Impactul statusului numelor de domenii internet asupra reputației acestora

Dragoș SMADA[1], Mihail DUMITRACHE[1,2,3], Carmen-Ionela ROTUNĂ[1,4], Cristian-Alexandru GHEORGHIȚĂ[1,4]

[1] Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București, România

[2] Facultatea de Litere, Universitatea din București, România

[3] Academia Oamenilor de Știință din România, România

[4] Universitatea Națională de Știință și Tehnologie Politehnica București, România

dragos.smada@ici.ro, mihail.dumitrache@ici.ro, carmen.rotuna@ici.ro, alexandru.gheorghita@ici.ro

Rezumat: Reputația numelor de domenii de Internet se referă la evaluarea credibilității, securității și fiabilității unui domeniu pe baza comportamentului și a caracteristicilor istorice ale acestuia. Aceasta implică analizarea factorilor care influențează calitatea percepută, securitatea și riscurile asociate pentru a determina reputația unui domeniu. Domeniile de nivel superior (TLD) reprezintă cel mai înalt nivel din ierarhia sistemului de nume de domenii. Reputația domeniului influențează clasamentele motoarelor de căutare, experiența utilizatorului și securitatea online. Registrele de domenii TLD, organizațiile și persoanele fizice au nevoie de sisteme de monitorizare automată a reputației domeniilor deținute din motive de securitate, în special atunci când utilizează date cu caracter personal, pentru a proteja utilizatorii și a menține o prezență online pozitivă. Principalele obiective ale acestui studiu includ identificarea parametrilor Sistemului de Nume de Domenii (DNS) relevanți pentru stabilirea reputației și analiza impactului stărilor unui domeniu asupra reputației, utilizând setul de date deținut de Registrul de domenii .ro.

Cuvinte cheie: DNS, domeniu internet, registry, DNSSEC, reputație domeniu, TLD.

The impact of internet domain name status on their reputation

Abstract: Internet domain name reputation refers to the assessment of the credibility, security and reliability of a domain based on its behavior and historical characteristics. This involves looking at factors that influence perceived quality, security and associated risks to determine a domain's reputation. Top Level Domains (TLDs) are the highest level in the domain name system hierarchy. Domain reputation impacts search engine rankings, user experience, and online security. TLD Domain Registry, Organizations and individuals need automated domain reputation monitoring systems for security reasons, especially when using personal data, to protect users and maintain a positive online presence. The main objectives of this study include the identification of DNS parameters relevant for establishing reputation and the analysis of the impact of a domain's statuses on reputation using the data set owned by the .ro Domain Registry.

Keywords: DNS, Internet Domain, Registry, DNSSEC, Domain Reputation, TLD.

1. Introducere

Reputația numelor de domenii internet se referă la evaluarea credibilității, securității și fiabilității acestora pe baza comportamentului și caracteristicilor sale istorice. Aceasta implică analiza factorilor care pot influența calitatea percepută, securitatea și potențialele riscuri asociate acestuia, pentru a determina reputația unui nume de domeniu.

Conceptul de reputație aplicat domeniilor adreselor IP și adreselor URL, permite tehnologiilor de securitate automatizate să ia decizii cu privire la permisiunea, refuzul sau permisiunea condiționată a diferitelor tipuri de conexiuni. În investigațiile cibernetice, ajută la ghidarea investigatorului către acele domenii care sunt cele mai susceptibile de a fi compromise. Spre deosebire de blacklist-uri, scorul reputației permite adaptarea poziției de securitate la nivelul de risc.

Reputația domeniilor afectează clasamentul motoarelor de căutare, livrarea e-mailului și experiența utilizatorului. Registrele de domenii, partenerii acestora și alte organizațiile au nevoie de soluții dinamice pentru a monitoriza și gestiona în mod activ reputația numelor de domenii, în

https://doi.org/10.33436/v34i1y202404

special dacă procesează date cu caracter personal, pentru a proteja utilizatorii și a spori securitatea în mediul online (Banciu, Petre & Dumitrache, 2019).

Domeniile de nivel superior (TLD) reprezintă cel mai înalt nivel al ierarhiei sistemului de nume de domenii (DNS). Sunt ultimul segment al unui nume de domeniu după punctul final și sunt folosite pentru a indica tipul și scopul domeniului. Există două tipuri principale de domenii de nivel superior de cod de țară (ccTLD) care corespund unei anumite țări sau locații geografice și domenii generice de nivel superior (gTLD) care nu sunt asociate cu o anumită țară (.net, .com etc.) (Akumiah, 2016; Marshal, 2019).

Obiectivele principale ale acestui studiu sunt identificarea funcționalităților DNS relevante pentru stabilirea reputației numelor de domenii, identificarea parametrilor esențiali în stabilirea reputației în setul de date deținut de Registrul de domenii .ro, identificarea unor servicii externe care furnizează informații relevante pentru reputația domeniului și analiza impactului statusului domeniilor în stabilirea reputației.

Capitolul 2 prezintă rezultatele studiilor recente care au avut ca obiectiv dezvoltarea unor soluții pentru stabilirea reputației numelor de domenii. În cadrul acestor studii sunt folosite tehnici de învățare automată pentru a îmbunătăți securitatea domeniilor și a sistemului DNS și pentru detectarea activităților cu potențial malițios.

Capitolul 3 identifică aspecte ale Sistemului de Nume de Domenii (DNS) cu rol esențial în determinarea reputației domeniilor. Înregistrările DNS precum vârsta, istoricul deținătorilor (trade-uri), prezența host-urilor și configurațiile DNS, influențează în mod semnificativ fiabilitatea unui domeniu. Caracteristicile de securitate precum DNSSEC cresc scorul reputației unui domeniu prin asigurarea integrității datelor. În plus, factori externi precum certificatele SSL, absența activităților de phishing și utilizarea serviciilor de reputație, contribuie pozitiv la creșterea gradului de încredere al domeniului. Astfel, DNS servește atât ca mecanism de navigare pe Internet, cât și ca factor critic în evaluarea reputației unui domeniu, influențând încrederea utilizatorilor și credibilitatea online.

Capitolul 4 detaliază metodologia utilizată pentru cuantificarea reputației unui domeniu în funcție de starea acestuia. Pentru a evalua impactul pe care statusul unui domeniu îl are asupra reputației acestuia, este necesară utilizarea unei metodologii de cercetare bine definite. În cadrul acestui capitol sunt definite etapele utilizate în cadrul cercetării.

