NAVIGAREA LA INTERSECȚIA DINTRE TEHNOLOGIILE EMERGENTE, ANALIZA AVANSATĂ A DATELOR ȘI SECURITATEA CIBERNETICĂ: STRATEGII PENTRU ERA DIGITALĂ

Alexandr DIMOGLO

Departamentul de Inginerie Software și Automatică, grupa SI-221M, Facultatea de Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Autorul corespondent: Alexandr Dimoglo, alexandr.dimoglo@isa.utm.md

Coordonator științific: BULAI Rodica, profesor universitar, Automatică și Tehnologii Informaționale

Rezumat. *Acest document prezintă o imagine de ansamblu a provocărilor și strategiilor de navigare la intersecția dintre tehnologiile emergente, analiza avansată a datelor și securitatea cibernetică. Discutăm despre amenințările cibernetice din ce în ce mai sofisticate și despre proliferarea dispozitivelor conectate care creează vulnerabilități în era digitală. Subliniem deficitul de profesioniști calificați în domeniul securității cibernetice și necesitatea unei guvernanțe și reglementări eficiente pentru a asigura protecția datelor și a vieții private. Pentru a aborda aceste provocări, propunem o abordare cu mai multe fațete care implică o combinație de soluții tehnice, politici și programe de educație și formare. Analiza noastră se bazează pe o gamă variată de surse din literatura de specialitate, inclusiv Ghidul practicianului în domeniul securității cibernetice, Extinderea speranței de sănătate, Cartografierea valului de digitalizare a industriei și Guvernanța globală a științei și tehnologiei, printre altele. Constatările noastre sugerează că strategiile eficiente în materie de securitate cibernetică necesită o abordare holistică care să cuprindă atât aspecte tehnice, cât și non-tehnice, și că colaborarea dintre mediul academic, industrie și guvern este crucială pentru a aborda provocările complexe ale erei digitale.*

Cuvinte cheie*: amenințări cibernetice, protecția datelor, blockchain, internetul lucrurilor, analiză predictivă.*

Introducere

Adoptarea din ce în ce mai frecventă a tehnologiei a adus numeroase beneficii în viața noastră de zi cu zi, dar a introdus, de asemenea, noi provocări în materie de securitate care trebuie abordate de către practicienii în domeniul securității cibernetice. Pentru a rămâne în fața amenințărilor emergente și pentru a atenua riscurile digitale în evoluție, este esențial să înțelegem și să dezvoltăm strategii eficiente pentru a atenua potențialele implicații de securitate ale tehnologiilor emergente, cum ar fi IoT și edge computing. Deși aceste tehnologii oferă niveluri de confort fără precedent, ele introduc, de asemenea, noi vulnerabilități și suprafețe de atac care necesită măsuri de securitate pentru a se proteja împotriva lor. În plus, utilizarea tehnicilor avansate de analiză a datelor în contextul securității cibernetice oferă un mare potențial de detectare și prevenire a atacurilor cibernetice, dar necesită competențe și instrumente sofisticate pentru a fi implementate în mod efficient [1]. Prin urmare, este esențial să se investească în formarea și dotarea profesioniștilor din domeniul securității cibernetice cu competențele necesare pentru a valorifica aceste tehnici. În plus, implicațiile etice ale dezvoltării și implementării inteligenței artificiale (AI) trebuie să fie luate în considerare în contextul securității cibernetice. Pe măsură ce IA continuă să evolueze și să devină tot mai omniprezentă în viața noastră de zi cu zi, este esențial să se evalueze impactul potențial al acesteia asupra securității cibernetice și să se abordeze orice preocupări de ordin etic care pot apărea. Acest lucru necesită o abordare cuprinzătoare a securității cibernetice, care să integreze considerentele etice în proiectarea și implementarea acesteia [2]. În concluzie, prin explorarea intersecției dintre tehnologiile emergente, analiza avansată a datelor și securitatea cibernetică și prin încorporarea considerentelor etice în abordarea noastră, putem dezvolta strategii eficiente pentru a naviga în peisajul complex și în continuă schimbare al securității digitale.

