Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

Studiul Securității Cibernetice și Protecției Datelor Sensibile în Administrația Publică Locală (Studiu de caz – București 2020-2025)

- lucrare de licență Administrație Europeană -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Bardici Luca-Alexandru

București
2026

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarația anti-plagiat și nici instrucțiunile** – acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile, Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării;
11. **Respectarea deadline**-urilor stabilite de profesorul coordonator este obligatorie.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development / Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository - ISSN: 3008-2196, ISSN-L: 3008-2196: https://scrd.eu/index.php/spr/issue/archive.

ATENȚIE: Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat

1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice).

2. Declar că nu am permis și nu voi permite nimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.

3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.

Numele și prenumele: Bardici Luca-Alexandru

Data și semnătura: 16.12.2025 

Cuprins

Glosar

- Administrație Publică = Ansamblul de instituții publice ce au ca rol principal implementarea legilor, politicilor și a valorilor statului, ce oferă servicii cetățenilor, mențin o linie de comunicare cu aceștia și gestionează resursele publice.
- TIC = Tehnologia Informației și a Comunicării
- Hardware = Componenta fizică a unui sistem digital
- Software = Componenta virtuală a unui sistem digital
- Infrastructură IT a Administrației Publice = Rețea de sisteme și echipamente de tip TIC din cadrul statului care asigură stocarea, gestionarea și protecția datelor publice.
- Digitalizarea în Administrația Publică = Procesul de adoptare a tehnologiilor informației și a comunicării în cadrul instituțiilor publice.
- Atac cibernetic = Infracțiune desăvârșită de un actor ce poate fi intern sau extern, individual sau un grup, cu scopul de a manipula date importante din cadrul unei infrasturcturi digitale sau chiar pentru funcționarea acesteia. [1]
- Securitate Cibernetică = eng. „Cybersecurity", concept definit ca ansamblul de măsuri și tehnologii adoptate pentru protejarea sistemelor digitale de pretutindeni împotriva accesului neautorizat sau altor tipuri de atacuri cibernetice.
- Breșă de securitate = Incident în urma căreia se constată manipularea, pierderea sau distrugerea unor date fără autorizație.
- Vulnerabilitate cibernetică = Punct slab ce poate fi exploatat pentru accesarea neautorizată a unui sistem, unei baze de date sau unei infrastructuri digitale cu scopul de a manipula datele stocate.
- DDoS = Denumire completă „Distributed Denial of Service", este un tip de atac cibernetic ce are ca rol îngreunarea unei infrastructure digitale prin coordonarea unei rețele de sisteme și conectarea repetată într-un tip foarte scurt a tuturor acestora.
- Phishing = Modalitate de atac folosită de actori infracționali pentru a păcăli utilizatorul unui sistem cu scopul de a afla informații sensibile, confidențiale, precum parole, adrese de e-mail, date de conectare la anumite platforme și sisteme.
- Program malițios = Aplicație sau proces software ce are ca rol afectarea în mod negativ a unui sistem digital.
- E-Guvernare = Reprezintă guvernarea fără hârtie sau interacțiune fizică dintre cetățean și funcționar public prin folosirea tehnologiei informației și a comunicării. [2]
- GDPR = Denumire completă „General Data Protection Regulation", reprezintă regulamentul adoptat de către Uniunea Europeană în anul 2016, fiind aplicat statelor membre și ratificat de acestea în anul 2018 ce reglementează protecția datelor personale. [3]
- Directiva NIS = eng. „Network and Information Systems Directive", tradus „Directiva privind securitatea rețelelor și a sistemelor informatice", directiva Uniunii Europene în ceea ce privește securitatea cibernetică.
- Directiva NIS2 = Varianta în vigoare a Directivei NIS.
- Politici de securitate = Proceduri implementate de o instituție sau organizație în vederea protejarea sistemelor digitale.
- DNSC = Directoratul Național de Securitate Cibernetică, autoritate națională din România responsabilă cu implementarea politicilor de securitate.

- Criptarea datelor = Transformarea datelor într-un format neinteligibil pentru posibili actori ostili prin utilizarea unor algoritmi criptografici.
- Inteligență Artificială (Artificial Intelligence/AI) = Tehnologie ce imită comportamentul uman prin analizarea unor date, să învețe modele și sa ia decizii în mod autonom pe baza unor algoritmi avansați.
- Tehnologie Cloud = Reprezintă sisteme hardware la care accesul este făcut prin intermediul internetului.
- Computer = Ansamblul de componente hardware și software ce permite vizualizarea, stocarea, procesarea și manipularea datelor în format electronic.
- •Server = Un server este un sistem mai puternic din punct de vedere al componentelor hardware ce este conceput să stocheze, proceseze și să livreze date și servicii altor „clienți" prin Internet sau printr-o rețea locală.
- Client = Denumirea unui computer conectat la o rețea.
- CERT = eng. Computer Emergency Response Team, Echipa de Răspuns la Incidente de Securitate Cibernetică.
- CSIRT = eng. Computer Security Incident Response Team, abreviere folosită pentru echipele CERT întâlnită des la nivel european.
- Cod sursă = Codul ce stă la baza programului.
- Dark Web = Reprezintă o parte a Internetului ce este, în mod normal, inaccesibila publicului, unde se pot găsi operațiuni ilegale precum vânzarea de contrabandă, licitații de date sensibile, etc.
- Internet-of-Things (IoT) = Tradus ca „Internetul lucrurilor", reprezintă dispozitive fizice echipate cu senzori și software special cu scopul de a conecta și face schimb de date cu alte dispozitive conectate la Internet și să afișeze datele interpretate pe o interfață de utilizator.
- Malware = Program malițios
- Firewall = „Paravanul de protecție" a unui sistem sau a unei rețele, acesta poate fi atât un element software cât și unul hardware și are rolul de a filtra conexiunile dintre două sisteme, acesta fiind cel care decide cine intră sau cine nu. [4]
- Port = Reprezintă portița de acces ce trebuie folosită pe lângă IP atunci când un sistem se conectează la server web prin intermediul Internetului.
- IP (Internet Protocol) = Adresă unică, numerică, atribuită fiecărui dispozitiv conectat la un server pentru identificarea acestuia.
- Zero-Day = Termenul se referă la lipsa de timp dintre momentul în care o vulnerabilitate este descoperită, în anumite cazuri și exploatată, și este recunoscută public sau chiar remediată de către furnizorul software.
- API = eng. Application Programming Interface, set de reguli și protocoale care permit comunicarea și schimbul de date dintre două aplicații, acesta acționând ca un intermediar.
- APT = eng. „Advanced Persistent Threat", tradus „Amenințare Persistentă Avansată", atacuri constante ce fac parte din operațiuni ofensive împotriva unui sistem, unei rețele sau infrastructuri cu mai multe scopuri ce vizează furtul de date sensibile.
- Hacker = Termen preluat din limba engleză pentru a desemna un individ specializat în atacuri cibernetice.
- Hacktivism = Activități de hacking realizate de actori ce au ca scop promovarea unor valori proprii ce pot fi de natură politică, religioasă etc.

- Doxing = Expunerea datelor personale ale unui individ în spațiul public.

- White Hat = Hacker ce acționează în mod legal, plătit de diferite firme și instituții publice pentru a testa gradul de securitate al infrastructurii IT din posesia acestora.

- Grey Hat = Hacker ce acționează atât în mod legal cât și ilegal în anumite cazuri pentru a arăta posesorilor de rețele de sisteme vulnerabilitățile și modul în care acesta le-a exploatat cu scopul de a primi o recompensă monetară.

- Black Hat = Hacker ce acționează în mod ilegal pentru a sparge baze de date cu scopul de a fura conținutul acestora sau a-l distruge.

- Adware = Program descărcat de obicei gratuit ce supraîncarcă interfața utilizatorului cu reclame.

- Ransomware = Program ce, odată activ pe un sistem, criptează fișiere și le ține „ostatice" până la plata unei sume monetare. Unele programe de acest tip includ și amenințări cu scoaterea la licitație pe Dark Web a datelor criptate în cazul neplății sumei cerute într-o anumită limită de timp. [5]

- Scareware = Program asociat des cu un escroc, acționează printr-un pop-up ce spune că sistemul pe care îl utilizăm este infectat, acesta propunând o soluție falsă de curățare a acestuia în schimbul unei sume de bani. Atât avertismentul cât și soluția propusă sunt false, apelând la utilizatorii mai naivi.

- Spyware = Program ce colectează în secret date și informații personale sau sensibile.

- Trojan Virus = Un virus ce se arată a fiind un program normal și inofensiv, dar odată accesat acesta poate face o multitudine de lucruri generând, în principiu, daune.

- Virus = Reprezintă cel mai clasic tip de malware, acesta se atașează de fișiere legitime și se răspândește infectând din ce în ce mai multe părți din sistem.

- Worm = Malware ce nu are nevoie de o aplicație „gazdă", acesta se înmulțește și face ravagii în rețele și computere, ca un parazit. [6]

- Terminal = Dispozitiv ce permite utilizatorului accesarea rețelei.

- HTTPS = eng. „HyperText Transfer Protocol Secure", protocol securizat folosit de site-uri web legitime.

- MFA = eng. „Multi-Factor Authentication", autentificare în mai mulți pași. Procedeul prin care se adaugă un pas în plus la autentificarea prin user și parolă, de obicei printr-un cod trimis pe telefon sau pe e-mail, pentru a minimiza riscul de furt al unui cont.

- SOC = eng. „Security Operation Center", centru de operațiuni de securitate. Echipă care se ocupă cu monitorizarea permanentă a traficului de date, prevenirea și detectarea amenințărilor și rezolvarea problemelor apărute în urma unei breșe de securitate cibernetică. [7]

- Backdoor = Portiță de acces folosită de un actor digital pentru a accesa mai ușor un sistem, rețea sau infrastructură IT.

Abstract

Lucrarea are ca scop să explice anumite concepte importante atât pentru siguranța publicului, cât și pentru cea a lucrătorilor din domeniul administrativ local. Un alt obiectiv este să evidențieze problemele existente în prezent în ceea ce privește securitatea digitală și protejarea datelor cu caracter sensibil și să ofere soluții relevante care vor asigura longevitatea sistemelor. Studiile realizate în prealabil cuprind, dar nu se limitează la: Suportul cursului „Managementul datelor cu caracter personal în sectorul public" din cadrul facultății de Administrație Publică din cadrul Școlii Naționale de Studii Politice și Administrative (SNSPA); concepte fundamentale de protecția datelor și de securitate cibernetică, o meta-analiză a diferitelor cercetări și studii din domenii tehnice și legislative. În realizarea acestui studiu stau la bază două surse de informații vitale: un interviu cu un specialist din domeniul tehnic și un studiu de caz realizat independent. Concluziile care reies din acest studiu propriu sunt că România are niște baze solide ale unui sistem de securitate digitală și de protecție a datelor personale și sensibile, dar implementarea este una defectuoasă, care lasă de dorit, existând foarte multe oportunități de îmbunătățire. Dacă soluțiile propuse de această lucrare ar fi implementate, societatea civilă și spațiul administrativ ar fi mult mai protejate împotriva atacurilor cibernetice și interferențelor străine. Valoarea lucrării este una sporită deoarece este una din puținele studii din aceste domenii în spațiul românesc, care propune soluții sustenabile pentru probleme actuale.

Cuvinte cheie: E-Guvernare, Administrație Publică, Cybersecurity, Breșe de securitate

Introducere

În prezent, în era digitalizării, informația și securitatea acesteia sunt niște aspecte mai mult decat importante atât pentru mediul privat cât și pentru cel public și pentru societatea civilă. Administrația publică, atât la nivel de vârf cât și la nivel local, se confruntă cu aceleași dileme, și anume protecția datelor sensibile și vitale pentru administrație și pentru cetățeni. Digitalizarea sistemului administrativ a adus, pe lângă multe beneficii, multe riscuri ce arată multe vulnerabilități ce instituțiile statului trebuie să minimizeze sau chiar să elimine dacă este posibil, altfel compromiterea unui sistem poate duce la căderea celorlalte, lucru ce ar putea produce un dezastru și nemulțumiri în rândul publicului. Actori infracționali independenți sau organizați denumiți "hackeri" mereu vânează puncte slabe pentru a compromite sisteme, iar cele de stat nu sunt o excepție [8].

Atacurile cibernetice sunt de mai multe tipuri, începând de la cele mai ușor de repins, precum cele de tip phishing, care urmăresc păcălirea personalului instituției prin e-mail-uri false, cel DDoS (Distributed Denial of Service), care urmărește să împiedice un sistem din a funcționa la capacitatea propusă și optimă [9], și ajungând chiar și la tentativele de spargere a unei baze de date cu scopul de a fura date și ulterior cerând sume de răscumpărare sau chiar vânzarea acestora pe Dark Web [5]. Cele mai complexe și grave atacuri vizează de obicei elementele de infrastructură vitală, precum cele de energie, sănătate și justiție, dar nu uită și de bazele de date ale primăriilor în care se găsesc date personale ale cetățenilor, precum buletinele acestora și datele ce se regăsesc pe ele.

Atacurile avansate ce vizează infrastructura critică menționată anterior ne-au arătat de-a lungul timpului că pot produce niște pierderi uriașe în ceea ce privește eficiența acestora, dar și pierderi financiare, orice moment în care un sistem nu funcționează costând statul sume monetare semnificative, iar cetățenii își pot pierde încrederea din cauza nefuncționării infrastructurii digitale, efectele fiind produse într-un lanț lung dar care își produce efectele în mod rapid [10], [11], autoritățile urmărind să rezolve aceste probleme încă din momentul în care apar.

Pe lângă necesitatea vigilenței autorităților, cetățenii trebuie și ei la rândul lor să ia măsuri de siguranță în ceea ce privește securitatea digitală. Aceștia necesită educație în acest sens, care îi va ajuta să navigheze sigur pe Internet și să recunoască momentele în care cunoștintele le sunt puse la încercare, fie când este vorba de un e-mail care le promite câștigarea unor sume de bani dacă își introduc toate datele personale într-un site web suspicios, fie când este vorba de un val de atacuri din partea unor actori ostili iar aceștia trebuie sa aibă grijă în ceea ce privește darea consimțământului pentru prelucracrea datelor personale.

Această lucrare de cercetare urmărește să analizeze riscurile existente în mediul digital, ce efecte produc acestea, atacurile cibernetice și tipurile intâlnite în mod regulat, impactul adus de ele în

viața administrației dar și a cetățenilor, să aducă soluții pentru aceste vulnerabilități, precum educarea personalului public și responsabil în ceea ce privește operarea sigură și eficientă a unui sistem digital pentru a reduce riscurile aduse de factorul uman și să arate cum GDPR (General Data Protection Regulation) [3] protejează interesele publice și cetățenești.

Unul din obiectivele acestei cercetări este cel de a aduce soluții unor probleme mai mult sau mai puțin grave ce au apărut odată cu modernizarea infrastructurii IT deja existentă sau deloc existentă în administrația publică locală sau chiar ce de stat. Atacurile cibernetice sunt în continuă evoluție, fapt ce obligă autoritățile și chiar și actorii cooptați din mediul privat să își dezvolte metodele de apărare, fiind un domeniu aflat într-un conflict continuu dintre ofensivă și defensivă.

Întrebările / ipotezele de cercetare

I1. Modificările aduse sistemului de funcționare al statului de către digitalizare aduc foarte multe beneficii în ceea ce privește lucrul cu cetățenii, comunicarea dintre stat și aceștia, facilitarea utilizării serviciilor publice de către civili și sporirea încrederii în stat prin transparență, însă cu cât mai mult este digitalizată infrastructura, cu atât mai mari sunt riscurile de a apărea breșe de securitate în sistem.
I2. Breșele de securitate sunt un risc major în ceea ce privește protecția datelor personale și sensibile atât ale cetățenilor cât și ale personalului administrativ al statului, ce necesită și el educație digitală.
I3. Care este cea mai mare amenințare pentru infrastructura IT a administrației publice locale?

Obiective

OP. Analizarea principalelor amenințări cu care se confruntă administrația publică locală în mediul digital și oferirea mai multor soluții pentru acestea.
OS1. Analiza tipurilor de atac întâlnite cel mai des în spațiul administrativ local.
OS2. Determinarea integrării, respectării și a impactului GDPR în procesul de funcționare al instituțiilor.
OS3. Studierea unor breșe de securitate care au adus un mare risc la adresa datelor personale și sensibile.

Metodologia de cercetare

Lucrarea va folosi o metodă de cercetare calitativă, și anume analiza desk research, completată de un studiu de caz și de un interviu, cu scopul de a realiza analizarea securității cibernetice și a protecției datelor sensibile în administrația publică locală din România, fiind pus accent pe Municipiul București în perioada anilor 2020-2025.

Sursele de date utilizate constau în rapoarte Agenția Uniunii Europene pentru Securitate Cibernetica (ENISA), DNSC, CERT-RO sau chiar rapoarte ale unor jurnale externe statului român, dar vor fi explicate și anumite acte normative ce au o importanță pentru acest domeniu și această cercetare, precum Directiva Network and Information Security a UE [12] care este transpusă în sistemul legislativ al României prin Legea nr. 362/2018 [13]. Rapoartele vor fi folosite pentru identificarea tendințelor și a standardelor de securitate cibernetică, pentru evaluarea situației la nivel național, pentru a analiza cadrul normativ și pentru a identifica incidentelor relevante pentru administrația publică.

Analiza rapoartelor a fost făcută în mai mulți pași, și anume citirea rapoartelor, selectarea datelor relevante cercetării prin extragerea categoriilor de informații importante (tipuri de amenințări cibernetice, vulnerabilități, incidente, măsuri de protecție), gruparea informațiilor în categorii comune, compararea sistematică a conținutului rapoartelor pe baza unor indicatori și sinteza

rezultatelor. Din aceste rapoarte sunt identificate și anumite tipare ale actorilor ostili din domeniul digital.

De asemenea, indicatorii folosiți sunt de mai multe tipuri, și anume indicatori de conținut (tipurile de atacuri sau amenințări cibernetice și tipul instituțiilor vizate), indicatori de abordare (nivelul analitic de detaliere al studiului și analizarea acțiunilor factorului uman pentru a determina cât de mult îi aparține vina în cazul breșelor), indicatori de impact (asupra protecției datelor personale/sensibile, impactul asupra operabilității sistemelor), indicatori de conformitate legislativă (referințe la Directiva NIS și evaluarea gradului de conformitate a instituțiilor publice) și indicatori de soluții (tipurile de măsuri propuse pentru minimizarea sau eliminarea riscurilor, cum ar fi cele educaționale, legislative, tehnice etc.).

Pentru a arăta și mai în detaliu problemele existente, importanța securității cibernetice, importanța educației digitale dar și soluții pentru minimizarea sau chiar eliminarea riscurilor, va fi utilizată și metoda interviului cu un specialist din domeniu. Metoda interviului este o tehnică de cercetare de obținere verbală a unor informații de la indivizi prin întrebări și răspunsuri, având ca scop verificarea ipotezelor sau pentru descrierea științifică a unor fenomene sau evenimente [14].

Capitolul 1. Concepte și drumul spre digitalizare al administrației publice

Odată cu apariția tehnologiei informației și a comunicării, statele din toată lumea au urmărit incorporarea acestora în procesul administrativ. Guvernele lumii au urmărit, în primă fază, simplificarea comunicării dintre acestea cu populațiile lor, minimizând cheltuielile și timpul alocat procedurilor precum întocmirea și eliberarea de documente pe care le cereau cetățenii și facilitarea comunicării dintre instituțiile statelor, eficientizând și mai mult procesul administrativ.

Accesul liber la Internet a ajutat acest proces și au apărut bazele de date și primele lor puncte slabe ce urmează să fie exploatate de către actori ostili, fie aceștia indivizi ce acționează independent, grupuri sau chiar organizații. Numărul acestor atacatori se află într-o rapidă creștere, însă și numărul de specialiști în apărare crește.

1.1. O scurtă istorie a digitalizării României

În România, procesul de digitalizare a început brusc și abrupt, odată cu aderarea la Uniunea Europeană în anul 2007, când statul a simțit pentru prima oară o presiune din partea Uniunii în ceea ce privește modernizarea prin adoptarea tehnologiei informației în instituții, adoptând strategiile europene și implementându-le în prioritățile proprii. Problema nu a venit din lipsa de idei sau cunoștiințe, ci din cauza faptului că România încă se chinuia să își creeze o fundație pentru ce urma a fi infrastructura IT.

Prin intermediul a mai multor instrumente de măsurare și comparare ale Uniunii Europene s-a observat că România este pe ultimul loc în ceea ce privește digitalizarea sistemului public, pe o durată îndelungată de timp, însă acest lucru nu a descurajat statul din a continua procesul de digitalizare.

În anul 2011, România a înregistrat primul succes în ceea ce privește modernizarea statului și a procesului administrativ cu lansarea platformei online Ghiseul.ro sau SNEP. (Sistemul Național Electronic de Plată online), ca parte componentă a SEN (Sistemul Energetic Național) [15]. Această platformă permite plata online a taxelor și impozitelor, numărul de utilizatori ai acesteia crescând pe parcursul anilor și chiar în prezent.