Capitolul 5 descrie analiza statusului numelor de domenii în stabilirea reputației. Aceasta implică examinarea indicatorilor și a parametrilor care reflectă starea și istoricul unui domeniu utilizând baza de date a Registrului.ro. Statusul este un aspect esențial în determinarea reputației, domeniile active fiind considerate mai credibile decât cele inactive sau expirate. Procesul de evaluare a reputației implică extragerea unui eșantion de 1000 de nume de domenii din baza de date a registrului, utilizarea de interogări SQL și analiza informațiilor relevante precum vârsta, status, numărul de tranzacții (trade-uri) și utilizarea DNSSEC. Datele sunt apoi exportate în format CSV pentru analiza ulterioară. Evaluarea reputației se concentrează pe impactul diferitelor stări ale domeniului asupra funcționalității, securității și credibilității percepute, fiecare status fiind evaluat pe o scară de la 1 la 10 pentru impactul său potențial.

Capitolul 6 sumarizează rezultatele cercetării ce vor fi utilizate pentru dezvoltarea unei soluții generice, reutilizabile și adaptabile pentru implementarea de către orice registru de domenii de nivel superior (ccTLD) sau registrarii săi afiliați pentru stabilirea reputației domeniilor.

2. Stadiul actual

Securitatea domeniilor este o preocupare majoră pentru organizații, deoarece atacatorii le pot exploata în scopuri rău intenționate, precum găzduirea de programe malware și recoltarea de date, ceea ce duce la deteriorarea reputației (OWASP, 2020). Dacă nu este securizat corespunzător, sistemul de nume de domeniu (DNS) poate fi vulnerabil la exploatarea de către persoane rău intenționate. Dezvoltatorii de programe malware sunt conștienți de importanța accesibilității DNS și caută în mod activ modalități de a perturba timpul de funcționare al DNS și serverele care îl întreține (Scalzo, 2017).

În prezent, există mai multe tehnici care pot fi folosite pentru a îmbunătăți acuratețea și eficacitatea unui sistem de reputație a numelui de domeniu. Acestea includ:

- Monitorizarea în timp real implică monitorizarea continuă a comportamentului domeniilor și actualizarea scorurilor reputației acestora în consecință. Acest lucru poate ajuta la identificarea și atenuarea rapidă a amenințărilor pe măsură ce sunt identificate (Cîrnu et al., 2018);
- Listele negre și listele albe sunt liste de domenii despre care se știe că sunt fie rău intenționate, fie sigure. Folosind aceste liste ca punct de plecare, un sistem de reputație a numelor de domeniu poate clasifica rapid domeniile ca fiind sigure sau riscante;
- Reputația IP poate ajuta la identificarea activităților rău intenționate care pot fi asociate cu o anumită adresă IP (Rotună et al., 2022).

Antonakakis a proiectat un sistem de detectare a „cache poissoning" bazat pe Machine Learning (ML) numit Anax, care detectează modificările făcute de atacatorii cibernetici în înregistrările DNS stocate în cache în timp real, cu o rată de 91,9% acuratețe a detecției (Antonakakis et al., 2010). În mod similar, Hao și Wang au antrenat algoritmi de învățare automată bazați pe arbori de decizie (Decision Tree) și Random Forest (RF) folosind caracteristici sintactice ale numelor de domenii precum șirul de caractere, lungimea acestuia etc., (Hao & Wang, 2017). Alrwais a utilizat doi algoritmi de învățare automată, și anume SVM și RF, pentru a construi un sistem de detectare și pentru a identifica blocurile de rețea compromise folosind caracteristici extrase din tendințele serviciilor BPH (Bulletproof hosting) (Alrwais et al., 2017). Khalil a proiectat un sistem de detectare a domeniilor compromise folosind modelul Random Forest (RF) bazat pe caracteristicile reprezentative ale IP-urilor ca spre exemplu numărul de nume de domenii complet calificate, numărul de domenii de nivel al doilea din blocul său IP /24 etc. (Khalil et al., 2017).

Kopis utilizează o abordare pasivă pentru a monitoriza traficul DNS la nivelurile superioare ale ierarhiei DNS. Analizând modelele de rezoluție a interogărilor DNS la nivel mondial, se poate identifica cu precizie domeniile ce prezintă vulnerabilități. Spre deosebire de sistemele de reputație DNS anterioare precum Notos și Exposure, care depind de monitorizarea traficului de la serverele DNS recursive locale, Kopis oferă o perspectivă nouă și încorporează noi caracteristici de trafic care valorifică vizibilitatea globală obținută prin observarea traficului de rețea (Antonakakis et al., 2011; Antonakakis et al., 2017).

Fukushima propune dezvoltarea unui sistem de liste negre (blacklist) cu capacitatea de a analiza caracteristicile site-urilor web rău intenționate folosind informațiile despre domeniul lor, precum sistemul autonom (AS), blocul adresei IP, adresa IP, domeniul și registrarul și propune o soluție de tip listă neagră care combină blocurile de adrese IP și registrarii cu o reputație scăzută, (Fukushima et al., 2011; Gheorghiță et al., 2023).

Modelul de flux bazat pe topologie propus de Mishsky & Gal-Oz, (2015) oferă o abordare promițătoare a reputației domeniului. Utilizând topologia rețelei și analiza fluxului, modelul are potențialul de a oferi o protecție precisă și eficientă împotriva domeniilor rău intenționate.

În general, un sistem eficient de reputație a numelor de domeniu trebuie să încorporeze o combinație de tehnici care, împreună cu algoritmi avansați de învățare automată și capabilități de monitorizare în timp real, funcționează împreună pentru a identifica domeniile cu potențial malițios. Procedând astfel, un astfel de sistem poate oferi informații precise și de încredere cu privire la reputația unui anumit nume de domeniu, ajutând la protejarea utilizatorilor de eventuale amenințări cibernetice, asigurând un mediu online rezistent și securizat (Dumitrache et al., 2023; Sarkar, Banerje & Hassanien, 2013).

3. Sistemul de nume de domenii

Sistemul de nume de domenii DNS (Domain Name System) este un sistem ierarhic și descentralizat pentru computere, servicii sau alte resurse conectate la Internet sau la o rețea privată. Asociază diverse informații cu nume de domenii atribuite fiecăreia dintre entitățile participante. Cea mai importantă funcție a sa este traducerea numelor de domenii ușor de memorat în adrese IP

numerice, necesare pentru localizarea și identificarea serviciilor și dispozitivelor computerizate cu protocoalele de rețea subdiacente. Prin furnizarea unui serviciu de directoare distribuit la nivel mondial, sistemul de nume de domenii reprezintă o componentă esențială a funcționalității Internetului încă din 1985 (Deland-Han, 2022).

