CREŞTEREA CONŞTIENTIZĂRII ASUPRA SECURITĂŢII CIBERNETICE PRIN PROGRAME EDUCAŢIONALE

RAISING AWARENESS ON CYBER SECURITY THROUGH EDUCATIONAL PROGRAMS

Căpitan ing. drd. Tiberiu ION*

Rezumat: *În prezent internetul este utilizat la scară largă, de la consumatorii individuali, la mediul de business şi guvernamental. Expansiunea digitalizării a înregistrat noi dimensiuni odată cu apariţia pandemiei Covid-19 şi dezvoltarea conceptului „lucrului de la distanţă”, iar multitudinea de tranzacţii electronice efectuate în această perioadă a atras interesul diverşilor terţi neautorizaţi în a compromite informaţiile tot mai accesibil în beneficiul lor. Importanţa înţelegerii acestui risc de către utilizatori este strâns legată de gradul de conştientizare a securităţii informaţiilor în rândul acestora.*

Având în vedere faptul că factorul uman reprezintă în mod specific o vulnerabilitate a oricărei organizaţii, spaţiul cibernetic este cu atât mai sensibil cu cât utilizatorii nu sunt conştienţi de riscurile acţiunilor efectuate pe internet şi „se aventurează” adesea în spaţiul cibernetic fără niciun fel de pregătire prealabilă. În acest sens, interesul atacatorilor din spaţiul cibernetic nu urmăreşte doar tehnologia informatică şi cum poate fi acestea compromisă, o atenţie aparte fiind acordată comportamentului utilizatorului de internet, fie din postura de utilizator casnic, fie din postura de angajat al unei companii sau instituţii guvernamentale.

Astfel, prezenta lucrare trasează un cadru-general al modului de abordare al factorului uman în contextul securităţii cibernetice, prin identificarea principalelor tipuri de comportamente vulnerabile, a principalelor tipuri de erori umane şi a celor mai uzuale metode de prevenire a riscului cibernetic prin raportarea la principiile securităţii datelor. De asemenea este subliniată importanţa programelor educaţionale specializate în creşterea gradului de conştientizare a ameninţărilor cibernetice.

Cuvinte cheie: *securitate cibernetică, resursa umană, conştientizare, resurse educaţionale.*

* Universitatea Naţională de Apărare „CAROL I”, ion.tiberiu@unap.ro.

Abstract: *Nowadays, the Internet is widely used, from individual consumers to business and government environment. The expansion of digitalization has taken on new dimensions with the emergence of the Covid-19 pandemic and the development of the "remote work" concept, the multitude of electronic transactions made during this period has drawing the interest of various unauthorized third parties to compromise information that is more accessible, for their benefit. The importance of understanding this risk by users is closely linked to the awareness of information security among them.*

Given that the human factor is specifically a vulnerability of any organization, cyberspace is more sensitive as users are unaware of the risks of their actions taken on the Internet and often "venture" into cyberspace without any prior training. In this sense, the interest of cyber attackers does not only pursue information technology and how it can be compromised, but a special attention being also paid to the behaviour of Internet users, either as a home user or as an employee of a company or government institution.

Thus, the present paper outlines a general approach on human factor in the context of cyber security, by identifying the most common types of vulnerable behaviours and types of human error in conjunction whit the most common methods of preventing cyber risk by referring to the principles of data security. The importance of specialized educational programs in raising awareness of cyber threats is also emphasized.

Keywords: *cybersecurtity, human resources, awareness, educational resources*

INTRODUCERE

Securitatea cibernetică reprezintă un instrument deosebit de important pentru societatea modernă, de la fiecare individ, companie mică sau mijlocie, corporație, organizație sau guvern. Rolul securității cibernetice în mediul virtual a devenit vital, în special în contextul intensificării procesului de digitalizare și a utilizării internetului la scară largă, pe fondul promovării lucrului de la distanță ca efect al pandemiei Covid-19.

