Factorul uman vs. securitatea cibernetică

Adrian Victor VEVERA, Alexandra Raluca ALBESCU
Institutul Naţional de Cercetare-Dezvoltare în Informatică – ICI Bucureşti
B-dul Mareșal Alexandru Averescu, Nr. 8-10, 011455, București, România
victor.vevera@ici.ro, raluca.albescu@ici.ro

Rezumat: Securitatea cibernetică a devenit o preocupare pentru toate organizațiile din lume, iar potențialele amenințări sunt tratate cu o seriozitate din ce în ce mai mare – fie că ne referim la recrutarea de personal specializat pentru a gestiona infrastructura IT, fie că ne referim la instruirea angajaților existenți cu privire la cele mai bune practici și politici de securitate cibernetică. Este foarte important să creștem numărul de experți în securitate pentru a depăși aceste preocupări și să le acordăm acestora o pregătire corespunzătoare în domeniul calității. O schimbare completă a focusului asupra securității cibernetice este alarmantă, deoarece nu doar confidențialitatea datelor sau neutralitatea rețelei necesită atenție. Una dintre soluții ar fi un pas suplimentar în securitatea cibernetică, prin educarea și formarea tuturor angajaților din companii, care poate avea o influență pozitivă asupra productivității globale a acestora, pe termen lung.

Cuvinte cheie: securitate cibernetică, educație, training, formare continuă.

Human resource vs. cyber security

Abstract: Cyber security has become a concern for all organizations in the world, and potential threats are treated with increasing seriousness - whether we are talking about recruiting specialized personnel to manage IT infrastructure, or about training the existing employees on best practices and cyber security policies. It is very important to increase the number of cyber security experts to overcome these concerns and to offer them appropriate training in the field of quality. A complete change of focus on cyber security is alarming, because it is not just the privacy rights of data or network neutrality that requires attention. One solution would be an additional step in cyber security by educating and training all employees in companies which could have a positive influence on their overall productivity, in the long run.

Keywords: cyber security, education, training, lifelong training.

1. Introducere

Internetul a devenit o parte integrantă a vieții noastre de zi cu zi. Ne permite să comunicăm, să socializăm și să facem afaceri în moduri noi și interesante. De asemenea, permite o mai mare libertate de exprimare, acționează ca un catalizator al inovării și este o piatră de temelie a vieții noastre sociale și economice.

Dezvoltarea IT și a telecomunicațiilor este un pas natural în progresul celei mai globalizate infrastructuri. Acest lucru implică multe oportunități și solicită o creștere a cercetării privind securitatea digitală, pentru a se asigura că spațiul cibernetic rămâne deschis, liber și sigur. Eforturile de a proteja securitatea cibernetică a societății trebuie să se desfășoare într-o manieră eficientă, pe termen lung și să servească interesele valorilor fundamentale ale societății - cum ar fi protecția vieții private.

Nevoia de personal calificat în domeniul securității cibernetice este foarte mare, lipsa de expertiză afectează atât sectorul privat, cât și sectorul public. Prin urmare, ar trebui să fie în interesul tuturor părților implicate să găsească soluții pe termen lung, pentru a satisface nevoile crescânde de forță de muncă calificată.

În ciuda progresului securității și a normelor organizatorice care au apărut în industrie, factorul uman este încă cel mai important pilon al securității cibernetice. În cele din urmă, toate tehnicile și măsurile de securitate organizatorice luate, trebuie acceptate și susținute de factorul uman, de aceea utilizatorul TIC trebuie să fie în centrul tuturor activităților.

În consecință, abordarea privind securitatea cibernetică trebuie să fie orientată spre om și bazată pe consolidarea culturii securității cibernetice. Această cultură va determina percepția, înțelegerea, atitudinea personală și cunoștințele necesare pentru acțiunea, conștientă, în privința securității.

2. Educația și formarea în domeniul securității cibernetice

O componentă semnificativă pentru creșterea cunoștințelor și sporirea capacității activităților de gestionare a incidentelor IT este educația și formarea. De aceea, acestea ar trebui să fie disponibile la toate nivelurile, începând cu învățământul primar (chiar dacă numai pentru a se atrage atenția asupra subiectului) până la învățământul terțiar.

