru că are opțiunea de a permite instalarea aplicațiilor provenite de la "surse necunoscute".

Man-in-Mobile-(Mitmo) - Permite atacatorilor să acționeze pârghiile malware-ului introdus pe dispozitivele mobile pentru a eluda sistemele de verificare a parolei, care transmit coduri prin SMS pe telefoanele utilizatorilor pentru confirmarea identității în cazul serviciilor de plăți electronice sau pentru a transmite băncii date modificate despre tranzacții (ex: numere de cont schimbate, efectuarea unor tranzacții suplimentare) .

1.1.2 Atacuri bazate pe telefon/SMS

Atacurile bazate pe telefon/SMS includ:

Atacurile Baseband - Atacuri care exploatează vulnerabilitățile procesorului de comunicații din cadrul telefoanelor mobile pentru a executa comenzi, a accesa datele conținute de dispozitivul mobil sau a prelua controlul total al dispozitivului.

SMiShing - Similar cu phishing, dar utilizează telefonul mobil pentru a transmite mesaje de tip text, în loc de mesaje e-mail. Atacatorii încearcă să determine utilizatorii să furnizeze date confidențiale, cum ar fi nume de

utilizator, parole și numere de carduri bancare, prin accesarea de site-uri nelegitime sau apelarea unor numere de telefon la care sunt conectate sisteme automate de răspuns.

Atacuri RF - Bluejacking, utilizarea bluetooth-ului pentru a transmite mesaje către alte dispozitive, atacuri NFC, asupra sistemelor de comunicații prin câmp electromagnetic pe distanțe scurte, și exploatarea vulnerabilităților sistemelor de comunicații pe frecvențe radio utilizate în serviciile dispozitiv-la-dispozitiv (ex: plăți electronice care utilizează cardul bancar prin apropierea acestuia de un dispozitiv conectat la POS).

1.1.3 Atacuri asupra aplicațiilor

Exista trei tipuri de aplicații relativ la dispozitivele mobile:

Web – Aplicațiile de acest tip utilizează tehnologii web standard, HTML5, JavaScript și CSS. Aceste aplicații sunt dezvoltate pentru a putea fi utilizate pe o multitudine de dispozitive mobile. Dezvoltarea acestor aplicații prezintă avantajul compatibilității cu multiple platforme, dar și unele limitări legate de managementul sesiunilor de lucru, securitatea datelor stocate local și accesul la funcționalitatea dispozitivului (cameră, calendar, geolocalizare, etc.).

Native – Sunt aplicațiile specifice pentru o anumită platformă mobilă (iOS sau Android), dezvoltate cu ajutorul instrumentelor și limbajelor de programare suportate de respectiva platformă. Aplicațiile native oferă funcționalitate și aspect de cea mai bună calitate, dar sunt dependente de platforma de operare.

Wrapper (Hybrid) – Reprezintă o combinație între cele două tipuri de aplicații, într-o aplicație nativă este încorporat conținut provenit de la un server web. Acest tip de aplicații oferă utilizatorului funcționalitatea aplicațiilor native cu posibilitatea accesării de conținut web, dar înglobează și vulnerabilitățile de securitate ale celor două tipuri.

Vectorii de atac asupra aplicațiilor includ:

Stocarea datelor sensibile – Statisticile arată că majoritatea aplicațiilor uzuale stochează date în mod nesecurizat. Atacatorii care obțin acces la resursele dispozitivelor mobile pot accesa datele stocate de aceste aplicații.

Lipsa criptării / criptarea slabă – Aplicațiile care permit transmiterea de date necriptate sau slab criptate sunt vulnerabile la atacuri care periclitează confidențialitatea informațiilor.

Validarea incorectă SSL – Implementarea greșită a serviciului SSL de către anumite aplicații (ex: combinarea traficului de informații securizate cu cel al informațiilor nesecurizate) duce la apariția unor erori în procesul de validare al secure socket layer (SSL) care permit încălcări ale securității datelor.

Manipularea configurării – Atacatorul modifică fișiere de configurare care afectează comportamentul aplicațiilor. Include obținerea accesului neautorizat la interfețele de administrare, la fișiere de configurare sau blocarea accesului aplicațiilor la datele de configurare cu scopul preluării controlului asupra aplicației.

Dynamic runtime injection - Permite unui atacator să manipuleze și să abuzeze de runtime-ul unei aplicații (perioada de utilizare a procesorului) pentru a evita măsurile de securitate, codul introdus de atacator rulează cu aceleași drepturi pe care le are și aplicația victimă. Atacatorul obține acces la părțile privilegiate ale unei aplicații și poate lansa aplicații malițioase care să îi permită preluarea controlului dispozitivului sau furtul datelor stocate.

Unintended permissions - Aplicațiile configurate greșit pot deschide calea pentru atacatori, prin acordarea de permisiuni necuvenite la resursele dispozitivului mobil (ex: crearea unor instrucțiuni sau fișiere cu permisiuni nedorite, datorită unor erori în proiectarea aplicațiilor).

Escalated privileges – Exploatarea unor erori de proiectare sau de configurare a sistemelor de operare sau a aplicațiilor pentru a obține acces la resurse care, în mod normal, sunt restricționate pentru utilizatori sau aplicații.

1.1.4 Atacuri asupra sistemului de operare

Punctele de atac OS-based pot include:

Parolă lipsă/slabă - Mulți utilizatori aleg să nu utilizeze o metodă de control al accesului la dispozitivele mobile sau utilizează cod PIN, cod de acces sau model de blocare ușor de ghicit/spart.

iOS Jailbreaking - Jailbreaking dezactivează semnarea codului pe telefoanele iPhone pentru a rula aplicații provenite din alte surse decât App Store. În același timp sunt îndepărtate aproape toate mecanismele de protecție oferite de sistemul iOS. Îndepărtarea semnării codului permite rularea de cod malițios, majoritatea aplicațiilor nesemante rulează la nivel maxim de acces (root) fără mediu propriu de execuție (sandbox) și sunt îndepărtate mecanismele care previn execuția necontrolată a codului, prin permiterea scrierii și execuției în memorie. Astfel, jailbreaking oferă o multitudine de vulnerabilități care pot fi exploatare de atacatorii cibernetici.