Până înainte de pandemia COVID-19, România nu reușea să înregistreze progrese semnificative în ceea ce privește digitalizarea instituțiilor statului, conform rapoartelor Indicelui Economiei și Societății Digitale din anii 2015-2019, care arată faptul că România s-a clasat pe ultimele locuri

din Uniunea Europeană în ceea ce privește nivelul existenței al serviciilor digitale pentru public și utilizarea serviciilor de e-guvernare.

Tabel 1.

Indicele Digitalizării al României	2015	2016	2017	2018	2019
Scorul DESI al integrării tehnologiilor digitale în serviciile publice	32.0	35.0	36.5	40.4	43.2
Scorul DESI al EU-28 al integrării tehnologiilor digitale în serviciile publice	48.0	52.0	54.0	57.9	62.9

Sursa: Digital Economy and Society Index (DESI)

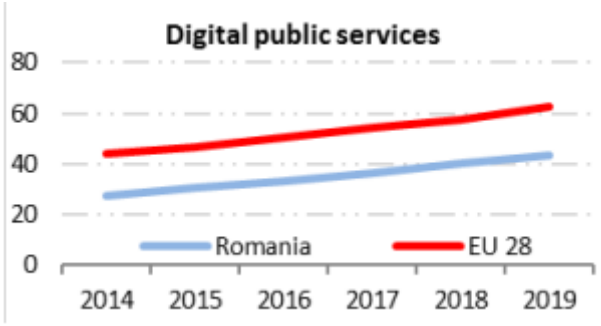


Fig. 1. Evoluția digitalizării serviciilor publice din România față de media UE 2015-2019
Sursa: DESI Index Report ROMANIA 2019

În timpul pandemiei, în schimb, până în prezent, România a înregistrat creșteri semnificative a nivelului de digitalizare al instituțiilor statului, rapoartele arătând că în ciuda faptului că România tot pe ultimele locuri se plasează, aceasta face pași importanți către digitalizarea serviciilor publice, anul 2020 fiind primul an cu o creștere semnificativă [16].

În ceea ce privește stadiul actual al digitalizării în țară, 2025 ne arată că deși România se află din nou pe ultimul loc în clasamentul european, statul persistă și își continuă drumul către digitalizarea serviciilor publice, dar acest drum trebuie luat și mai în serios, deoarece serviciile publice digitale ale statului suferă de o gravă problemă, și anume lipsa interoperabilității, lucru ce statul și l-a propus să îl rezolve până la sfârșitul deceniului curent.

1.2. Administrația Publică și digitalizarea

Administrația Publică reprezintă mecanismul fundamental al unui stat modern ce are ca obiective realizarea prerogativelor și a obiectivelor stabilite de autoritățile guvernamentale, transpunerea valorilor politice în societate [17] și reprezintă brațul administrativ prin care guvernul își exercită autoritatea. Aceasta este formată din instituțiile publice aflate în puterea executivă a statului, facilitând atingerea obiectivelor menționate anterior. Administrația publică are rol în gestionarea resurselor de tip capital uman și financiar, în reglementare prin menținerea ordinii sociale plin aplicarea legii și asigurarea accesului la educație, sănătate și securitate. [18]

În ceea ce privește Administrația Publică Locală, aceasta este reprezentată de către autoritățile publice alese de către cetățeni (primarul și consiliile locale) la nivelul comunelor și al orașelor. În cazul Municipiului București, actuala capitală a României, acesta este și mai divizat în 6 sectoare,

având primării de sector pentru fiecare dintre ele, acestea lucrând cu Primăria Generală a Bucureștiului pentru a administra largul teritoriului al orașului. Fiecare dintre primăriile de sector are propria sa infrastructură IT la nivel instituțional și o bază de date pentru cetățenii ce locuiesc în zona în care acestea acționează. [19]

Pe parcursul timpului și a evoluției nevoilor cetățenești, organele administrative au resimțit nevoia de crearea a unor sisteme digitale prin adoptarea tehnologiei informației și a comunicațiilor, ce au ca rol principal ușurarea demersurilor necesare comunicării dintre cetățean și instituții, precum și facilitarea accesului la informații al populației, acest proces fiind numit „Digitalizare". [20]

Acest proces aduce, pe lângă beneficiile pentru cetățeni, alte avantaje și pentru sistemul instituțional public, precum reducerea cheltuielilor publice, reducerea birocrației, reducerea corupției prin sporirea semnificativă a transparenței și promovarea utilizării tehnologiilor de vârf în cadrul instutițiilor publice. [21]

Digitalizarea a început cu transpunerea metodelor deja existente, precum stocarea de informații și documente din format fizic, de pe hârtie, în format digital, virtual, în fișiere și documente de format electronic. Comunicatele au devenit și ele digitale, multe informații de actualitate fiind valabile pe site-urile web ale instituțiilor, legile apărând pe Monitorul Oficial valabil online și pe site-urile camerelor Parlamentului în cazul celor emise de parlamentari, criterii de îndeplinire pentru emiterea și eliberarea unor documente sunt și ele valabile online și nu doar în sediile instituțiilor aferente. Mai mult, a fost îmbunătățită și infrastructura de comunicare dintre instituții prin intermediul e-mail-urilor sau al platformelor de comunicare apărute de-a lungul timpului. Prin luarea acestor măsuri, statul a redus efectiv timpul necesar rezolvării unor probleme, emiterii de documente, de comunicare către populație a informațiilor de ultimă oră și și-a ridicat gradul de transparență al instituțiilor și a funcționării acestora semnificativ, reducând în același timp și costurile aferente acestor proceduri administrative. [10], [8]

Acest proces nu permite doar administrației publice să evolueze din propriile idei, ci să fie ajutată de către cetățeni în ceea ce privește îmbunătățirea serviciilor statului în raport cu aceștia prin mai multe canale unde populația își poate exprima opinia față de servicii și să ofere un feedback. [22]

Din platformele apărute de-a lungul timpului, se remarcă Ghișeul.ro, platforma online pentru plata taxelor și impozitelor, ROeID, platforma dedicată identității digitale, e-factura și e-transport (ambele având legătura cu monitorizarea fiscală și a mărfurilor) și e-guvernare.ro, portalul oficial al administrației publice în România. Pe lângă platforme, au apărut și instituții dedicate digitalizării, precum DNSC (Directoratul Național de Securitate Cibernetică), ADR (Autoritatea pentru Digitalizarea României) și Institutul Național pentru Cercetare și Dezvoltare în Informatică (ICI București).

O infrastructură IT reprezintă ansamblul de sisteme formate din componente hardware cu un sistem de operare dedicat manipulării de date în masă și stocarea acestora. În cadrul infrastructurii statului se regăsesc și alte funcții de legătură cu paginile web aferente instituțiilor publice pentru a simplifica și automatiza anumite procese ce țin de relația cu publicul. [2] Mai mult, elementele de infrastructură a statului includ și componente de tip IoT (Internet-of-Things), ce includ diferiți senzori, camere de luat vederi conectate la Internet și altele.

Importanța acestei infrastructuri vine din simplul fapt că fără aceasta nu există digitalizare, fiind componenta fizică și tehnică a acestui proces vital administrației publice din prezent. Cel mai simplu de dat exemplu în acest caz îl reprezintă interacțiunea prin intermediul paginilor web dintre stat și cetățean. Un alt exemplu ar fi stocarea datelor în format digital.

Evoluția infrastructurii IT a administrației publice în România a fost inițial lentă, dar începând cu anul 2020 aceasta a început să se dezvolte din ce în ce mai rapid, statul aflându-se, totuși, pe

ultimul loc în Uniunea Europeană în ceea ce privește digitalizarea serviciilor publice atât în relațiile cu cetățenii, cât și în relațiile cu afacerile private.

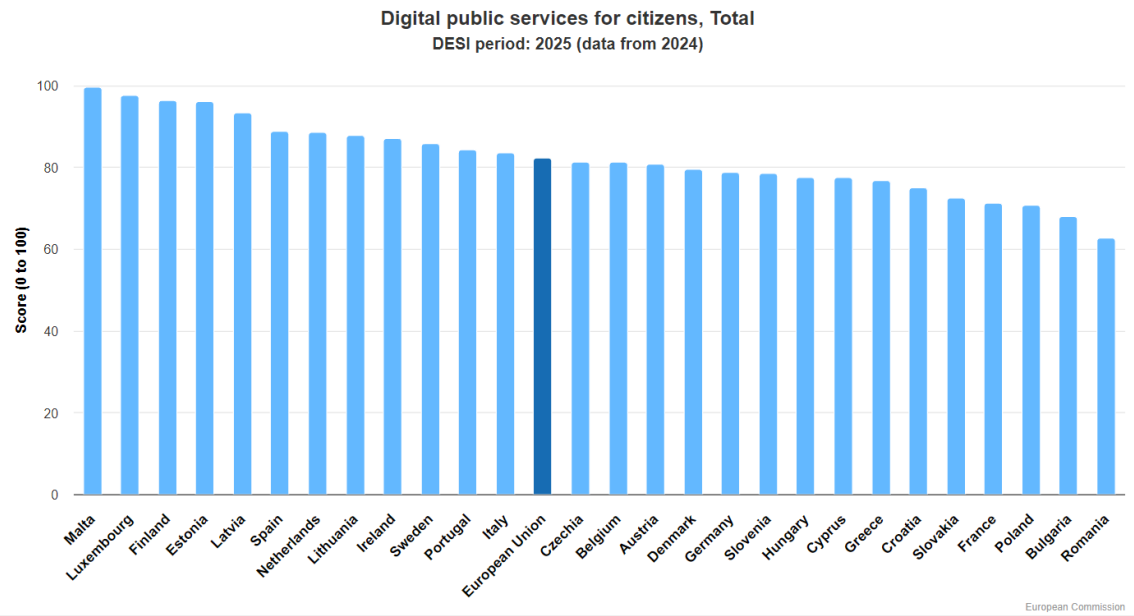


Fig. 2. Digitalizarea serviciilor publice în relațiile cu cetățenii
Sursa: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/

După cum se poate observa în figura 1, România se află pe ultimul loc în clasamentul Uniunii Europene în ceea ce privește digitalizarea serviciilor publice în relațiile cu cetățenii, însă nu are un scor foarte jos comparativ cu Bulgaria.

Statul român se află, după cum ne arată statisticile și rapoartele DESI, într-o creștere lentă dar sigură în ceea ce privește nivelul digitalizării.

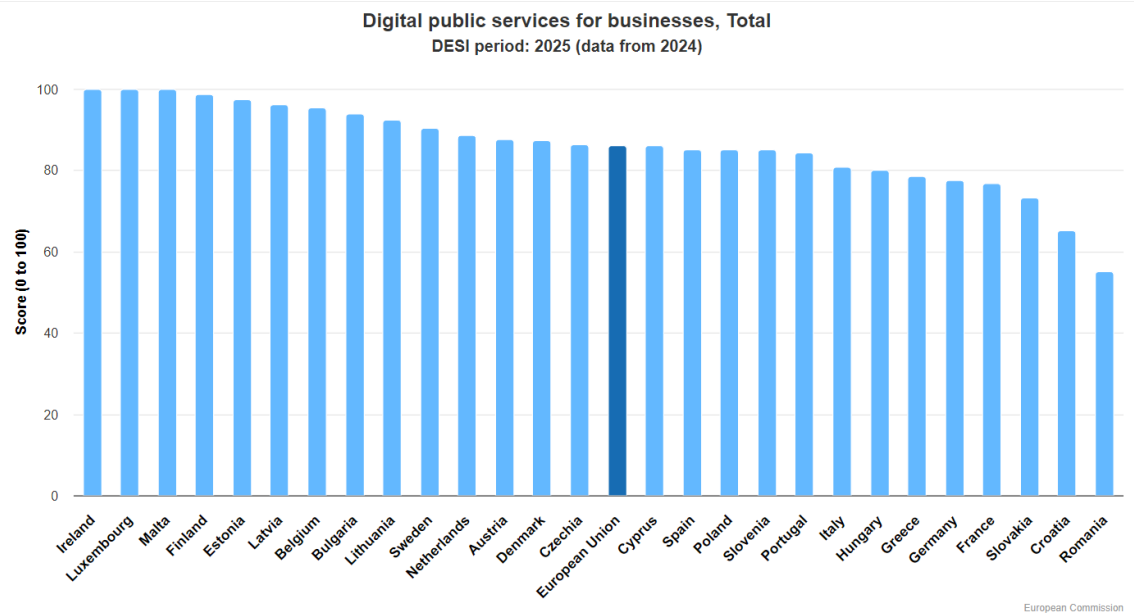


Fig. 3. Digitalizarea serviciilor publice în relațiile cu afacerile
Sursa: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/

Conform figurii 2, România se află pe ultimul loc în clasamentul Uniunii Europene în ceea ce privește digitalizarea serviciilor publice în relațiile cu afacerile private, scorul digitalizării fiind mai redus față de cel ce ne arată relațiile publice cu cetățenii.

Odată cu adoptarea Strategiei Naționale privind Agenda Digitală pentru România 2020, priorităților administrației publice li s-au adăugat și e-guvernarea, securitatea cibernetică, educația digitală, investițiile în infrastructura de internet de mare viteză și tehnologii cloud, pe lângă obiectivele deja existente precum eliminarea birocrației, creșterea nivelului de transparență, ridicarea accesibilității informației pentru cetățeni și întreprinderi, optimizarea costurilor, dar și simplificarea procedurilor în mod normal birocratice, precum plata taxelor, obținerea de documente și depunerea de cereri [23], [20]. Pe lângă aceasta, statul român a aprobat și Planul Național de Acțiune privind Deceniul Digital pentru România, declarându-și angajamentul pentru transformarea digitală a țării și pentru redresarea și securitatea infrastructurii sale IT. [24]

O altă provocare pentru Administrația Publică este creșterea nivelului de educație în ceea ce privesc competențele digitale ale personalului administrativ, nivelul scăzut ducând la probleme majore în ceea ce privește interoperabilitatea și eficiența sistemelor și echipamentelor digitale din infrastructura IT atât la nivel central cât și local.

Totuși, pe lângă cele deja menționate, cu digitalizarea a apărut și o foarte mare responsabilitate a instituțiilor publice, și anume protejarea cetățenilor și a datelor acestora. Această responsabilitate fiind interconectată cu cea a protejării infrastructurii IT în sine, această provocare fiind însuși domeniul securității cibernetice.

1.3. Securitatea cibernetică

Odată cu apariția instrumentelor digitale, a platformelor online și a modalităților de stocare digital, a apărut și nevoia de apărare sau protejare a datelor existente în bazele de date ale oricărui sistem, apărând astfel, pentru prima oară, conceptul de cybersecurity, iar după acesta, în timp, a metodelor de atac și de apărare din ce în ce mai avansate, numărul de incidente de securitate cibernetică crescând, ulterior fiind create și elemente legislative ce au rolul de a reglementa acest domeniu.

În cadrul administrației publice din România, a fost înființat, CERT-RO (Centrul Național de Răspuns la Incidente de Securitate Cibernetică) în anul 2011 prin Hotărârea Guvernului nr. 494/2011 [25]. Ulterior, în septembrie 2021, acesta a fost înlocuit de DNSC (Directoratul Național de Securitate Cibernetică) prin Ordonanța de Urgență a Guvernului (OUG) nr. 104/2021 [26].

Directoratul Național de Securitate Cibernetică acționează în domeniul securității cibernetice conform legii NIS nr. 362/2018, ulterior și a Directivei NIS 2 [27], și are rolul de a analiza, reacționa și preveni incidente de securitate cibernetică. DNSC a conturat și rolul structurilor de tip CERT sau CSIRT, formate din specialiști în securitate cibernetică ce au rolul de a interveni urgent în situații complexe cât și rolul de a preveni apariția complicațiilor [28]. Pe pagina web a DNSC se pot găsi și rapoarte semestriale privind situația globală a securității cibernetice, tipurile de atacuri, resursele financiare alocate pentru combaterea amenințărilor cyber și alte date relevante.

Apariția acestei nevoi de protejare nu a apărut doar la nivelul României ci la un nivel european. Uniunea Europeană, după ce a observat aceste nevoi, a elaborat directiva NIS, denumire completă „Network and Information Systems Directive”, denumirea din limba română fiind „Directiva privind securitatea rețelelor și a sistemelor informatice”, aceasta a intrat în vigoare în anul 2016 de către statele membre ale Uniunii, inclusiv de către România. Aceasta a apărut în contextul în care rețelele, sistemele și serviciile informatice au devenit vitale și creșterea frecvenței și a impactului incidentelor de securitate cibernetică și are ca scop crearea unei abordări „globale” europene față de aceste incidente și reducerea acestora și a riscului lor prin noi metode de protejare și de cooperare în ceea ce privește securitatea cibernetică a infrastucturilor IT ale statelor membre

cât și pe cele din spațiul privat [29]. Ulterior, în anul 2022, a apărut Directiva NIS2, ce a actualizat metodele deja menționate în prima versiune a NIS, a adăugat metode noi apărute de-a lungul timpului și a consolidat securitatea cibernetică la nivel european, abrogând-o pe cea din 2016 și fiind aflată în vigoare în prezent. Directivele NIS și NIS2 mai abordează și certificările de specialitate în domeniu, acestea putând fi suspendate temporar de către autoritățile competente, autorizațiile putând, și ele, fi supuse la același tratament în cazul încălcării de către o entitate sau persoana de specialitate din cybersecurity a prevederilor directivei. Mai mult, NIS2 încurajează statele membre să colaboreze nu numai în protejarea sistemelor și infrastructurilor, ci și în ceea ce privește supravegherea respectării legilor apărute din adoptarea directivei. [30]

Tot în anul 2016, din nevoia protecției persoanelor fizice în ceea ce privește prelucrarea, stocarea și utilizarea datelor cu caracter personal, Uniunea Europeană a adoptat Regulamentul General privind Protecția Datelor (denumirea originală din limba engleză fiind „The General Data Protection Regulation", abreviată ca „GDPR"). Aceasta a apărut cu scopul de a reglementa utilizarea datelor cu caracter personal fie de către instituții publice, fie de către entități din spațiul privat, ale cetățenilor europeni în relațiile cu aceștia, fiind necesar un consimțământ în ceea ce privește prelucrarea acestor date vitale pentru populație [31]. Relevanța GDPR pentru domeniul securității cibernetice o reprezintă faptul că aceste date sunt stocate electronic pe sisteme ce pot cădea pradă actorilor ostili, protejarea acestor baze de date fiind de o importanță maximă pentru buna funcționare a societății. Încălcarea acestui regulament ce a fost adoptat de către fiecare stat membru UE rezultă în sancțiuni de mai multe tipuri acordate de către autoritățile membrilor Uniunii, în cazul României de către ANSPDCP (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) [32].

În literatura de specialitate întâlnim 3 principale categorii de hacker, și anume White Hat, Grey Hat și Black Hat hackers. Aceștia sunt catalogați așa, după „culoarea pălăriei", pentru a crea o paralelă între apartenența și scopul acestor indivizi, albul însemnând intenția curată, și anume cei care lucrează legal, negrul fiind asociat cu întunericul și răul arătându-i pe cei ce lucreaza ilegal în domeniu, iar griul fiind folosit pentru cei ce actionează atât legal cât și ilegal, dar care într-un final sunt de ajutor pentru deținătorii rețetelor și sistemelor pe care aceștia le atacă.

Importanța securității cibernetice la nivelul Administrației Publice atât la nivel central cât și local este una sporită în această eră a digitalizării și a tehnologiei informatice, deoarece odată cu apariția tehnologiei apar și vulnerabilitățile din sisteme. Aceste vulnerabilități sunt exploatate de către actori ostili, din categoria Hackerilor de tip Black Hat, ce urmăresc să fure date sensibile și posibil scoaterea acestora la licitație pe Dark Web, îngreunarea sau chiar distrugerea sistemelor informaționale din infrastructura IT a administrației publice.

Vulnerabilitățile, în anumite cazuri, sunt produse de implementarea defectuoasă a sistemelor digitale. Această implementare defectuasă se poate referi la parolele personalului slab configurate, fenomen denumit adesea și „user error", iar în momentul în care un singur dispozitiv pică pradă atacatorilor, aceștia reușind să abuzeze această vulnerabilitate, toata infrastructura se află într-un risc major de expunere al datelor și informațiilor sensibile, personale și uneori vitale funcționării tututor sistemelor legate la infrastructura-mamă [33], [34], [35]. Pe lângă acest fenomen cunoscut de tip „user error", mai există și atacurile de tip „Phishing", ce implică păcălirea utilizatorului cu un e-mail sau mesaj, care, odată accesat link-ul din cadrul acestuia, redirecționează utilizatorul către o pagină falsă, de obicei o pagină-clonă de logare într-un cont sau o pagină care simulează un formular unde utilizatorul este așteptat să își introducă datele personale, cum ar fi detaliile de pe cardul bancar sau e-mail-ul și parola utilizate de acesta la un anumit tip de cont [36], [37]. Vulnerabilitățile reieșite din greșelile produse de către utilizator sunt cele mai des exploatate atunci când nivelul educației digitale este redus, iar acestea se numesc adesea atacuri de tip „social engineering" sau inginerie socială.