Provocări existente

Domeniul securității cibernetice se confruntă cu numeroase provocări care trebuie abordate. Una dintre provocările majore este natura din ce în ce mai sofisticată a amenințărilor cibernetice, care continuă să evolueze odată cu tehnologia. Atacatorii cibernetici devin din ce în ce mai pricepuți și mai plini de resurse, ceea ce face mai dificilă prevenirea atacurilor și protecția împotriva încălcărilor de date [3]. O altă provocare este reprezentată de proliferarea dispozitivelor conectate, cum ar fi cele din Internetul obiectelor (IoT), care reprezintă vulnerabilități potențiale ce pot fi exploatate de atacatori. În plus, există un deficit semnificativ de profesioniști calificați în domeniul securității cibernetice, ceea ce face dificilă gestionarea eficientă a riscurilor de securitate cibernetică de către organizații. De asemenea, este nevoie de o guvernanță și de o reglementare eficace în domeniul securității cibernetice pentru a gestiona aceste riscuri în mod corespunzător, ceea ce necesită cooperarea între diverse părți interesate. În cele din urmă, cantitatea tot mai mare de date colectate și stocate de organizații a făcut mai importantă ca niciodată prioritizarea confidențialității și a protecției datelor [4]. Acest lucru necesită punerea în aplicare a unor măsuri solide de protecție a datelor și a unor politici și reglementări eficiente pentru a se asigura că datele cu caracter personal nu sunt utilizate în mod abuziv sau gestionate în mod necorespunzător. Aceste provocări trebuie abordate cu o abordare cuprinzătoare a securității cibernetice care să țină cont de peisajul tehnologic în continuă schimbare și de natura evolutivă a amenințărilor cibernetice [5].

Răspândirea dispozitivelor conectate

"Răspândirea dispozitivelor conectate" sau a dispozitivelor IoT reprezintă o provocare majoră în privința securității cibernetice, după cum se menționează în diverse lucrări de cercetare. Se preconizează că numărul dispozitivelor IoT va crește până la 75 de miliarde până în 2025, ceea ce deschide oportunități semnificative de atac pentru infractorii cibernetici [6]. Una dintre provocările legate de securizarea dispozitivelor IoT este reprezentată de resursele și puterea de calcul limitate ale acestora, precum și de localizarea lor în locații îndepărtate sau greu accesibile. Botnet-urile, care sunt rețele de dispozitive compromise, reprezintă o amenințare deosebită pentru mediile IoT [7]. Detectarea și combaterea botnet-urilor în mediile IoT este dificilă din cauza numărului mare de dispozitive și a rețelelor complexe. Abordarea problemei proliferării dispozitivelor conectate în mediile IoT va necesita inovare și colaborare constantă între industrie, mediul academic și guvern. Pentru a aborda aceste provocări este necesară o abordare coordonată care să ia în considerare aspectele tehnice, sociale și etice ale securității cibernetice.

Deficitul de profesioniști calificați în domeniul securității cibernetice

Lipsa de profesioniști calificați în domeniul securității cibernetice este o provocare semnificativă cu care se confruntă în prezent domeniul securității cibernetice. Potrivit "Cybersecurity Practitioner's Guide", există un deficit de peste 3 milioane de profesioniști la nivel global, ceea ce reprezintă o problemă gravă, deoarece cererea de profesioniști în domeniul securității cibernetice a depășit oferta [1]. Acest deficit are implicații semnificative asupra capacității organizațiilor de a se apăra împotriva atacurilor cibernetice, după cum se arată în lucrarea "Mapping the Wave of Industry Digitalization by Co-Word Analysis: An Exploration of Four Disruptive Industries" [3]. Complexitatea tot mai mare a amenințărilor la adresa securității cibernetice înseamnă că organizațiile au nevoie de o serie de competențe foarte specializate pentru a se apăra eficient împotriva atacurilor. Rezolvarea problemei lipsei de profesioniști calificați în domeniul securității cibernetice va necesita un efort concertat din partea industriei, a mediului academic și a guvernelor pentru a forma și dezvolta următoarea generație de profesioniști în domeniul securității cibernetice [8].

O provocare majoră cu care se confruntă domeniul, cu bariere precum lipsa de conștientizare în rândul studenților cu privire la carierele în domeniul securității cibernetice, resursele limitate pentru educația în domeniul securității cibernetice și natura rapid schimbătoare a domeniului. Rezolvarea problemei lipsei de personal va necesita o colaborare între industrie, mediul academic și guvern, inclusiv inițiative de sensibilizare, investiții în programe de educație și formare și eforturi de promovare a diversității și incluziunii. Procedând astfel, putem construi un viitor digital mai rezistent și mai sigur.

