

Cuprins

Argument	11
Capitolul 1	
Transformări conceptuale ale spațiului informațional și financiar	17
1.1. Cloud computing	18
1.1.1. Noțiuni introductive	18
1.1.2. Clasificare	20
1.1.3. Comparație	25
1.2. Evoluții ale spațiului financiar	31
1.2.1. Considerații generale	31
1.2.2. Globalizare	36
1.2.2.1. Cloud accounting – o nouă provocare pentru contabilitate	36
1.2.2.2. Proiectul SEPA în România	39
1.2.2.3. Plățile electronice	44
1.3. Frauda	45
1.3.1. Frauda ca business	46
1.3.2. Frauda și transferurile financiare electronice	48
1.3.3. Costul fraudei	49
Capitolul 2	
Impactul noilor tehnologii asupra domeniului financiar	61
2.1. Skimming – re-poziționări ale criminalității	63
2.1.1. ATM	63
2.1.1.1. Dispozitive de copiat banda magnetică	68
2.1.1.2. Dispozitive de copiere a PIN-ului	69
2.1.1.3. Door skimmer și cameră video	70
2.1.1.4. Vandalizări	70
2.1.1.5. Capcane de numerar la ATM	71
2.1.1.6. Black Box	74
2.1.2. PoS	77
2.2. Atacul informatic prin vectori de infecție	81
2.2.1. Tipuri de malware	86
2.2.2. Vectori de infecție	94
2.2.2.1. E-mail	94
2.2.2.2. Dispozitive media externe/portabile	98
2.2.2.3. Browser	100
2.2.3. Tipuri de atacuri	101
2.2.4. Studii de caz	112
2.2.4.1. Malware instalat local	112

2.2.4.2. Malware instalat la furnizorul de servicii	116
2.2.4.3. Malware instalat în interiorul băncilor	118
2.3. Phishing-ul și domeniul financiar: o problemă de management al securității informației?	122
2.3.1. Vulnerabilități	126
2.3.2. Tipologii sub care este întâlnit atacul de tip phishing	129
2.4. IoT provocări și evoluție	136
2.4.1. Reglementare, evaluare și certificare IoT	137
2.4.2. Securitatea IoT	141
2.5. AI/ML	149
2.5.1. AI/ML și criminalitatea informatică	153
2.5.2. Evaluare, Reglementări și Certificare	155

Capitolul 3

Criminalitate informatică și circuite financiare	159
3.1. Contextul internațional	161
3.2. Argumente pro și contra crypto-monedelor	164
3.3. Spălarea banilor, element fundamental al strategiei financiare a grupărilor criminalității organizate	175
3.3.1. Etapele spălării banilor	177
3.3.2. Cyber-Crime ca sursă de fonduri pentru spălarea banilor	179
3.3.2.1. Mișcarea banilor	181
3.3.2.2. Crypto-monedele și criminalitatea informatică	183
3.3.2.3. Monedele virtuale și spălarea banilor	193
3.3.3. Indici de anomalie și tehnici de simulare	198
3.3.4. Metode de spălarea banilor	200
3.3.4.1. Spălarea banilor din fraude cu carduri	200
3.3.4.2. Spălarea banilor prin activități de e-commerce	201
3.3.4.3. Spălarea banilor prin intermediul ATM-urilor	202
3.3.4.4. Spălarea banilor în interiorul aceluiași grup de firme	203
3.3.4.5. Spălarea banilor și scrisorile nigeriene	203
3.3.4.6. Spălarea banilor și sistemul Prepaid	203
3.3.4.7. Spălarea banilor și Mobile Payments (M-commerce)	204
3.3.4.8. Spălarea banilor și asset-urile virtuale	206

Capitolul 4

Propuneri și măsuri privind managementul riscurilor transferurilor financiare	207
4.1. Implicații juridice și răspuns la incidente	210
4.1.1. Legislația actuală în condițiile implementării noilor tehnologii	210
4.1.2. Fraudele cu carduri	216
4.1.3. Cadrul legislativ privind spălarea banilor	218
4.1.4. Protecția utilizatorului și recuperarea datelor	223
4.1.5. Considerații privind managementul strategic al infrastructurilor critice și domeniul financiar	228
4.2. Managementul riscului de fraudă în cazul tranzacțiilor financiare cu cardul	233
4.2.1. Elemente de identificare și de operabilitate	235

4.2.2. Recomandările emitenților	241
4.2.2.1. Noi tehnologii de autentificare	244
4.2.2.2. Sistem Rotativ de Securitate (SRS)	255
4.2.3. Tendințe și evoluție	256
4.3. Combaterea spălării banilor	257
4.3.1. Identificarea și prevenirea tranzacțiilor suspecte	257
4.3.2. Raportarea tranzacțiilor suspecte	262
4.3.3. Monitorizarea respectării standardelor	263
4.3.3.1. Recomandări și sancțiuni	263
4.3.3.2. Analiză și investigare	267
4.3.3.3. Etape de acțiune	268
4.4. Domeniul financiar în contextul managementului strategic al infrastructurilor critice	271
4.4.1. Risc și necesitate	273
4.4.2. Stabilitate și strategie financiară	279
Capitolul 5	
Concluzii și direcții de dezvoltare ulterioară	287
Bibliografie	301
Anexa 1	333
A1. Elemente generale privind impactarea instituțiilor financiare	335
A2. Planificare strategică	337
A2.1. Bune practici pentru gestionarea securității rețelei	338
A2.2. Securitatea fizică	343
A2.3. Continuitatea afacerii	346
A3. Poziționare în raport cu activitatea cyber-crime	348
A3.1. Identificarea unui atac de tip phishing	351
A3.2. Metode de contracarare a unor atacuri de tip phishing	354
A4. Strategii de combatere a atacurilor asupra ATM-urilor	358
A4.1. Instituții și producători	358
A4.2. Auto-protecție	359
A5. IoT	361
A6. Propuneri suplimentare de măsuri	366