Bogdan Alexandru Urs

Accesul ilegal
în mediul Cloud Computing

Editura
Hamangiu
2023

CUPRINS

INTRODUCERE 1

TITLUL I. ACCESUL ÎN MEDIUL CLOUD COMPUTING ŞI INFRACȚIONALITATEA INFORMATICĂ 9

CAPITOLUL I. MEDIUL ŞI TEHNOLOGIA CLOUD COMPUTING 9

Secțiunea 1. Definiția mediului informatic şi a tehnologiei Cloud Computing 9

Secțiunea a 2-a. Caracteristicile tehnologiei Cloud Computing 11

§1. Servicii proprii la cerere 12

§2. Acces extins la servicii prin rețea 13

§3. Alocarea dinamică a resurselor 14

§4. Servicii flexibile 15

§5. Servicii măsurabile 15

Secțiunea a 3-a. Modele de livrare a serviciilor Cloud Computing 16

§1. „Infrastructure as a Service” 17

§2. „Platform as a Service” 19

§3. „Software as a Service” 21

Secțiunea a 4-a. Modele de implementare a serviciilor Cloud Computing 22

§1. Cloud-ul public 24

§2. Cloud-ul privat 28

§3. Cloud-ul hibrid 32

§4. Cloud-ul de comunitate 37

CAPITOLUL AL II-LEA. ACCESUL LEGAL ÎN MEDIUL CLOUD COMPUTING **42**

Secțiunea 1. Controlul accesului în Cloud Computing 42

Secțiunea a 2-a. Mecanisme de autentificare 44

§1. Mecanismele fizice de securitate 45

§2. Mecanismele digitale de securitate 45

Secțiunea a 3-a. Mecanisme de autorizare 46

§1. Mecanismul de control obligatoriu al accesului 47

§2. Mecanismul de control discreționar al accesului 47

§3. Mecanismul de control al accesului bazat pe roluri 48

§4. Mecanismul de control al accesului bazat pe atribute 49

§5. Mecanismul de control hibrid al accesului de tip „fine-grained” 49

Secțiunea a 4-a. Sisteme de control al accesului în Cloud Computing 50

CAPITOLUL AL III-LEA. ACCESUL ILEGAL ÎN MEDIUL CLOUD COMPUTING ____ 54
Secțiunea 1. Aspecte generale. Reglementare ____ 54
Secțiunea a 2-a. Elemente de drept comparat ____ 55
§1. Statele Unite ale Americii ____ 56
§2. Regatul Unit al Marii Britanii şi al Irlandei de Nord ____ 59
§3. Australia ____ 61
§4. Germania ____ 63
§5. Franța ____ 64
§6. Tipologia accesului ilegal în dreptul comparat ____ 65
Secțiunea a 3-a. Obiectul infracțiunii ____ 66
Secțiunea a 4-a. Subiecții infracțiunii ____ 68
Secțiunea a 5-a. Latura obiectivă ____ 69
§1. Mediul Cloud Computing – „sistem informatic” ____ 70
§2. Noțiunea de „acces” la un sistem informatic ____ 72
§3. Accesul „fără drept” sau ilegal ____ 74
§4. Particularitățile accesului ilegal în mediul Cloud Computing ____ 77
§5. Tipologia atacurilor informatice prin care se materializează accesul ilegal ____ 80
5.1. Atacurile de autentificare şi cele de autorizare ____ 82
5.2. Atacurile de împachetare ____ 85
5.3. Atacul de tip „side channel” ____ 87
5.4. Atacul de tip „Man in the Cloud” ____ 91
5.5. Atacul de tip „Man in the Middle” ____ 94
5.6. Atacurile din „interior” ____ 96
§6. Aspecte practice ____ 99
6.1. Accesul ilegal în mediul Cloud Computing ____ 99
6.2. Accesul ilegal în diferite servicii bazate pe tehnologia Cloud ____ 101
6.3. Accesul ilegal în servicii Cloud Computing de tip e-mail ____ 103
6.4. Accesul ilegal în Cloud realizat de angajați sau foşti angajați ____ 105
6.5. Accesul ilegal în mediul Cloud Computing şi diverse fraude informatice conexe ____ 107
6.6. Accesul ilegal în Cloud asociat cu alte infracțiuni informatice ____ 109
6.7. Accesul în diferite medii Cloud Computing cu implicații în pornografia infantilă ____ 111
Secțiunea a 6-a. Latura subiectivă ____ 112
Secțiunea a 7-a. Formele infracțiunii ____ 113
Secțiunea a 8-a. Modalități normative agravate ____ 115
§1. Prima modalitate agravată (obținerea de date informatice) ____ 115