Pe lângă ce s-a menționat mai sus, mai există și erorile umane la crearea codului-sursă. Acestea duc la apariția unor oportunități pentru actorii ostili ce urmăresc încetinirea, scăderea nivelului de

eficiență a sistemelor din infrastructura IT și furtul de date. Inițial au apărut programele malițioase, denumite de către specialiști „Malware” (termenul a fost format prin combinarea cuvintelor „Malicious” și „Software”), ce au ca scop coruperea sistemelor, îngreunarea sau distrugerea acestora sau furtul de date de pe o bază de date sau o rețea de sisteme. Mai mult, acesta evoluează în funcție de măsurile de securitate ce există sau apar pe parcursul timpului, creatorii de software tip malware fiind unii din mulții adversari ai celor ce au responsabilitatea de a proteja sisteme, baze de date și infrastructuri IT [6]. Dacă vorbim despre cazuri extreme, de-a lungul timpului au fost afectate întregi infrastructuri IT globale de către aceste tipuri de programe software.

Malware-ul este și acesta de mai multe tipuri, cele mai des întalnite fiind Adware (programul ce supraîncarcă sistemul cu reclame), Ransomware (cel ce ține date ostatic în schimbul unei sume de răscumpărare), Scareware (programul „escroc” ce doar sperie utilizatorul și încearcă să-i vândă soluții false pentru a rezolva probleme), Spyware (programul folosit pentru spionarea sistemului), Trojan Virus (calul troian al aplicațiilor malițioase, cel ce se deghizează într-o aplicație inofensivă), Virus (cel mai clasic program malițios) și Worm (aplicația malițioasă ce acționează ca un parazit pentru sistem).

În lumea securității cibernetice mai există și atacurile ce se întâmplă „live”, sau în timp real. Acestea sunt mult mai complexe decât păcălirea unor utilizatori nepregătiți sau crearea unor programe malițioase și eliberarea acestora în mediul online cu speranța că vor infecta sisteme importante. Aceste atacuri caută vulnerabilități în firewall-ul rețelelor sau chiar în sistemele acestora de operare, iar în cazul găsirii uneia, aceasta este exploatată până când actorul ostil are acces total asupra sistemului, rețelei sau chiar a întregii infrastructuri compromise. Aceste atacuri necesită o vigilență continuă din partea celor ce protejează infrastructura.

Aceste atacuri se folosesc adesea de vulnerabilități zero-day, ce reprezintă niște portițe pentru atacatorii de sisteme. Aceste vulnerabilități se observă după ce un software este publicat sau actualizat, dezvoltatorii nefiind atenți la anumite detalii ce lasă posibilități de atac neobservate. Aceste vulnerabilități sunt exploatate prin intermediul unui exploit zero-day, ce reprezintă o tehnică specifică folosită de atacatori pentru a profita de vulnerabilitatea menționată mai sus. Odată ce atacatorii descoperă vulnerabilitățile, aceștia pot dezvolta kit-uri de exploit-uri ce se pot vinde pe site-urile de pe Dark Web. Atacurile zero-day pot avea ca scop furtul de date dar și instalarea de software neautorizat și, de multe ori, distructiv. [38]

Metodele de atacuri menționate mai sus pot fi folosite drept pași sau stagii în cadrul unui atac de tip APT. Atacurile de tip Advanced Persistent Threat sunt sofisticate și acționează într-un mod continuu de-a lungul timpului, combinând mai multe tehnici cu scopul de a penetra măsurile de protecție ale unei infrastructuri. Acestea, odată ce au success, oferă intrusului o prezență nedetectabilă într-o rețea, oferindu-i acces liber la datele prezente pe aceasta, el putând să fure date sensibile de la organizații private sau chiar instituții publice. De obicei, în spatele atacurilor APT stau echipe antrenate și pregătite în domeniu, apărarea necesitând un grad de expertiză și mai mare decât cel al ofensivei. Actorii ostili au, în cele mai multe cazuri, 4 categorii generale de obiective, și anume spionaj cibernetic, beneficii financiare, hacktivism-ul și distrugerea datelor sau a echipamentului folosit de sisteme. În cadrul acestor operațiuni sunt cel mai des întâlnite 3 metode de atac, și anume DoS (Denial of Service), Doxing, Data Theft (Furt de date) [39].

Atacurile APT sunt cele mai des întâlnite în cazul instituțiilor Administrației Publice, deoarece acestea reprezintă operațiunile actorilor ostili, de obicei externi, ce încearcă să fure datele sensibile stocate pe bazele de date ale instituțiilor și să distrugă cât mai mult din infrastructura IT a statului.

Capitolul 2. Atacurile Cibernetice în Administrația Publică, amenințări și măsuri existente

Evoluțiile din domeniul digital și mai ales a tehnologiilor ce depind de o conexiune la Internet au permis statelor un nou mod în care se pot administra, infrastructurile informaționale digitale și rețelele acestora ajutând atât personalul instituțiilor publice cât și cetățenii în ceea ce privește eficientizarea procesului administrativ. Mai mult, aceste elemente tehnologice au ajuns critice, nu numai în domeniul public dar și în cel privat. Aceste creșteri în nivelul de utilizare al serviciilor online au atras din ce în ce mai mult atenția unor actori ce sunt considerați amenințări pentru siguranța sistemelor, publicului sau chiar întregii infrastructuri. Aceste amenințări cibernetice, odată cu trecerea timpului, devin din ce în ce mai complexe, atacurile devenind ample operațiuni de compromitere, furt, distrugere sau chiar toate cele trei în anumite cazuri [40].

Anual, în Uniunea Europeană au loc câteva mii de atacuri cibernetice. În 2020, costul mondial al criminalității informatice a fost dublu față de anul 2015 [41].

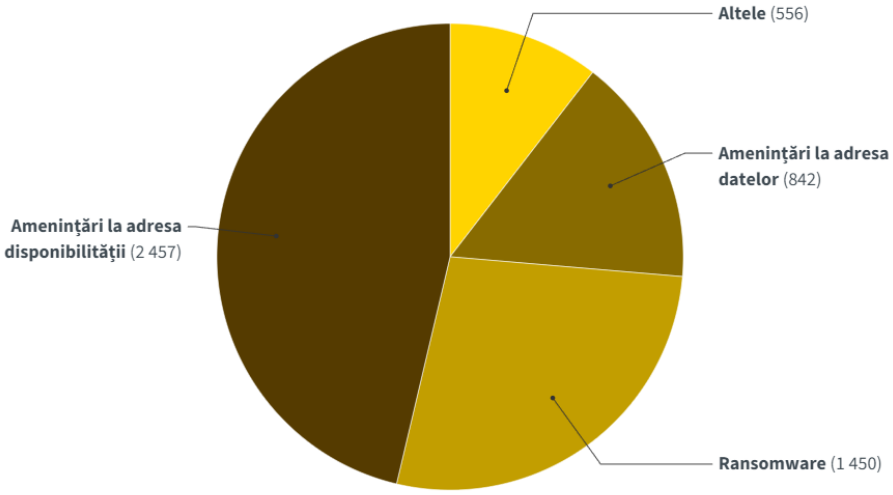


Fig. 4. Clasificarea amenințărilor la adresa disponibilității identificate de către ENISA
Sursă: https://www.consilium.europa.eu/ro/policies/top-cyber-threats/#0

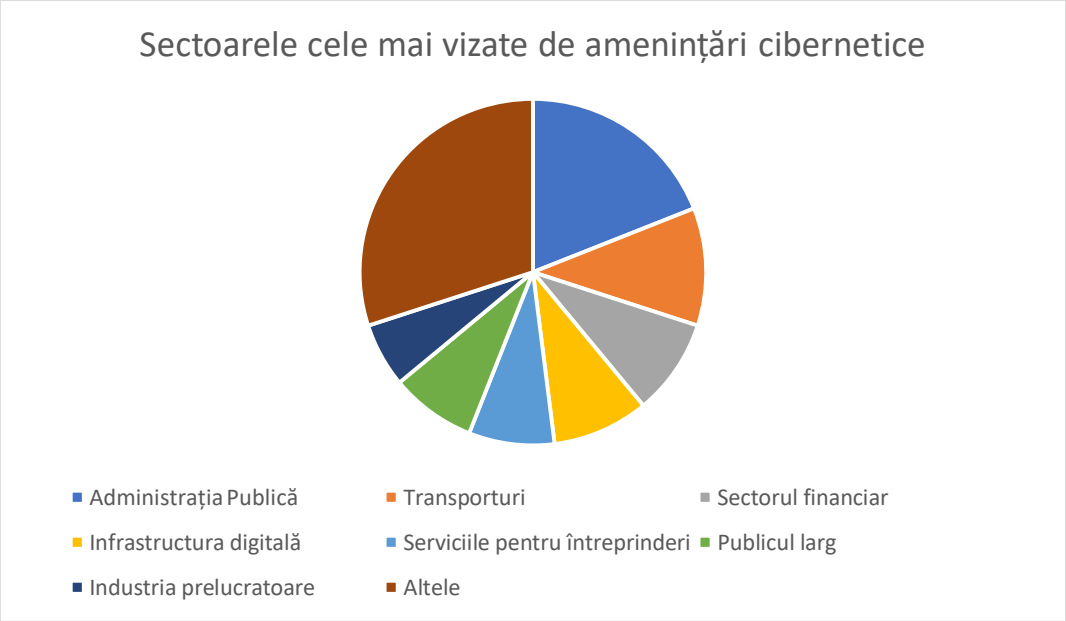


Fig. 5. Sectoarele cele mai vizate de amenințări cibernetice
Sursă: https://www.consilium.europa.eu/ro/policies/top-cyber-threats/#0

După cum se poate observa în figura 4, cele mai multe amenințări au fost la adresa disponibilității serviciilor, aceste atacuri având ca scop supraîncărcarea sau epuizarea resurselor infrastructurii rețelei vizate de atacuri [41]. Rețeaua, pe durata atacului, este din ce în ce mai îngreunată, fapt ce reduce disponibilitatea prin încetinire sau, în unele cazuri, căderea acesteia din pricina lipsei de resurse rezultate a metodelor folosite de actorii ostili. Tot din figura 4 reiese și faptul că al doilea cel mai întâlnit tip de atac este cel ransomware, ce are ca rol furtul și apoi criptarea datelor aflate pe rețeaua afectată, fiind promisă restituirea acestora și ștergerea lor de pe bazele de date ale hackerilor în schimba unei sume monetare de obicei majore. Din figura 5 reiese că administrația publică este cel mai afectat sector digital din Uniunea Europeană.

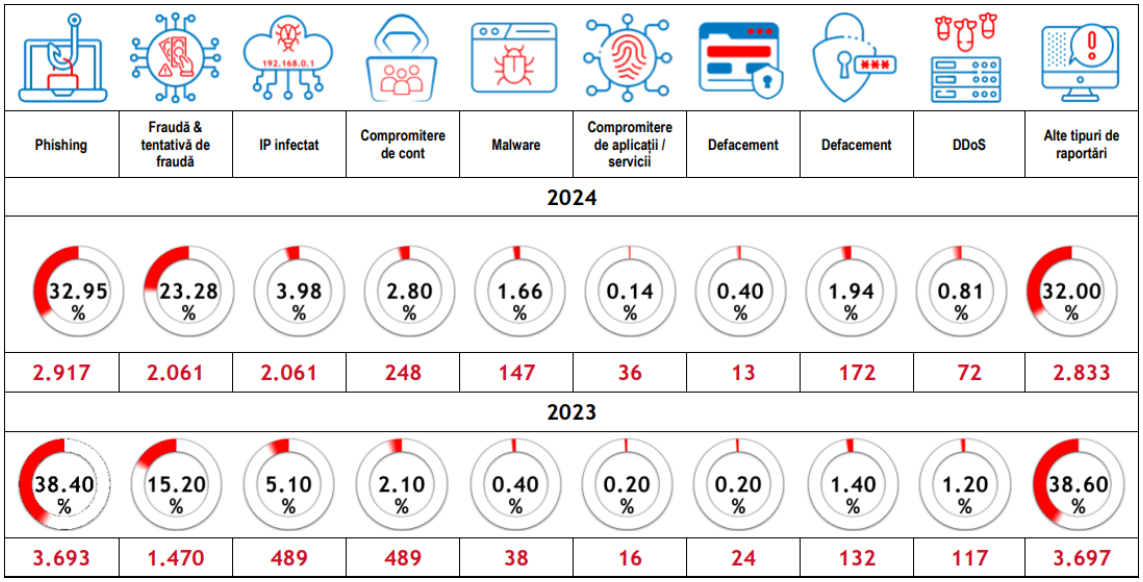
Datele celor două figuri combinate ne arată cele mai des întâlnite amenințări, metode de atac și sectoarele cele mai des vizate de acestea. Dacă administrația publică din toate țările europene ar fi cel mai des afectată doar de atacuri de tip ransomware și cele ce vizează disponibilitatea rețelelor, atunci lucrurile ar fi mai simple în ceea ce privește securitatea cibernetică, însă după cum reiese atât din imaginile de mai sus și din surse media, atacurile nu sunt doar de aceste două tipuri, metodele fiind parte din operațiuni complexe ce folosesc metode mixte de compromitere a sistemelor.

Fig. 6. Metodele de atac identificate de către ENISA
Sursă: https://www.consilium.europa.eu/ro/policies/top-cyber-threats/#0

Atacurile întâlnite în figura 6 pot face parte dintr-o operațiune mult mai mare a unor grupuri de hackeri, aceste 6 tipuri de atac funcționând în lanț de cele mai multe ori.

Dintre acestea trebuie să dăm o atenție sporită și metodelor de inginerie socială, deoarece oricine se poate confrunta cu ele oricând, fie printr-un e-mail din categoria „Spam”, fie printr-o reclamă etc. Amenințările de acest fel au ca scop manipularea unor oameni și inducerea acestora în eroare

pentru a își dezvălui date sensibile, precum parole la anumite conturi, date din conturile bancare sau de pe cardurile bancare personale și, uneori, accesul la infrastructuri digitale [42].



Phishing	Fraudă & tentativă de fraudă	IP infectat	Compromitere de cont	Malware	Compromitere de aplicații / servicii	Defacement	Defacement	DDoS	Alte tipuri de raportări
2024									
32.95 %	23.28 %	3.98 %	2.80 %	1.66 %	0.14 %	0.40 %	1.94 %	0.81 %	32.00 %
2.917	2.061	2.061	248	147	36	13	172	72	2.833
2023									
38.40 %	15.20 %	5.10 %	2.10 %	0.40 %	0.20 %	0.20 %	1.40 %	1.20 %	38.60 %
3.693	1.470	489	489	38	16	24	132	117	3.697

Fig. 7. Analiza DNSC a incidentelor raportate 2023-2024
Sursa: https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024

Pentru a înțelege mai bine pericolele atacurilor cibernetice anterior menționate, voi aprofunda definițiile acestora.

2.1 Definiții și exemple ale atacurilor cibernetice

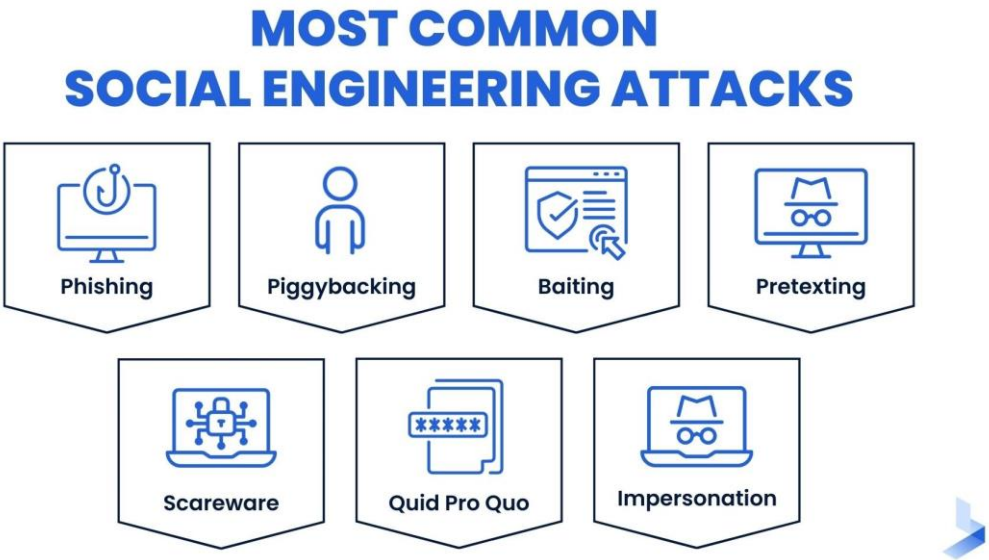


Fig. 8. Cele mai des întâlnite forme de atacuri de tip social engineering
Sursa: https://www.bitlyft.com/resources/what-is-social-engineering-avoiding-manipulative-tactics

Ingineria socială implică decepționarea utilizatori pentru a-i convinge să divulge informații sensibile, să trimită bani unor necunoscuți sub anumite pretexte sau să ofere liber acces la o rețea. Criminalii sau grupările infracționale din mediul virtual se folosesc de manipulare psihologică

sau emoțională și urmăresc să exploateze slăbiciunile unor oameni inocenți [43], deseori apelând la empatia sau frica acestora.

În cadrul atacurilor de tip inginerie socială, cele mai frecvente metode de operare sunt:

- Phishing
- Piggybacking
- Baiting
- Pretexting
- Scareware
- Quid Pro Quo
- Impersonation

Cea mai des întâlnită metodă din clasament este Phishing-ul. Acesta ia, de obicei, forma unui e-mail ce pare fi trimis de o companie legitimă sau instituție guvernamentală existentă, dar pentru cei ce sunt vigilenți, acestea conțin semne conform cărora poate fi determinată falsitatea e-mail-ului. Acestea conțin pretexte ce au ca rol obținerea de informații sensibile de la receptorul mesajului, având în cadrul lor link-uri periculoase care imită aspectul unor pagini oficiale.

De-a lungul timpului au evoluat noi forme de phishing, și anume spear-phishing, vishing și whaling. Diferența dintre phishing și *spear-phishing* este că cea ulterior menționată se folosește de mesaje personalizate în urma unei operațiuni de cercetare a victimei (ocupație, familie, locație, preferințe etc.). *Whaling* reprezintă un fel de spear-phishing, singura diferență fiind faptul că acesta are în vizor directori sau alte poziții înalte din ierarhia unei companii sau instituții. *Vishing*-ul este o metodă din ce în ce mai des întâlnită datorită apariției și disponibiltății modelelor de inteligență artificială generativă, deoarece acesta implică abordarea unei potențiale victime printr-un apel vocal, de regulă telefonic, fiind generate voci a unor oameni fictivi ce par a se afla în pericol sau, în cele mai rele cazuri, care imită vocea unui cunoscut. [43]

Cel mai simplu mod de a te apăra de atacurile de tip phishing este de a citi de mai multe ori expeditorul e-mail-ului și luarea în vedere a faptului că niciun actor legitim nu va cere prin intermediul unui e-mail date de logare la conturi.

Piggybacking, cunoscut ca și *Tailgating*, reprezintă tactica de a urmări o persoană autorizată într-un spațiu ce nu este valabil pentru toată lumea, de exemplu, o cameră de servere. Acest lucru se poate realiza atât fizic cât și virtual prin infiltrarea unei rețele închise print-un terminal nesecurizat [44]. Această tactică se bazează pe câștigarea încrederii victimei și exploatarea acesteia, având mai multă legătură cu instituții, nu cu indivizi. Monitorizarea atentă a cine însoțește personalul angajat în incintă este cea mai bună măsură de prevenție împotriva piggybacking.

Baiting, sau *Momirea*, reprezintă utilizarea unor promisiuni false, de obicei a unei recompense monetare pentru a determina un individ să divulge informații sensibile sau să acceseze link-uri periculoase ce pot infecta o rețea [42]. Este recomandată evitarea ofertelor ce par a fi prea bune să fie adevărate.

Pretexting reprezintă crearea unui pretext, o identitate falsă, un scenariu fals, pentru a câștiga încrederea victimelor pentru a obține date sensibile. Un exemplu ar fi un apel în care atacatorul pretinde că este un angajat al unei bănci și minte victima că are un credit deschis, cerând apoi date

sensibile ce au ca rol autentificarea în sistemul bancar legitim [44]. Se aplică aceleași măsuri de prevenție ca la phishing.

Scareware reprezintă o tentativă de a speria utilizatorul unui terminal cu scopul ca acesta să ofere o sumă monetară în schimbul eliminării problemei [45]. „Urgența" ce reiese din notificările trimise de acest tip de aplicație este una falsă și pur manipulatorie. Ca metode de prevenție avem neaccesarea link-urilor sau paginilor web ce nu sunt oficiale, evitarea descărcării atașamentelor dăunătoare din surse nesigure și menținerea barierelor de protecție uzuale ale terminalului.

Quid pro quo este definit ca tactica ce implică oferirea unui câștig în schimbul informațiilor sensibile ale unei victime. De exemplu, un atacator oferă să „ajute" un utilizator în vederea reparării unui computer în schimbul datelor bancare sau unor carduri cadou pre-plătite [44]. Măsurile de prevenție aferente phishing-ului și pretexting-ului se aplică și aici.