Sectorul digital se mișcă extrem de rapid, la fel și lumea securității cibernetice, de aceea, este important să ne asigurăm că avem abilitățile necesare, nu doar pentru prezent ci și pentru viitor, iar acest lucru va necesita un parteneriat și o colaborare puternică cu mediul de afaceri și cu instituțiile de învățământ.

Problemele de securitate cibernetică reflectă, de multe ori, o lipsă a know-how-ului dezvoltatorilor implicați. TIC este un domeniu în care cunoștințele devin depășite foarte rapid, programele de formare și calificare, realizate în mod continuu, sunt o condiție primordială pentru menținerea angajaților TIC și pentru productivitatea acestora.

În această epocă digitală aproape tot ceea ce fac oamenii la locul de muncă îi conectează la internet și, prin urmare, îi face vulnerabili la atacurile cibernetice. Un aspect al politicii de securitate cibernetică, pe care companiile de multe ori îl neglijează, este educația și acest lucru reprezintă un defect critic deoarece, în condițiile în care membrii unei echipe nu înțeleg cum funcționează securitatea cibernetică, vor crea, neintenționat, vulnerabilități în sistem.

O echipă bine educată este una dintre cele mai puternice active de securitate pe care le poate avea o companie. În comunicarea beneficiilor unei politici puternice de securitate cibernetică trebuie să susținem și educația în domeniul securității. O companie se poate echipa cu o suită de instrumente de securitate excelente, dar nu va fi pe deplin eficientă dacă membrii echipei nu își înțeleg responsabilitatea, ca indivizi, pentru a sprijini cultura de securitate a companiei.

Angajații se află în centrul fiecărei afaceri și pot reprezenta cel mai mare avantaj al companiei sau cea mai mare amenințare a acesteia atunci când vine vorba de securizarea datelor și a informațiilor sensibile.

Lipsa educației și a conștientizării angajaților, în materie de securitate cibernetică, împreună cu erorile umane sau comportamentul neatent au fost cauza multor încălcări majore ale securității cibernetice. Angajații sunt cei care, în necunoștință de cauză, pot ajuta hackerii oferindu-le parole, pierzând informații sau dispozitive de back-up, eliberând din greșeală informații sensibile sau intrând în capcanele de phishing.

O abordare proactivă și continuă de a educa întreaga forță de muncă cu privire la amenințările securității cibernetice și contramăsurile care pot fi luate, pot transforma angajații în apărătorii de vârf ai companiei. Angajații trebuie să înțeleagă, pe deplin, riscurile și consecințele, precum și rolurile și responsabilitățile acestora atunci când vine vorba de protejarea organizației în fața amenințărilor și atacurilor cibernetice.

Odată ce o companie și-a auditat sistemele și a pus în aplicare politici pentru a maximiza securitatea cibernetică, următorul pas vital este educarea angajaților din companie, astfel încât aceștia să devină parte din soluția de securitate. Este vital ca managementul să se angajeze în politica privind securitatea informatică iar crearea unei culturi de securitate cibernetică puternice necesită o comunicare eficientă, nu numai între echipa de IT și management, ci și între management și ceilalți angajați ai companiei.

Scopul educației privind securitatea informatică într-un mediu de afaceri este acela de a oferi membrilor echipei o înțelegere funcțională a modului în care pot evita potențialele amenințări. O companie își îmbunătățește, în mod semnificativ, rezistența liniei de front prin educarea angajaților cu privire la modul în care funcționează securitatea informatică. Deși nu toată lumea poate fi (sau își dorește să fie) un expert în securitatea informatică, toți angajații ar trebui să înțeleagă practicile de bază. Acestea includ selectarea și utilizarea parolei, drepturile de acces ale utilizatorilor, instalarea actualizărilor, învățarea modului de recunoaștere și detectare a potențialelor amenințări (cum ar fi e-mailurile de phishing).

Instruirea continuă în domeniul securității cibernetice pentru toți angajații organizațiilor ar trebui să fie specifică meseriei fiecărei persoane. Instruirea și conștientizarea ar trebui să se desfășoare la un nivel adecvat rolului, responsabilităților și profilului de risc al angajatului și ar trebui să fie susținută de politici realiste și aplicabile, care să evolueze în contextul amenințării. De asemenea, este foarte importantă crearea unei culturi bazate pe securitate, care se desfășoară în întreaga organizație, unde toată lumea împărtășește responsabilitatea pentru securitate și înțelege importanța rolului său în protejarea împotriva riscurilor de atacuri cibernetice și consecințele acestora.