Android rooting - Similar cu "Jailbreaking", rooting permite utilizatorilor Android să-și modifice sau schimbe aplicațiile de sistem și setările, să ruleze aplicațiile specializate care necesită permisiuni la nivel de administrator. Ca și "Jailbreaking", această operațiune duce la apariția unui număr ridicat de vulnerabilități.

Parole și date accesibile - Dispozitive cum ar fi linia de dispozitive Apple iOS, au cunoscut vulnerabilități în mecanismele lor criptografice pentru stocarea de parole și date criptate. Un atacator poate exploata aceste vulnerabilități pentru a penetra sistemul de management al parolelor (keychain), expunând parolele utilizatorilor, cheile de criptare și alte date private.

Aplicații preinstalate de furnizorul de servicii mobile – Software-ul preinstalat pe dispozitive poate conține probleme de securitate. Recent, în unele aplicații pre-încărcate pe telefoanele Android, și nu numai, au fost identificate vulnerabilități de securitate care ar putea fi utilizate pentru a șterge telefonul, fura date și chiar asculta ilegal convorbirile telefonice.

Zero-day exploits - Atacuri care se desfășoară în intervalul de timp dintre momentul în care o vulnerabilitate este exploatată pentru prima dată și momentul în care dezvoltatorii de software sunt în măsură să emită un comunicat cu măsuri de contracarare a problemei de securitate.

1.2 Rețeaua de comunicații

Punctele de atac bazate pe rețeaua de comunicații pot include:

Wi-Fi (criptare slabă / fără criptare) – Confidențialitatea datelor este în pericol atunci când se transmit date prin intermediul rețelelor wireless dacă nu sunt utilizate sisteme de criptare a datelor sau cele implementate sunt vulnerabile la atacuri. Un anumit nivel de protecție se obține prin utilizarea protocoalelor SSL/TLS, dar modul de proiectare al unor aplicații (în special unele sisteme de e-banking) prezintă vulnerabilități care pot fi exploatare de atacatori pentru a obține date critice ale utilizatorilor.

Rogue access points – Acest tip de atac presupune instalarea unui punct de acces wireless de către o persoană neautorizată în interiorul unei organizații. Sunt două tipuri de atacuri care utilizează instalarea neautorizată a unui punct de acces wireless. Conectarea la rețeaua securizată a organizației pentru a oferi acces atacatorului din exteriorul acesteia sau simularea rețelei wireless a organizației cu scopul obținerii datelor de autentificare ale utilizatorilor.

Packet sniffing - Permite unui intrus rău intenționat captura și analiza traficului de rețea. Atacatorul monitorizează și înregistrează toate datele transmise printr-o rețea, wireless sau prin cablu, în scopul analizei ulterioare pentru a obține date confidențiale care pot fi valorificate (ex: informații bancare, conturi de acces în sistemele informatice).

Man-in-the-middle (MITM) – Implică interpunerea atacatorului între două părți ale unei comunicații care are loc într-o rețea. Atacatorul interceptează traficul și modifică informațiile transmise fără știrea interlocutorilor. Aceștia pot fi sistemele a doi utilizatori sau pot fi de tip client/server, în acest caz obiectivul atacatorului îl

reprezintă obținerea datelor de conectare la server ale utilizatorului sau modificarea informațiilor transmise în beneficiul său (ex: modificarea unei tranzacții bancare pentru a transmite fonduri în conturile sale fără știrea utilizatorului).

SSLStrip - O formă de atac man-in-the-middle care exploatează slăbiciuni în implementarea SSL/TLS pe site-uri web, care nu folosesc metode de control pentru a verifica existența unei conexiuni HTTPS. Atacul retrogradează conexiunile la HTTP, fără criptare, utilizatorii nu observă modificarea sau nu pot ști când este cazul să fie utilizată o conexiune HTTPS, mai sigură.

Session hijacking - Presupune exploatarea unei chei de sesiune valide pentru a avea acces neautorizat la informații și servicii de rețea. Este o vulnerabilitate frecventă la site-urile/aplicațiile web care utilizează cookie-uri pentru a menține activă conexiunea utilizatorului la server, deoarece un atacator poate fura acest cookie, printr-un computer intermediar sau dacă obține acces direct la spațiul de memorie unde browser-ul salvează aceste cookie-uri.

DNS poisoning – Atacatorul redirecționează utilizatorul aplicațiilor web către site-uri malițioase, fără știrea utilizatorului. Acest tip de atac presupune coruperea tabelor de adresare ale serverelor DNS sau simularea unui DNS valid care să răspundă solicitărilor aplicației client utilizate. Acest tip de atac urmărește obținerea combinațiilor utilizator/parolă pentru aplicații și servicii on-line.

HOSTS file poisoning – Atac similar cu DNS poisoning, dar localizat la nivelul sistemului de operare. În urma infectării cu soft malițios diferite adrese uzuale din fișierul HOSTS sunt modificate pentru a direcționa utilizatorii către site-uri cu reclame sau care urmăresc obținerea de informații sensibile ale utilizatorilor (ex; redirecționarea către site-uri de phishing pentru obținerea datelor bancare).

1.3 Centrul de Date

Atacatorii care vizează centrele de date utilizează două puncte principale de atac:

- Serverele Web
- Bazele de date

1.3.1 Atacuri asupra serverelor Web

Vulnerabilități ale platformelor - Sistemul de operare, software-ul de tip server sau module de aplicații care rulează pe serverul de web prezintă vulnerabilități care pot fi exploatare de un atacator. Monitorizarea comunicațiilor dintre serverele web și dispozitivele mobile poate ajuta atacatorii să descopere aceste vulnerabilități.

Configurarea necorespunzătoare a serverului – Serverele web sau de aplicații au configurații implicite care permit acces la diferite resurse și servicii. Necontrolate aceste configurații pot permite atacatorilor să ocolească măsurile de securitate instalate și configurate corespunzător. Este foarte important ca toate aspectele configurației să fie verificate și reglate corespunzător de administratori.

Cross-site scripting (XSS) – Implică injectarea de cod malițios într-o pagină web, pentru a fi executat când utilizatorii accesează pagina respectivă. Atacatorul urmărește ocolirea sistemelor de control acces prin utilizarea browserului utilizatorului.

Cross-site Request Forgery (CSRF) – Este un mod de exploatare a vulnerabilităților siteurilor web pentru a accesa un server cu drepturile utilizatorului victimă, încrederea pe care serverul o are în utilizatorul respectiv este utilizată de atacator în scopuri proprii (ex: o comandă ascunsă sub un link este executată fără știrea utilizatorului atunci când acesta încearcă să acceseze acel link).