Impersonation sau *Uzurparea identității* este tactica ce implică asumarea de către atacator a unei identități false [42], de obicei a unui apropiat al victimei, cum ar fi un membru de familie, de regulă deja aflat într-o situație delicată, cum ar fi probleme de sănătate sau cu legea. Se aplică aceleași măsuri deja menționate.

Cum am menționat anterior, mecanismul din spatele unui atac de tip ransomware este blocarea fișierelor rețelei afectate și oferirea de chei pentru deblocarea acestora în schimbul unei sume de răscumparare. Acest malware afectează un sistem în urma exploatării unor lacune deja existente în sistem sau prin metodele de inginerie socială precum e-mail-urile înșelătoare sau link-uri false. În urma infilitrării sistemului, acesta criptează fișiere valoroase sau de importanță sporită, cel mai des fiind afectate fișierele în care se află date sensibile în masă, folosind algoritmi de criptare asimetrică, creând seturi de chei publice și private diferite, cea privată fiind necesară recuperării fișierelor afectate. Decriptarea se efectuează doar în urma plății sumei cerute [46].

De-a lungul timpului, în comunitățile de hacktivism și grupări de hacking, a fost popularizată metoda Ransomware as a Service (prescurtat „RaaS"), ce funcționează în următorul fel: Programatori de programe malițioase creează seturi de unelte, protocoale, fișiere deja infectate unor utilizatori ce au ca scop atacarea și compromiterea unor rețele în urma unui schimb de bani, fie printr-o singură plată, fie printr-un abonament lunar [47]. RaaS facilitează propagarea acestor amenințări la nivel global prin distribuirea acestor linii de cod periculoase către din ce în ce mai mulți utilizatori.

În urma apariției în anul 2022 a pachetelor ransomware as a service denumite „Black Basta" [47], actorii ostili din mediul digital au început accentuarea presiunii puse pe victime, pe lângă sumele cerute pentru recuperarea fișierelor afectate au apărut și amenințările de dezvăluire a datelor sensibile, precum parole, date de logare sau informații personale în mediul public.

În anul 2024, un atac cibernetic de tip ransomware a avut loc în domeniul sănătății din România, fiind afectate 26 de spitale ce utilizau sistemul digital „Hipocrate". Programul malițios ce face parte din familia de malware intitulată „Phobos" a fost denumit „Backmydata", fiind o altă aplicație ce face parte dintr-un set de tip RaaS [48]. Răspunsul autorităților din cadrul DNSC au decuplat sistemele afectate de la rețele, bazele de date fiind restaurate prin intermediul backup-urilor efectuate periodic de către personalul tehnic din cadrul instituțiilor de sănătate.

Pentru a ne proteja de acest fel de atacuri, sunt sugerate mai multe metode de apărare, precum precauția față de link-urile suspicioase, sporirea vigilenței în ceea ce privește navigarea pe internet sau deschiderea de conținut primit pe e-mail, folosirea de protocoale sau aplicații firewall avansate, crearea de copii de siguranță a datelor importante pe care le avem stocate în mod digital și evitarea descărcării de fișiere de pe site-uri necunoscute, suspicioase sau raportate ca fiind periculoase.

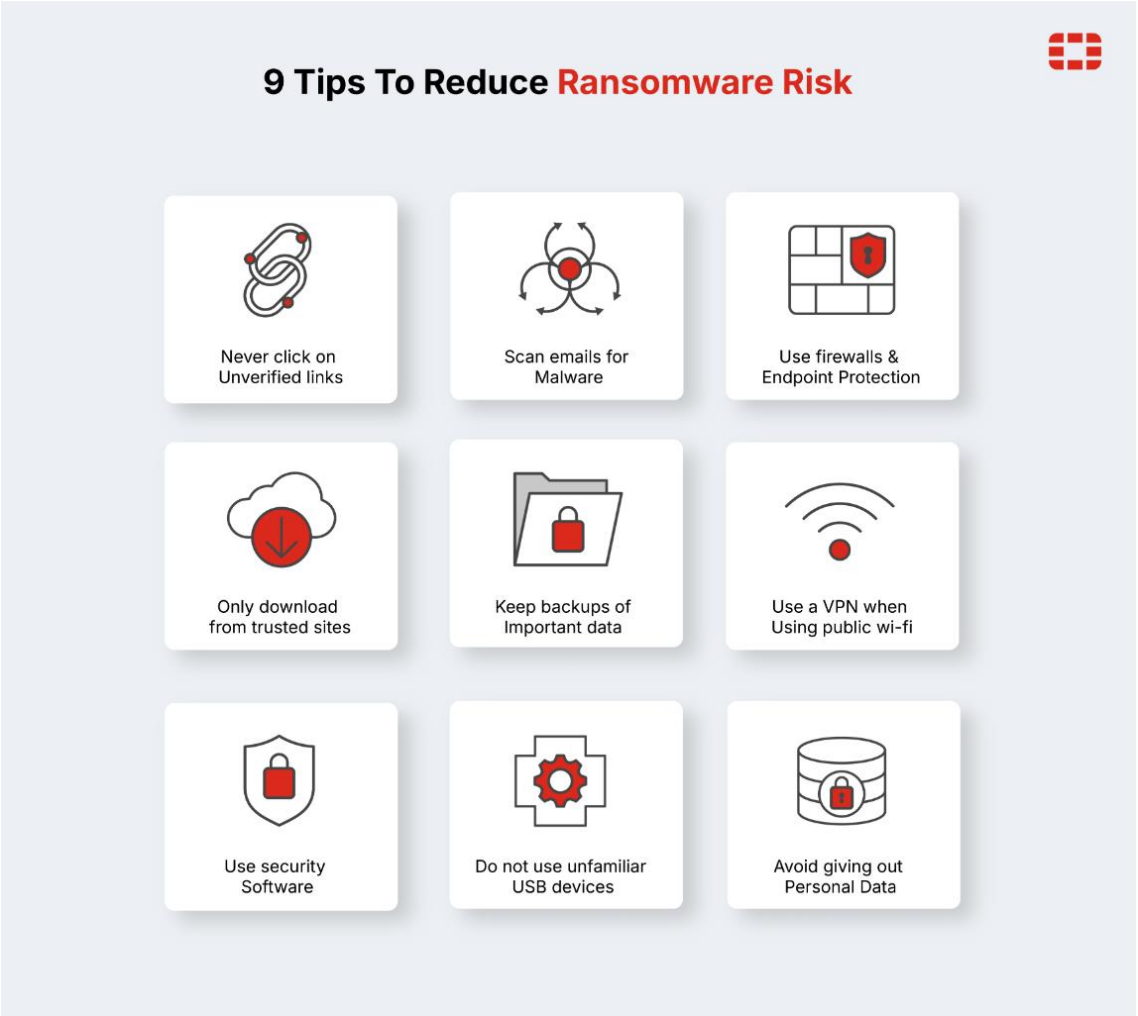


Fig. 9. „9 Ponturi pentru a reduce riscul de Ransomware”
Sursa: https://www.fortinet.com/resources/cyberglossary/how-to-prevent-ransomware

La baza atacurilor mai sofisticate, cum ar fi operațiunile APT, stau căutarea informațiilor despre victimă și vulnerabilitățile rețelei din care aceasta face parte. După ce această fază de recunoaștere este încheiată, hackerii trec la următoarea fază, și anume cea a creării „armelor” necesare pentru infiltrarea unui sistem. Aceste „arme” sunt, defapt, aplicații malițioase, numite *Malware*.

Malware-ul este primul lucru la care ne gândim atunci când auzim despre un atac cibernetic, un sistem afectat de unul, sau o breșă de securitate realizate de o grupare de actori ostili. La bază, a fost conceput ca un mod de a prelua controlul datelor dintr-un terminal fără a cere permisiunea proprietarului și, ulterior, de a le modifica. Acesta poate fi definit ca orice software ce este creat strict pentru a exploata un sistem și a perturba funcționarea sa uzuală, fiind dezvoltat de criminali sau grupări de criminali cibernetici [6].

Fiind un termen general, malware înglobează toate programele, aplicațiile sau protocoalele ce au scopuri dăunatoare sau chiar distructive, create în mod intenționat de către un actor ostil. De-a lungul timpului au apărut din ce în ce mai multe tipuri de malware, inițial începând de la un simplu *worm* ce purta denumirea de „Creeper”. Acesta a fost creat și lansat în anul 1971 cu scopul de a se reproduce în din ce în ce mai multe sisteme din ARPANET (strămoșul Internetului de astăzi) [49]. În timp, mai ales după lansarea Internetului, au apărut mai multe tipuri de aplicații malițioase.

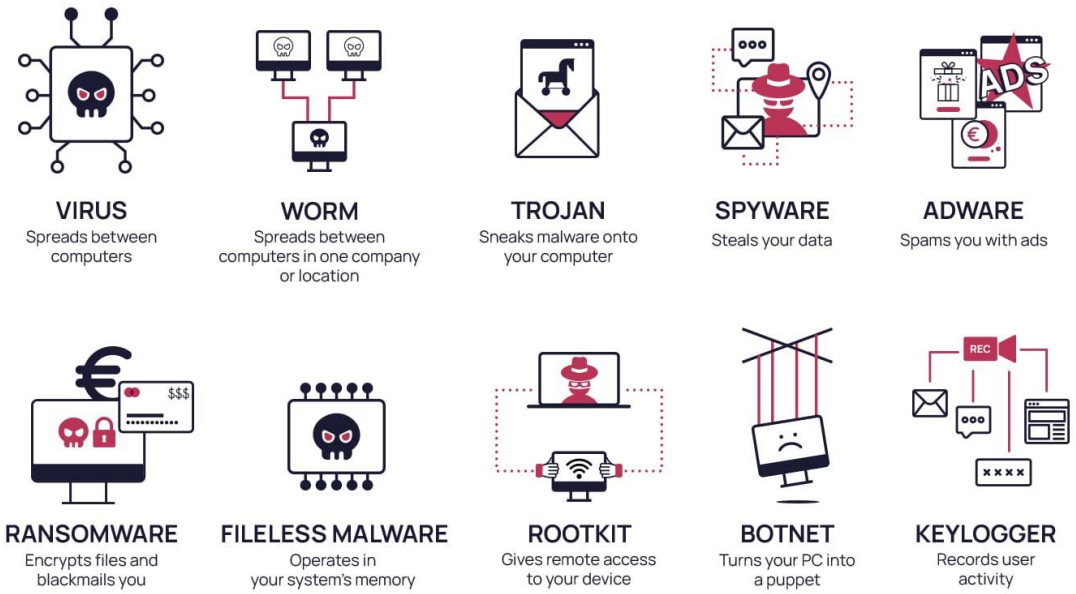


Fig. 10. Tipuri de Malware
Sursa: https://sosafe-awareness.com/glossary/malware/

Un *virus* reprezintă un subtip de Malware ce se atașează unei aplicații legitime și funcționează doar atunci când această este activă pe computer și poate fi folosit pentru a modifica, fura sau distruge datele utilizatorului. Aceasta este cea mai veche formă de program malițios cunoscută de publicul larg [50]. Acesta se răspândește doar prin intermediul interacțiunii umane cu un link malițios, o aplicație sau un fișier infectate.

Worm-ul, sau viermele digital, este software-ul malițios ce exploatează vulnerabilități în securitatea rețelei pentru a se răspândi fără interacțiunea umană, ulterior oferind posibilitatea actorilor ostili să realizeze atacuri de tip DDoS, furt de informații cu caracter sensibil, ransomware sau chiar distrugerea sistemelor [51]. Un exemplu de program tip Worm este Stuxnet, ce a fost creat de autorități legitime pentru a împiedica programul nuclear din Iran [52]. Creatorii nu s-au așteptat însă ca acesta să scape din mediul în care se afla, rezultând într-o răspândire a acestuia în tot restul lumii digitale, însă, deoarece nu putea identifica țintele împotriva cărora a fost creat să lucreze, nu a cauzat daune.

Deși similari, virușii și viermii digitali (worm), aceștia sunt separați de două diferențe cheie: virusul se răspândește în mai multe sisteme prin interacțiune umană, iar worm-ul se răspândește, fără factorul uman, în mai multe sisteme dintr-o rețea specifică, fie aceasta a unei companii sau a unei instituții, viermele digital este limitat la o „locație”.

Următorul tip de malware este unul întâlnit des, și anume *Trojan*. Acesta a primit denumirea după faimosul Cal Troian, deoarece apare a fi un program benign, dar defapt, odată instalat, acesta lucrează în umbre pentru a dăuna rețelei compromise, ducând la îngreunarea sistemelor, manipularea acestora în scop ilicit și, în cel mai rău caz, distrugerea lor. Un exemplu clasic de cal troian este cel identificat în anul 2007, intitulat Zeus, cunoscut și ca Zbot, ce a afectat sisteme bancare, furând date sensibile asociate conturilor clienților [53].

Virușii, viermii digitali sau troienii pot fi folosiți și pe post de Backdoor, adică o portiță pentru actorii ostili, oferindu-le acces la distanță la rețelele afectate, creând posibilitatea de inserție a malware și mai periculos.

Cu toții am văzut filme cu spioni, cel mai cunoscut fiind James Bond, în care aceștia se infiltrează în diferite locații confidențiale și inexpugnabile, colectând informații, câteodată și sabotând ample operațiuni. Într-o manieră asemănătoare, la începutul secolului XXI, a apărut termenul de *Spyware*, fiind un spion ce nu trece prin la fel de multă acțiune ca în filme, dar rolul lui este asemănător, infiltrându-se în „fortărețe" digitale, colectând date sensibile și reducând performanța sistemelor. O aplicație spyware notorie, ce acționează și în prezent, este DarkHotel. Acest program malițios se infiltrează în rețelele de Wi-Fi din hoteluri atunci când persoane influente precum politicieni sau directori de companii se cazează, urmărind furtul datelor și supravegherea acestora.

Cel mai enervant dar inofensiv tip de malware este *Adware*. Acesta supraîncarcă interfața utilizatorului cu reclame, împiedicând buna funcționare prin simple distrageri ce eventual îngreunează sistemul din punct de vedere al performanței. Această aplicație malițioasă este considerată inofensivă deoarece nu manipulează datele existente în rețea, însă monitorizează activitatea [54]. Malware-ul de acest fel este mai mult decât reprezentat și întâlnit, oricine împiedicându-se de el la un moment dat.

Cel mai periculos tip de malware apărut și emblematic pentru lumea hackingului, este *Rootkit*-ul. Acesta este cel ce oferă acces complet asupra unui sistem unui actor ostil, ulterior rețele dacă reușește să compromite cel puțin un terminal. Poate fi injectat în aplicații legitime, ba chiar și în sistemul de operare, putând să ascundă și alte tipuri de malware [51]. Un prime exemeplu de rootkit notoriu este numit Zacinlo, ce se deghizează a fi o aplicație legitimă, ce scanează computer-ul pentru alte aplicații malițioase, eliminându-le pentru a nu se afla în competiție cu alți actori ostili. Acesta deschide pagini de căutare invizibile și accesează bannere de reclame, actorul ostil primind bani din comisioanele de accesare a reclamei [55]. Un alt exemplu este cel al Sony BMG, care a dorit, în primul deceniu al anilor 2000, să introducă un nou software anti-piraterie pe toate CD-urile vândute direct de compania japoneză. Problema acestei aplicații era, însă, vulnerabilitatea gravă pe care o aducea pe sistemele publicului, și anume o portiță de rootkit pentru orice hacker ce avea suficientă voință de a abuza această slăbiciune [56]. Datele a mii de utilizatori au fost furate în acest fel, Sony ulterior retrăgând această inițiativă. Trebuie, de asemenea, menționat că aplicația transmitea companiei japoneze date despre preferințele utilizatorului, chiar dacă acesta refuza acordul de licență pentru utilizatorul final (eng. EULA) [57].

Botnet-ul este o aplicație malițioasă relativ inofensivă pentru utilizatorul de rând, ce are ca scop agregarea mai multor terminale și utilizarea acestora în atacuri de tip DDoS. Un exemplu de botnet este intitulat Mirai, ce a fost responsabil pentru marele atac din 2016 asupra Dyn, distribuitorul de domenii web [54].

Keylogger-ul este un subtip specializat de spyware. Acesta are rolul de a monitoriza input-ul utilizatorului, înregistrarea acestuia și ulterior transmiterea activității către programatorul aplicației. Acesta are totuși și uzuri legitime, precum monitorizarea copiilor [51]. Un exemplu din anii 2020 este intitulat „Agent Tesla". Acesta era capabil de a efectua capturi de ecran, furt de parole și transmiterea datelor vizate către actorii ostili ce l-au creat, fără ca utilizatorul să observe cu ochiul liber [58].

De menționat și un tip rar întâlnit de malware, și anume *Fileless Malware*, ce se infiltrează și lucrează din memoria volatilă, temporară, a unui terminal, nu în cea de stocare [54].

Din moment ce toate tipurile de Malware au la bază ceva ce trebuie descărcat de pe Internet, cele mai bune măsuri de protecție și remediere în cazul infectării sistemelor, sunt educația digitală (cunoașterea diferenței dintre link-uri suspecte și legitime), actualizarea sistemelor de operare, folosirea exclusivă a site-urilor securizate și oficiale (de tip HTTPS), utilizarea aplicațiilor anti-virus și crearea de copii de rezervă a informațiilor sensibile [6].

Până acum am discutat despre ostiliăți pasive, ostilități ce nu vizează o entitate anume, utilizatorii din lume trebuind să facă un pas greșit, atacatorii nefiind direct implicați în ofensivă. În continuare vom discuta despre ostilități active, ce vizează o entitate anume, hackerii fiind nevoiți să ia parte la un rol activ în atac.

Cel mai cunoscut exemplu de asemenea atac este cel de tip *DDoS (Distributed-Denial-of-Service)*. Această metodă implică utilizarea botnet-urilor menționate anterior, folosind sute, mii sau chiar milioane de dispozitive infectate, conectate la internet, pentru a bombarda o țintă cu un numar exagerat de mare de conexiuni într-un interval de timp minuscul, îngreunând toată infrastructura rețelei din spatele sistemelor și făcând-o inaccesibilă. Scopul unui atac DDoS este cauzarea de daune financiare prin căderea intenționată a platformelor online. Pe lângă pierderile monetare pe care le poate cauza, acest atac poate și să expună rețeaua din spatele platformelor, actorii ostili putând exploata mult mai ușor vulnerabilități în sistem [59].

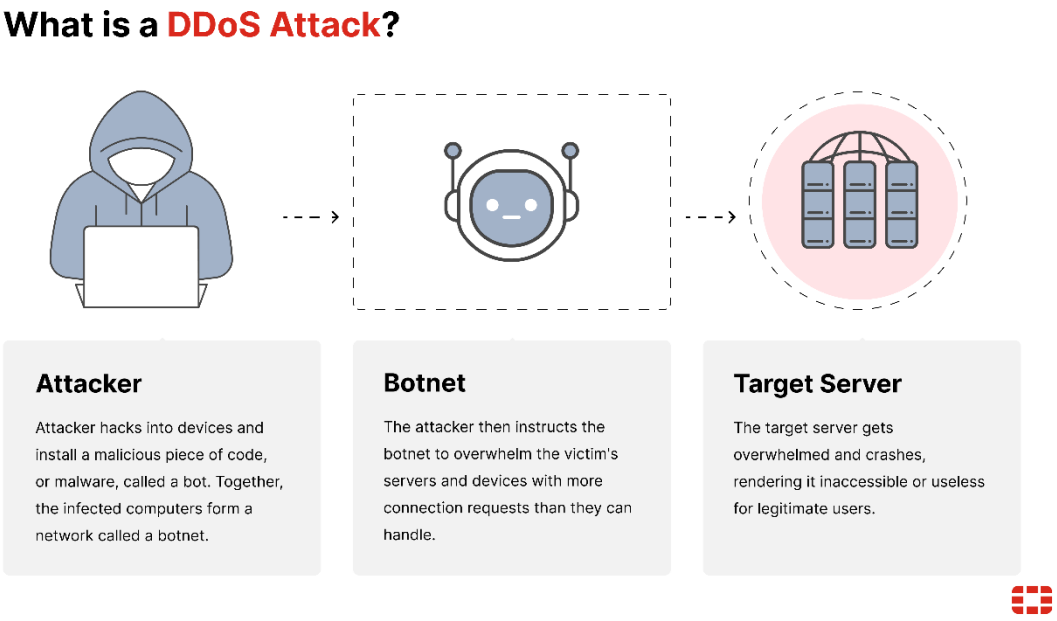


Fig. 11. „Ce este un atac DDoS?”
Sursa: https://www.fortinet.com/resources/cyberglossary/ddos-attack

Protejarea împotriva acestor atacuri este dificilă, dar nu imposibilă, existând mai multe posibilități de apărare, cum ar fi achiziționarea de firewall-uri avansate, auditarea sistemelor și a rețelei, de soluții anti-DDoS de la dezvoltatori legitimi, limitarea ratei de transfer al datelor rețelei într-o anumită perioadă de timp și crearea de echipe specializate de monitorizare a traficului de date [60].