Angajații trebuie să fie conștienți de procesele și protocoalele de securitate ale companiei și să fie familiarizați cu măsurile pe care le pot lua pentru a proteja organizația. Politicile de securitate IT ar trebui să conțină un plan de remediere și răspuns clar documentat, în plus față de acoperirea tuturor surselor posibile de atac, inclusiv cele mai recente amenințări. Ca atare, aceste politici trebuie să fie actualizate și comunicate în mod regulat. Pentru a fi eficienți, personalul trebuie să cunoască, să înțeleagă și să respecte regulile și liniile directoare ale companiei pentru a utiliza e-mailurile, navigarea pe Internet, rețelele sociale, dispozitivele mobile, laptop-ul și desktop-ul. Personalul ar trebui să știe exact ce măsuri să ia în caz de suspectare a unei încălcări și au nevoie de o persoană de contact, pentru a raporta e-mailuri suspecte, apeluri sau activități neobișnuite sau un dispozitiv pierdut. Dacă are loc un atac sau o încălcare, comunicarea internă ar trebui să fie rapidă, pentru a limita impactul atacului.

Educația trebuie să fie urmată de evaluări ale angajaților și ale sistemelor pentru a afla cât de vulnerabilă este organizația. Testarea cunoștințelor angajaților privind securitatea informatică se poate face printr-un sondaj online sau prin simularea atacurilor. De exemplu, echipa de securitate ar putea trimite e-mailuri false de phishing tuturor angajaților pentru a vedea câte persoane îl accesează, iar un astfel de test poate fi un instrument educațional util. De asemenea, regăsim atât cursuri de inițiere sau de specializare în domeniul securității cibernetice cât și reviste de specialitate sau platforme web, pe care angajații le pot accesa pentru a se informa sau specializa în acest domeniu.

3. Programe de formare continuă

Longlife learning reprezintă continuarea și auto-motivarea în vederea însușirii de cunoștințe, atât din motive personale cât și profesionale. Formarea continuă nu numai că sporește incluziunea socială și dezvoltarea personală, dar și autonomia, competitivitatea și capacitatea de inserție pe piața muncii. Printre cursurile de inițiere și de specializare în domeniile tehnologiei informației se regăsesc următoarele:

- UTI Academy - oferă cursuri dedicate specialiștilor IT care sunt implicați în securitatea sistemelor informatice, forensic, răspuns la incidente, monitorizarea și detectarea incidentelor de securitate cibernetică;

- Crystal Mind Academy, InfoAcademy, Telecom Academy, Academia Credis, BIT Academy: oferă cursuri de rețelistică, programare, sisteme de operare și securitate cibernetică;
- EC Council - este cel mai mare organism de certificare tehnică în materie de securitate cibernetică din lume. Consiliu Internațional al Consultanților pentru Comerțul Electronic, a fost format pentru a crea programe de instruire și certificare în domeniul securității informațiilor. EC Council a câștigat rapid sprijinul cercetătorilor și al experților din lumea întreagă și a lansat primul său Program de Securitate a Informațiilor - certificatul Ethical Hacker. Cu o echipă, din ce în ce mai mare, consiliul continuă să elaboreze standarde, certificări și programe de formare în domeniul comerțului electronic și al securității informațiilor.

4. Publicații în domeniul securității cibernetice

Aceste publicații au rolul de a promova, în mediul tipărit dar și în mediul online, cele mai noi tendințe din domeniul securității cibernetice.

Principalele publicații identificate în mediul online, care au ca obiectiv principal diseminarea informațiilor privind securitatea cibernetică sunt următoarele:

„Intelligence”, editată de Serviciul Român de Informații – este o publicaţie ce s-a impus prin calitatea materialelor publicate şi prin analiza specializată asupra proceselor şi provocărilor globale cu care se confruntă societatea din zilele noastre. De asemenea, reprezintă un mod de comunicare cu societatea civilă, urmărindu-se educarea cititorilor şi crearea unei culturi de securitate. Revista cuprinde o gama largă de teme, de la interviuri cu personalităţi marcante din mediul universitar la analize asupra criminalităţii cibernetice, ameninţărilor biologice, organizaţiilor criminale transfrontaliere și analize asupra informaţiilor în spaţiul euro-atlantic.