Astfel, securitatea cibernetică implică atât tehnologie informatică, cât și multiple procese și resurse virtuale cu rol în protejarea datelor și a sistemelor informatice. La baza acesteia stau o serie de strategii defensive ce urmăresc 3 piloni principali: confidențialitatea (datele să nu fie accesate de persoane neautorizate), disponibilitatea (datele pot fi accesate ori de câte ori este necesar) și integritatea (datele nu au fost șterse sau modificate neautorizat). Toate aceste strategii și tehnologii reprezintă resurse

importante, însă eficiența acestora poate fi diminuată print-o utilizare incorectă de către persoane nefamiliarizate cu conceptul de securitate cibernetică şi care nu conştientizează posibilele consecințe ale acțiunilor sau inacțiunilor acestora în mediul virtual.

Conştientizarea securității cibernetice a devenit o preocupare permanentă pentru multiple companii, instituții sau organizații, odată cu intensificarea atacurilor informatice şi identificarea vulnerabilității resursei umane drept una dintre principalele cauze ale acestor atacuri. Institutului Național de Standarde şi Tehnologie descrie conştientizarea securității cibernetice astfel: „*conştientizarea securității cibernetice nu înseamnă pregătire. Scopul prezentărilor în domeniul conştientizării este pur şi simplu de a concentra atenția asupra acestui subiect. Prezentările în acest domeniu sunt destinate să permită persoanelor să recunoască problemele de securitate a tehnologiei informației şi să răspundă în consecință.*”[1]

Având în vedere aceste aspecte, prezentul articol urmărește identificarea unui cadru general cu privire la implicațiile avute de factorul uman în menținerea securității cibernetice, prin identificarea principalelor comportamente ce pot genera riscuri cibernetice şi cauzele aferente acestora. Mai mult, o serie de propuneri şi recomandări sunt evidențiate în vederea elaborării unui ghid de îndrumare (Abc), care să ofere utilizatorului de servicii din spațiul cibernetic minimul de informații pentru conştientizarea securității cibernetice şi dezvoltarea unei atitudini proactive.

1. Factorul uman – o provocare critică pentru securitatea cibernetică

Încă din ultimul deceniu, mediul cibernetic reprezintă un subiect de interes la nivel global, domeniul securității cibernetice fiind într-o continuă expansiune în vederea prevenirii şi atenuării atacurilor cibernetice. Amenințările cibernetice au căpătat noi dimensiuni, atacurile devenind mai frecvente odată cu începutul pandemiei COVID-19, în contextul lucrului de la distanță. În prezent conceptul de „lucru de la distanță” a devenit o practică comună pentru multiple companii şi sectoare, tendința actuală fiind aceea de a nu se renunța la acest mod de lucru, în următorii ani. În acest sens,

[1] National Institute of Standards and Technology, 1998. *NIST Special Publication 800-16*, p. 15. disponibil la https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf, accesat la 25.08.2021.

sectoarele critice, marile companii, întreprinderile, precum și structurile statului, mai ales cele din domeniul apărării, trebuie să-și adapteze strategiile de securitate cibernetică noilor practici și amenințări. Lipsa unei strategii de apărare cibernetică bine definită sau orice întârziere în adaptarea acesteia la noul mediu de lucru se poate traduce în pierderi financiare. Spre exemplu, la nivelul anului 2020, impactul creat de intruziunile atacatorilor cibernetici în serverele companiilor private, cauzate de lucrul la distanță, a determinat pierderi în valoare de aproximativ 5.54 milioane de dolari[2].

Din cercetările companiei ESET, ce activează în domeniul securității IT, a reieşit faptul că, încă de la începutul carantinei cauzată de pandemie, criminalitatea cibernetică a crescut cu 63%[3], iar continuitatea activității la nivelul multiplelor organizații este în pericol, din cauza unei forțe de muncă tot mai dispersate. Totodată, ESET menționează faptul că 80% dintre companiile care au participat în cadrul sondajului realizat în anul 2020, au raportat factorul uman (eroarea umană) ca reprezentând principala provocare pentru securitatea cibernetică.