Sistemul de nume de domenii deleagă responsabilitatea de a atribui nume de domenii și de a mapa aceste nume la resursele de Internet prin desemnarea serverelor de nume autorizate pentru fiecare domeniu (Stăicuț, 1995). Administratorii de rețea pot delega autoritatea asupra sub-domeniilor din spațiul de nume alocat altor servere de nume. Acest mecanism oferă servicii distribuite și tolerante la erori și a fost conceput pentru a evita o singură bază de date centrală de mari dimensiuni (Albitz & Liu, 2006).

Figura 1 prezintă delegarea unei zone DNS.

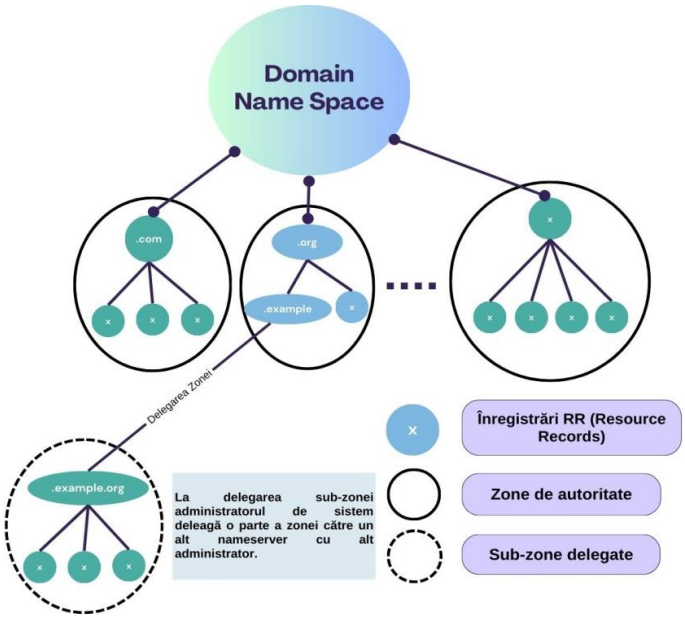

Figura 1. Delegarea unei zone DNS

Internetul menține două spații de nume principale, ierarhia numelor de domenii și spațiile de adrese IP. Sistemul de nume de domenii menține ierarhia domeniilor și oferă servicii de translatare între DNS și spațiile de adrese. Un server de nume DNS este un server care stochează înregistrările DNS pentru un domeniu și răspunde la interogările adresate bazei sale de date.

Cele mai comune tipuri de înregistrări DNS includ:

- înregistrările de mapare a adreselor (A și AAAA) care potrivește un nume de host la o adresă IP;
- înregistrările serverului de nume (NS) care specifică serverele DNS pentru domeniu;
- înregistrările de schimb de e-mail (MX) care direcționează e-mailul SMTP;
- înregistrările text (TXT) care pot conține text arbitrar și pot fi, de asemenea, utilizate pentru a defini date ce pot fi citite de mașină, precum informații de securitate sau de prevenire a abuzului.

DNS reflectă structura responsabilității administrative în Internet. Fiecare subdomeniu este o zonă de autonomie administrativă delegată unui manager. Pentru zonele operate de un Registru, informațiile administrative sunt adesea completate de baza de date RDNS a Registrului. Aceasta reprezintă depozitul de informații cu numele de domenii înregistrate despre domeniile de nivel superior pe care le administrează. Baza de date RDNS (Registry DNS) a registrului conține numele domeniului, numele registrarului, serverul WHOIS și informațiile serverului de nume pentru fiecare domeniu. Aceste informații sunt furnizate printr-un sistem cunoscut sub numele de protocol WHOIS.

DNSSEC (Domain Name System Security Extensions) reprezintă un set de extensii al DNS (Domain Name System) cu scopul de a elimina vulnerabilitățile DNS, asigurând integritatea și autenticitatea răspunsurilor primite în urma interogărilor DNS.

DNSSEC adaugă un strat suplimentar de securitate, permițând utilizatorului să verifice autenticitatea informațiilor primite de la un server DNS, evitând posibilitatea modificării acestora pe parcurs. O altă soluție de eliminare a breșelor în securitate a fost utilizarea semnăturilor digitale bazate pe criptografia cu chei publice.

Protocolul DNSSEC utilizează o structură de tip „lanț de încredere" (Chain of Trust), pornind de la rădăcinile DNS până la domeniul solicitat. Ca rezultat, toate serverele DNS se verifică reciproc prin intermediul semnăturilor digitale autorizate, asigurând o legătură strânsă între domenii pentru a garanta integritatea și autenticitatea datelor DNS.

Câteva tipuri de înregistrări pe care DNSSEC-ul le adaugă DNS-ului sunt:

- RRSIG conține semnătura pentru DNSSEC;
- DNSKEY conține cheia publică de verificare;
- NSEC și NSEC3 pentru negarea explicită a existenței unei înregistrări DNS (denial-of-existence);
- DS pentru o zonă specifică, „child zone" care solicită actualizări către „parent zone".

DNSSEC-ul întărește securitatea răspunsurilor DNS prin informarea utilizatorului cu privire la originea datelor DNS, dacă aceste date au fost prelucrate pe parcurs, și dacă domeniul respectiv există sau nu.

4. Metodologie pentru cuantificarea reputației unui domeniu în funcție de starea acestuia

Pentru a evalua impactul pe care statusul unui domeniu îl are asupra reputației acestuia, este necesar să se folosească o metodologie de cercetare bine definită. În cadrul acestui capitol scopul este de a descrie metodologia care va fi urmată pentru realizarea cercetării propuse constând din următoarele etape:

- Clarificarea scopului cercetării și a întrebărilor specifice în evaluarea impactului statusului unui domeniu asupra reputației sale;
- Etapa 2 o constituie identificarea parametrilor relevanți. Această etapă constă în enumerarea și definirea statusurilor de domeniu relevante care vor fi luate în considerare în evaluarea reputației;
- Determinarea metodelor de evaluare a reputației ce cuprinde selectarea indicatorilor și metodelor adecvate pentru evaluarea reputației domeniului, precum analiza datelor deținute de Registru, analiza informațiilor de trafic web, evaluarea listărilor în motoarele de căutare, analiza feedback-ului utilizatorilor sau analiza calității conținutului. Această etapă include colectarea datelor relevante despre domenii din baza de date a Registrului .ro, inclusiv statusurile lor actuale și istoricul acestora;
- Analiza datelor pentru a identifica diferențele semnificative în reputația domeniilor în funcție de statusurile lor. Acestă etapă implică utilizarea unui eșantion de 1000 de domenii cu statusuri diferite din baza de date a Registrului, care sunt utilizate pentru analiză. Ca rezultat sunt identificate relații statistice între statusurile domeniilor și reputația acestora, pentru a determina dacă există o corelație semnificativă între acestea. Aceste domenii sunt analizate și evaluate în prima fază manual, pentru a identifica corelații între statusul domeniului și reputația acestuia;
- Etapa 5 constă în interpretarea rezultatelor ce presupune extragerea unor concluzii semnificative cu privire la impactul statusului unui domeniu asupra reputației sale;
- Reînceperea cercetării, în cazul în care este necesar, presupune repetarea cercetării utilizând metodologia revizuită pentru a obține rezultate mai precise sau pentru a investiga alte aspecte relevante.

Implementarea acestei metodologii va asigura o abordare riguroasă și sistematică în evaluarea impactului statusului unui domeniu asupra reputației sale, furnizând rezultate fiabile și utile pentru determinarea reputației unui domeniu internet.

5. Analiza statusului numelor de domenii în stabilirea reputației

Analiza statusului numelor de domenii în contextul stabilirii reputației este un proces esențial în evaluarea credibilității și a riscului asociat cu un anumit domeniu internet. Acestă analiză implică examinarea unei game variate de indicatori și parametri care reflectă starea și istoricul unui domeniu în cadrul registrelor și infrastructurii internet. Un aspect extrem de relevant în analiza reputației unui domeniu este starea sa de înregistrare sau statusul. Domeniile active, care sunt înregistrate și nu sunt expirate, sunt de obicei considerate mai credibile decât cele care sunt inactive sau expirate.

Figura 2 indică sursele de date de intrare și conexiunile dintre ele.

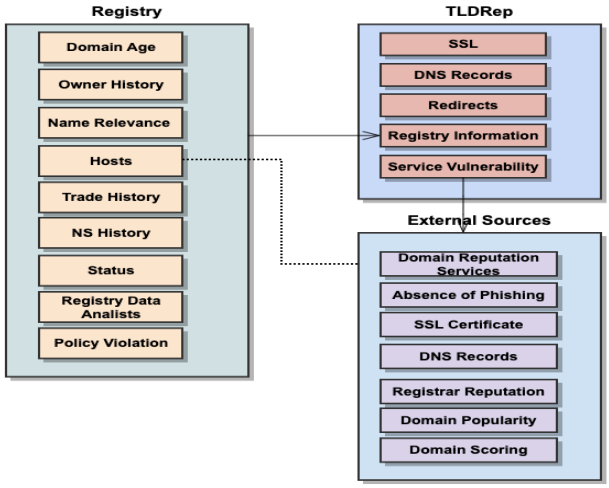

Figura 2. Criterii pentru stabilirea reputației numelor de domenii

Parametrii care determină o bună reputație pentru un nume de domeniu pot varia în funcție de context. Factorii generali care sunt în mod obișnuit luați în considerare pentru determinarea reputației unui domeniu, sunt din datele deținute de către Registrul .ro:

- Vechimea domeniului. Un domeniu care a fost înregistrat pentru o perioadă mai lungă de timp poate avea o reputație mai bună;
- Istoricul deținătorului. Un domeniu care a avut un istoric curat, fără transferuri frecvente, are mai multe șanse să aibă o bună reputație;
- Relevanța numelui de domeniu. Un nume de domeniu care este relevant pentru conținutul, afacerea sau scopul său are mai multe șanse să fie de încredere și să aibă o reputație bună;
- Istoricul host-urilor poate oferi informații valoroase ce pot fi explorate pentru a determina reputația unui domeniu;
- Istoricul trade-urilor poate oferi informații despre cât de des este schimbat deținătorul domeniului;
- Istoricul NS oferă istoricul modificărilor serverelor de nume și atunci când serverele de nume sunt schimbate frecvent, de exemplu zilnic, când poate fi un indicator pentru un nume de domeniu compromis;
- Starea domeniului este un indicator al reputației acestuia;
- Datele colectate de către analiștii de date ai Registrului includ parametri existenți ai unui domeniu și feedback-ul utilizatorilor, iar rezultatele pot fi înregistrate ca indicator pentru determinarea reputației unui domeniu;

- Încălcarea politicilor arată cât de des un nume de domeniu a fost supus unor dispute legate de numele de domeniu: soluționate prin acord, acțiune în justiție sau arbitraj.

De asemenea, informații din surse externe Registrului pot fi utilizate pentru a stabili reputația unui nume de domeniu. Astfel de informații includ:

- Evaluarea furnizată de către servicii terțe de reputație de domeniu. Un domeniu care este listat ca fiind sigur pentru navigarea pe Google sau Norton Safe Web, poate avea o reputație bună, deoarece sugerează că domeniul a fost examinat și verificat ca sigur de către servicii terțe de încredere;
- Absența activităților de phishing. Un domeniu care nu este implicat în activități de phishing precum trimiterea de e-mailuri nesolicitate, postarea de reclame nedorite sau participarea la activități de tip phishing, are o reputație bună;
- Un domeniu cu un certificat SSL valid poate indica faptul că proprietarul domeniului ia în serios securitatea și acordă importanță securității;
- Înregistrări DNS: este mai probabil să fie de încredere un domeniu cu înregistrări DNS configurate corect și fără indicii de deturnare a DNS;
- Reputația registrarului. Există registrari care înregistrează și domenii cu reputație proastă, iar acesta este alt factor care trebuie luat în calculul reputației;
- Popularitatea domeniului. Un domeniu care este frecvent vizitat și are un volum mare de trafic poate indica faptul că este de încredere și util;
- Scorul domeniului este furnizat de serviciile externe de scoring ale domeniilor utilizate pe scară largă pentru a determina dacă un domeniu este de încredere sau nu;
- Informații DNS;
- Numărul de redirecționări;
- Service Vulnerability evaluează reputația domeniului utilizând surse externe de informații.

Dintre aspectele menționate mai sus acest studiu are ca obiectiv analiza statusului domeniilor în contextul stabilirii reputației. Pentru aceasta a fost extras un eșantion de 1000 de nume de domenii împreună cu informațiile relevante din baza de date a registrului pentru evaluarea reputației unui domeniu.