Weak input validation - Atunci când aplicațiile nu validează corespunzător datele introduse de utilizator, un atacator poate modifica aceste date într-o formă specifică, diferită de cea normală pentru funcționarea aplicației. Astfel, atacatorul trimite comenzi neintenționate sistemului, obține acces neautorizat la resurse sau modifică modul de operare al aplicației.

Brute-force attacks – Atacurile de acest tip sunt efectuate asupra sistemelor criptografice care nu prezintă vulnerabilități ce pot fi exploate pentru spargerea lor. Ele presupun introducerea sistematică a tuturor combinațiilor posibile de chei, până este descoperită cea corectă. Șansele de reușită scad cu cât cheia de criptare este mai complexă, conține un număr mai mare de caractere și nu este alcătuită din cuvinte uzuale.

1.3.2. Atacuri asupra bazelor de date

SQL injection (introducerea de cod SQL) – Utilizat pentru a forța o bază de date să returneze rezultate neintenționate de către proiectant. Prin exploatarea lipsei de filtrare a datelor introduse de utilizatori și transmiterii acestora direct către baza de date, atacatorul poate introduce comenzi SQL pe care sistemul de gestiune al bazei de date le execută.

Executarea de comenzi asupra sistemului de operare – Sistemele de gestiune a bazelor de date asigură dezvoltatorilor de aplicații posibilitatea să interacționeze cu resursele și serviciile sistemului de operare în cadrul căruia funcționează. Prin exploatarea unor vulnerabilități ale aplicațiilor, atacatorul obține posibilitatea de a executa comenzi în sistemul de operare și îi deschide acestuia calea spre obținerea controlului asupra acestuia.

Privilege escalation – Exploatarea unor erori de proiectare sau de configurare a bazelor de date pentru a obține acces la resurse care, în mod normal, sunt restricționate pentru utilizatori sau aplicații.

Data dumping – Este procesul utilizat pentru depanarea sau refacerea bazelor de date. Acesta permite exportarea conținutului și structurii unei baze de date sub formă de cod SQL. Prin exploatarea unor vulnerabilități, atacatorii pot compromite confidențialitatea datelor.

Anexa 2: Statistici plăți

2.1 Statistici la nivel național

Data	Valoare tranzacții de plată cu carduri cu funcție de debit	Valoare tranzacții de plată cu carduri cu funcție de debit amanat	Valoare tranzacții de plată cu carduri cu funcție de credit	Valoare tranzacții de retragere numerar de la ATM din țară cu carduri emise în țară	Valoare tranzacții de depunere numerar la ATM din țară cu carduri emise în țară	Valoare tranzacții la POS din țară cu carduri emise în țară
	(milioane lei)	(milioane lei)	(milioane lei)	(milioane lei)	(milioane lei)	(milioane lei)
dec. 2012	5.711,44	26,59	1.214,47	28.597,76	1.278,78	5.287,67
sep. 2012	5.293,04	26,41	1.091,26	27.427,95	1.309,03	4.501,44
iun. 2012	4.731,28	28,47	1.002,43	26.472,91	1.212,70	4.358,28
mar. 2012	4.361,97	26,92	880,63	23.910,47	1.064,53	3.820,50
dec. 2011	4.750,63	30,83	986,59	25.635,74	1.171,49	4.424,66
sep. 2011	4.413,28	28,32	904,61	25.084,20	1.136,80	3.744,08
iun. 2011	4.040,78	29,63	831,49	24.119,40	1.042,02	3.605,72
mar. 2011	3.633,30	28,47	750,29	21.595,90	930,43	3.080,08
dec. 2010	3.844,05	20,00	724,11	22.549,01	933,44	3.396,29
sep. 2010	3.593,64	17,91	654,94	22.293,70	930,46	2.923,75
iun. 2010	3.290,72	18,22	588,93	22.402,45	923,51	2.856,91
mar. 2010	2.983,11	16,72	531,29	20.257,17	839,84	2.552,12
dec. 2009	3.181,22	15,39	628,56	21.749,95	892,24	3.157,24
sep. 2009	3.036,60	14,21	606,63	21.621,59	867,31	2.781,93
iun. 2009	2.883,41	14,36	572,99	21.422,80	876,17	2.723,11
mar. 2009	2.654,22	14,07	508,26	19.951,53	764,53	2.421,86
dec. 2008	3.284,01	59,34	897,42	21.750,47	840,62	2.896,46
sep. 2008	3.083,41	58,61	705,28	21.083,32	716,08	2.551,13
iun. 2008	2.700,41	57,83	623,21	19.415,91	699,08	2.229,84
mar. 2008	2.285,31	51,35	547,96	16.575,80	588,91	1.714,19

Sursa: Banca Națională a României

Indicatori privind cardurile și numărul de terminale

Data	Valoare tranzacții de retragere de numerar de la ATM din țară cu carduri emise în afara țării	Valoare tranzacții de depunere de numerar la ATM din țară cu carduri emise în afara țării	Valoare tranzacții la POS din țară cu carduri emise în afara țării	Valoare tranzacții de retragere de numerar de la ATM din afara țării cu carduri emise în țară	Valoare tranzacții de depunere de numerar la ATM din afara țării cu carduri emise în țară	Valoare tranzacții la POS din afara țării cu carduri emise în țară
	<i>(milioane lei)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>
dec. 2012	820,12	0,00	406,12	560,22	0,00	1.228,82
sep. 2012	1.087,49	0,00	459,86	557,88	0,00	1.347,14
iun. 2012	755,75	0,00	353,80	512,71	0,00	1.154,84
mar. 2012	629,60	0,00	255,32	457,73	0,00	1.085,65
dec. 2011	702,23	0,00	308,95	479,09	0,00	1.031,62
sep. 2011	955,74	0,00	388,56	483,28	0,00	1.177,83
iun. 2011	649,35	0,00	319,41	409,10	0,00	960,06
mar. 2011	514,54	0,00	227,07	371,44	0,00	925,44
dec. 2010	566,93	0,00	257,14	393,74	0,00	869,01
sep. 2010	821,64	0,00	300,08	379,74	0,00	953,80
iun. 2010	539,96	0,00	229,85	320,74	0,00	761,87
mar. 2010	520,51	0,00	183,84	284,11	0,00	729,71
dec. 2009	548,05	0,00	293,17	300,25	0,00	674,45
sep. 2009	752,80	0,00	328,75	324,72	0,00	771,09
iun. 2009	551,32	0,00	232,91	275,24	0,00	574,52
mar. 2009	451,25	0,00	185,04	263,56	0,00	570,50
dec. 2008	421,18	0,00	232,44	300,70	0,00	600,71
sep. 2008	562,41	0,00	200,22	321,83	0,00	687,15
iun. 2008	455,62	0,00	174,71	263,10	0,00	563,49
mar. 2008	389,99	0,00	171,28	209,20	0,00	496,87