În contextul securității cibernetice, eroarea umană poate fi definită prin acțiuni neintenționate sau lipsa de acțiuni a utilizatorilor de sisteme informatice, care cauzează, răspândesc sau permit încălcarea regulilor privind securitatea cibernetică. De altfel, având în vedere noua normalitate a lucrului de la distanță, securitatea cibernetică a unei organizații cade în responsabilitatea fiecărui angajat care interacționează cu sistemele informatice și nu mai poate fi considerată o problemă doar pentru echipa IT sau pentru manageri.

Un alt studiu publicat de compania Oracle conchide către aceleași rezultate, respectiv faptul că eroarea umană rămâne cel mai mare risc pentru securitatea cibernetică[4], în ciuda numărului crescut de alte amenințări, precum atacurile hackerilor sau chiar atacurile cibernetice cauzate de alte state.

---

[2] IBM, 2021. *Cost of Data Breach Report,* p. 47*,* disponibil la https://-liangroup.net/blog/wpcontent/uploads/2021/07/Cost-of-a-Data-Breach-Report-2021.pdf, accesat la 25.08.2021.

[3] ESET. *Cyberchology the Human Element*, disponibil la https://workplaceinsight.net/wp-content/uploads/2020/ 11/ESET_Cyberchology.pdf, accesat la 25.08.2021.

[4] ORACLE, 2018. *Security in the Age of AI*, disponibil la https://www.oracle.com/-a/ocom/docs/data-security-report.pdf, accesat la 26.08.2021.

Mai mult, National Institute of Standards and Technology, susține încă din anul 2018 faptul că aproximativ 90% din incidentele de securitate cibernetică sunt legate de erorile umane[5], riscul cibernetic fiind cu atât mai mare cu cât angajații sunt mai puțin preocupați de securitatea cibernetică.

Printre cele mai întâlnite erori cauzate de factorul uman cu privire la securitatea cibernetică pot fi menționate[6]:

-utilizarea dispozitivelor de lucru ale organizației pentru activități/tranzacții personale;

-deschiderea emailurilor malițioase fără a lua în considerare expeditorul acestora sau relevanța mesajului în contextul activității desfășurate;

-conectarea la sistemele informatice ale organizației prin utilizarea unei rețele nesecurizate.

Referitor la tipurile de erori în securitatea cibernetică, cauzate de factorul uman, acestea se pot clasifica astfel: erori bazate pe abilități și erori bazate pe decizii. Diferența dintre cele două tipuri de erori se reduce în esență la nivelul de cunoaștere/know-how al utilizatorului, respectiv dacă utilizatorul sistemului informatic a avut sau nu cunoștințele necesare pentru a efectua corect acțiunea.

Astfel, erorile bazate pe abilități reprezintă acele deficiențe sau mici greșeli care apar atunci când se efectuează activități repetitive sau familiare pentru utilizator. În aceste scenarii, utilizatorul final ştie care este cursul corect de acțiune, dar nu reușește să îl urmeze din cauza grabei sau a neglijenței. Principalele cauze ale erorilor bazate pe abilități pot fi gradul de extenuare al angajatului, lipsa atenției cauzată de multitudinea de sarcini repetitive sau de factori externi ce pot distrage atenția.

Pe de altă parte, erorile bazate pe decizie apar atunci când un utilizator ia o decizie defectuoasă. Pot exista o serie de factori diferiți pentru care utilizatorul ia o decizie defectuoasă: utilizatorul nu are nivelul necesar de cunoștințe în realizarea acțiunii sau utilizatorul nu are acces la suficiente informații referitoare la circumstanțele specifice acțiunii sale. În cazul

[5] Calvin Nobles, 2018. *Shifting the Human Factors Paradigm in Cybersecurity*, NIST, disponibil la https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/17.pdf, accesat la 26.08.2021.

[6] Grayson K et al, 2019. *Improve employees' cyber security awareness.* Computer Fraud & Security, August 2019, vol. 8, pp. 12-13.

ambelor scenarii, decizia nu este voluntară, aceasta fiind reprezentată prin lipsa de acțiune.