În primă fază au fost utilizate instrumente de interogare a bazei de date bazate pe utilizarea limbajului de interogare structurat (SQL) pentru a prelua datele relevante. A fost creată o interogare care selectează un eșantion aleatoriu de 1000 de nume de domenii din baza de date. În continuare au fost identificate informațiile despre domeniile relevante pentru evaluarea reputației domeniului. Acestea includ Vvârsta, numărul de trade-uri, status, și dacă utilizează sau nu DNSSEC.

După ce au fost generate datele relevante, acestea au fost exportate din baza de date într-un format adecvat pentru analiză CSV (Comma-Separated Values), asigurând totodată păstrarea integrității înregistrărilor originale ale bazei de date.

Având în vedere politica GDPR - General Data Protection Regulation (GDPR, 2018) cu privire la protecția datelor cu caracter personal, în cadrul acestui studiu vom anonimiza exemplele de nume de domenii prin hashing, folosind o funcție hash criptografică. Acest proces convertește numele de domeniu într-un șir unic de caractere (hash) care nu poate fi reproiectat pentru a dezvălui numele de domeniu original. În acest sens a fost dezvoltat următorul script în Python:

```
import hashlib
def anonymize_domain(domain):
    # Convert the domain name to bytes (required by hashlib)
    domain_bytes = domain.encode('utf-8')
    # Use SHA-256 hash function to hash the domain name
    hashed_domain = hashlib.sha256(domain_bytes).hexdigest()
    return hashed_domain
# Example usage
```

```
domains = ['example.com', 'google.com', 'facebook.com']
anonymized_domains = {}
for domain in domains:
    anonymized_domains[domain] = anonymize_domain(domain)
print(anonymized_domains)
```

Tabelul 1 descrie o fracțiune din setul de date utilizat în cadrul acestui studiu pentru analiza impactului statusului unui domeniu asupra reputației. Pe lângă informații referitoare la status au fost extrase și alte informații relevante precum vârsta, numărul de trade-uri și utilizarea DNSSEC (DsData) pentru a observa eventuale corelații.

Tabel 1. Date despre domenii deținute de Registru

Nume domeniu	Vârsta	Nr trade-uri	Status	DsData
358632832e34c03f7caa751a0e06f037c7251d34bf47a54f942bfec491d44a76	1 year 5 mons 6 days 04:39:56	0	pD , Rp	No
6b02b94b8b879dacb77129ee4ff023cd547b51ed148d6b1db9354958a9c111aa	1 year 5 mons 6 days 04:40:55	0	pD , Rp	No
0924599784352701819 50aaa3f4fdcf4c5e1c67d6446b8f1497233a79ec0346b	7 years 11 mons 8 days 09:20:31	1	Ok	No
59c9da2776eb783e9282a8f2c95fa6a4912eb413ea3ca77eb5356e0a6ceeefb1	4 years 7 mons 6 days 14:19:50	0	Ok	No
084d06d1a8a5aa7ef689166922eedeb6c987f2c23707bb64cc27c6dffa5079d4	8 years 8 mons 18 days 13:42:38	0	Ok	No
83ed3890d7e8bd97ec8f5a3b6d8fd6816a40e5728eee0e9bd234401dbd5dcda5	1 year 6 mons 4 days 13:11:56	0	Rp , pD	No
3974f37ad86d25b029276255a4af72ffa690c6c45480db130ff1df0057aacf2f	1 year 4 mons 22 days 05:20:56	0	Rp , pD	No
186d382b8b4c1bd87540390f046b15c44a40387e793ef685cdee2cebe8ee7c43	1 year 5 mons 20 days 18:40:55	0	pD , Rp	No
96d857d213f0388835c170bccd46671efb003525e1981cba4dd8ef73e420ce0a	1 year 4 mons 22 days 05:21:56	0	Rp , pD	No
0118e79164dc162be1cfcdc512419baf8c8d84512a7b28403d3ad28b9c2cbec7	1 year 4 mons 22 days 05:22:55	0	pD , Rp	No
09dfccb5835b4459d829df7a6fa37fbaabec179745716a9e25e91b9654da4f0f	9 mons 16 days 09:02:54	0	Rp , RTp , Tp , Up , H	No
4bc61e1126cad4cf502c46f8f4a2a1463d8dc8fd7087017553ded8ee64b6bea2	9 mons 16 days 09:48:44	0	H , Up , Tp , RTp , Rp	No

Utilizând datele extrase, în continuarea studiului, a fost evaluată reputația fiecărui domeniu raportat la statusurile identificate.

Evaluarea se bazează pe potențialele implicații ale fiecărui statutus asupra funcționalității, securității și credibilității percepute a unui domeniu. Domeniile cu stări precum "OK", „Reserved" și „ RegistrantTransferProhibited" contribuie pozitiv la reputație, în timp ce stări precum „Hold" și „PendingDelete" pot avea un impact negativ. Altele, precum „DeleteProhibited" și „UpdateProhibited" servesc în primul rând scopuri administrative sau de securitate, dar contribuie indirect la creșterea gradului de încredere al unui nume de domeniu. Statusurile domeniilor .ro sunt detaliate în continuare:

1. Starea „Ok" indică faptul că domeniul este în stare optimă în baza de date a Registrului și îndeplinește toate cerințele necesare, precum informații de contact valide și conformitatea cu politicile de înregistrare. Domeniile cu statutul „OK" sunt considerate active și funcționale, și au un scor de reputație pozitiv. Acestea sunt, în general, accesibile utilizatorilor și sunt mai puțin susceptibile de a întâmpina probleme cu clasarea în cadrul motoarelor de căutare.

2. Domeniile cu starea „DeleteProhibited" nu pot fi șterse din baza de date a Registrului. Această stare se aplică de obicei pentru a preveni ștergerea accidentală sau neautorizată a domeniului. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, asigură stabilitatea domeniului și previne pierderea neintenționată a proprietății, care poate contribui indirect la menținerea unei reputații pozitive.

3. Starea „Hold" indică faptul că domeniul este suspendat sau plasat în așteptare de către registrar sau Registru. Acest lucru se poate datora diverselor motive, precum neplata taxelor de înregistrare, încălcarea politicilor de înregistrare sau probleme juridice în curs. Domeniile aflate în starea „În așteptare" pot avea un scor de reputație negativ, deoarece sugerează probleme care fac ca domeniul să fie temporar inaccesibil sau neconform.