Sursa: Banca Națională a României

Data	Număr tranzacții de retragere numerar de la ATM din țară cu carduri emise în țară	Număr tranzacții de depunere numerar la ATM din țară cu carduri emise în țară	Număr tranzacții la POS din țară cu carduri emise în țară	Număr tranzacții de retragere de numerar de la ATM din țară cu carduri emise în afara țării
	(milioane)	(milioane)	(milioane)	(milioane)
dec. 2012	57,07	1,59	37,80	1,22
sep. 2012	56,59	1,56	33,86	1,64
iun. 2012	57,41	1,57	33,41	1,19
mar. 2012	53,25	1,54	30,82	1,00
dec. 2011	55,06	1,59	31,29	1,05
sep. 2011	55,00	1,49	28,21	1,53
iun. 2011	55,20	1,51	27,31	1,07
mar. 2011	50,71	1,47	24,67	0,85
dec. 2010	52,07	1,34	24,41	0,95
sep. 2010	51,93	1,24	22,34	1,32
iun. 2010	53,58	1,30	21,64	0,93
mar. 2010	50,04	1,28	19,55	1,04
dec. 2009	52,26	1,27	21,30	0,93
sep. 2009	52,34	1,17	19,49	1,35
iun. 2009	54,09	1,20	18,90	0,97
mar. 2009	51,07	1,14	17,21	0,92
dec. 2008	53,69	1,08	17,68	0,75
sep. 2008	52,16	0,89	16,16	1,10
iun. 2008	51,84	0,86	14,26	0,94
mar. 2008	45,99	0,78	11,58	0,93

Sursa: Banca Națională a României

Data	Număr tranzacții la POS din țară cu carduri emise în afara țării	Număr tranzacții de retragere de numerar de la ATM din afara țării cu carduri emise în țară	Număr tranzacții la POS din afara țării cu carduri emise în țară
	<i>(milioane)</i>	<i>(milioane)</i>	<i>(milioane)</i>
dec. 2012	1,42	0,67	4,12
sep. 2012	1,61	0,72	4,13
iun. 2012	1,19	0,67	3,61
mar. 2012	0,89	0,59	3,51
dec. 2011	1,00	0,62	3,36
sep. 2011	1,54	0,67	3,61
iun. 2011	1,17	0,58	3,09
mar. 2011	0,83	0,50	2,98
dec. 2010	0,87	0,51	2,75
sep. 2010	1,07	0,54	2,79
iun. 2010	0,70	0,45	2,30
mar. 2010	0,54	0,39	2,22
dec. 2009	0,71	0,40	2,00
sep. 2009	0,90	0,47	2,15
iun. 2009	0,72	0,39	1,74
mar. 2009	0,53	0,35	1,66
dec. 2008	0,79	0,40	1,65
sep. 2008	0,73	0,47	1,85
iun. 2008	0,69	0,36	1,48
mar. 2008	0,77	0,29	1,29

Sursa: Banca Națională a României

Data	Număr tranzacții de transfer credit	Număr tranzacții cu cecuri (inclusiv bilete la ordin)	Număr tranzacții de debitare directă	Număr tranzacții cu alte instrumente de plată	Valoare tranzacții de transfer credit	Valoare tranzacții cu cecuri (inclusiv bilete la ordin)	Valoare tranzacții de debitare directă	Valoare tranzacții cu alte instrumente de plată (inclusiv cambii)
	<i>(milioane)</i>	<i>(milioane)</i>	<i>(milioane)</i>	<i>(milioane)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>	<i>(milioane lei)</i>
2011	181,38	6,57	3,87	0,01	5.965.563,93	68.127,70	5.391,22	488,09
2010	185,79	10,79	1,67	0,01	5.349.346,71	91.191,77	3.416,23	1.702,16
2009	187,40	9,01	3,60	0,01	4.879.282,79	61.011,39	3.696,29	940,55
2008	179,09	10,75	6,71	0,02	5.873.561,27	90.457,99	2.391,56	2.235,50
2007	258,28	11,43	10,22	0,10	4.870.864,13	75.777,27	1.270,01	1.619,69