Necesitatea reglementării eficiente în domeniul securității cibernetice

Guvernanța și reglementarea eficientă în domeniul securității cibernetice sunt vitale pentru protejarea infrastructurilor critice, informațiilor personale și a datelor sensibile. Guvernanța și reglementarea inadecvate pot duce la utilizarea necorespunzătoare a tehnologiei, la încălcări ale confidențialității și la atacuri cibernetice. Importanța guvernanței și a reglementării în materie de securitate cibernetică este evidențiată în bibliografie, unde studiile subliniază necesitatea guvernanței pentru a aborda provocările complexe care decurg din progresele tehnologice. Documentele "Global Science and Technology Governance" și "Toward a Transformed and Unequal World" subliniază în special necesitatea unor cadre de guvernanță și de reglementare pentru a gestiona riscurile și oportunitățile prezentate de progresele tehnologice, cum ar fi inteligența artificială[9-10].

În plus, lucrarea "BLOCKCHAIN CNN DEEP LEARNING EXPERT SYSTEM FOR HEALTHCARE EMERGENCY" explorează utilizarea blockchain și a învățării profunde pentru a îmbunătăți asistența medicală de urgență[11]. Acesta subliniază importanța cadrelor de reglementare pentru asigurarea securității și confidențialității datelor din domeniul sănătății. Lucrarea "INTERNET OF THINGS EXPERT SYSTEM FOR SMART CITIES USING THE BLOCKCHAIN TECHNOLOGY" evidențiază, de asemenea, potențialul blockchain pentru securizarea dispozitivelor IoT în orașele inteligente[12].

Importanța confidențialității și a protecției datelor

Confidențialitatea și protecția datelor sunt componente esențiale ale securității cibernetice, mai ales pe măsură ce utilizarea tehnologiei și generarea de date continuă să crească. Protejarea informațiilor sensibile împotriva furtului, a utilizării abuzive sau a accesului neautorizat este o prioritate absolută. Bibliografia oferă informații suplimentare despre acest subiect, cu lucrări precum "Cybersecurity Practitioner's Guide", care oferă orientări pentru protejarea datelor sensibile, și "Extending Health Expectancy", care subliniază importanța protejării informațiilor personale de sănătate. Lucrările "Global Science and Technology Governance", "Internet of Things Expert System for Smart Cities", "Authentication and Secure Communications for Internet of Vehicles" și "A Comprehensive Solution for Ensuring Information Security" evidențiază, de asemenea, importanța confidențialității și a protecției datelor în peisajul digital actual[9-16]. Aceste lucrări subliniază necesitatea unor măsuri eficiente de protejare a informațiilor sensibile, deoarece nerespectarea acestor măsuri poate avea consecințe grave pentru persoane și organizații.

Concluzie

În concluzie, analiza literaturii de specialitate privind tehnologiile emergente, analiza avansată a datelor și securitatea cibernetică a evidențiat oportunitățile și provocările pe care le prezintă era digitală. Pentru a ține pasul cu aceste schimbări, strategiile de securitate cibernetică trebuie să evolueze, adoptând o abordare holistică care să țină cont de interconectarea sistemelor tehnologice și de diversele amenințări care pot apărea. Sunt necesare colaborarea și un angajament față de învățarea și adaptarea continuă. Pentru a asigura un viitor digital mai sigur și mai prosper, sunt necesare investiții în profesioniști calificați în domeniul securității cibernetice, o guvernanță și o reglementare solide în materie de securitate cibernetică, precum și măsuri eficiente de protecție a vieții private și a datelor. Provocările sunt numeroase și complexe, dar cercetarea și colaborarea continuă pot duce la strategii și tehnologii inovatoare care să atenueze riscurile asociate tehnologiilor emergente, permițându-ne să le valorificăm întregul potențial.