Una din principalele soluții în combaterea acestei vulnerabilități este reprezentată de organizarea unor programe de conștientizare și chiar de pregătire în securitate cibernetică pentru angajați. În acest sens, organizațiile trebuie să își prioritizeze cheltuielile pentru a putea investi în componenta de instruire, dar și de achiziție de noi soluții software bazate pe tehnologia Inteligenței Artificiale (AI) sau Machine Learning (ML). Chiar dacă software-ul modern și aplicațiile anti-malware sau de detectare a amenințărilor au devenit mai sofisticate, infractorii din mediul cibernetic sunt conștienți de faptul că măsurile tehnice de securitate sunt eficiente numai în măsura în care angajații le folosesc în mod corespunzător.

În acest sens, combaterea erorilor cauzate de factorul uman prin schimbarea practicilor, rutinelor și tehnologiilor de lucru reduce în mod sistematic oportunitățile de eroare. În plus, o cultură organizațională axată pe securitate trebuie să implice o strategie bine definită, aceasta fiind esențială în prevenirea și reducerea erorilor umane în mediul cibernetic (Figura nr. 1). În acest context, promovarea securității ca element determinat pentru fiecare decizie și acțiune îi va determina pe utilizatorii finali să caute activ resursele necesare acțiunii lor și să discute probleme de securitate pe măsură ce le întâmpină.

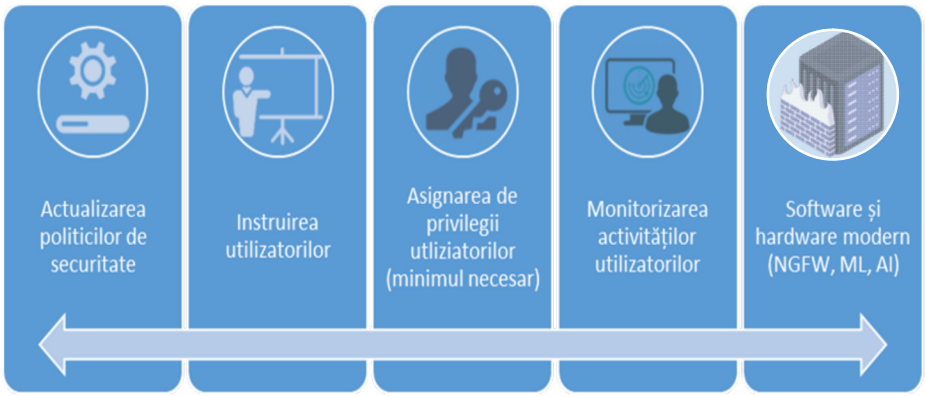

Figura nr. 1 – Exemplu de strategie organizațională axată pe securitatea cibernetică
(Concepție proprie)

Astfel, resursa umană insuficient instruită poate reprezenta cea mai slabă verigă din lanțul de securitate al unei organizații și nicio investiție în resurse de resortul IT, precum firewall-uri sau diverse software-uri de criptare, nu poate compensa un program specializat sau un curs de securitate cibernetică și comportament proactiv. Decalajul în materie de securitate cibernetică poate fi redus doar prin asigurarea unui flux permanent de comunicare la nivel organizațional și prin asigurarea componentei de instruire a resursei umane.

Conștientizarea importanței securității cibernetice în activitatea unei organizații și chiar în activitatea cotidiană, nu trebuie să aibă loc doar la nivel organizațional. Pentru a putea fi tratată ca o acțiune sustenabilă, aceasta trebuie să înceapă mult mai devreme, încă din perioada de specializare a utilizatorului, respectiv cea de studii. Abordarea securității cibernetice ca o preocupare de zi cu zi poate fi realizată doar dacă utilizatorii capătă interes pentru aceasta, iar programe educaționale axate pe securitatea cibernetică sunt o importantă resursă de pregătire în acest sens.

2. Propuneri și recomandări – Abc-ul utilizatorului serviciilor din spațiul cibernetic

Specialiștii în securitate cibernetică iau în considerare trei principii fundamentale atunci când evaluează protecția informațiilor. Acestea sunt confidențialitatea, integritatea și disponibilitatea, componentele constitutive a ceea ce este cunoscut sub numele de triada CIA (Confidentiality, Integrity și Availability), ilustrată în Figura nr. 2. Triada este utilizată pe scară largă de către organizații pentru a implementa controale și politici de securitate adecvate, ceea ce ajută la identificarea problemelor și a soluțiilor necesare.