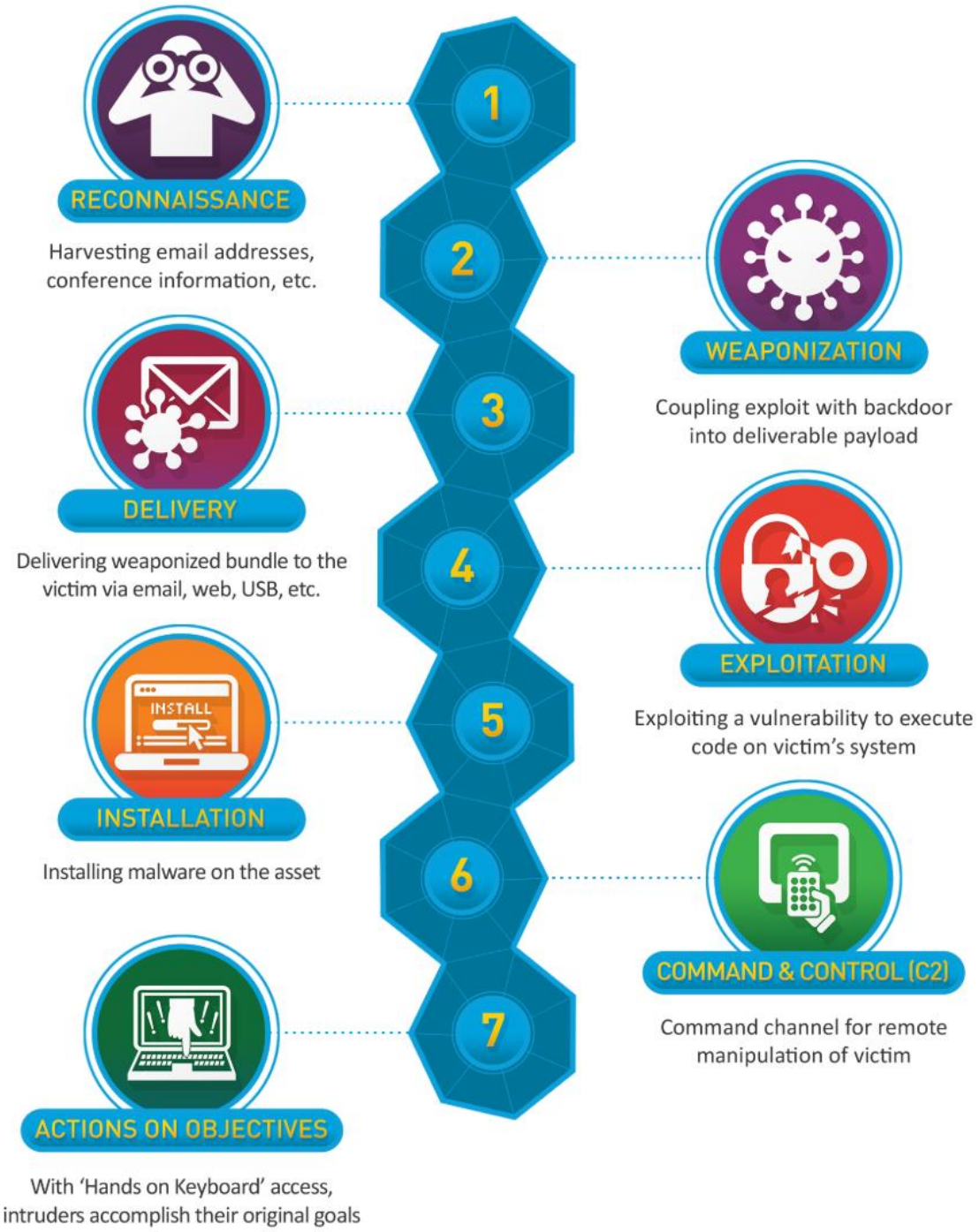


Fig. 12. Pașii operațiunilor digitale ofensive
Sursa: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Toate tipurile de atac menționate pot fi parte dintr-o complexă operațiune de preluare forțată de control a unei rețele. Figura 12 ne arată pașii, în larg, a acestui tip de operațiune.

2.2 Actorii ostili

Dacă în subcapitolul trecut am prezentat uneltele folosite în atacuri cibernetice, în acesta vom aborda utilizatorii acestora, criminalii din mediul digital, hackerii. Aceștia pot fi definiți ca actori rău intenționați ce au ca scop infiltrarea, furtul și sabotarea rețelelor și conținutul acestora [61].

În continuare vom clasifica tipurile de actori ostili.

Fig. 13. Tipuri de criminali cibernetici
Sursa: https://www.geeksforgeeks.org/ethical-hacking/cyber-criminals-and-its-types/

Primul și cel mai emblematic tip de criminal cibernetic este cel de *Black Hat Hacker*. Aceștia sunt cei mai notorii deoarece atunci când este vorba de un atac cibernetic, sursele media portretizează cel mai des acest fel de actori. Pe parcursul acestei lucrări ne vom referi la ei ca „Black Hats". Acești criminali se infiltrează în sisteme, cauzând prejudicii la nivelul rețelor și bazelor de date, preluând controlul acestora. Aceștia acționează ca niște mercenari virtuali, fie în grupuri organizate, fie individual, cu scopul de a primi sume semnificative de bani [62]. Cel mai comun exponent al acestei categorii este black hat-ul care sparge rețele bancare cu scopul de a fura bani.

Cel mai des întâlnit tip de hacker este *script kiddie*. Aceștia nu sunt criminali înrăiți, ci doar delicvenți ce folosesc unelte deja create de alți hackeri experimentați. Ei folosesc uneltele nu pentru beneficii monetare semnificative, ci pentru perturbarea rețelelor. Un exemplu întâlnit în mediul online este atunci când un adolescent se enervează pe jocul video intitulat „Team Fortress 2". Aceștia recurg la unelte pentru atacuri de tip DDoS de pe internet pentru a supraîncarca serverul de joc, deconectând toți jucătorii, runda oprindu-se prematur [61].

Cyber Terrorists sunt categoria de actori ostili ce acționează cu aceleași scopuri ca și grupările teroriste, doar că în mediul digital, ele fiind instigarea de frică, crearea de panică și sabotajul infrastructurilor digitale [63]. Cel mai notabil caz de terorism cibernetic este atacul ransomware WannaCry, ce a afectat rețele medicale din toată lumea. Se presupune că cei responsabili pentru aceste daune provocate sunt grupul Lazarus din Coreea de Nord [64].

Următoarea categorie de actori ostili din mediul virtual sunt cei ce nu caută câștiguri monetare, ci defapt urmăresc susținerea agresivă a unor cauze politice sau sociale. Aceștia sunt cunoscuți ca *Hacktivists* și scopul lor este să trimită mesaje prin aceste agresiuni. De-a lungul istoriei, ei nu s-au limitat doar la supraîncărcarea rețelelor unor organizații sau instituții publice, ci au ajuns până la furtul și mai târziu lansarea de date sensibile pe internet ale unor asociații sau instituții cunoscute sau indivizi (precum politicieni) controversați [61]. Un exemplu de hacktivism este

chiar cazul WikiLeaks. Acesta a constat în crearea unui site web ce urmărea expunerea către public activităților guvernului Statelor Unite, mai ales în cadrul conflictului cu Afganistan [65].

De foarte multe ori în mediul privat se aude despre *Insider Threats*. Aceștia sunt, defapt, angajati ai unor firme sau funcționari ai unor instituții ce își abuzează autorizația și accesul la sistemele din cadrul instituției pentru a da mai departe informații confidențiale unor instituții rivale, fie acestea private sau publice din alte state [66].

Cum există firme sau grupuri ce prestează servicii la scară largă, așa există și *Organized Cybercrime Groups*, sau grupări criminale cibernetice organizate. Acestea funcționează ca un business, acceptând contracte și prestându-și serviciile în schimba unor sume de bani. Mai mult, acestea pot să acționeze și de bună voie, țintind spre mari organizații, furând, criptând sau distrugând date, ulterior cerând sume de răscumpărare pentru a restaura sistemele compromise [67]. Un exemplu de grupare criminală cibernetică organizată este „Lapsus$", grupare de actori ostili ai căror membri sunt specializați în atacuri de tip social engineering și operațiuni de extorsiune [68].

Ultimul tip de actor ostil întâlnit în ecosistemul digital este *State-Sponsored Hacker*. Aceștia sunt specialiști plătiți de către autoritățile unui stat pentru a lansa atacuri și a procura date sensibile, oferi acces la baze de date și sabotarea infrastructurilor altor state. Aceștia au ca ținte, cel mai des, guvernele altor țări sau instituții subordonate acestora [61].

2.3 Măsurile României în domeniul Securității Cibernetice

Odată cu apariția acestor amenințări la nivel global, a trebuit ca și statul român să ia măsuri de apărare a noilor rețele apărute în infrastructura națională. De la simplele elemente de legislație până la înființarea de instituții publice subordonate guvernului dedicate domeniului securității cibernetice, România caută să își protejeze datele sensibile atât ale cetățenilor cât și pe cele ale funcționarilor publici.

Drumul României spre apărarea digitală a fost unul anevoios, care a început cu adoptarea legii nr. 51/1991, ce a autorizat ca Serviciul Român de Informații, Serviciul de Informații Externe și Serviciul de Protecție și Pază să îndeplinească îndatoriri în ceea ce privește securitatea informațiilor digitale. Acesta a continuat cu înființarea unității denumite Centrul Național Cyberint (CNC) din cadrul SRI în anul 2008, aceasta fiind desemnată ca autoritatea națională de identificare, prevenție și securizarea vulnerabilităților [69].

Odată cu apariția acestora și a digitalizării atât a lumii în mod general și a României în mod particular, a apărut și nevoia de specializare în mai multe domenii, cum ar fi cel civil și cel militar. În dimensiunea militară a securității cibernetice a fost înființat, în 2018, Comandamentul Apărării Cibernetice (CApC), ce se ocupă de partea virtuală a posibilelor conflicte din lumea contemporană, fiind o structura subordonată Ministerului Apărării Naționale [70]. În ceea ce privește dimensiunea civilă, în schimb, drumul a fost puțin mai lung, inițial înființându-se prin Hotărârea Guvernului nr. 494/2011 a „Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO", ce avea ca rol coordonarea și furnizarea de servicii în ceea ce privește creșterea nivelului de securitate a rețelelor informatice [25]. Un deceniu mai târziu, în anul 2021, Guvernul României emite Ordonanța de Urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică (DNSC), înlocuind CERT-RO, ca răspuns la noile amenințări, î apariției în discuție a Directivei NIS2 și nevoia de noi competențe în ceea ce privește răspunsul la atacuri cibernetice [26].

Tot în anul 2021, Guvernul României a adoptat Strategia de securitate cibernetică a României pentru perioada 2022-2027 prin Hotărârea de Guvern nr.1321/2021, având 5 obiective principale: Asigurarea securității cibernetice în cadrul rețelelor și sistemelor informatice, cadrul normativ și instituțional consolidat, un parteneriat public-privat pragmatic între autorități naționale și entități

private, cetățeni și mediul academic, abordarea de noi măsuri de prevenție și de sancțiuni privind atacurile cibernetice și implicarea României în cadrul scenei internaționale, promovând statul ca un actor important în acest aspect al relațiilor dintre state [71].

Prin cele prezentate anterior, putem determina seriozitatea statului român în privința securității cibernetice proprii. Am enumerat și explicat atacurile cibernetice, uneltele folosite de hackeri pentru a realiza aceste ilegalități, tipurile de actori ostili, cum acționează și diversele motive din care se pot realiza breșe de securitate și măsurile existente luate de către statul român.

Capitolul 3. Studiu de caz - București 2020-2025

În acest capitol vom avea o abordare practică a acestui subiect, în care vom prezenta și cazuri concrete și potențiale soluții pentru rezolvarea problemelor apărute în infrastructura IT a administrației publice locale din București, care nu se limitează doar la aspecte tehnice, ci se extind până la modul de utilizare a sistemelor digitale de către funcționarii publici. În primul subcapitol se vor arăta două cazuri, un exemplu negativ și unul pozitiv în ceea ce privește acțiunea în cazul unei breșe majore de securitate, iar în cel de-al doilea subcapitol vor fi introduse răspunsuri reieșite din interviuri cu specialiști ce au experiență de cel puțin 5 ani în domeniu, care au lucrat sau lucrează atât în sistemul public cât și în cel privat. În ambele părți vor fi aduse în discuție potențiale soluții propuse atât de către Directoratul Național de Securitate Cibernetică, cât și de către specialiștii intervievați.

3.1. Studiu de caz

Pentru a înțelege cum sunt mai exact desăvârșite atacurile cibernetice, trebuie să trecem printr-o scurtă istorie a metodelor de infiltrare a virușilor în sistemele de pretutindeni, chiar și cele complet deconectate de la internet, din alte colțuri ale lumii. Totul a început în anul 1981, când unul din primii viruși a fost prezent pe o dischetă (floppy disk) ce în mod normal conținea o instalare pentru un joc video. În acele vremuri, trebuia ca atacatorul să meargă fizic la calculatorul victimei pentru a planta virusul, asta în cazul civililor și a celor ce nu aveau acces la „ARPANET", strămoșul internetului de astăzi. Mai târziu, au apărut și virușii de tip worm în toată lumea, asta după ce a apărut, oficial, „Internetul". În 1999, Melissa, un virus de tip worm, a reușit să se infiltreze în multe sisteme, ba chiar a reușit să își facă simțită prezența și pe serverele de e-mail Microsoft și Intel, prin e-mail-uri ce reprezentau, la bază, o tactică de inginerie socială [72]. Acum, revenim în metodele apărute în prezent. Dacă acum zeci de ani erau folosite dischete și plantarea manuală a virușilor, acum ajungem la metode mai sofisticate. Desigur, acestea conțin, la bază, vechile modalități, însă duse la un alt nivel. În zilele noastre, e-mail-urile, paginile false, de pe care unii oameni descarcă fișiere nelegitime care infectează sistemul pe care au ajuns și ulterior toată rețeaua la care acesta este conectat, și mesajele SMS false sunt pretutindeni, foarte multă lume știind despre ele dar, totodată, și mai multă lume neștiind despre aceste metode de inginerie socială și accesează conținutul mesajelor, compromițând-uși dispozitivele.

Mergând la nivel înalt, guvernele lumii au observat că acești viruși pot fi folosiți pe post de „spioni digitali", nemaifiind necesară infiltrarea unui om într-o locație țintă, ci doar a unui virus pe un calculator care apoi se conectează la rețeaua internă a respectivei organizații sau țări. Un astfel de exemplu este *Stuxnet*, cel mai avansat worm descoperit și despre care am mai vorbit în capitolul 2. Acesta a fost făcut de către Statele Unite în colaborare cu Israel pentru a împiedica proliferarea armelor nucleare în Iran. Au fost plasate stick-uri USB în jurul unor zone și locuințe unde se presupunea că locuiau funcționari sau chiar savanți ce lucrau la baza nucleară iraniană Natanz din Iran. Eventual, unele din stick-urile USB au fost inserate în dispozitivele conectate la rețeaua respectivei baze, făcând operațiunea un succes, sabotajul constand în uzarea accelerată a unor centrifuge și eventual stricarea acestora. Problema a fost când *Stuxnet* a fost descoperit și înafara acestui „circuit închis" din Iran, adică din Orientul Mijlociu până în Europa, însă, din fericire, acesta avea un set de instrucțiuni foarte bine definit și căuta doar centrifugele din Natanz după codurile unice de identificare ale acestora. [72]

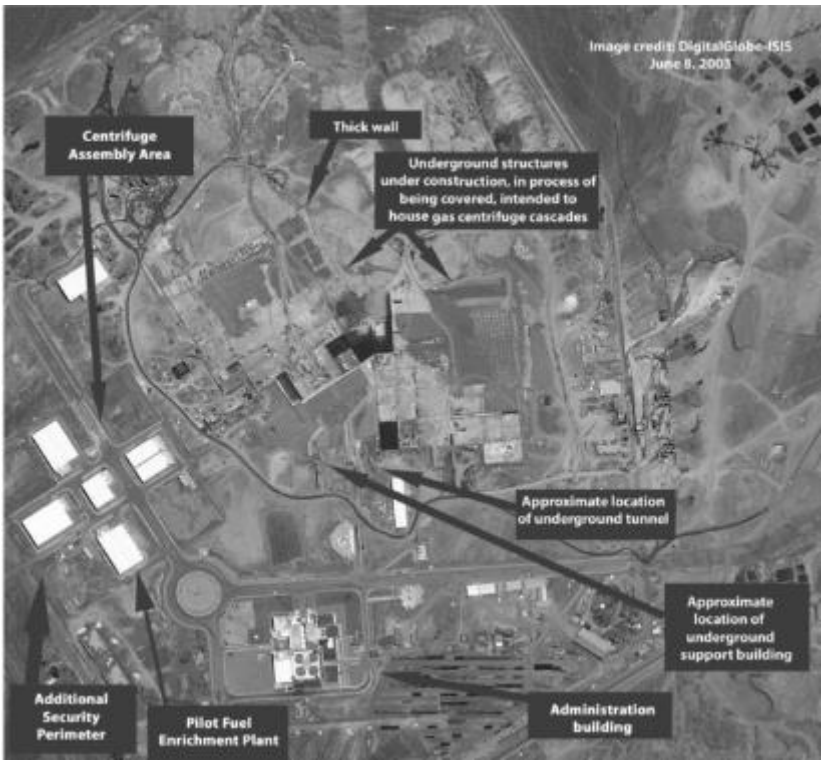


Fig. 14. Natanz, ținta *Stuxnet*
Sursa: https://scrd.eu/index.php/scic/article/view/225/188

Nu putem, dacă menționăm *Stuxnet*, să nu menționăm și *The Flame*. Acesta era un malware asemănător unui virus troian prin modul său de acțiune, însă era o aplicație de sine stătătoare. Acest program malițios a fost depistat tot în Orientul Mijlociu și avea capacități sporite de monitorizare și colectare de informații de pe sistemele infectate. Acesta putea să capteze sunete din microfoanele conectate la sistem, având senzori software ce declanșau protocolul de înregistrare atunci când anumite aplicații pentru comunicare online erau deschise, efectua capturi de ecran (screenshots) la anumite intervale de timp definite, reținea parole și alte date de logare, înregistra ce scria utilizatorul pe propria tastatură, scana dispozitive ce erau vizibile prin Bluetooth și fura date din documente ce păreau a fi de interes, de multe ori, acestea fiind fix ce își doreau dezvoltatorii *The Flame*. Acest malware se propaga prin aceleași modalități ca *Stuxnet*. [73]

În continuare vom prezenta cele două cazuri emblematice care ne arată cum nu trebuie să acționeze și cum ar trebui să o facă cei responsabili de securitatea bazelor de date ale rețelelor instituțiilor publice din București. În primul exemplu vom cerceta efectele negative ale unei administrații defectuoase cum ar fi lipsa transparenței, ineficiența și alocarea necorespunzătoare a resurselor financiare. În cel de-al doilea exemplu, o să observăm cum o administrație eficientă și un răspuns prompt din partea organelor competente duc la soluționarea breșelor de securitate fără pierderi monetare semnificative. În final, vom studia câteva posibile soluții în ceea ce privește breșele de securitate cibernetică.

3.1.1 Atac de tip Ransomware la Primăria Sectorului 5 – Octombrie 2024

La finalul lunii Octombrie 2024, angajații Primăriei Sectorului 5, București, au fost primiți cu o serie de mesaje pe ecranele sistemelor digitale ale administrației. Aceste mesaje erau din partea grupării infracționale „RansomHub", care cereau o sumă enormă de bani în schimbul restaurării bazelor de date afectate și garanția că datele furate nu vor fi publicate pe dark web [74]. Conform unui specialist ce monitoriza activitatea din colțurile clandestine ale Internetului, datele afectate aparțineau a circa 200.000 de cetățeni ai Sectorului 5 și urmau a fi publicate în cazul neplății sumei de răscumpărare, cauza principală a succesului unui asemenea atac a fost lipsa unui sistem de protecție adecvat, întrucât entitatea responsabilă de acest lucru a fost o firmă-fantomă, cu un

singur angajat, ce se ocupa de vânzarea de freze pentru strunguri [75]. Ulterior acestor evenimente, Directoratul Național pentru Securitate Cibernetică a propus, prin mai multe comunicate oficiale diferite soluții pentru prevenirea și remedierea atacurilor de tip ransomware. Conform comunicatului oficial de presă a DNSC, metodele propuse sunt:

- Crearea de copii de rezervă a datelor și sistemelor digitale din infrastructura IT a instituției;
- Folosirea de aplicații anti-virus actualizate la zi;
- Limitarea sau eliminarea programelor ce oferă acces la distanță la sistemele din infrastructură;
- Utilizarea de soluții avansate de tip firewall și actualizate zilnic;
- Utilizarea unor parole complexe și schimbarea lor în mod regulat;
- Segmentarea rețelei digitale. [76]

Până la momentul redactării acestei lucrări, nu au fost publicate soluțiile concrete implementate de către administrația sectorului 5, București, acest caz fiind exemplul negativ în ceea ce privește modul în care au acționat autoritățile responsabile de securitatea cibernetică a unei instituții importante din București.