4. Domeniile cu starea „UpdateProhibited" nu pot fi actualizate. Această stare se aplică de obicei pentru a preveni modificările neautorizate ale informațiilor de înregistrare a domeniului. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, asigură integritatea detaliilor de înregistrare ale domeniului, contribuind indirect la menținerea încrederii și stabilității.

5. O stare „Locked" înseamnă că domeniul este blocat pentru a preveni transferurile neautorizate. Această stare este o măsură de securitate standard pentru a proteja împotriva furtului de domeniu sau a modificărilor neautorizate de proprietate. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, asigură securitatea și stabilitatea proprietății domeniului, contribuind indirect la menținerea încrederii și stabilității.

6. Domeniile cu statutul „RenewProhibited" nu pot fi reînnoite la nivel de registru. Acest statut se aplică de obicei atunci când există probleme precum plăți restante sau chestiuni legale în curs, care împiedică reînnoirea domeniului. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, indică probleme potențiale care trebuie abordate pentru a menține starea activă și reputația pozitivă a domeniului.

7. Starea „RegistrantTransferProhibited" împiedică transferul domeniului către un alt solicitant. Similar cu starea „Locked", este o măsură de securitate pentru a preveni modificările neautorizate de proprietate sau deturnarea domeniului. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, asigură securitatea și stabilitatea proprietății domeniului, contribuind indirect la menținerea încrederii.

8. Domeniile cu statutul „Reserved" sunt de regulă rezervate pentru scopuri specifice, cum ar fi utilizarea viitoare. Această stare indică faptul că domeniul nu este în prezent disponibil pentru înregistrare. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, înseamnă circumstanțe speciale legate de disponibilitatea domeniului, care pot afecta sau nu valoarea percepută a acestuia.

9. Starea „RegistrantPendingTransfer" indică faptul că un transfer al domeniului către un alt solicitant de înregistrare este în așteptare. Este o stare temporară în timpul procesului de transfer, de obicei după ce solicitantul actual al înregistrării a inițiat transferul, dar înainte ca acesta să fie finalizat. Deși nu afectează în mod direct funcționalitatea sau reputația domeniului, semnalează un proces administrativ în curs de desfășurare care va duce la o schimbare a proprietății, care poate sau nu afecta valoarea percepută a acestuia.

10. Domeniile cu starea „PendingDelete" sunt programate pentru ștergere din registru.

Această stare apare de obicei după ce un domeniu a expirat și a trecut prin perioada de grație fără reînnoire sau răscumpărare. Domeniile în acest statut sunt efectiv inactive și vor deveni în curând disponibile pentru înregistrare de către publicul larg. Această stare poate avea un impact negativ asupra reputației, deoarece sugerează probleme precum abandonul sau utilizarea greșită, care au dus la ștergerea iminentă a domeniului.

Fiecare dintre stările unui nume de domeniu are implicații diferite asupra reputației acestuia. Tabelul 2 reproduce fiecare stare pe baza impactului său potențial asupra reputației unui domeniu, folosind o scală de la 1 la 10, unde 10 reprezintă un impact pozitiv și 1 reprezintă un impact negativ.

Stările posibile pentru domeniile .ro și impactul acestora asupra reputației sunt prezentate în Tabelul 2:

Tabel 2. Statusul domeniile .ro și impactul acestora asupra reputației

Nr.	Stare	Semnificație	Impact
1.	OK	Această stare indică un domeniu în stare bună, având un impact pozitiv asupra reputației sale.	10
2.	DeleteProhibited	Deși nu afectează în mod direct reputația, asigură stabilitatea domeniului, ceea ce contribuie indirect la o reputație pozitivă.	9
3.	Hold	Această stare sugerează probleme cu domeniul, care pot duce la un impact negativ asupra reputației.	4
4.	UpdateProhibited	Asigură integritatea detaliilor de înregistrare a domeniului, contribuind indirect la o reputație pozitivă.	6
5.	Locked	Această măsură de securitate ajută la prevenirea modificărilor neautorizate de proprietate, contribuind indirect la o reputație pozitivă.	10
6.	RenewProhibited	Indică probleme potențiale care necesită rezolvare, care ar putea avea un impact neutru până la ușor negativ asupra reputației.	5
7.	RegistrantTransferProhibited	Similar cu „Locked”, ajută la prevenirea modificărilor neautorizate de proprietate, contribuind indirect la o reputație pozitivă.	8
8.	Reserved	Deși nu are un impact direct asupra reputației, poate semnifica un domeniu valoros sau special, care poate avea un impact pozitiv asupra reputației.	10
9.	RegistrantPendingTransfer	Indică o stare temporară în timpul unui proces de transfer, care poate să nu afecteze în mod direct reputația, dar înseamnă activitate administrativă.	8
10.	PendingDelete	Această stare sugerează abandonarea domeniului sau utilizarea greșită, care poate avea un impact negativ semnificativ asupra reputației.	3

6. Concluzii

Prin stabilirea nivelului de reputație al domeniului/domeniilor deținute, actualii și viitorii proprietari ai acestora (autorități, instituții de stat, companii private, persoane fizice etc.) vor avea o imagine corectă a gradului de încredere al domeniului deținut, creând astfel un spațiu de Internet mai sigur.

Scopul acestui studiu este de a crea premisele pentru dezvoltarea unui framework pentru determinarea reputației numelor de domenii .ro cu rolul de a spori nivelul de încredere și a proteja domeniile împotriva activităților rău intenționate din spațiul Internet. Natura extrem de dinamică a ecosistemului de nume de domenii și proliferarea domeniilor rău intenționate care reprezintă o amenințare reală și imediată la adresa confidențialității și securității persoanelor și companiilor, sunt principalele cauze care necesită găsirea unei soluții automate pentru stabilirea nivelului de reputație al unui domeniu .ro și monitorizarea continuă a acestuia de-a lungul vieții sale.

Rezultatele oferă o imagine de ansamblu cuprinzătoare a diferitelor stări ale numelor de domenii, semnificațiile acestora și impactul lor asupra reputației și subliniază importanța critică a stabilității, integrității și securității domeniului, pentru a menține o reputație pozitivă în peisajul digital. Domeniile în stare bună, precum cele etichetate „Ok" sau „Reserved" sunt asociate cu un scor al reputației pozitiv, în timp ce stări precum „PendingDelete" sau „RenewProhibited" semnalează probleme potențiale care ar putea afecta reputația. Înțelegerea și gestionarea eficientă a acestor stări de domeniu sunt esențiale pentru companii și persoane deopotrivă, pentru a-și proteja reputația online și pentru a menține încrederea și credibilitatea cu publicul lor.