„Infosfera”, editată de Direcția Generală de Informații a Apărării, Ministerul Apărării Naționale – contribuie la realizarea unei culturi de securitate prin abordarea problemelor generale ale securităţii cât şi prin prezentarea unor aspecte specifice activităţii de informaţii pentru apărare. Publicația oferă acces la informaţii privind următoarele aspecte: cadrul instituţional şi resorturile politico-militare ale activităţii de informaţii pentru apărare; obiectivele, principiile şi particularităţile activităţii de informaţii pentru apărare; organizarea şi funcţionarea unor servicii moderne de informaţii etc.

„International Journal of Information Security and Cybercrime”, editată de Asociația Română pentru Asigurarea Securității Informației - publicația are ca scop principal analizarea securității informației, a sistemelor informatice, a comunicațiilor și identificarea noilor caracteristici ale fenomenului criminalității informatice. Se adresează specialiștilor din domeniul securității informațiilor, celor care urmează un program de studii, precum și tuturor celor care doresc să își îmbunătățească sau să își actualizeze cunoștințele în acest domeniu.

„Cybersecurity Trends”, editată de Agora Group împreună cu Swiss WebAcademy - dorește să sporească gradul de conștientizare în privința amenințărilor provocate de atacurile cibernetice și să ofere sfaturi și soluții de apărare împotriva acestora, prin furnizarea de informații de la principalele companii specializate pe securitate informatică, asociații de profil și instituții de stat. Publicația conține știri despre amenințările și atacurile cibernetice, modificările din legislația românească și europeană, cazuri ajunse în justiție și exemple de aplicare a legii, interviuri cu principalii actori din piață, studii de caz, analize și sfaturi practice. Publicația este distribuită și către instituțiile educaționale, pentru a ajuta la rezolvarea uneia dintre cele mai mari probleme ale prezentului – asigurarea accesului la forță de muncă calificată.

„Revista Română de Studii de Intelligence”, editată de Academia Națională de Informații „Mihai Viteazul” prin Institutul Național de Studii de Intelligence - reunește articole, studii și recenzii din domeniul studiilor de securitate și intelligence. Scopul acestei publicații este acela de a crea un cadru adecvat pentru dezbatere academică, în domeniul studiilor de securitate și intelligence și reprezintă o platformă accesibilă cercetătorilor, doctoranzilor și practicienilor. Temele de interes ale publicației sunt următoarele: paradigme de securitate în secolul XXI, mediul internațional și regional de securitate, strategii și politici de securitate, cultura de securitate și diplomație publică, Intelligence în secolul XXI, analiză de Intelligence, Open Source Intelligence OSINT etc.

„Romanian Cyber Security Journal”, editată de Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București - revista română de Cyber Security (ROCYS) este o resursă de cunoștințe pentru practicieni, oameni de știință și cercetători care lucrează în diverse domenii de securitate cibernetică, hacking, criminalistică digitală, război cibernetic, sau în zona de protecție a infrastructurilor critice. Articolele sunt scrise de profesioniști în domeniul securității cibernetice, bazându-se pe experiența practică în infrastructurile critice naționale, guvernamentale, corporații, financiare, militare și organizații non-profit. Unul dintre cele mai importante obiective ale acestei reviste este acela de a spori impactul cunoștințelor și vizibilitatea rezultatelor științifice.

5. Platforme Web pentru promovarea și conștientizarea securității cibernetice

Portalurile dedicate domeniului securității cibernetice contribuie atât la crearea unei culturi în acest domeniu, cât și pentru promovarea activităților și evenimentelor publice: workshop-uri, conferințe, hackathon-uri și publicații. Aceste portaluri au rolul de a disemina informațiile, cu scopul de a crește conștientizarea securității cibernetice în rândul populației deoarece, în mediul online, acest lucru joacă un rol foarte important în creșterea culturii de securitate cibernetică.