3.1.2 Atac de tip Ransomware asupra mai multor spitale din București – Februarie 2024

În luna Februarie 2024, mai multe spitale din București au fost atacate de o grupare anonimă de infractori cibernetici prin intermediul aplicației „Backmydata". Aceasta face parte din familia ransomware „Phobos" (prezentată în capitolul anterior), ceea ce înseamnă că face parte dintr-un pachet de tip Ransomware-as-a-Service. Programul malițios a criptat toate datele aflate pe serverele instituțiilor afectate. La fel ca și alte atacuri de acest fel, au fost cerute sume de răscumpărare a datelor. DNSC a răspuns în urma unei notificări primite, deconectând sistemele afectate de la Internet pentru a efectua investigații. După ce au determinat „arma" atacatorilor, specialiștii trimiși au început să restaureze datele din bazele de date ale spitalelor. Directoratul Național de Securiatea Cibernetică a emis o serie de mai multe recomandări pentru toate spitalele ce foloseau platforma „Hipocrate", cele mai notabile fiind îndemnarea de a nu opri echipamentul pentru a nu se pierde dovezi ale infracțiunii din memoria RAM și de a le „carantina" (izolarea acestora din rețeaua internă). Factorul decisiv din acest caz îl reprezintă faptul că administrația bazelor de date ale spitalelor a făcut, în mod periodic, copii de rezervă ale sistemelor și au reușit să restaureze majoritatea datelor criptate [77].

Acesta reprezintă un exemplu pozitiv al modalității de prevenție a atacurilor digitale și remediere a efectelor acestora asupra infrastructurii cibernetice a mai multor instituții. Aici putem vedea avantajele unei gândiri proactive ale administrației și a unei mobilizări prompte și eficiente din partea celor ce au ca rol rezolvarea problemelor de acest fel.

3.1.3 Soluții propuse

În ceea ce privește prevenirea breșelor de securitate sau remedierea efectelor ce apar din cauza atacurilor cibernetice, există o multitudine de modalități prin care se pot realiza cele două procese menționate. Bineînțeles, acestea sunt mai ușor de menționat decât aplicat, deoarece acest domeniu aflat într-o perpetuă stare de competiție dintre ofensivă și defensivă, soluțiile ce vor fi propuse trebuind a fi adaptate la condiții noi sau care se schimbă constant, breșele de securitate având o similaritate între ele, dar niciodată una totală. Atât instituțiile publice cât și companiile private au

nevoie de oameni cel puțin versați în ceea ce privește utilizarea corectă și sigură a unei rețele informatice, factorul uman fiind, până la urmă, cel decisiv. Orice măsură luată la nivelul sistemului poate fi ușor dată la o parte de un utilizator care nu este suficient de educat în domeniu, infrastructura având riscul de a pica pradă unui actor ostil ce, de obicei, are ca scop furtul și încetinirea (sau chiar distrugerea) unei rețele IT.

Întorcându-ne la instituțiile publice din București, organul competent din ambele cazuri menționate mai sus, Directoratul Național de Securitate Cibernetică, a emis mai multe recomandări și soluții pentru prevenire și remediere, dar și reguli de bună practică pentru funcționarii din administrație și utilizatorii de pretutindeni. Cele mai notabile și des întâlnite soluții propuse sunt:

- Utilizarea unui software de tip anti-virus pe toate calculatoarele din cadrul instituției sau companiei;
- Utilizarea exclusivă a surselor de încredere în ceea ce privește descărcarea de fișiere și aplicații software;
- Utilizare de soluții tip Firewall;
- Utilizarea sistemelor automate de detectare și prevenție în ceea ce privesc conexiunile externe la sistemele interne;
- Instruirea celor din mediul intern al instituției sau companiei în buna utilizare a infrastructurii IT;
- Crearea și utilizarea de copii de rezervă ale bazelor de date și ale sistemelor digitale.

Majoritatea celor propuse de către DNSC sunt practici ce se regăsesc în multe alte liste din lume, însă acestea sunt considerate „fundația" procesului de protejare a unei rețele de sisteme digitale, metodele putând fi folosite atât în prevenție, cât și remediere. [77], [78]

Din cele două exemple menționate în acest subcapitol, se poate observa cum factorul uman este cel ce prezintă cel mai decisiv factor în lumea digitală, primul, cel negativ, arătându-ne cum delăsarea și aprecierea greșită a amenințărilor cibernetice combinate cu administrația defectuoasă duc la pierderi financiare semnificative, dar și degradarea încrederii cetățenilor în instituția ce le stochează și utilizează datele personale, promisiunile făcute față de aceștia fiind încălcate, lucru ce poate fi interpretat ca o lipsă de interes față de oameni și viețile lor private.

În cel de-al doilea exemplu, considerat cel „pozitiv", ni se arată cum, atunci când organele competente sunt ascultate și practica digitală este una bună, cei responsabili de administrație fiind mai mult decât versați și instruiți, administrația este una eficientă, răspunsul la breșa de securitate este unul prompt, datele personale ale cetățenilor sunt restaurate, iar sistemele IT din cadrul instituțiilor sunt intacte și funcționale.

3.2 Studiul experienței specialiștilor

Pentru aprecierea nivelului implementării soluțiilor de securitate cibernetică și pentru aflarea unor noi potențiale soluții pentru problemele existente din domeniu, au fost realizate interviuri cu mai mulți specialiști. Aceștia au sau au avut legătură cu procesul de digitalizare al instituțiilor publice din București, lucrând cu funcționari publici și instruindu-i în noua infrastructură. Scopul principal al acestor interviuri îl constituie realizarea unei sinteze a implementării sistemelor digitale în administrația publică locală a Bucureștiului. Răspunsurile reieșite din interviuri sunt, în mare parte, similare, lucru care ne ajută să ne dăm seama mai ușor de situația reală în care se află instituțiile publice și problemele pe care le întâmpină în ceea ce privește siguranța datelor din

sistemele digitale. Structura interviului (Anexa A) este una simplă, întrebările fiind împărțite în 5 categorii principale, acelea fiind contextul și amenințările cibernetice actuale, elemente despre educația digitală și factorul uman, infrastructura digitală, implementarea legislației și propuneri de soluții pentru viitor, fiecare dintre acestea conținând câte 4 întrebări. Specialiștii intervievați și-au dat consimțământul ca răspunsurile lor să fie transpuse în această lucrare (subsecțiunile A1, A2 și A3 din cadrul Anexei), însă au dorit să rămână anonimi pentru a-și proteja identitatea.

Din răspunsurile obținute de la participanții la interviu, reiese faptul că în ultimii 5 ani majoritatea atacurilor cibernetice nu mai sunt realizate de către „script kiddies", ci de grupări infracționale organizate, grupuri sponsorizate, în secret, de state și chiar de actori ce provin din servicii de informații din alte state. Aceștia au adăugat că astfel de atacuri aduc atât daune financiare asupra infrastructurii din cauza costurilor de funcționare, dar și presiune socială și politică. Atunci când o mulțime de oameni observă ca o platformă nu funcționează corespunzător, primul instinct este să își exprime frustrarea față de instituții în sinea lor, nefiind cunoscut la momentul unui atac cu scopul de a îngreuna o platformă online motivul acestei probleme.

Cele mai des întâlnite atacuri în infrastructura administrației publice locale din București sunt cele Ransomware. Această amenințare apărută de cele mai dese ori dintr-o eroare umană prin descărcarea unui fișier dintr-o sursă nelegitimă sau de pe un e-mail provenit dintr-o sursă neverificată reprezintă cea mai mare problemă la momentul actual pentru rețelele de informații din București. Criptarea forțată a datelor sensibile și extragerea acestora cu scopul de a le vinde mai târziu este o amenințare gravă la buna funcționare a instituțiilor publice, dar și pentru siguranța cetățenilor. Pe lângă ransomware, infrastructura IT a Bucureștiului se confruntă și cu atacurile DDoS (Distributed Denial of Service), care îngreunează platforme online, Malware și tacticile de inginerie socială sau Phishing.

O altă mare problemă în instituțiile de administrație publică locală o reprezintă factorul uman și lipsa acestuia de experiență, referindu-ne la funcționarii publici. După cum am mai spus, anumiți angajați ai instituțiilor mai au tendința să apese, în mod normal din necunoștință de cauză, pe link-uri suspicioase și nelegitime. Pe lângă aceste simple descărcari de fișiere într-un sistem digital, mai există și riscul ca aceștia să își introducă datele de logare pe platformele asociate muncii lor pe pagini web neoficiale, actorii ostili putând ulterior să folosească aceste date pentru propriile lor scopuri. Aici a fost propusă drept soluție introducerea autentificării Multi-Factor obligatorie în rândul funcționarilor, ce presupune adăugarea unui pas în plus logării pe sistemele critice, fie printr-un cod de acces ce se schimbă odată la 30 de secunde, fie prin autentificare biometrică, cea mai sigură, așa cum reiese din răspunsuri, fiind cea ce presupune recunoașterea corneei. S-a mai constatat și o lipsă de programe de instruire suficient de regulate și riguroase în sistemul public, acestea fiind tratate cu nepăsare de multe ori însă, cu cât ne apropiem de prezent, se poate constata o creștere în atenția acordată subiectului securității cibernetice. Specialiștii consideră și că ar trebui introdusă în programa școlară a cel puțin o oră pe săptămână a unei ore de educație în securitatea digitală.

La cea de-a treia categorie, și anume „Infrastructura Digitală", se poate constata o variație în răspunsurile specialiștilor, mai ales la prima întrebare. În anumite instituții, auditurile periodice de securitate în cadrul platformelor utilizate de cetățeni se fac în mod repetat, însă în alte cazuri, aceste audituri nu au aceeași frecvență sau rigurozitate. Ca măsuri de redundanță și de backup pentru a răspunde ferm unui atac ransomware, instituțiile creează pe sistemele „de redundanță" (servere suplimentare și în general aparatură ce este folosită strict în cazul unui atac) copii de rezervă ale sistemelor, însă frecvența creări acestora variază de la instituție la instituție, iar practica testării backup-urilor rămâne și ea sub semnul întrebării. Specialiștii au răspuns ultimei întrebări din cateogrie în mai multe feluri, însă integritatea datelor rămâne problema identificată de toți. Unul dintre ei a menționat și faptul că nu există neapărat o protecție totală față de alte perechi de ochi, deoarece centrele de servere pe care ar fi stocate datele nu se află în România și, fizic vorbind, oricine ar putea accesa datele respective dacă află o parolă sau trece de metodele de criptare ale datelor. Cel mai important lucru rămâne educația în acest domeniu, soluțiile tehnice

cum ar fi implementarea de aplicații anti-virus, schimbarea în mod regulat a parolelor și actualizarea la zi a sistemelor de operare și a protocoalelor de securitate fiind vulnerabile modului în care un utilizator își folosește aparatura.

Trecând la următoarea categorie, cea ce ține de partea legislativă a domeniului. Participanții la interviu nu consideră primăriile de sector pregătite să își asume total responsabilitatea legală în cazul expunerii datelor sensibile ale cetățenilor pe Dark Web, fiind într-o fază de „învățare". Totodată, când vine vorba de implementarea GDPR, specialiștii au remarcat implementarea la nivelul legislativ, însă nu în totalitate la nivel tehnic, fapt reieșit nu din practica de zi cu zi, ci din cum răspund funcționarii în cazul unei breșe de securitate, opiniile sunt aceleași și când vine vorba despre introducerea unei legislații mai riguroase în acest domeniu, eliminând pe cât posibil zonele gri, iar pedepsele pentru atacurile cibernetice săvârșite în mod ilegal și neautorizat ar trebui înăsprite.

În ceea ce privește ultima categorie de întrebări, și anume „Propuneri de soluții pentru viitor", răspunsurile variază. Crearea unei echipe sau centru care să monitorizeze permanent traficul de date în instituțiile din București și implementarea obligatorie a autentificării Multi-Factor sunt soluțiile favorite ale intervievaților, iar implementarea inteligenței artificale a ajuns, în mare parte, la nivel de discuție în instituții, însă este o idee promițătoare care în unele cazuri se află la începutul implementării. Perspectivele asupra dilemei sporirii atribuțiilor de monitorizare a serviciilor de informații diferă, două dintre opinii fiind că nu ar fi o idee rea dar cu condiția existenței unui organ de control civil care să supravegheze aceste autorități, iar celălalt răspuns fiind că aceștia ar trebui să-și extindă atribuțiile de monitorizare în rândul personalului administrativ strict pentru securitatea cibernetică, nu supravegherea cetățenilor. Opiniile față de extinderea jurisdicției DNSC sunt și ele împărțite, doi considerând că Directoratul Național de Securitate Cibernetică ar trebui să beneficieze de această lărgire a capacităților sale din punct de vedere legislativ, iar unul considerând că nu trebuie pusă problema capacităților juridice, ci a creșterii numărului de angajați specializați în instituție.

Întorcându-ne puțin la întrebarea ce pune aduce în temă sporirea atribuțiilor de supraveghere ale serviciilor de informații, unul din specialiști a menționat proiectul „PRISM" al Statelor Unite ale Americii, ce nu este un simplu „ochi" ce veghează răufăcătorii, ci pe absolut toată lumea, inocentă sau nu. Acest proiect implică, pe lângă altele precum „XKeyscore", existența unui backdoor în fiecare sistem din lume pentru a colecta date despre oricine. [79], [80]

Recomandări

În urmă cercetării proprii și a interviurilor, reies mai multe soluții pentru instituțiile ce țin de administrația Bucureștiului. Aceste soluții vizează atât infrastructura în sine, cât și componenta umană:

1. *Introducerea autentificării Multi-Factor*. Aceasta reprezintă o soluție ce poate fi introdusă imediat în rândul funcționarilor publici ce nu prezintă un grad de complexitate ridicat, deoarece implementarea poate ține și de simplul mesaj primit prin SMS în momentul introducerii datelor de logare corecte pe o platformă pentru confirmarea identității, minimizând riscul de breșe rezultate din acces neautorizat și al metodelor de inginerie socială. Cea mai sigură metodă de implementare a autentificării în mai mulți pași este prin folosirea unei aplicații special gândită pentru asta, deoarece SMS-urile pot fi interceptate și ele.

2. *Crearea automată de copii de rezervă a tuturor dispozitivelor din rețea și testarea acestora la zi*. Soluția se adresează cel mai des atacurilor ransomware. În urma unei astfel de breșe, în mod normal, toate datele din rețea sunt compromise și inaccesibile. Dacă personalul creează și testează copii de rezervă, acestea pot fi folosite pentru a restaura

buna funcționare a sistemelor informatice. Este imperios ca respectivele copii de rezervă să fie complet izolate de rețea.

3. *Întărirea sistemelor de protecție DDoS*. Acest lucru poate fi realizat prin utilizarea de servicii de mitigare a acestor atacuri folosind tehnologia Cloud, introducerea de limitare a ratei de transfer către un singur client, monitorizarea traficului de date și detectarea de anomalii în acesta.

4. *Introducerea de politici pentru actualizarea tuturor elementelor din infrastructura IT*. Personalul administrativ trebuie să își actualizeze sistemele la zi pentru a preveni potențialele breșe reieșite din vulnerabilități depistate în versiuni anterioare ale sistemului de operare sau ale protocoalelor de securitate.

5. *Instruirea personalului din instituții*. Cea mai mare vulnerabilitate în orice sistem o reprezintă factorul uman nepregătit. Această problemă poate fi rezolvată prin introducerea unui program de instruire trimestrial și prin campanii de informare cel puțin odată pe săptămână în rândul funcționarilor publici.

6. *Crearea unei echipe de elită pentru monitorizarea permanentă a traficului de date*. Autoritățile responsabile pentru siguranța datelor sensibile ale cetățenilor ar putea să își facă o selecție de cei mai competenți oameni pentru a îi reuni într-o singură echipă dedicată monitorizării traficului de date și apărarea sistemelor digitale în timp real.

7. *Compartimentarea rețelelor pentru dispozitivele IoT*. Camerele de luat vederi, senzorii de trafic și restul dispozitivelor ce fac parte din infrastructura „Smart City” pot fi foarte ușor atacate de infractori digitali. Pe lângă actualizarea parolelor și a sistemelor de operare, este necesară separarea rețelelor pe care sunt conectate aceste dispozitive.

Concluzii

Această lucrare și-a propus să analizeze modificările aduse sistemului de funcționare al administrației publice locale din București în ceea ce privește securitatea cibernetică. Am studiat sistematic implementarea efectivă a sistemelor digitale în procesul administrativ, cei mai comuni factori de risc, exemple de abordări diferite a unor breșe de securitate și am oferit potențiale metode de îmbunătățire a siguranței digitale.

Conform primei ipoteze, digitalizarea poate aduce un număr de beneficii ce au un impact major, cum ar fi transparența sporită, eficientizarea lucrului cu cetățenii, facilitarea comunicării dintre stat și cetățeni, prin folosirea metodelor de stocare virtuală a informației, crearea de platforme online ce au ca scop fluidizarea procesului administrativ și ameliorarea cozilor apărute în fața ghișeelor, oricine putând să acceseze aceste pagini web pentru a își depune cereri, plăti taxe și impozite și pentru a pune întrebări funcționarilor publici. Aceste beneficii sunt confirmate încă din primul capitol al lucrării, însă tot din acesta reiese și ultima parte a ipotezei, și anume apariția vulnerabilităților ale bazelor de date. Dacă sistemul nu este protejat și menținut adecvat, datele sensibile pot pica pradă cu ușurință în mâinile infractorilor.

Cea de-a doua ipoteză este cea mai discutată în lucrare, pe marginea acesteia fiind evidențiate modurile de atac ale actorilor ostili din mediul digital, uneltele folosite de aceștia și alți factori de risc ce pot expune punctele slabe ale rețelelor, facilitând compromiterea acestora. Aici am putut observa diferitele motive din care sunt lansate aceste atacuri, de la delicvențe puerile la activism și războaie hibride purtate între state.

În partea practică am identificat și cea mai mare amenințare pentru infrastructura IT a administrației publice locale, dar și pentru orice altă bază de date, fie din sistemul public sau privat, și anume factorul uman atunci când acesta este nepregătit și ignorant în ce privește utilizarea și menținerea corectă a sistemelor digitale.

Obiectivul principal al cercetării nu a fost doar identificarea celei mai grave amenințări la adresa integrității și siguranței datelor, ci a fost analizarea tuturor riscurilor existente în prezent și oferind soluții pentru a rezolva deficiențele din rețele, cum ar fi backup-ul regulat, implementarea autentificării în mai mulți pași și instruirea personalului instituțiilor.

În cel de-al doilea capitol au fost analizate tipurile de atacuri cibernetice, ce pot face parte și ele, la rândul lor, din ample operațiuni APT ale unor grupuri de hacktiviști sau actori statali. Ce a rezultat din propria cercetare și din interviuri este că Ransomware și DDoS rămân cele mai des utilizate metode de atac împotriva sistemelor din administrația publică locală a capitalei, astfel atingând primul obiectiv secundar. O parte pozitivă ce reiese din această statistică este că personalul competent se poate hiperspecializa în contracararea acestor tipuri de breșe de securitate.

Obiectivele secundare 2 și 3 au fost atinse în studiul propriu din capitolul 3, când am analizat două breșe de securitate la instituții importante din București și modul în care cei responsabili au acționat privind protecția datelor sensibile ale cetățenilor. Primul exemplu este unul negativ, deoarece, chiar dacă GDPR este introdus în legislația românească și în modul de funcționare al instituției prezentate, nu au fost respectate prevederile acestui regulament. Cel de-al doilea exemplu, în schimb, ne-a arătat respectarea GDPR și un plan de acțiune bine pus la punct și executat cu o maximă eficiență.

Drept concluzie finală, domeniul securității cibernetice se află într-o perpetuă evoluție, noi metode de a compromite baze de date apărând zilnic, operațiunile infractorilor digitali sunt din ce în ce mai ample și sofisticate, aceștia ajungând să fie chiar actori sponsorizați de către alte state pentru a le purta războaiele informatice. Autoritățile responsabile pentru protejarea datelor sensibile atât din propriile sisteme cât și din bazele de date ce conțin datele personale ale cetățenilor trebuind să fie din ce în ce mai vigilente. Cu toate acestea, tot utilizatorul rămâne cel mai mare factor de risc, o singură greșeală umană putând compromite infrastructuri IT întregi, nimeni nefiind complet în siguranță în lumea digitală.

Anexa A. Interviu: Securitatea Cibernetică și protecția datelor în administrația publică locală

C1. Contextul actual și Amenințările cibernetice

1. Din experiența dumneavoastră, ați putut observa o tranziție de la atacurile oportuniste, de tip „script kiddie”, către operațiuni de spionaj cibernetic sau hacktivism mai bine structurate în ultimii 5 ani?

2. Din punctul dumneavoastră de vedere, care sunt cele mai frecvente tipuri de atacuri cibernetice identificate la nivelul instituțiilor din București în ultimii ani?

3. În ce măsură atacurile de tip DDoS au devenit un instrument de hacktivism sau presiune politică asupra infrastructurii administrative locale?

4. Având în vedere importanța strategică a capitalei, observați o incidență mai mare a atacurilor cibernetice susținute de actori statali față de restul țării?

C2. Educația Digitală, Factorul Uman

1. În ce măsură considerați că „eroarea umană” rămâne principala vulnerabilitate a infrastructurii IT din administrația publică?

2. Considerați că autentificarea multi-factor la nivelul tuturor funcționarilor publici ajută la minimizarea riscului atacurilor cibernetice?