Pe baza acestui studiu va fi dezvoltat un model experimental care va acționa asupra setului de date anonimizate din registrul de domenii .ro. Prototipul dezvoltat va fi folosit pentru detectarea și monitorizarea domeniilor înregistrate rău intenționate. Folosind un sistem de reputație a domeniilor (Rotună et al., 2023), Registrele și registrarii pot obține informații valoroase despre domeniile compromise și pot lua măsuri proactive pentru a atenua amenințările cibernetice.

Confirmare

Acest articol a fost realizat în cadrul proiectului „Platforma de monitorizare automată a domeniilor Internet prin dezvoltarea unui sistem dinamic de stabilire a reputației (TLDRep)" finanțat de către Ministerul Cercetării, Inovării și Digitalizării (MCID), prin Programul Nucleu PN 2338 02 01 și al proiectului „Instrumente de transformare digitală pentru eGuvernare prin utilizarea domeniilor .ro" finanțat de Academia Oamenilor de Știință din România prin competiția „AOSR-TEAMS-II" EDIȚIA 2023-2024 – „Transformarea digitală în științe". Mulțumim colegilor participanți pentru colaborare.

REFERINȚE BIBLIOGRAFICE

Akumiah, E. (2016) ccTLD Best Practices. https://www.slideshare.net/gsorkpor/cctld-best-practices [Accessed 17th January 2024]

Albitz, P. & Liu, C. (2006) *DNS and BIND*. O'Reilly Media.

Alrwais, S. et al. (2017) Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks. In *2017 IEEE Symposium on Security and Privacy (SP), 2017. San Jose, CA, USA*. pp. 805-823. doi: 10.1109/SP.2017.32.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J. et al. (2017) Understanding the Mirai Botnet. *In Proceedings of the 26th USENIX Security Symposium, August 16-18, 2017, Vancouver, Canada.* pp.1093-1110.

Antonakakis, M., Dagon, D., Luo, X., Perdisci, R., Lee, W. & Bellmor, J. (2010). A Centralized Monitoring Infrastructure for Improving DNS Security. In: Jha, S., Sommer, R., Kreibich, C. (eds) *Recent Advances in Intrusion Detection*. RAID 2010. Lecture Notes in Computer Science, 6307. Springer. pp.18-37.

Antonakakis, M., Perdisci, R., Dagon, D. & Lee, W. (2011) Detecting Malware Domains at the Upper DNS Hierarchy. In *Proceedings of the 20th USENIX Security Symposium, August 10-12,2011, San francisco, CA.* pp.1-16.

Banciu, D., Petre, I. & Dumitrache, M. (2019) Electronic system for assessing and analysing digital competences in the context of Knowledge Society. In: *Proceedings of the 11th International*

Conference on Electronics, Computers and Artificial Intelligence, ECAI 2019, June 27-29, 2019, Pitesti, Romania.pp.1-4. IEEE. doi: 10.1109/ECAI46879.2019.9042151.

Cîrnu, C.E., Rotună, C.-I., Vevera, A.-V. & Boncea, R. (2018) Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Studies in Informatics and Control*. 27(3), 359-368. doi: 10.24846/v27i3y201811.

Deland-Han (2022) *Troubleshooting Domain Name System (DNS) issues.* https://learn.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/troubleshoot-dns-data-collection [Accessed 17th January 2024].

Dumitrache, M., Sandu, I.-E., Udroiu, A.M. & Gheorghiță, C.-A., (2023) Considerații teoretice privind stabilirea reputației unui domeniu Internet (Theoretical considerations about establishing the Internet domain reputation). *Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control)*. 33(1), 81-92.doi:10.33436/v33i1y202307.

Fukushima, Y., Hori, Y. & Sakurai, K. (2011) *Proactive Blacklisting for Malicious Web Sites by Reputation Evaluation Based on Domain and IP Address Registration*. doi:10.1109/TrustCom.2011.46.

GDPR (2018) *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/ [Accessed 10th February 2024].

Gheorghiță, C.-A., Smada, D., Vevera, A.-V., Dumitrache, M., Sandu, I.-E. & Rotună, C.-I. (2023) Listele negre și listele albe în cadrul unui sistem de reputație a domeniilor (Blacklists and whitelists in the framework of a domain reputation system). *Revista Română de Informatică și Automatică* (*Romanian Journal of Information Technology and Automatic Control*). 33(4), 33-46. doi:10.33436/v33i4y202303.

Hao, S. & Wang, Haining. (2017) Exploring Domain Name Based Features on the Effectiveness of DNS Caching. ACM SIGCOMM Computer Communication Review. 47 (1). doi:10.1145/3041027.3041032.

Khalil, I.M., Guan, B., Nabeel, M. & Yu, T. (2017) Killing Two Birds with One Stone: Malicious Domain Detection with High Accuracy and Coverage. [Preprint] http://arxiv.org/abs/1711.00300.

Marshall, D. (2019) *History of the Internet: Timeline*. http://www.netvalley.com/archives/mirrors/davemarsh-timeline-1.htm [Accessed 2th February 2024].

Mishsky, I & Gal-Oz, N. (2015) A Topology Based Flow Model for Computing Domain Reputation. *IFIP Annual Conference on Data and Applications Security and Privacy*. pp. 277-292. Doi:10.1007/978-3-319-20810-7_20.

OWASP (2020) *Open Source Foundation for Application Security*. https://www.owasp.org [Accessed 28th January 2023].

Rotună, C.-I., Dumitrache, M. & Sandu, I.-E. (2022) Evaluarea algoritmilor de învățare automată pentru monitorizarea automata (Assessment of Machine Learning algorithms for automated monitoring). *Revista Română de Informatică şi Automatică (Romanian Journal of Information Technology and Automatic Control)*. 32(3), 73-84. doi:10.33436/v32i3y202206.

Rotună, C.-I., Gheorghiță, C.-A., Sandu, I.-E., Dumitrache, M., Udroiu, A.M. & Smada, D. (2023) A Generic Architecture for Building a Domain Name Reputation System. *Studies in Informatics and Control*. 32(2), 39-49. doi: 10.24846/v32i2y202304.

Sarkar, M., Banerjee, S. & Hassanien, A. (2013) Searching DNS for malicious domain registration: identification through hybrid cuckoo search metaphor and object-oriented implementation. *International Journal of Reasoning-based Intelligent Systems*. 5(4), 280 - 289. doi:10.1504/IJRIS.2013.058773.