Referinţe

1. A. G. HESSAMI, *Cyber security practitioner's guide*. Hackensack: World Scientific, 2020.
2. G. TERRY SHARRER, *Extending Health Expectancy*, Mol. Front. J., т. 03, ed. 02, cc. 147–165, dec. 2019, doi: 10.1142/S252973251940011X.
3. L. BZHALAVA, S. S. HASSAN, J. KAIVO-OJA, B. KÖPING OLSSON, AND J. IMRAN, *Mapping the Wave of Industry Digitalization by Co-Word Analysis: An Exploration of Four*

Disruptive Industries, Int. J. Innovation Technol. Management, т. 19, ed. 02, с. 2250001, apr. 2022, doi: 10.1142/S0219877022500018.
4. S. FENG, *Toward a Transformed and Unequal World: The AI Revolution and the New International System*, China Q of Int' l Strategic Stud, т. 05, ed. 02, cc. 267–287, jan. 2019, doi: 10.1142/S2377740019500118.
5. R. C. AGUILERA, M. P. ORTIZ, A. A. BANDA, AND L. E. C. AGUILERA, *Blockchain CNN Deep Learning Expert System For Healthcare Emergency*, Fractals, т. 29, ed. 06, с. 2150227, sep. 2021, doi: 10.1142/S0218348X21502273.
6. S. HAIYONG, *Global Science and Technology Governance: Impetus, Challenges, and Prospects*, China Q of Int' l Strategic Stud, т. 07, ed. 01, cc. 61–78, jan. 2021, doi: 10.1142/S2377740020500244.
7. R. C. AGUILERA, M. P. ORTIZ, J. P. ORTIZ, AND A. A. BANDA, *Internet of Things Expert System For Smart Cities Using The Blockchain Technology*, Fractals, т. 29, ed. 01, с. 2150036, feb. 2021, doi: 10.1142/S0218348X21500365.
8. I. AFANASIEVA, N. GOLIAN, O. HNATENKO, Y. DANIIEL, AND K. ONYSHCHENKO, *Data Exchange Model In The Internet Of Things Concept*, Telecom Rad Eng, т. 78, ed. 10, cc. 869–878, 2019, doi: 10.1615/TelecomRadEng.v78.i10.30.
9. A. ARAL AND T. OVATMAN, *A Decentralized Replica Placement Algorithm for Edge Computing*, IEEE Trans. Netw. Serv. Manage., т. 15, ed. 2, cc. 516–529, jun. 2018, doi: 10.1109/TNSM.2017.2788945.
10. XI. LIU, *Data Information Security of Communication Network Based on Edge Computing Technology and BP Neural Network*, Telecom Rad Eng, т. 78, ed. 20, cc. 1837–1845, 2019, doi: 10.1615/TelecomRadEng.v78.i20.60.
11. I. E. VILINOV, A. V. VOLODIN, AND V. V. DERGACHEV, *A Comprehensive Solution for Ensuring Information Security of an Industrial Facility Infrastructure*, Telecom Rad Eng, т. 72, ed. 3, cc. 181–193, 2013, doi: 10.1615/TelecomRadEng.v72.i3.10.
12. J. I. NASER, H. A. G. ALSALMAN, AND A. J. KADHIM, *Authentication and Secure Communications for Internet of Vehicles (IoV)-Assisted Fog Computing*, Telecom Rad Eng, т. 78, ed. 18, cc. 1659–1670, 2019, doi: 10.1615/TelecomRadEng.v78.i18.40.
13. S. K. PRASAD, J. RACHNA, O. I. KHALAF, AND D.-N. LE, *Map Matching Algorithm: Real Time Location Tracking for Smart Security Application*, Telecom Rad Eng, т. 79, ed. 13, cc. 1189–1203, 2020, doi: 10.1615/TelecomRadEng.v79.i13.80.
14. A. I. TSOPA, *Estimation of Signal Encoding and Scrambling Impact on Information Transmission System Security*, Telecom Rad Eng, т. 74, ed. 1, cc. 51–60, 2015, doi: 10.1615/TelecomRadEng.v74.i1.50.
15. X. MENG AND W. LU, *Container-Based Fast Service Migration Method for Mobile Edge Computing*, J CIRCUIT SYST COMP, т. 30, ed. 15, с. 2250117, dec. 2021, doi: 10.1142/S0218126622501171.
16. A. SUKHOV, A. SIHVONEN, L. E. OLSSON, AND P. R. MAGNUSSON, *That Makes Sense to Me: Openness to Change and Sensemaking in Idea Screening*, Int. J. Innov. Mgt., т. 22, ed. 08, с. 1840009, dec. 2018, doi: 10.1142/S1363919618400091.