3. Ce tip de programe de instruire în securitate cibernetică sunt oferite personalului administrativ pentru a recunoaște tacticile de inginerie socială?

4. În opinia dumneavoastră, ar trebui introdusă în programa școlară o oră de educație în securitate digitală?

C3. Infrastructura Digitală

1. Se realizează audituri periodice de securitate în cadrul platformelor utilizate de cetățeni pentru a identifica eventuale vulnerabilități zero-day?

2. Ce măsuri specifice de redundanță și backup sunt implementate pentru a asigura continuitatea serviciilor în cazul unui atac ransomware?

3. Cum sunt securizate dispozitivele de tip IoT (camere, senzori smart city) pentru a nu deveni porți de intrare pentru malware?

4. Care sunt provocările în asigurarea integrității datelor atunci când instituțiile optează pentru soluții de stocare în Cloud?

C4. Implementarea legislației

1. Cât de pregătită este administrația publică locală să își asume responsabilitatea legală în cazul în care datele cetățenilor sunt expuse pe Dark Web?

2. Cum apreciați gradul de conformitate cu regulamentul GDPR în procesul de digitalizare a bazelor de date atribuite primăriilor de sector?

3. Considerați că avem nevoie de o legislație mai riguroasă în domeniul securității cibernetice?

4. Din punctul dumneavoastră de vedere, ar trebui înăsprite pedepsele aplicate celor ce săvârșesc atacuri digitale?

C5. Propuneri de soluții pentru viitor

1. Dacă ați putea implementa o singură măsură urgentă pentru a securiza digital Bucureștiul, care ar fi aceea?

2. În ce măsură au început instituțiile din București să integreze Inteligența Artificială (AI) pentru monitorizarea autonomă a traficului de date? Considerați aceasta o potențială soluție pentru securitatea cibernetică a instituțiilor din oraș?

3. Din perspectiva dumneavoastră, serviciile de informații ar trebui să primească atribuții sporite în ceea ce privește monitorizarea dispozitivelor populației?

4. Ar trebui ca DNSC să beneficieze de o extindere a jurisdicției sale?

A.1. Interviu 1

C1. Contextul actual și Amenințările cibernetice

1. În ultimii 5 ani, nu mai avem de-a face doar cu indivizi ce se cred a fi hackeri. În prezent ne confruntăm cu organizații formate din profesioniști ce sunt, în mod special, plătite pentru a procura și vinde date sensibile.

2. Cele mai frecvent întâlnite în instituțiile din București sunt sistemele neactualizate la zi, atacurile Phishing și virușii Ransomware.

3. În mare parte, atacurile DDoS sunt folosite pentru îngreunarea sistemelor, însă, ca efect secundar, în cazul instituțiilor publice, pot fi folosite și pentru a aduce presiune din partea cetățenilor nemulțumiți cu site-urile instituțiilor pe care le accesează.

4. Ca în orice alt stat, fiind vorba despre capitală, unde se află „centrul" administrației, este normal ca Bucureștiul să prezinte mai mult interes față de alte orașe din România pentru actori statali.

C2. Educația Digitală, Factorul Uman

1. În cea mai mare măsură, deoarece indiferent de măsurile luate la nivel tehnic, cum ar fi utilizarea de soft anti-virus, o greșeală umană este tot ceea ce îi trebuie unui hacker. Omul poate da un click unde nu trebuie și să compromită toată rețeaua, mai ales în cazul lipsei educației în acest sens.

2. Este un factor crucial, pentru că utilizarea autentificării în doi pași reduce semnificativ eterna problemă a parolelor furate sau „găsite" de cine nu trebuie.

3. Se mai fac, ocazional, ore de „educație digitală" în instituții, dar în mare parte, atunci când s-a întâmplat ceva, fie o breșă serioasă, fie ceva infim. Consider că e nevoie de mult mai mult de atât pentru a pregăti funcționarul public în privința atacurilor de tip inginerie socială.

4. Ar fi ideal să avem o astfel de programă școlară ce ar include cel puțin o oră de securitate digitală în școli. Dacă începem de la copii, atunci vom ajunge departe în utilizarea corectă a calculatoarelor și a telefoanelor și navigarea sigură pe Internet.

C3. Infrastructura Digitală

1. De obicei, se fac scanări și audituri de securitate cibernetică, însă este dificil pentru un număr limitat de oameni să fie la curent cu noile vulnerabilități găsite de hackeri în fiecare zi.

2. În cazul ransomware, copiile de rezervă sunt cele mai bune deoarece ele permit restaurarea imediată a bazelor de date afectate.

3. Aceste dispozitive reprezintă un mare risc pentru infrastructura IT a orașului. Ele sunt izolate în rețea și utilizează parole foarte greu de descifrat și schimbate periodic.

4. Două dintre cele mai mari provocări în ceea ce privește stocarea datelor pe Cloud sunt: controlul accesului și autonomia datelor. Conform legislației reieșite din GDPR, datele cetățenilor trebuie să fie stocate pe servere din Uniunea Europeană.

C4. Implementarea legislației

1. Administrația publică locală, cel puțin în București, încă mai învață despre responsabilitatea lor legală față de cetățeni în domeniul digital. Mulți ori se tem de potențiale consecințe, ori nu-i interesează aproape deloc până se întâmplă ceva.

2. Legal, primăriile de sector au implementat regulamentul GDPR în întregime. Pe partea tehnică, mereu vor exista mici piedici, mai ales atunci când vine vorba despre mutarea datelor dintr-o parte în alta.

3. Consider necesar un set de reguli bine definite, care să nu permită apariția „zonelor gri” din punct de vedere legislativ. Avem nevoie, în același timp, de niște consecințe clare în cazul nerespectării normelor de securitate cibernetică, nu doar de recomandări.

4. Da. Atacurile cibernetice, în prezent, nu se mai rezumă doar la farse, ci la blocarea sistemului sănătății sau celui administrativ. Pedepsele ar trebui să fie direct proporționale cu fapta săvârșită.

C5. Propuneri de soluții pentru viitor

1. O soluție pe care aș implementa-o ar fi crearea unei echipe de elită care să acționeze ca un „Dispecerat” al securității cibernetice, ce ar avea ca rol monitorizarea permanentă a tuturor instituțiilor din București. Consider asta mult mai eficientă decât mai multe echipe răsfirate și slab pregătite în fiecare instituție.

2. Ne aflăm la un început de drum în ceea ce privește implementarea inteligenței artificiale cu scopul de a monitoriza traficul de date suspect. Acesta a fost implementat în foarte puține locuri, însă drumul pare a fi promițător.

3. Nu ar trebui ca serviciile de informații să primească acces liber la dispozitivele cetățenilor, însă, acestea ar trebui să aibă capacități de monitorizare puțin mai lărgite în ceea ce privește infrastructura critică, precum rețelele din administrație.

4. Consider că DNSC-ul ar trebui să beneficieze de o extindere a jurisdicției sale, acesta ar trebui să nu fie doar un organ legislativ ce emite doar recomandări, ci ar trebui să acționeze direct pe teren în cazul unei breșe de securitate cibernetică.

A.2. Interviu 2

C1. Contextul actual și Amenințările cibernetice

1. Da, clar. De ceva vreme nu ne mai confruntăm doar cu grupuri organizate, ci cu actori statali. Adică grupuri sponsorizate de anumite state, precum China sau Rusia, de care autoritățile lor se dezic, dar defapt sunt „recrutate” de către acestea.

2. Cele mai des întâlnite sunt cele de tip ransomware, urmate de DDoS, Malware (cel mai des info-stealer, cum ar fi keylogger) și atacuri ce se folosesc de tehnici de inginerie socială.

3. Da, atacurile de acest fel pun din ce în ce mai multă presiune politică, făcând parte din războiul hibrid purtat de Rusia. S-a observat acest lucru din ce în ce mai mult odată cu începerea războiului din Ucraina din anul 2022.

4. Da, este și normal ca orașul capitală să fie vizat de mai multe atacuri decât orice alt oraș strict din cauza faptului că „centrul” administrației publice se află în București. Statistic, avem în jur de zece mii de atacuri pe zi doar în instituțiile ce țin de capitală.

C2. Educația Digitală, Factorul Uman

1. Mereu va rămâne factorul uman cea mai mare vulnerabilitate în ceea ce privește securitatea cibernetică. Indiferent de măsurile luate de tehnicieni, un om care nu știe ce face va apăsa click pe un site dubios sau un link de descărcare ce conține fișiere infectate și se va dărâma tot ce a putut face specialistul din instituție.

2. MFA este una din cele mai bune soluții ce poate fi implementată în momentul actual la nivelul administrației, așa s-ar reduce din riscul breșelor de securitate fără să apară

complicații pentru funcționari. Cea mai sigură modalitate de autentificare, din experiență, ar fi cea biometrică, mai specific cea cu recunoaștere de cornee. Cele prin recunoaștere facială și vocală sunt deja redundante având în vedere evoluția DeepFake-urilor, iar legându-ne de recunoașterea amprentelor, și aceasta poate fi păcălită dacă răufăcătorul este suficient de determinat în ceea ce face.

3. Nu se prea fac programe de instruire digitală în instituțiile în care am lucrat sau cu care am colaborat, însă am mai auzit de la foști colegi că s-ar face prezentări odată la ceva timp în care se prezintă riscurile apărute din cauza celor neexperimentați, acum contează și cât de atenți sunt oamenii respectivi.

4. Da, clar ar trebui introdusă această ora de educație în securitate cibernetică, însă nu doar una. Din perspectiva mea, cu cât mai mult cu cât mai bine. Aș spune minim două ore pe săptămână.

C3. Infrastructura Digitală

1. Da, se realizează audituri de securitate, însă în opinia mea acestea ar trebui să fie mult mai riguroase și făcute mai des decât se fac deja. În viitorul apropiat și în contextul în care se află lumea, cred că se va ajunge ca frecvența necesară realizării acestor audituri să fie zilnic. Momentan nici odată pe săptămână ca fiind suficient pentru astfel de acțiuni.

2. La nivel uman, educația digitală primează. La nivel tehnic, software-ul de anti-malware este foarte bun, software-ul de tip firewall la fel, însă cel mai important este crearea și testarea de backup-uri la zi. Nu se poate face un backup fără să fie testat. O altă soluție ar fi crearea de planuri de acțiune, ce constau în cine ce, când și unde face.

3. Din păcate, de obicei nu prea sunt, în cazul nostru la noi nu prea se agită populația. Soluțiile sunt implementate pe zone, acestea fiind schimbarea de parole în mod regulat, actualizarea soft-ului de operare, se criptează comunicațiile și se separă rețelele pe care sunt conectate dispozitivele. Sunt soluții bune, dar trebuie a fi implementate peste tot, nu doar acolo unde sunt oamenii mai interesați și informați la zi. Există și o directivă europeană numită CRA, Cyber Resilience Act, ce se referă la securitatea dispozitivelor ce prezintă caracteristici digitale. Nu știu dacă este obligatorie acum, dar în cazul în care nu este, consider că ar trebui cât de curând să devină obligatorie implementarea acesteia.

4. Provocările pentru date în sine ar fi accesul neautorizat și respectiv data breaches, pierderile de date reieșite din fie o pană de curent fie din bombardamente mai nou, cum a fost bombardat cloud-ul Amazon-ului de către Iran și nici acum nu au reușit să se pună pe picioare, datele în sine se pot corupe în timpul transferului. Pe acel Cloud este mai multă populație, trebuie ca datele să fie compartimentate cum trebuie, însă tu fiind client nu ai control asupra cine poate vedea mai exact ce e stocat pe acele servere. Mai ajungem și la dilema „unde se află x?” în sensul de unde mai exact se află baza de date. Mai trebuie luat în calcul și faptul că nu știm mai exact pe unde merg acele date în timpul transferului.

C4. Implementarea legislației

1. Este un subiect complicat, însă pot da un răspuns pe moment. Instituțiile cum ar fi primăriile de sector nu sunt pregătite momentan pentru a răspunde legal în fața cetățenilor în cazul unei breșe de acest fel. Avem totuși DNSC-ul care răspunde către ENISA, însă există și dilema implementării directivei NIS2 de fiecare stat. Avem un framework de bază care este adaptat la fiecare dintre statele membre, modurile de implementare diferă de la stat la stat și se produc anumite piedici în timp.

2. În principiu, măsuri sunt luate în conformitate cu regulamentul GDPR, dar nu în totalitate sau mai degrabă spus nu la viteza necesară. E bine că nu se poate spune că nu se face nimic, dar nu se fac nici prea multe. Aș spune un „so-so”.

3. Absolut. Este clar nevoie de o legislație care nu permite apariția zonelor gri în domeniu.

4. Cu siguranță. Majoritatea facerilor de rău se produc digital în zilele noastre, iar de multe ori au tendința ca din digital să sară în lumea fizică. E totuși o linie foarte fină între fascism digital și securitate reală, aceasta trebuind luată în vedere.

C5. Propuneri de soluții pentru viitor

1. Aș spune în primul rând despre implementarea Multi-Factor Authentication. Dacă ar fi să mai pot implementa și alte soluții, ar fi introducerea de echipe specializate pentru monitorizarea traficului de date general și pentru a acționa împotriva atacatorilor și introducerea de planuri de acțiune pentru toți oamenii ce lucrează în administrație cu tot cu simulări ale scenariilor.

2. Momentan, din ce știu, se discută despre introducerea inteligenței artificiale pentru monitorizarea traficului de date, însă din ce știm și eu și alți colegi, doar se discută.

3. Da, doar dacă serviciile respective sunt controlate cum trebuie de către societatea civilă. Daca nu, atunci consider că nu, deoarece nu trebuie lăsați de capul lor. E o dilemă veche, „Cine îl păzește pe paznic?”.

4. Nu aș spune că are nevoie de o extindere a competențelor sale, însă mai degrabă de o sporire a capacității lor. DNSC-ul, momentan, prezintă un mare deficit de forță de muncă. Pe partea de apărare cibernetică aș accepta totuși să primească mai multă putere, partea ofensivă fiind oricum ale altor instituții.

A.3. Interviu 3

C1. Contextul actual și Amenințările cibernetice

1. Da, diferența se observă foarte ușor, deoarece înainte de anul 2020, majoritatea breșelor de securitate erau făcute de amatori ce găseau o serie de linii de cod pe internet, le rulau și vedeau ce iese. Acum, în schimb, în acest deceniu, vorbim despre operațiuni avansate ale unor actori statali, grupuri sponsorizate de anumite state cum ar fi Killnet, o grupare pro-rusă ce în anii 2022 și 2023 au atacat site-uri ale guvernului nostru cu scopul de a trimite mesaje de natură politică.

2. Din ce se observă statistic vorbind, ne confruntăm din ce în ce mai mult cu ransomware, DDoS și phishing. Mai putem vorbi și despre malware deoarece anumite instituții încă nu și-au actualizat sistemele cu anii.

3. DDoS a devenit fix instrumentul numărul 1 al hacktiviștilor și al grupurilor sponsorizate de state pentru a pune presiune politică pe administrația Bucureștiului, acest lucru este clar. Se observă cel mai ușor în exemplul pe care l-am mai dat, și anume grupul pro-rus Killnet și atacurile lor.

4. Da, este logic. Până la urmă cele mai importante instituții se află în capitala majoritatea statelor din lume, nu în toate ce-i drept. România se află în acea majoritate, totuși.

C2. Educația Digitală, Factorul Uman

1. Într-adevăr, factorul uman este și va rămâne pe veci cea mai mare vulnerabilitate a oricărui sistem, indiferent de natura lui, digital sau nu. În cazul nostru, administrația publică locală din București se confruntă cu breșe apărute aproape exclusiv în urma unei greșeli ale utilizatorului dispozitivului.

2. Multi-Factor Authentication chiar ajută și este cel mai simplu pas pe care îl poate face absolut oricine, nu doar instituțiile statului. Desigur, nu este perfect pentru că există și noi metode precum „MFA Fatigue", un utilizator fiind supraîncărcat cu notificări în cazul SMS-urilor sau e-mail-urilor și acesta eventual poate să le aprobe din diverse motive. Aici recomand utilizarea aplicațiilor făcute pentru autentificarea în mai mulți pași.

3. Nu avem un set de instrucțiuni standard, nu avem nici cine știe ce programe de instruire pentru funcționarii publici în fiecare primărie, de exemplu. Alte state au nu doar cursuri special gândite pentru a-i învăța pe cei ce fac parte din personalul administrativ să se apere de phishing și alte feluri de atacuri cibernetice, ci au, periodic, simulări de atacuri de tip inginerie socială, iar cei ce pică aceste teste intră într-un program și mai riguros de educare în acest sens.

4. Cel mai cert lucru atunci când vine vorba de măsuri ce trebuie adoptate. Educația de la cel mai mic la cel mai mare este cea mai bună apărare pe termen lung. Sigur, oricât de educat este un om tot poate face greșeli, dar s-ar reduce semnificativ breșele de securitate.

C3. Infrastructura Digitală

1. Se fac, în mod teoretic. Acum, nu zic că defapt nu se fac și e totul lăsat în aer, mă refer la faptul că acestea nu sunt realizate la fel de conform cu legislația reieșită din NIS2. Și oricum, chiar dacă aceste audituri ar fi perfecte, vulnerabilitățile zero-day rămân problematice. De ce? Acest lucru reiese fix din definiția acestui concept, sunt lacune necunoscute apărute încă din prima zi a apariției soft-ului sau hardware-ului.

2. Backup-ul este cea mai bună soluție pentru ransomware în cazul în care acesta se infiltrează într-o rețea, însă nu orice backup, ci cel stocat pe o bază de date complet deconectată de la orice rețea. S-a observat, în urma incidentulelor recente cu Lockbit, că ransomware-ul actual caută să cripteze backup-uri de pe dispozitive conectate la rețea, fie cea internă a unei instituții sau direct la internet. A da, și să nu uităm testarea acestor copii înainte de a le lăsa stocate. Nu se știe niciodată când dă greși chiar sistemul de operare, se întâmplă.

3. Din păcate și din fericire, dispozitivele Internet-of-Things sau IoT sunt cam cele mai ignorate „portițe". Zic asta deoarece doar atacatorii serioși, pregătiți și care chiar doresc să ajungă la datele stocate pe rețelele administrației ajung să se folosească de senzori trafic de exemplu. Însă nu ne putem baza pe ignoranța atacatorului, nu? Pe unde am mai lucrat eu, se făceau actualizările de rutină a firmware-ului și se schimbau parolele odată la două saptămâni-o lună a camerelor de luat vederi. Eu sugerez și izolarea în rețele mai mici a acestor dispozitive pentru a asigura cât mai multă securitate posibilă.

4. Aici este o problemă mai complexă. Cloud-ul, la nivel tehnic, defapt este o fermă de servere conectate la Internet ce pot fi accesate de către utilizator doar prin intermediul calculatorului, nu fizic, deoarece acestea sunt, bineînțeles, păzite și de obicei în locații grele de accesat în general. Există și fortărețe pentru asta în munți, dar acolo vorbim deja de companii private de top. În cazul nostru, cele mai mari provocări ar fi integritatea datelor în timpul și în urma transferului datelor pe sau de pe acest cloud. Mai există și dilema apărută din GDPR care ne spune că dacă vrem să apelăm la o astfel de modalitate

de stocare a datelor din instituții, trebuie neapărat să utilizăm infrastructura Uniunii Europene. Oricum, nici această soluție nu e cea mai sigură, dar, depinzând de instituție, poate fi mai sigură decât să le păstreze pe propriile servere.

C4. Implementarea legislației

1. În România, nu doar în București, în cazul unei breșe de securitate ce vizează datele cu caracter personal, instituția compromisă trebuie să notifice ANSPDCP în maxim trei zile de la descoperirea breșei, însă în practică, la noi se cam amână, nu se descoperă breșa sau doar nu face nimeni notificarea cu speranța că nu e nimic sau se rezolvă de la sine. Nu avem nici foarte mulți oameni care să monitorizeze Dark Web-ul pentru a vedea dacă apar date ale cetățenilor acolo din partea sistemului public. Când a fost compromisă Primăria Sectorului 5 relativ recent, breșa a fost descoperită de către un om ce lucrează în sistemul privat. Pe scurt, nu consider că instituțiile din administrația publică locală sunt pregătite de a-și asuma responsabilitatea legală în cazul unui leak al datelor cetățenilor pe Dark Web.

2. Cred că voi oferi un răspuns similar cu cel de la întrebarea anterioară, însă în teorie primăriile acționează conform GDPR. În practică, în spate, multe baze de date nu sunt nici măcar criptate cu un algoritm de bază, sunt efectiv lăsate așa, în forma lor de bază. Nu mai zic de cum acționează unii în cazul unei breșe.

3. Eu zic că ce ne-a oferit Uniunea Europeană este suficient de rigid, aici mă refer la regulamentul GDPR, la directiva NIS2 și la CRA. Problema pe care o văd eu, personal, nu este implementarea legilor, ci modul în care este aplicată. Avem o nevoie clară de resurse suplimentare în domeniul securității cibernetice pentru a reuși să acționăm conform acestor legi.