Sursa: Banca Națională a României

2.2 Statistici plăți la nivel european

Numar tranzactii per tip de instrument					
Austria	2007	2008	2009	2010	2011
Plati	↑ 985	↑ 961	↑ 950	↑ 959	↑ 1,002.00
Plati suport hartie	↗ 175	↗ 162	↗ 151	↗ 147	↗ 145
Plati electronice	↗ 810	↗ 799	↗ 799	↑ 812	↑ 857
Direct debits	↗ 719	↗ 794	↑ 841	↑ 843	↑ 871
Tranzactii cu carduri	↗ 315.68	↗ 344.29	↗ 383.61	↗ 421.54	↗ 446.36
CEC-uri	↘ 3	↘ 3	↘ 2	↘ 2	↘ 2
Alte instrumente de plata	↘ 5.55	↘ 8.14	↘ 10.51	↘ 14.3	↘ 15.59
Total general	↑ 2,057.51	↑ 2,139.37	↑ 2,214.18	↑ 2,266.45	↑ 2,363.10
Belgia	2007	2008	2009	2010	2011
Plati	↑ 897.56	↑ 925.58	↑ 953.26	↑ 1,005.50	↑ 1,025.31
Plati suport hartie	↗ 113.58	↗ 108.85	↘ 89.59	↘ 65.76	↘ 39.56
Plati electronice	↗ 783.98	↑ 816.73	↑ 863.67	↑ 939.75	↑ 985.76
Direct debits	↗ 239.98	↗ 247.94	↗ 260.27	↗ 246.02	↗ 264.55
Tranzactii cu carduri	↑ 861.49	↑ 934.09	↑ 997.4	↑ 1,066.89	↑ 1,154.32
CEC-uri	↘ 10.59	↘ 8.82	↘ 7.94	↘ 7.2	↘ 6.5
Alte instrumente de plata	↘ 0.27	↘ 0.22	↘ 0.18	↘ 0.16	↘ 0.12
Total general	↑ 2,099.71	↑ 2,197.82	↑ 2,289.54	↑ 2,386.39	↑ 2,501.31
Cipru	2007	2008	2009	2010	2011
Plati	↘ 12.93	↗ 20.911	↗ 23.163	↗ 25.495	↗ 26.256
Plati suport hartie	↘ 5.96	↘ 6.507	↘ 6.446	↘ 6.676	↘ 7.4
Plati electronice	↘ 6.97	↘ 14.404	↘ 16.717	↘ 18.819	↘ 18.856
Direct debits	↘ 11.76	↘ 8.074	↘ 7.285	↘ 7.898	↘ 7.7
Tranzactii cu carduri	↗ 25.87	↗ 30.19	↗ 31.871	↗ 35.775	↗ 38.958
CEC-uri	↗ 26.19	↗ 25.724	↗ 23.494	↗ 22.56	↗ 20.084
Alte instrumente de plata	↓ 0	↓ 0	↓ 0	↓ 0	↓ 0
Total general	↗ 76.86	↗ 84.899	↗ 85.813	↗ 91.728	↗ 93.696
Germania	2007	2008	2009	2010	2011
Plati	↑ 5,595.48	↑ 5,681.80	↑ 5,829.45	↑ 5,871.19	↑ 6,090.12
Plati suport hartie	↑ 1,095.92	↑ 1,056.40	↑ 997.67	↑ 940.14	↑ 896.88
Plati electronice	↑ 4,499.56	↑ 4,625.40	↑ 4,831.78	↑ 4,931.05	↑ 5,193.24
Direct debits	↑ 7,677.23	↑ 7,914.26	↑ 8,197.95	↑ 8,697.12	↑ 8,661.41
Tranzactii cu carduri	↑ 2,148.20	↑ 2,313.06	↑ 2,459.18	↑ 2,678.08	↑ 2,947.89
CEC-uri	↗ 75.48	↗ 65.42	↗ 57.02	↗ 48.27	↗ 40.49
Alte instrumente de plata	↓ 0	↓ 0	↓ 0	↓ 0	↓ 0
Total general	↑ 15,548.21	↑ 16,021.96	↑ 16,586.68	↑ 17,333.60	↑ 17,775.92
Estonia	2007	2008	2009	2010	2011
Plati	↗ 89.49	↗ 100.06	↗ 97.21	↗ 96.92	↗ 97.33
Plati suport hartie	↘ 2.95	↘ 3.14	↘ 2.62	↘ 1.93	↘ 1.74
Plati electronice	↗ 86.55	↗ 96.92	↗ 94.59	↗ 95	↗ 95.59
Direct debits	↘ 16.13	↘ 17.84	↘ 18.67	↘ 18.88	↘ 18.87
Tranzactii cu carduri	↗ 130.84	↗ 148.33	↗ 155.47	↗ 167.36	↗ 197.39
CEC-uri	↘ 0.01	↘ 0.01	↓ 0	↓ 0	↓ 0
Alte instrumente de plata	↘ 0.01	↘ 0.01	↓ 0	↓ 0	↓ 0
Total general	↗ 236.48	↗ 266.25	↗ 271.36	↗ 283.16	↗ 313.59
Spania	2007	2008	2009	2010	2011
Plati	↗ 733	↗ 780.43	↗ 808.74	↗ 807.93	↑ 812.34
Plati suport hartie	↗ 108.09	↗ 111.5	↗ 112.41	1 1 3.45	↗ 111.44
Plati electronice	↗ 624.92	↗ 668.93	↗ 696.33	↗ 694.47	↗ 700.9
Direct debits	↑ 2,222.26	↑ 2,308.85	↑ 2,431.32	↑ 2,364.86	↑ 2,210.98
Tranzactii cu carduri	↑ 1,945.66	↑ 2,098.36	↑ 2,157.01	↑ 2,286.90	↑ 2,386.27
CEC-uri	↗ 153.46	↗ 136.04	↗ 113.35	↗ 103.49	↗ 94.65
Alte instrumente de plata	↗ 70.34	↗ 61.69	↗ 46.56	↗ 39.02	↗ 31.53
Total general	↑ 5,125.32	↑ 5,385.77	↑ 5,557.34	↑ 5,602.48	↑ 5,535.92