Următoarele portaluri din domeniul securității și criminalității informatice, au o activitate susținută și sunt printre cele mai accesate:

www.securitatea-informatiilor.ro – reprezintă canalul oficial al Asociației Române pentru Asigurarea Securității Informației și are ca scop principal informarea specialiștilor din domeniu, dar și a celor interesați să-și optimizeze sau să-și actualizeze cunoștințele în domeniul securității. Acest portal cuprinde informații despre: manifestările științifice din domeniu; mastere universitare și cursuri de specialitate în domeniu; cărți, manuale universitare, tratate și reviste științifice.

Portalul conține tutoriale și soluții de securitate clasificate în următoarele categorii:

- Alerte de securitate;
- Soluții de securitate IT - securitatea datelor, securitatea aplicațiilor, securitatea sistemului informatic și securitatea rețelelor.
- Standarde de securitate;
- Programe de asigurare a securității - programe antivirus, programe firewall, programe antispyware și suite de securitate;
- Tipuri de atacuri informatice;
- Audit de securitate - managementul riscurilor și vulnerabilități informatice;
- Survivabilitatea sistemului informatic;
- Știri de ultimă oră.

www.securitatea-cibernetica.ro – acest portal are ca scop educarea şi formarea profesională în domeniul securității cibernetice și are următoarele obiective: avertizarea publicului privind principalele vulnerabilități, riscuri și amenințări în domeniul securității cibernetice; creșterea nivelului de instruire în securizarea sistemelor informatice; promovarea evenimentelor științi-

fice în domeniu; dezvoltarea cooperării dintre sectorul public și cel privat prin stimularea schimbului de informații în vederea creșterii nivelului de securitate în spațiul cibernetic. De asemenea, platforma prezintă informații legate de: alerte de securitate cibernetică; ghiduri și strategii de securitate cibernetică; strategii de monitorizare a securității cibernetic; interviuri cu experții din domeniu; strategia de securitate cibernetică a țării și proiectul de lege privind securitatea cibernetică a României.

www.criminalitatea-informatica.ro – obiectivul portalului este reprezentat de comunicarea informațiilor de interes major privind atacurile cibernetice și mijloacele de protecție împotriva acestora, pentru a oferi metode cât mai eficiente de prevenire și combatere a criminalității informatice. Portalul oferă informații legate de: manifestările științifice din domeniu; cărți, manuale universitare, tratate și reviste științifice în domeniu; aplicații folosite în investigarea adreselor IP, a domeniilor sau a e-mail-urilor. Portalul constituie o platformă de comunicare între specialiștii din domeniul investigării criminalității informatice și utilizatorii interesați să-și optimizeze sau să-și actualizeze cunoștințele în acest domeniu.

www.criminalitate.info – portalul dorește a fi un blog juridic, cu rol informativ, atât pentru persoanele implicate în prevenirea și combaterea criminalității informatice cât și pentru persoanele care doresc să fie informate cu privire la modalitățile de protecție și șansele pe care le poate avea în justiție.

www.cyberm.ro – Cyber Media Awareness este un spaţiu în care subiectele media şi cyber security devin complementare, cu scopul conştientizării pericolelor domeniului securităţii cibernetice. Siguranţa jurnaliştilor, a informaţiilor şi a consumatorilor de produse media sunt principalele teme de discuţie pe acest portal.

6. Concluzii

Nu doar numărul de atacuri cibernetice sunt cele care cresc, gradul acestor atacuri este, de asemenea, în creștere. Aceste atacuri devin progresiv distructive și vizează o gamă largă de vectori de informare și de atac.

Pe măsură ce sunt evaluate riscurile și expunerea la atacurile cibernetice și furtul de date, trebuie să ținem cont de faptul că nu există niciun fel de evitare a impactului pe care aceste amenințări îl au asupra tuturor întreprinderilor, de orice dimensiune. De aceea, recunoașterea amenințărilor cibernetice și posibilitatea de a proteja organizația de aceste atacuri sunt primordiale pentru a opera o afacere de lungă durată.

Pe măsură ce devenim mai dependenți de tehnologie, navigăm pe un câmp minat al securității cibernetice. Siguranța depinde foarte mult de modul în care suntem proactivi în ceea ce privește securitatea și conștientizarea riscurilor. De aceea, problemele de securitate cibernetică reflectă, de multe ori, o lipsă a know-how-ului dezvoltatorilor implicați.