4. Aici voi răspunde cu un da absolut, pedepsele pentru atacurile cibernetice trebuiesc să fie mai mari. Trăim în era în care dorim să digitalizăm tot, problema este că făcând asta, stocăm date extraordinar de sensibile, așa că potențialele pedepse pentru compromiterea intimității unui individ trebuie să fie pe măsură.

C5. Propuneri de soluții pentru viitor

1. Sincer, am două soluții, nu prea pot alege doar una. Cea mai simplă este implementarea MFA, iar cea mai complicată este crearea unui SOC al Bucureștiului. SOC se referă la „Security Operations Center”, sau centru de operațiuni de securitate, care să fie cel ce veghează în timp real toate instituțiile din capitală și traficul lor de date. Dacă nu am fi presați de faptul că durează mult crearea unui astfel de centru, totuși, aș alege centrul. Dar la cum arată lucrurile, mai bine mergem pe calea simplă și alegem MFA.

2. Suntem la început, încă se mai discută. Da, sunt anumite sisteme în curs de implementare pe care nu le pot încă specifica. În alte țări deja s-au intergrat complet agenți AI specializați în monitorizarea traficului de date și raportarea anomaliilor într-un timp pe care un om pur și simplu nu poate să îl atingă.

3. Nu aș răspunde neapărat cu un „nu” categoric, se poate face acest lucru, dar trebuie făcut cum trebuie. Adică reglementat corespunzător, altfel riscăm să ajungem într-o situație povestită într-o celebră carte ce este văzută ca fiind controversată în anumite părți ale lumii, publicată în anul 1949. Am drept exemplu „PRISM” al SUA.

4. Eu cred că da, dar are nevoie și de mai mulți oameni. Ni s-a demonstrat că personalul DNSC este suficient de competent când vine vorba de acțiune în urma unei breșe. Au reușit să dea de cap problemelor cu sistemul Hipocrate utilizate de spitale, au reușit să

restaureze bazele de date din acele instituții. Emit recomandări chiar bune din punct de vedere al securității cibernetice și mai și anunță vulnerabilități grave în cazul în care apar. Cum aș extinde această jurisdicție? Păi, le-aș dărui competența de audit obligatoriu, iar în cazul în care instituția audiată nu este conformă, dreptul de a îi sancționa pe cei care se ocupă de baza de date respectivă.

References

[1] Microsoft, „Ce este un atac cibernetic?," Microsoft, [Interactiv]. Available: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack. [Accesat 18 02 2026].

[2] C. Vrabie, Elemente de E-Guvernare, Editura Pro Universitaria, 2024.

[3] The European Union, „GDPR.eu," The European Union, [Interactiv]. Available: https://gdpr.eu/what-is-gdpr/. [Accesat 19 02 2026].

[4] Microsoft, „Ce este un firewall?," Microsoft, [Interactiv]. Available: https://support.microsoft.com/ro-ro/office/ce-este-un-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603. [Accesat 20 02 2026].

[5] R. Koch, „Hidden in the Shadow: The Dark Web," în *11th International Conference on Cyber Conflict: Silent Battle*, NATO Cooperative Cyber Defence Centre of Excellence, 2019, pp. 267-268.

[6] Bitdefender, „Ce este Malware-ul?," Bitdefender, [Interactiv]. Available: https://www.bitdefender.com/ro-ro/business/infozone/what-is-malware. [Accesat 20 02 2026].

[7] Microsoft, „Ce este un centru de operațiuni de securitate (SOC)?," Microsoft, [Interactiv]. Available: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-security-operations-center-soc. [Accesat 18 02 2026].

[8] A. C. Turmac, „DIGITALIZAREA ADMINISTRATIEI LOCALE DIN ROMANIA - Instrumentarul tehnic pentru digitalizarea serviciilor sociale,"," *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV),* vol. 1, nr. 1, 2023.

[9] A. Hasan, „Understanding Distributed Denial of Service (DDoS) Attacks and its analysis," ResearchGate, 2023.

[10] T. M. Ciucă, „Securitatea cibernetică în administrația publică din România: Provocări și măsuri de protecție în contextul digitalizări," *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV),* vol. 3, nr. 2, 2025.

[11] A. Nedelcu și A. Nimu, „Emerging trends: how is the Internet of Things (IoT) transforming our homes," *Emerging trends: how is the Internet of Things (IoT) transforming our homes,* vol. 5, pp. 78-89, 2017.

[12] U. Europeană, „EUR-Lex, Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului," 2022. [Interactiv]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=ro. [Accesat 5 Ianuarie 2026].

[13] Ministerul Justiției, „legislație.just.ro,” 9 Ianuarie 2019. [Interactiv]. Available: https://legislatie.just.ro/public/detaliidocument/209670. [Accesat 5 Ianuarie 2026].

[14] S. Chelcea, *Tehnici de cercetare sociologică - interviul,* Suport de curs, 2001.

[15] Guvernul României, „Ghiseul.ro - Legislatie,” 6 12 2010. [Interactiv]. Available: https://www.ghiseul.ro/ghiseul/docs/HG%201235%20SNEP.doc. [Accesat 27 02 2026].

[16] Comisia Europeană, „Sph3ra,” 2021. [Interactiv]. Available: https://sph3ra.ro/wp-content/uploads/2021/07/DESI-2020-Country-Analysis-Romania.pdf. [Accesat 27 02 2026].

[17] C. Antonovici, *Suport de curs - Management Public.*

[18] M. Cărăușan, *Suport de curs - Drept Administrativ.*

[19] C. Rădulescu, *Suport de Curs - Bazele Constituționale ale Administrației Publice.*

[20] C. C. Manda, *Digitalizarea administrației publice din România –între nevoile și aspirațiile unei societăți moderne a secolului XXI,* 2023.

[21] Ministerul Cercetării, Inovării și Digitalizării (MCID), „Ghidul Digitalizării,” MCID, 07 2024. [Interactiv]. Available: https://www.mcid.gov.ro/wp-content/uploads/2024/07/20240702_Ghidul_Digitalizarii.pdf. [Accesat 18 02 2026].

[22] L.-S. BEH, M. J. LEE, N. H. A. RAHMAN și S.-L. LAI, „Smart Cities and Digitalisation: A Research Agenda of Public Administration,” [Interactiv]. Available: https://www.scrd.eu/index.php/scrd/article/view/135/108. [Accesat 19 02 2026].

[23] Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), „Strategia națională privind Agenda Digitală pentru România 2020,” [Interactiv]. Available: https://www.ancom.ro/uploads/links_files/Strategia_nationala_privind_Agenda_Digitala_pentru_Romania_2020.pdf. [Accesat 18 02 2026].

[24] Ministerul Cercetării, Inovării și Digitalizării (MCID), „PLANUL NAȚIONAL DE ACȚIUNE PRIVIND DECENIUL DIGITAL PENTRU ROMÂNIA,” [Interactiv]. Available: https://www.mcid.gov.ro/wp-content/uploads/2024/04/Plan-national-de-actiune-roadmap-pentru-publicare.pdf. [Accesat 19 02 2026].

[25] Guvernul României, „HOTĂRÂRE nr. 494 din 11 mai 2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO,” 11 05 2011. [Interactiv]. Available: https://legislatie.just.ro/Public/DetaliiDocument/129052. [Accesat 19 02 2026].

[26] Guvernul României, „ORDONANȚĂ DE URGENȚĂ nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică,” 22 09 2021. [Interactiv]. Available: https://legislatie.just.ro/Public/DetaliiDocument/246652. [Accesat 19 02 2026].

[27] Directoratul Național de Securitate Cibernetică, „DNSC - Legislație - Directiva NIS 2,” [Interactiv]. Available: https://www.dnsc.ro/pagini/legislatie-nis2. [Accesat 19 02 2026].

[28] Directoratul Național de Securitate Cibernetică (DNSC), „Ghid Referitor la rolul structurilor de tip CERT şi utilitatea CERT-urilor private,” [Interactiv]. Available:

https://www.dnsc.ro/vezi/document/rolul-certurilor-si-utilitatea-celor-private#:~:text=Acestea%20sunt%20formate%20din%20specialişti%20în%20securitate,cât%20şi%20rol%20de%20prevenire%20a%20apariţiei. [Accesat 19 02 2026].

[29] Parlamentul European, Consiliul Uniunii Europene, „DIRECTIVA (UE) 2016/1148 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI,” 19 07 2016. [Interactiv]. Available: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148. [Accesat 21 02 2026].

[30] Parlamentul European, Consiliul Uniunii Europene, „DIRECTIVA (UE) 2022/2555 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 14 decembrie 2022,” 27 12 2022. [Interactiv]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=ro. [Accesat 21 02 2026].

[31] Parlamentul European, Consiliul Uniunii Europene, „Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date,” 05 04 2016. [Interactiv]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accesat 21 02 2026].

[32] Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), „Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal,” 2016. [Interactiv]. Available: https://www.dataprotection.ro. [Accesat 21 02 2026].

[33] National Cyber Security Centre (NCSC), „Understanding vulnerabilities,” [Interactiv]. Available: https://www.ncsc.gov.uk/collection/vulnerability-management/understanding-vulnerabilities. [Accesat 19 02 2026].

[34] M. Alsharif, S. Mishra și M. Alshehri, „Impact of Human Vulnerabilities on Cybersecurity,” 09 2021. [Interactiv]. Available: https://www.researchgate.net/publication/354879445_Impact_of_Human_Vulnerabilities_on_Cybersecurity. [Accesat 19 02 2026].

[35] National Cyber Security Centre (NCSC), „Common cyber attacks: reducing the impact,” 01 2016. [Interactiv]. Available: https://www.ncsc.gov.uk/files/common_cyber_attacks_ncsc.pdf. [Accesat 19 02 2026].

[36] Directoratul Național de Securitate Cibernetică (DNSC), „ALERTĂ: Atacuri de tip spoofing/phishing/vishing asupra utilizatorilor din România,” Guvernul României, 06 09 2024. [Interactiv]. Available: https://www.dnsc.ro/citeste/alerta-atacuri-de-tip-spoofing-phishing-vishing-asupra-utilizatorilor-din-romania. [Accesat 19 02 2026].

[37] Directoratul General de Securitate Cibernetică (DNSC), „Scam Phishing, Vishing,” 2024. [Interactiv]. Available: https://www.dnsc.ro/citeste/alerta-atacuri-de-tip-spoofing-phishing-vishing-asupra-utilizatorilor-din-romania. [Accesat 20 02 2026].

[38] Bitdefender, „Ce este o vulnerabilitate de tip Zero-Day?,” Bitdefender, [Interactiv]. Available: https://www.bitdefender.com/ro-ro/business/infozone/what-is-zero-day-vulnerability. [Accesat 20 02 2026].

[39] Crowdstrike, „Advanced Persistent Threats (APT) Explained,” Crowdstrike, 04 03 2025. [Interactiv]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/. [Accesat 21 02 2026].

[40] A.-E. BRĂILESCU, „Impactul atacurilor cibernetice asupra administrației publice,” *Student Papers on Smart Cities and E-Governance (SPoSC&EGOV) Repository,* vol. 3, nr. 2, 2025.

[41] Consiliul Uniunii Europene, „Care sunt principalele amenințări cibernetice în UE?,” Consiliul Uniunii Europene, 30 06 2025. [Interactiv]. Available: https://www.consilium.europa.eu/ro/policies/top-cyber-threats/. [Accesat 15 03 2026].

[42] Consiliul Uniunii Europene, „Securitatea cibernetică: ingineria socială,” Consiliul Uniunii Europene, 05 02 2025. [Interactiv]. Available: https://www.consilium.europa.eu/ro/policies/cybersecurity-social-engineering/. [Accesat 15 03 2026].

[43] International Business Machines Corporation (IBM), „What is social engineering?,” International Business Machines Corporation (IBM), [Interactiv]. Available: https://www.ibm.com/think/topics/social-engineering. [Accesat 17 03 2026].

[44] Bitlyft, „What is Social Engineering? Tips for Preventing Manipulative Tactics,” Bitlyft, 12 05 2023. [Interactiv]. Available: https://www.bitlyft.com/resources/what-is-social-engineering-avoiding-manipulative-tactics. [Accesat 17 03 2026].

[45] Fortinet, „What is Scareware?,” Fortinet, [Interactiv]. Available: https://www.fortinet.com/resources/cyberglossary/scareware. [Accesat 17 03 2026].

[46] Bitdefender, „Ce este ransomware?,” Bitdefender, [Interactiv]. Available: https://www.bitdefender.com/ro-ro/business/infozone/what-is-ransomware. [Accesat 17 03 2026].

[47] International Business Machines Corporation (IBM), „What is ransomware as a service (RaaS)?,” International Business Machines Corporation (IBM), 2025. [Interactiv]. Available: https://www.ibm.com/think/topics/ransomware-as-a-service. [Accesat 17 03 2026].

[48] Directoratul Național de Securitate Cibernetică (DNSC), „ALERTĂ: Backmydata Ransomware,” Directoratul Național de Securitate Cibernetică (DNSC), 15 02 2024. [Interactiv]. Available: https://www.dnsc.ro/citeste/alert-backmydata-ransomware-spitale-romania. [Accesat 17 03 2026].

[49] International Business Machines Corporation, „The history of malware,” International Business Machines Corporation, 2022. [Interactiv]. Available: https://www.ibm.com/think/topics/malware-history. [Accesat 18 03 2026].

[50] Microsoft, „What is malware?,” Microsoft, [Interactiv]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-malware. [Accesat 18 03 2026].

[51] Crowdstrike, „The 12 Most Common Types of Malware,” Crowdstrike, 27 02 2023. [Interactiv]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/. [Accesat 18 03 2026].

[52] Academia Forțelor Aeriene "Henri Coandă" (AFAHC), „Case Study #5 - The Stuxnet Virus,” Academia Forțelor Aeriene "Henri Coandă" (AFAHC), [Interactiv]. Available:

https://www.afahc.ro/ro/erasmus/DDHE/Courses/Information%20Warfare/case_study_5__the_stuxnet_virus.html. [Accesat 18 03 2026].

[53] Proofpoint, „What Is a Trojan Horse?," Proofpoint, [Interactiv]. Available: https://www.proofpoint.com/us/threat-reference/trojan-horse. [Accesat 18 03 2026].

[54] International Business Machines Corporation, „What is malware?," International Business Machines Corporation, [Interactiv]. Available: https://www.ibm.com/think/topics/malware. [Accesat 19 03 2026].

[55] NHS Digital, „Zacinlo Rootkit Adware," NHS Digital, 20 06 2018. [Interactiv]. Available: https://digital.nhs.uk/cyber-alerts/2018/cc-2497. [Accesat 19 03 2026].

[56] British Broadcasting Corporation, „Anti-piracy CD problems vex Sony," British Broadcasting Corporation, 08 12 2005. [Interactiv]. Available: http://news.bbc.co.uk/2/hi/technology/4511042.stm. [Accesat 19 03 2026].

[57] D. K. Mulligan și A. K. Perzanowski, „THE MAGNIFICENCE OF THE DISASTER: Reconstructing the Sony BMG Rootkit Incident," 2010. [Interactiv]. Available: https://download.ssrn.com/07/12/14/ssrn_id1072229_code698753.pdf?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEOf%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEaCXVzLWVhc3QtMSJHMEUCIQDRTLwPkTVKCgCEK0QWVQ2F6Js7MgjZCaamAQyAsJtEzAIgMIE2ZY4HiM1ca. [Accesat 19 03 2026].

[58] Cofense, „What is Agent Tesla?," Cofense, 21 02 2023. [Interactiv]. Available: https://cofense.com/blog/the-rise-of-agent-tesla-understanding-the-notorious-keylogger/. [Accesat 19 03 2026].

[59] Microsoft, „Ce este un atac DDoS?," Microsoft, [Interactiv]. Available: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-ddos-attack. [Accesat 19 03 2026].

[60] Fortinet, „What Is DDOS Attack?," Fortinet, [Interactiv]. Available: https://www.fortinet.com/resources/cyberglossary/ddos-attack. [Accesat 19 03 2026].

[61] GeeksforGeeks.org, „Cyber Criminals and their types," GeeksforGeeks, 23 03 2026. [Interactiv]. Available: https://www.geeksforgeeks.org/ethical-hacking/cyber-criminals-and-its-types/. [Accesat 24 03 2026].

[62] Kaspersky, „What is a Black-Hat hacker?," Kaspersky, [Interactiv]. Available: https://www.kaspersky.com/resource-center/threats/black-hat-hacker. [Accesat 24 03 2026].

[63] Wigan Council, „Cyber terrorism," Wigan Council, [Interactiv]. Available: https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx. [Accesat 24 03 2026].

[64] Cloudflare, „What was the WannaCry ransomware attack?," Cloudflare, [Interactiv]. Available: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. [Accesat 24 03 2026].

[65] British Broadcasting Corporation, „Wikileaks: Document dumps that shook the world,” British Broadcasting Corporation, [Interactiv]. Available: https://www.bbc.com/news/technology-47907890. [Accesat 24 03 2026].

[66] Cybersecurity & Infrastructure Security Agency (CISA), „Defining Insider Threats,” Cybersecurity & Infrastructure Security Agency (CISA), [Interactiv]. Available: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats. [Accesat 24 03 2026].

[67] United Nations office on Drugs and Crime, „Organized Crime,” United Nations office on Drugs and Crime, [Interactiv]. Available: https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html. [Accesat 25 03 2026].

[68] MITRE Corporation, „LAPSUS$, DEV-0537, Strawberry Tempest, Group G1004,” MITRE Corporation, 09 06 2022. [Interactiv]. Available: https://attack.mitre.org/groups/G1004/. [Accesat 25 03 2026].

[69] NATO Cooperative Cyber Defence Centre of Excellence, „National Cybersecurity Organisation: Romania,” 2020. [Interactiv]. Available: https://ccdcoe.org/uploads/2020/11/NCS_organisation_ROM-2020_FINAL.pdf. [Accesat 25 03 2026].

[70] Comandamentul Apărării Cibernetice, „Organizare,” Comandamentul Apărării Cibernetice, 2018. [Interactiv]. Available: https://cybercommand.ro/pages/organizare. [Accesat 25 03 2026].

[71] Ministerul Afacerilor Externe, „Strategia de securitate cibernetică a României 2022-2027,” Ministerul Afacerilor Externe, 02 2022. [Interactiv]. Available: https://www.mae.ro/node/28367. [Accesat 26 03 2026].

[72] C. VRABIE, „Convergenta securitatii digitale,” 11 03 2023. [Interactiv]. Available: https://scrd.eu/index.php/scic/article/view/225/188. [Accesat 16 05 2026].

[73] C. VRABIE, „O operatiune cu stil - The Flame,” 12 03 2023. [Interactiv]. Available: https://scrd.eu/index.php/scic/article/view/267/231. [Accesat 16 05 2026].

[74] Primăria Sectorului 5 București, „ATAC CIBERNETIC ASUPRA SERVICIILOR PRIMĂRIEI SECTORULUI 5 - HACKERII CER RĂSCUMPĂRARE 5 MILIOANE DE DOLARI,” Primăria Sectorului 5, 26 10 2024. [Interactiv]. Available: https://sector5.ro/atac-cibernetic-asupra-serverelor-primariei-sectorului-5-hackerii-cer-rascumparare-5-milioane-de-dolari/. [Accesat 3 05 2026].

[75] snoop.ro, „Piedone a angajat o firmă fantomă, care vindea freze de strung, pentru securitatea IT a Primăriei Sector 5. Apoi hackerii au furat datele a 200.000 de români,” snoop.ro, 11 02 2025. [Interactiv]. Available: https://snoop.ro/piedone-a-angajat-o-firma-fantoma-care-vindea-freze-de-strung-pentru-securitatea-it-a-primariei-sector-5-apoi-hackerii-au-furat-datele-a-200-000-de-romani/. [Accesat 3 05 2026].

[76] Directoratul Național pentru Securitate Cibernetică, „Raspunsul DNSC pentru Buletin de Bucuresti,” 8 11 2024. [Interactiv]. Available: https://buletin.de/bucuresti/wp-content/uploads/Raspunsul-DNSC-pentru-Buletin-de-Bucuresti.pdf. [Accesat 3 05 2026].

[77] Directoratul Național de Securitate Cibernetică, „Un atac cibernetic de tip ransomware a afectat spitale din România,” Directoratul Național de Securitate Cibernetică, 15 02 2024. [Interactiv]. Available: https://www.dnsc.ro/citeste/atac-cibernetic-ransomware-spitale-Romania. [Accesat 3 05 2026].

[78] Directoratul Național de Securitate Cibernetică, „Bune practici pentru elaborarea unei politici de prevenire și combatere a aplicațiilor software dăunătoare,” 01 2026. [Interactiv]. Available: https://www.dnsc.ro/vezi/document/dnsc-bune-practici-pentru-elaborarea-unei-politici-de-prevenire-si-combatere-a-aplicatiilor-software-daunatoare. [Accesat 04 05 2026].

[79] C. VRABIE, „Libertatea ta incepe unde se termina intimitatea mea,” 12 03 2023. [Interactiv]. Available: https://scrd.eu/index.php/scic/article/view/239/202. [Accesat 16 05 2026].

[80] The Guardian, „NSA Prism program taps in to user data of Apple, Google and others,” The Guardian, 2013.

[81] V. Baltac, „Smart cities—A view of societal aspects,” *Smart Cities,* vol. 2, nr. 4, 2019.