Finlanda	2007	2008	2009	2010	2011
Plati	↗ 701	↗ 749	↗ 773	↗ 861.23	↗ 1,009.32
Plati suport hartie	↗ 47	↗ 46	↗ 34	↗ 39.35	↘ 11.65
Plati electronice	↗ 654	↗ 703	↗ 739	↗ 821.88	↗ 997.66
Direct debits	↗ 76	↗ 82	↗ 84	↗ 84	↗ 81.85
Tranzactii cu carduri	↗ 918	↗ 992	↗ 899	↗ 1,040.00	↗ 1,091.82
CEC-uri	↘ 0.6	↘ 0.6	↘ 0.5	↘ 0.4	↘ 0.38
Alte instrumente de plata	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Total general	↗ 1,695.60	↗ 1,823.60	↗ 1,756.50	↗ 1,985.63	↗ 2,183.36
Franta	2007	2008	2009	2010	2011
Plati	↗ 2,614.12	↗ 2,697.30	↗ 2,789.45	↗ 2,989.65	↗ 2,977.54
Plati suport hartie	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Plati electronice	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Direct debits	↗ 2,909.78	↗ 3,023.63	↗ 3,265.48	↗ 3,411.19	↗ 3,533.32
Tranzactii cu carduri	↗ 6,144.66	↗ 6,542.50	↗ 6,923.25	↗ 7,391.64	↗ 7,911.01
CEC-uri	↗ 3,650.41	↗ 3,487.44	↗ 3,302.56	↗ 3,122.80	↗ 2,971.44
Alte instrumente de plata	↗ 114.27	↗ 110.42	↗ 105.53	↗ 101.11	↗ 98.45
Total general	↗ 15,459.67	↗ 15,893.46	↗ 16,422.32	↗ 17,057.49	↗ 17,538.26
Grecia	2007	2008	2009	2010	2011
Plati	↗ 34.52	↗ 43.54	↗ 54.76	↗ 63.39	↗ 68.97
Plati suport hartie	↘ 12.55	↘ 18.78	↘ 18.87	↘ 16.64	↘ 18.9
Plati electronice	↗ 21.98	↗ 24.76	↗ 35.9	↗ 46.75	↗ 50.07
Direct debits	↘ 17.87	↘ 12.25	↘ 14.03	↘ 17.04	↗ 21.61
Tranzactii cu carduri	↗ 77.54	↗ 85.34	↗ 84.47	↗ 78.99	↗ 74.85
CEC-uri	↗ 29.46	↗ 28.81	↗ 25.33	↗ 22.6	↗ 19.43
Alte instrumente de plata	↘ 1.12	↘ 0.91	↘ 0.74	↘ 0.54	↘ 0.42
Total general	↗ 161.04	↗ 171.73	↗ 181.14	↗ 185.11	↗ 189.23
Irlanda	2007	2008	2009	2010	2011
Plati	↗ 147.92	↗ 154.42	↗ 155.86	↗ 155.57	↗ 152.33
Plati suport hartie	↗ 19.82	↗ 19.12	↘ 18.26	↘ 17.07	↘ 16.07
Plati electronice	↗ 128.1	↗ 135.3	↗ 137.6	↗ 138.5	↗ 136.26
Direct debits	↗ 109.1	↗ 112.5	↗ 110.9	↗ 108	↗ 107.01
Tranzactii cu carduri	↗ 262.34	↗ 318.05	↗ 323.4	↗ 333.29	↗ 339.2
CEC-uri	↗ 124.6	↗ 117.2	↗ 101.8	↗ 90.9	↗ 84.21
Alte instrumente de plata	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Total general	↗ 643.96	↗ 702.17	↗ 691.96	↗ 687.76	↗ 682.75
Italia	2007	2008	2009	2010	2011
Plati	↗ 1,094.72	↗ 1,062.86	↗ 1,204.56	↗ 1,227.20	↗ 1,261.72
Plati suport hartie	↗ 783.74	↗ 743.95	↗ 794.76	↗ 762.48	↗ 765.33
Plati electronice	↗ 310.98	↗ 318.91	↗ 409.8	↗ 464.73	↗ 496.4
Direct debits	↗ 508.79	↗ 554.08	↗ 575.83	↗ 593.17	↗ 600.7
Tranzactii cu carduri	↗ 1,329.26	↗ 1,395.92	↗ 1,471.46	↗ 1,502.41	↗ 1,566.87
CEC-uri	↗ 426.38	↗ 384.93	↗ 335.2	↗ 315.43	↗ 291.62
Alte instrumente de plata	↗ 351.54	↗ 345.87	↗ 280.68	↗ 247.94	↗ 286.77
Total general	↗ 3,760.26	↗ 3,816.22	↗ 3,957.44	↗ 4,004.43	↗ 4,159.58
Luxembourg	2007	2008	2009	2010	2011
Plati	↗ 59.72	↗ 62.96	↗ 65.07	↗ 66.8	↗ 68.9
Plati suport hartie	↘ 13.27	↘ 12.75	↘ 12.02	↘ 11.66	↘ 11.77
Plati electronice	↗ 46.45	↗ 50.21	↗ 53.05	↗ 55.13	↗ 57.13
Direct debits	↘ 12.89	↘ 14.08	↘ 14.92	↘ 15.72	↘ 16.72
Tranzactii cu carduri	↗ 45.4	↗ 50.2	↗ 54.37	↗ 65.01	↗ 71.36
CEC-uri	↘ 0.24	↘ 0.21	↘ 0.21	↘ 0.19	↘ 0.2
Alte instrumente de plata	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Total general	↗ 120.66	↗ 436.23	↗ 543	↗ 703.47	↗ 927.84

Sursa: ECB Payment Statistics 04.09.2012

Malta	2007	2008	2009	2010	2011
Plati	↗ 4.364	↗ 4.928	↗ 5.513	↗ 6.103	↗ 6.897
Plati suport hartie	↗ 0.621	↗ 0.593	↗ 0.305	↗ 0.217	↗ 0.23
Plati electronice	↗ 3.743	↗ 4.335	↗ 5.208	↗ 5.886	↗ 6.667
Direct debits	↗ 0.782	↗ 1.054	↗ 1.196	↗ 1.214	↗ 1.332
Tranzactii cu carduri	↗ 8.154	↗ 10.125	↗ 11.241	↗ 12.987	↗ 13.835
CEC-uri	↗ 13.089	↗ 11.941	↗ 11.373	↗ 10.269	↗ 9.745
Alte instrumente de plata	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Total general	↗ 26.389	↗ 28.048	↗ 29.323	↗ 30.573	↗ 31.83
Olanda	2007	2008	2009	2010	2011
Plati	↗ 1,483.65	↗ 1,544.16	↗ 1,497.09	↗ 1,640.30	↗ 1,686.33
Plati suport hartie	↗ 159.5	↗ 143.49	↗ 123.86	↗ 105.57	↗ 93.12
Plati electronice	↗ 1,324.15	↗ 1,400.66	↗ 1,373.22	↗ 1,534.73	↗ 1,593.21
Direct debits	↗ 1,176.94	↗ 1,225.54	↗ 1,272.13	↗ 1,310.15	↗ 1,340.38
Tranzactii cu carduri	↗ 1,695.06	↗ 1,874.11	↗ 2,067.71	↗ 2,294.28	↗ 2,444.28
CEC-uri	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Alte instrumente de plata	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Total general	↗ 4,530.48	↗ 4,819.93	↗ 5,013.98	↗ 5,422.99	↗ 5,647.85
Portugalia	2007	2008	2009	2010	2011
Plati	↗ 151.98	↗ 164.64	↗ 180.59	↗ 182.57	↗ 201.99
Plati suport hartie	↗ 15.19	↗ 16.6	↗ 17.64	↗ 18.34	↗ 19.39
Plati electronice	↗ 136.8	↗ 148.04	↗ 162.95	↗ 164.23	↗ 182.6
Direct debits	↗ 185.2	↗ 223.13	↗ 231.91	↗ 236.94	↗ 243.04
Tranzactii cu carduri	↗ 952.6	↗ 1,006.31	↗ 1,069.49	↗ 1,170.47	↗ 1,237.47
CEC-uri	↗ 189.2	↗ 167.88	↗ 144.08	↗ 127.53	↗ 106.66
Alte instrumente de plata	↗ 0.92	↗ 0.8	↗ 0.66	↗ 0.5	↗ 0.41
Total general	↗ 1,481.55	↗ 1,564.75	↗ 1,628.92	↗ 1,720.13	↗ 1,791.74
Slovenia	2007	2008	2009	2010	2011
Plati	↗ 177.33	↗ 171.05	↗ 164.66	↗ 167.72	↗ 167.37
Plati suport hartie	↗ 76.55	↗ 72.94	↗ 65.98	↗ 68.05	↗ 60.65
Plati electronice	↗ 100.78	↗ 98.12	↗ 98.68	↗ 99.67	↗ 106.72
Direct debits	↗ 41.73	↗ 41.51	↗ 46.3	↗ 50	↗ 51.43
Tranzactii cu carduri	↗ 104.41	↗ 108.64	↗ 110.89	↗ 116.84	↗ 120.81
CEC-uri	↗ 0.29	↗ 0.32	↗ 0.27	↗ 0.21	↗ 0.14
Alte instrumente de plata	↗ 0.02	↗ 0.01	↗ 0.01	↘ 0	↘ 0
Total general	↗ 323.8	↗ 321.52	↗ 322.13	↗ 334.78	↗ 339.75
Slovacia	2007	2008	2009	2010	2011
Plati	↗ 261.59	↗ 210.7	↗ 229.45	↗ 252.36	↗ 278.07
Plati suport hartie	↗ 41.27	↗ 30.24	↗ 24.87	↗ 20.99	↗ 14.97
Plati electronice	↗ 220.31	↗ 180.46	↗ 204.58	↗ 231.36	↗ 263.1
Direct debits	↗ 65.06	↗ 60.96	↗ 70.59	↗ 69.59	↗ 73.19
Tranzactii cu carduri	↗ 72.86	↗ 87.33	↗ 114.39	↗ 129.49	↗ 152.61
CEC-uri	↗ 0.09	↗ 0.08	↗ 0.06	↗ 0.05	↗ 0.05
Alte instrumente de plata	↘ 0	↘ 0	↘ 0	↘ 0	↘ 0
Total general	↗ 399.6	↗ 359.07	↗ 414.5	↗ 451.51	↗ 503.97