Know-how-ul și abilitățile în domeniul securității cibernetice, sunt necesar a fi disponibile în orice țară dezvoltată, iar acestea pot fi asigurate printr-o oferta de programe educaționale și de formare (specifice nivelului profesional și pregătirii), prin accesul la platforme web, reviste de specialitate și prin schimbul de experiență.

BIBLIOGRAFIE

1. Alexandrescu, G., Văduva, G., (2006), *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, București, Editura Universității Naționale de Apărare;
2. Banciu, D. (2015). *Educație și cultură în era digitală,* București, Editura Niculescu;
3. https://www.arasec.ro/;
4. https://www.verticalonline.ro/o-revista-dedicata-fenomenelor-si-provocarilor-globale-contemporane;
5. https://www.scribd.com/document/30328505/INFOSFERA-Revista-de-Studii-de-Securitate-Si-Informatii-Pentru-Aparare-Nr-1-2009;
6. https://www.arasec.ro/comunicate-de-presa/revista-stiintifica-ijisc/;
7. https://cybersecuritytrends.ro/concept-2/;
8. http://animv.ro/revista-romana-de-studii-de-intelligence/;
9. http://www.securitatea-informatiilor.ro/despre-site/;
10. http://www.criminalitatea-informatica.ro/despre-site/;
11. https://www.criminalitate.info/p/despre-noi.html;
12. https://cyberm.ro/about/;
13. http://anssi.ro/;
14. https://ascensiongt.com/2018/02/12/boost-cyber-defense-strategy-educated-employees/;
15. https://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/ID%20CMD%20Cyber%20Security%20Strategy%2020171026%20PA.pdf;
16. https://www.mailguard.com.au/partner-blog/education-cybersecurity;
17. Leidigh, C., (2005), *Fundamental Principles of Network Security*; American Power Conversion;
18. Mihai, I.C., Ciuchi, C., Petrică, G.M. (2018), *Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu*, Studii de Strategie și Politici SPOS 2017, Studiul nr. 4, București;
19. Vevera, A. V. (2014, vol. 24 nr. 3). *O NOUĂ EPOCĂ DIGITALĂ*. Revista Română de Informatică și Automatică , pp. 23-28;
20. Vevera, A. (2014), *România în noua eră digitală*, Volumul 7 teme fundamentale pentru România. Editura RAO, București.

Adrian Victor VEVERA este Director Tehnic, cercetător științific gradul II și membru în Consiliul Științific al Institutului Național de Cercetare-Dezvoltare în Informatică. Doctor în științe militare și informații, fiind la bază atât jurist cât și inginer specializat în fizică nucleară, deține o vastă experiență în ceea ce înseamnă securitatea națională, ocupând, de-a lungul timpului, numeroase poziții manageriale și de consiliere în diverse organisme ale statului. A publicat numeroase articole și lucrări pe teme de securitate națională și internațională, securitate energetică, criminalitate informatică, protecția infrastructurilor critice și a fost coordonatorul a numeroase proiecte de interes național.

Adrian Victor VEVERA is a Senior Researcher II, the Technical Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics. Doctor of Military Sciences and Information, being both a lawyer and a nuclear physics engineer, Mr. Vevera has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counseling positions in different state organisms. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.

Raluca Alexandra ALBESCU a absolvit Facultatea de Litere din cadrul Universității din București și este proaspăt absolventă a programului de masterat din cadrul Facultății de Management, Academia de Studii Economice din București. În prezent își desfășoară activitatea în cadrul Departamentului de Securitate Cibernetică și Infrastructuri Critice la Institutul Național de Cercetare-Dezvoltare în Informatică - ICI București. Este interesată să se dezvolte în domeniul securității cibernetice, smart city și protecția infrastructurilor critice.

Raluca Alexandra ALBESCU graduated the Faculty of Letters from the University of Bucharest and is a fresh graduate of the master program from the Faculty of Management, Academy of Economic Studies of Bucharest. She is currently working in the Department of Cyber Security and Critical Infrastructure at the National Institute for Research and Development in Informatics - ICI Bucharest. She is interested in developing in the field of cyber security, smart city and critical infrastructure protection.