§2. A doua modalitate agravată (încălcarea măsurilor de securitate) 117
Secțiunea a 9-a. Aspecte jurisdicționale 119
Secțiunea a 10-a. Relația dintre accesul ilegal şi alte infracțiuni informatice 131
§1. Relația cu frauda informatică (art. 249 C. pen.) 132
§2. Relația cu falsul informatic (art. 325 C. pen.) 133
§3. Relația cu alterarea integrității datelor informatice (art. 362 C. pen.) 134
§4. Relația cu perturbarea funcționării sistemelor informatice (art. 363 C. pen.) 135
§5. Relația cu operațiuni ilegale cu dispozitive sau programe informatice (art. 365 C. pen.) 135

CAPITOLUL AL IV-LEA. ACCESUL ILEGAL ŞI FENOMENUL INFRACȚIONAL DIN MEDIUL CLOUD COMPUTING 137
Secțiunea 1. Mediul Cloud Computing în paradigma infracționalității informatice 137
Secțiunea a 2-a. Migrația infracționalității informatice spre mediul Cloud Computing 144
Secțiunea a 3-a. Factorii ce influențează fenomenul migrației infracționalității informatice 155
§1. Cantitatea vastă de date procesate şi stocate în Cloud Computing 156
§2. Puterea de procesare a informației şi infrastructura dinamică a mediului 158
§3. Disponibilitatea extinsă a serviciilor şi a tehnologiei Cloud Computing 159
§4. Posibilitatea de a şterge rapid eventualele dovezi ale activității infracționale 160
§5. Facilitatea de a lansa rapid atacuri informatice la scară largă 162
§6. Existența unor instrumente propice săvârşirii de infracțiuni informatice 163
§7. Diversitatea infracțiunilor informatice comise în mediul Cloud Computing 165
Secțiunea a 4-a. Formele criminalității informatice din mediul Cloud Computing 167
§1. Cloud Computing-ul în calitate de țintă a infracțiunilor informatice 170
§2. Cloud Computing – un instrument pentru săvârşirea de infracțiuni informatice 173

Secțiunea a 5-a. Implicațiile fenomenului infracțional din mediul Cloud Computing 176
§1. Fraude informatice complexe 177
§2. Fraude informatice clasice 180
§3. Accesul ilegal şi perturbarea funcționării sistemelor Cloud Computing 182
§4. Pornografia infantilă prin intermediul sistemelor Cloud Computing 184
§5. Cloud Computing-ul şi pornografia infantilă în România 186

TITLUL AL II-LEA. PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING 189

CAPITOLUL I. ORGANIZAREA ŞI FUNCȚIILE MECANISMELOR DE PREVENIRE 189
Secțiunea 1. Cadrul general de prevenire a infracționalității informatice 189
Secțiunea a 2-a. Principiile şi formele de organizare a mecanismelor de prevenire 193
Secțiunea a 3-a. Mecanisme legale, tehnice şi manageriale de prevenire a infracționalității informatice 197
Secțiunea a 4-a. Prevenirea prin prisma utilizatorilor, a sectorului privat şi a celui de stat 201
Secțiunea a 5-a. Implementarea strategiilor de prevenire a infracționalității cibernetice 205

CAPITOLUL AL II-LEA. MECANISME LEGALE DE PREVENIRE A ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING 209
Secțiunea 1. Politici privind utilizarea legală şi responsabilă a serviciilor Cloud Computing 209
Secțiunea a 2-a. Implicațiile măsurilor legale în securitatea mediului Cloud Computing 215
Secțiunea a 3-a. Directiva (UE) 2016/1148 216
Secțiunea a 4-a. Regulamentul (UE) 2016/679 222
Secțiunea a 5-a. Directiva (UE) 2016/680 229
Secțiunea a 6-a. Directiva 2013/40/UE 232
Secțiunea a 7-a. Directiva 2002/58/CE 237
Secțiunea a 8-a. Comunicarea (2019) 250 244
Secțiunea a 9-a. Regulamentul (UE) nr. 910/2014 252

CAPITOLUL AL III-LEA. MECANISME TEHNICE DE SECURITATE CU ROL ÎN PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING 265
Secțiunea 1. Securitatea ca metodă de prevenire a accesului ilegal 265
Secțiunea a 2-a. Importanța implementării tehnicilor de securitate cibernetică 270
Secțiunea a 3-a. Mijloace şi proceduri tehnice de protecție a datelor 272
Secțiunea a 4-a. Criptarea ca mijloc tehnic de securitate şi prevenire a accesului ilegal în mediul Cloud Computing 278
§1. Criptarea prin intermediul funcției „hash” 283
§2. Criptarea tradițională (criptarea „simetrică”) 284
§3. Criptarea cu două chei (criptarea „asimetrică”) 286
§4. Criptarea homomorfică („homomorphic encryption”) 289