Sursa: ECB Payment Statistics 04.09.2012

Anexa 3: Principalele metode de plată per țară pentru cumpărături online la nivel european

Austria

În Austria sunt folosite mai multe metode de plată online. ELV precum și metoda de plată multibank EPS (Standard Electronic de Plăți) reprezintă mai mult de o treime din toate plățile online. EPS este unul dintre mijloacele cele mai populare de plată pentru cumpărături online în Austria, 80% din toți comercianții utilizează EPS în magazinele lor.

Belgia

În Belgia consumatorii utilizează în principal carduri și metode de plată online bancare pentru plăți online. În special, fraudarea cărților de credit pe Internet aproape că s-a dublat în ultimii trei ani, în Belgia, potrivit unui reprezentant al Unității Federale de Criminalitate Informatică (FCCU). Numărul de belgieni care au cardurile lor de credit utilizate în mod fraudulos pe internet a ajuns la câteva mii în fiecare an, dar cifrele exacte nu au fost dezvăluite.

Bulgaria

Dintr-un total de 82% de posesori de carduri bulgari care folosesc internetul, 33% dintre aceștia achită facturile online sau fac achiziții prin intermediul site-urilor online

Republica Cehă

Consumatorii cehi, la fel ca alții din Europa Centrală și de Est, în marea lor majoritate fac plăți în numerar, urmate de transferuri bancare și cărți de credit. E-portofelele și cartelele pre-plătite sunt, de asemenea, utilizate. Pe o bază comparativă, situația din țările occidentale este inversată, metoda de plată dominantă este cardul de credit (pentru aproape 80% din cazuri). Băncile din Republica Cehă încearcă să implementeze pe scară largă sisteme online, care le permit să ofere plăți on-line și, de asemenea o taxă de mai favorabilă decât în cazul unui card de credit.

Danemarca

Cardurile de credit și de debit sunt utilizate pentru marea majoritate a plăților online în Danemarca (89%). Alte metode de plată utilizate în Danemarca sunt metodele plată online, prin internet banking sau în numerar la livrare.

Finlanda

În Finlanda transferurile bancare online sunt frecvent utilizate pentru a plăti online. Serviciile sunt oferite de bănci individuale, cum ar fi Nordea, Sampo, OKO și Aktia. Acestea sunt urmate de carduri, facturi, plata la livrare, e-portofelele și plăți mobile. Consumatorii nordici decid cu privire la metoda de plată online în funcție de ușurința de utilizare, securitate și preț. Astfel, cardurile de credit și de debit reprezintă cel mai înalt rang în ceea ce privește preferințele lor, ca un întreg, urmată de transferuri bancare online și facturile. În ciuda diferențelor în ceea ce privește obiceiurile de consum și modele cumpărături în regiunea nordică, piața de vânzare la distanță arată o creștere susținută, din cauza popularității comerțului online, gamei largi de produse și servicii activate de internet și cererea consumatorilor semnificativă. Acesta este motivul pentru care are suficient potențial de a deveni o provocare pentru companii și clienți să se implice în astfel de activități.

Franța

Pentru achiziții online, consumatorii francezi preferă să utilizeze carduri bancare, inclusiv Carte Bleue, carduri private sau cardurile de magazin. Din aceasta rezultă tranzacțiile cu carduri de credit, reprezentând 80% din totalul preferințelor online. În primele șase luni ale anului 2011, cifra de afaceri pentru toate site-urile

de comerț electronic din Franța a ajuns la 17,5 miliarde de EUR, în creștere cu 20% fata de 2010. În anul precedent, veniturile e-commerce au totalizat 31 EUR miliarde de euro 36.2 miliarde înregistrat în vânzări la distanță. În prezent, Franța are 90000 site-uri web de vânzare cu amănuntul, inclusiv 20.000 de site-uri noi, create în 2010.