Scalzo F. (2017) *DNS-based threats: DNS reflection and amplification attacks*. https://blog.verisign.com/security/dns-based-threats-dns-reflection-amplification-attacks/ [Accessed 17th January 2023].

Stăicuț, E. (1995) Domain Name Systems, InterNic and RIPE Procedure. In: *Proceedings of the NATO Advanced Networking Workshop, The First CEENet Workshop on Networks Technology, The road to Global connectivity*. *A CEEet Publication, September 15-24, Varşovia, Polonia.*

Dragoș SMADA a absolvit Facultatea de Electronică, Telecomunicații și Tehnologia Informației, Universitatea Națională de Știință și Tehnologie Politehnica București. Absolvent de Master în Managementul Informațiilor și Documentelor din cadrul Universității București. În prezent este cercetător științific la ICI București. Principalele sale domenii de interes sunt Big Data, Internetul obiectelor, inginerie software, securitate informatică, arhitectură software. A participat în proiecte de cercetare naționale și internaționale din domeniul TIC și a publicat rezultatele în articole de specialitate din reviste și conferințe IT.

Dragoș SMADA graduated the Faculty of Electronics, Telecommunications and Information Technology at the National University of Science and Technology Politehnica Bucharest. He has a Master's Degree in Information and Documents Management at the National University of Science and Technology Politehnica Bucharest. He is currently a scientific researcher at ICI Bucharest. His main areas of interest are Big Data, Internet of Things, software engineering, information security, software architecure. He participated in both national and international research projects in the IT&C. He published as author and co-author of journal articles and scientific presentations at conferences.

Mihail DUMITRACHE este absolvent al Facultății de Electrotehnică, Universitatea Națională de Știință și Tehnologie Politehnica București, specializarea „Inginerie Asistată de Calculator”, inginer și doctor în Inginerie Electrică. Deține două diplome de master în specializarea „Inginerie Electrică”, Universitatea Națională de Știință și Tehnologie Politehnica București și în specializarea „Administrație Publică Electronică”, Universitatea din București. Și-a început activitatea profesională în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București în anul 2002, ca programator. În prezent este Cercetător științific gradul II, Șef la Departamentul „Administrare domenii RoTLD” – ICI București și Lector Universitar la Universitatea din București. Este autor și coautor al unor studii și articole de specialitate.

Mihail DUMITRACHE graduated from National University of Science and Technology Politehnica Bucharest, the Faculty of Electrical Engineering with the specialization “Computer Assisted Engineering”, he is an engineer and holds a Ph.D. degree in Electrical Engineering. In between, he obtained two Master’s Degrees, one in Electrical Engineering at National University of Science and Technology Politehnica Bucharest and one in Electronic Public Administration, at the National University of Science and Technology Politehnica Bucharest. His professional career started at the National Institute for Research and Development in Informatics – ICI Bucharest in 2002 as a computer programmer. Currently, he is a Scientific Researcher II and Head of the .ro Domain Administration Department (RoTLD) – ICI Bucharest and also a Lecturer at the University of Bucharest. He is the author and co-author of several scientific studies and articles.

Carmen-Ionela ROTUNĂ este Doctorand la Universitatea Națională de Știință și Tehnologie Politehnica București, domeniul „Ingineria Sistemelor” și a absolvit programul de master la Facultatea de Matematică și Informatică din cadrul Universității din București. În prezent este Cercetător Științific în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București, unde desfășoară activități de cercetare în domeniile: eGovernment, eServices, Cloud, Big Data și AI, fiind autor și coautor al unor articole publicate în reviste de specialitate și volume de conferință recunoscute la nivel național și internațional, precum livrabile de proiect și cărți. Totodată a participat la proiecte naționale și europene din aria IT&C: SPOCS – Simple Procedures Online for Cross-border Services (CIP-ICTPSP), eSENS - Electronic Simple European Networked Services (CIP ICT), Cloud for Europe C4E (FP7), TOOP - The “Once-Only” Principle Project (H2020), unde a avut rolul de coordonator la nivel național pentru pachetul de lucru WP2: Arhitectură și WP3: Pilotare. În prezent este implicată în proiectul EUROCC – National Competence Centres in the framework of EuroHPC cu rol de coordinator în cadrul pachetului de lucru WP3.

Carmen-Ionela ROTUNĂ is a Ph.D. student at the National University of Science and Technology Politehnica Bucharest, in the field of Systems Engineering and graduated with a Master's Degree from the Faculty of Mathematics and Computer Science of the University of Bucharest. Currently, she is a Scientific Researcher at the National Institute for Research and Development in Informatics – ICI Bucharest, where she conducts research activities in eGovernment, eServices, Cloud, Big Data and AI, also being the author and co-author of various articles published in specialized journals and conference proceedings recognized nationally and internationally, of project deliverables and books. She was also a team member in national and European projects in the IT&C area: SPOCS - Simple Procedures Online for Cross-border Services (CIP-ICT PSP), eSENS - Electronic Simple European Networked Services (CIP ICT), Cloud for Europe C4E (FP7), TOOP - The "Once-Only" Principle Project (H2020), where she was the national coordinator for the WP2: Architecture work package and national coordinator for WP3: Project Piloting. She is currently WP3 leader in EUROCC – National Competence Centres in the framework of EuroHPC project.

Cristian-Alexandru GHEORGHIȚĂ a absolvit Facultatea de Informatică din cadrul Universității din București, în anul 2013. Este doctorand la Facultatea de Automatică și Calculatoare, Universitatea Națională de Știință și Tehnologie Politehnica București. În prezent lucrează ca cercetător în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. Principalele sale domenii de interes sunt: Cyber Security, Big Data, Cloud Computing, Cloud-Native, DevOps. Este implicat în proiecte de cercetare specifice societății informaționale. Cercetările sale au fost publicate în articolele revistelor de specialitate și în lucrările conferințelor științifice.

Cristian-Alexandru GHEORGHIȚĂ graduated the Faculty of Informatics, University Bucharest in 2013. He is a Ph.D. student at Faculty of Computer Science and Automatics, National University of Science and Technology Politehnica Bucharest. Currently he works as Researcher at I.C.I Bucharest. His main areas of interest are Cyber Security, Big Data, Cloud Computing, Cloud-Native, DevOps. He is involved in research projects specific to the Information Society. His research was published in journal articles and proceedings of conferences.