CAPITOLUL AL IV-LEA. ASPECTE PRIVIND MANAGEMENTUL PREVENIRII ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING 291
Secțiunea 1. Principiile de organizare a serviciilor Cloud Computing 291
Secțiunea a 2-a. Managementul securității serviciilor şi procedurile de organizare a acesteia 296
Secțiunea a 3-a. Instrumente de management şi audit al securității serviciilor 303
Secțiunea a 4-a. Organizații internaționale cu rol în managementul securității mediului Cloud Computing 309
§1. Cloud Security Alliance (CSA) 310
§2. Institutul Național de Standarde şi Tehnologie din Statele Unite ale Americii (NIST) 311
§3. Agenția Uniunii Europene pentru Securitatea Rețelelor şi a Informațiilor (ENISA) 312
§4. Centrul de Cercetare în Cloud Computing al companiei Microsoft (MCCRC) 314
Secțiunea a 5-a. Standarde internaționale care asigură un management al securității în mediul Cloud Computing 315

CAPITOLUL AL V-LEA. PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING ŞI ROLUL SECTORULUI PUBLIC 322
Secțiunea 1. Strategii naționale de prevenire a infracțiunilor informatice 322
Secțiunea a 2-a. Prevenirea accesului ilegal şi protecția datelor în România 323

Secțiunea a 3-a. Cooperarea internațională şi lupta împotriva infracționalității informatice 327
Secțiunea a 4-a. Importanța investigațiilor digitale în prevenirea şi combaterea accesului ilegal în mediul Cloud Computing 330
Secțiunea a 5-a. Descentralizarea datelor şi problema accesului ilegal în Cloud Computing 336
Secțiunea a 6-a. Investigatorii şi accesul acestora la datele stocate în Cloud 344
Secțiunea a 7-a. Obținerea datelor referitoare la utilizatori 345
Secțiunea a 8-a. Analiza traficului de date din Cloud Computing 349
Secțiunea a 9-a. Probleme referitoare la datele de conținut şi stocarea acestora 351

CAPITOLUL AL VI-LEA. PREVENIREA ACCESULUI ILEGAL ÎN MEDIUL CLOUD COMPUTING ŞI ROLUL SECTORULUI PRIVAT **355**
Secțiunea 1. Prevenirea accesului ilegal prin procedurile de securitate 355
Secțiunea a 2-a. Riscul şi prevenirea accesului ilegal în sectorul privat 359
Secțiunea a 3-a. Rolul şi funcțiile furnizorilor de servicii în prevenirea accesului ilegal în mediul Cloud Computing 363
Secțiunea a 4-a. Studii de caz privind implementarea mecanismelor de prevenire a accesului ilegal în sectorul privat 368
§1. Google Cloud Platform 369
1.1. Implementarea de către Google Cloud a mecanismelor de prevenire 370
1.2. Securitatea şi protecția datelor în Google Cloud 374
§2. Amazon Web Services 377
2.1. Mecanismele de prevenire şi securitate ale Amazon Web Services 378
2.2. Protecția şi securitatea datelor în Amazon Web Services 381
§3. Microsoft Azure 384
3.1. Prevenirea accesului ilegal în Microsoft Azure 384
3.2. Protecția datelor în Microsoft Cloud Azure 387
§4. IBM Cloud Computing 389
4.1. Securitatea serviciilor IBM Cloud 390
4.2. Protecția datelor cu caracter personal în IBM Cloud 392
§5. Sistec IT Solutions 393
Secțiunea a 5-a. Analiza principalelor mecanisme de prevenire din sectorul privat 395

Secțiunea a 6-a. Implementarea de către furnizorii de servicii a noilor tehnologii de prevenire a accesului ilegal 397
§1. Sistemele de detectare a intruziunilor de tip IDS 397
1.1. Sistemele de detectare a intruziunilor bazate pe gazdă 399
1.2. Sistemele de detectare a intruziunilor bazate pe rețea 401
1.3. Sistemele de detectare a intruziunilor bazate pe „hypervisor” 401
1.4. Sistemele distribuite de detectare a intruziunilor 402
§2. Sistemele de detectare şi prevenire a intruziunilor de tip IDPS 403
§3. Utilizarea unui Cloud Privat Virtual 405
§4. Virtualizarea şi izolarea maşinăriilor virtuale 406

CONCLUZII **409**

BIBLIOGRAFIE SELECTIVĂ **423**