Germania

Numarul cartelele preplătite au crescut cel mai rapid în 2011, cu o creștere a valorii curente de 15%, în timp ce cardurile de debit, charge cards, carduri de credit și carduri de magazin au avut rate de creștere de între 3-5%. În ceea ce privește volumul de plată, ratele de creștere au fost chiar mai mari, deoarece consumatorii utilizează cardurile de de microplati mai frecvent. În general, volumul de carduri a cunoscut doar o creștere slabă din cauza cardurilor de debit, care alcătuiesc cea mai mare parte din toate cardurile, este deja o categorie saturată. Numărul de tranzacții efectuate prin intermediul cardurilor a crescut de la 2,698.1 milioane de euro în 2010 la 2,831.6 milioane de euro în 2011, 97.9 milioane prin intermediul cardurilor de credit și 2,188.7 prin intermediul cardurilor de debit. Valoarea tranzacțiilor electronice directe / ACH a crescut, de asemenea, în 2011, ajungând la 5.3 milioane

Ungaria

În Ungaria plata în numerar la livrare este cel mai des folosită pentru comenzi on-line, urmată de către transferurile bancare și cărți de credit. E-portofelele sunt utilizate într-o măsură mai mică. Cartelele pre-plătite primit un impuls prin introducerea cardurilor pre-paid contactless MasterCard PayPass de OTP Bank în 2009. Produsul a fost puternic promovat, iar acum există aproximativ 30.000 de astfel de carduri aflate în circulație, dintre care 18.000 sunt cartelele pre-plătite.

Italia

În Italia consumatorii primari utilizează cardurile de credit pentru a plăti online, deși metodele numerar la livrare și de plată alternativă sunt, de asemenea, frecvent utilizate.

Țările de Jos

Aproape 70% din populația olandeză fac cumpărături online și 10% din toate achizițiile în Țările de Jos sunt acum realizate online, iDEAL fiind metoda de plată preferată. În prezent, mai mult de 40.000 de companii și instituții în Țările de Jos acceptă plăți iDEAL. Mai mult decât atât, iDEAL își extinde poziția sa în afara comerțului electronic așa cum utilizarea plăților, ideale pentru bilete de intrare și mijloacele de transport public crește vertiginos. iDEAL a înregistrat 250 milioane tranzacții finalizate la Fietspunt.nl webshop, deoarece metoda de plată online a fost introdusă în 2005. Succesul iDEAL în rândul consumatorilor constă în faptul că aceasta este o metodă de plată sigură și ușor de utilizat. În plus, produsul a fost lansat pe piață cu susținerea sectorului de .home-shopping.

Norvegia

În Norvegia, cardurile sunt cel mai comun mod de a plăti online. Transferuri bancare online, cum ar fi prin BankAxxess multi-banca de servicii, precum și facturile sunt de asemenea utilizate pentru a plăti online. Plățile în numerar la livrare și e-portofelele sunt mult mai puțin populare.

Polonia

În Polonia, cele mai populare metode de plată sunt numerar sau card la livrare și prin transferuri bancare. Transferurile bancare sunt de multe ori transferuri de credit standard, uneori inițiate offline, dar pot fi de asemenea efectuate prin una din multele metode de plată online mono-bănci. A existat o recuperare notabilă marginală în carduri de credit în 2011. Numărul de carduri de credit emise a crescut cu 2% față de 2010.

România

Consumatorii români utilizează în principal metodele de plată offline, cum ar fi plata la livrare și transferuri bancare pentru a plăti pentru cumpărăturile online. P Cardurile de credit și de debit sunt rar utilizate. P În 2011, valoarea tranzacțiilor de plată cu cardul a ajuns la 18,030,000 lei. P Din 9 milioane de carduri în România, doar 200.000 au avut securizat 3D standardul activat, care este utilizat de sistemul Verified by Visa. Piața comerțului electronic a depășit 160 milioane EUR până la sfârșitul anului 2011. În primele trei trimestre ale anului 2011, volumul de plăți online a crescut cu 11% față de aceeași perioadă a anului trecut, ajungând la 121.4 milioane EUR.

Rusia

Rușii încă mai cred în numerar. Mulți dintre ei nu au încredere în bănci, în timp ce cardurile de credit sunt rare. Cardurile de debit sunt folosite în principal pentru a retrage salariile din bancomate. Lipsa infrastructurii card este înlocuit de diverse soluții de bani electronici, inclusiv sistemele de facturare SMS-based. Cele mai multe sisteme de plată online aici sunt în principal elaborate pentru comunitatea online rusă: e-portofelele, cum ar fi WebMoney, Yandex.dengi, QIWI, Pilot Kredit, E-Port, Moneta, sisteme Rapida (multe dintre ele sunt procesate prin intermediul Cyberplat și Assist). Unele bănci locale oferă servicii de prelucrare online de carduri de (creditImpexbank), și există, de asemenea, procesatori de plată terți (Chronopay).

Slovacia

Consumatorii slovaci plătesc cea mai mare parte prin numerar la livrare urmat de transferuri bancare și carduri de credit în timp ce e-portofelele și cartelele pre-plătite sunt, de asemenea, utilizate. Slovacia și Republica Cehă rămân diferite de restul Europei, în calitate de cumpărători din aceste țări preferă să plătească pentru ordinele lor de la livrare. Peste jumătate dintre consumatorii slovaci online folosesc această metodă de plată întrucât două treimi din valoarea totală a achizițiilor este dispusă ca plata la livrare.

Suedia

În ceea ce privește volumul tranzacțiilor, sistemul de plăți suedez este dominat de sistemele Giro, sistemul Bankgirot și sistemul de Postgirot, care reprezintă mai mult de 71% din tranzacțiile fără numerar (din care 86% sunt tranzacții inițiate electronic).

Regatul Unit

Cardurile de credit sunt metoda de plată utilizată cel mai frecvent pentru achiziții online, reprezentând 40% din tranzacțiile online, urmate de Cardurile de debit - 35%, în timp ce PayPal este a treia metodă cea mai utilizată de plată.

Anexa 4: Referințe

R1: Banca Națională a României – statistică plăți

R2: Banca Centrală Europeană – statistici plăți 04.09.2012;

R3: SPECIAL EUROBAROMETER 390 "Cyber security"

R4: THE ECONOMIC IMPACT OF A EUROPEAN DIGITAL SINGLE MARKET -
http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

R5: ECB, Prof. Dr. Schneider, A.T. Kearney Analysis



R6: VISA Europe – The future of every day payments in Europe

R7: ECOMMERCE & INNOPAY - Online payments 2012

R8: ECB Recommendations for the Security of the Internet Payments

R9: An ISACA Emerging Technology White Paper November 2011 - Mobile Payments: Risk, Security and Assurance Issues