Figura nr. 2 – Triada CIA
(Concepție proprie)

În ceea ce priveşte ***principiul confidenţialităţii***, acesta stabileşte utilizatorii şi de procesele, cu nivelul de autorizare adecvat pentru a putea accesa anumite date.

În acest caz, ameninţările cibernetice se pot manifesta printr-un acces intenţionat, cum ar fi un intrus care pătrunde în reţeaua de calculatoare şi citeşte informaţii confidenţiale sau printr-un acces neintenţionat, cauzat de neglijenţă sau lipsa anumitor cunoştinţe sau competenţe ale persoanelor care manipulează informaţiile confidenţiale. Cele mai comune ameninţări la adresa confidenţialităţii informaţiilor sunt: ascultarea traficului în reţea (eavesdropping), decriptarea (encryption cracking), software maliţios în interiorul sistemului (malicious insider), atac de interceptare a datelor de tipul man-in-the-middle.

Există o serie de măsuri care pot fi luate pentru a garanta confidenţialitatea, cum ar fi autentificarea multi-factor, parole puternice, criptare, segregarea datelor şi atribuirea utilizatorilor niveluri de privilegii de utilizator adecvate, utilizarea unei arhitecturi a reţelei în care există o zonă/subreţea demilitarizată (DMZ) şi o zonă/subreţea internă (privată).

În ceea ce priveşte ***principiul integrităţii***, acesta se referă la asigurarea faptului că informaţiile rămân nealterate de procesele sau accesul neautorizat, de la originea lor până la utilizarea lor şi pe tot parcursul ciclului de viaţă al datelor, având în vedere principalele provocări ce ar putea afecta integritatea acestora, respectiv factorul uman şi compromiterea sistemului informatic.

Pentru a preveni modificările nedorite şi pentru a garanta că informaţiile pot fi restabilite dacă sunt modificate, implementarea copiilor de rezervă (data backup) regulate este esenţială, precum şi implementarea eficientă a privilegiilor de acces, controale de versiune, sume de control (checksum), hashing, utilizarea reţelelor private virtuale (VPN) şi utilizarea unei arhitecturi a reţelei în care există o zonă/subreţea demilitarizată (DMZ) şi o zonă/subreţea (privată).

În ceea ce priveşte ***principiul disponibilităţii***, acesta se referă la obiectivul de a garanta că informaţiile sunt disponibile utilizatorilor ori de câte ori este necesar. Indisponibilitatea informaţiilor poate apărea adesea din cauza atacurilor de tip DDOS (Distributed *Denial of Service*), a pierderii capacităţii de procesare cauzate de calamităţi naturale sau incendii, de

software maliţios sau de utilizarea unei lăţimi de bandă insuficientă pentru traficul de date.

Printre cele mai utilizate metode de asigurare a disponibilităţii datelor unei organizaţii regăsim următoarele: actualizarea tuturor sistemelor critice, protecţia împotriva atacurilor DDOS (Distributed *Denial of Service*), asigurarea redundanţei, clustere cu disponibilitate ridicată, recuperare în caz de dezastre, firewall şi servere proxy, asigurarea lăţimilor de bandă adecvate şi utilizarea controalelor de acces.

Unele cercetări în domeniul securităţii cibernetice au extins acest model de securitate a informaţiilor şi sugerează incluzând o a patra caracteristică, considerată de altfel esenţială. Astfel, noul model urmăreşte următoarele principii: confidenţialitate, integritate, disponibilitate şi responsabilitate (cunoscută şi sub numele de nonrepudiere[7]). În acest context, **principiul responsabilităţii** se referă la capacitatea organizaţiei de a urmări activităţile informatice efectuate de un individ sau de un proces specific, acestea neputând fi negate. Trasabilitatea activităţii informatice asigură faptul că un utilizator nu poate nega acţiunea sau inacţiunea sa (spre exemplificare: autenticitatea semnăturii sale sau acţiunea de a trimite un email).

Având în vedere faptul că aceste principii dispun de o serie de resurse ce pot fi dificil de identificat, înţeles sau implementat de către utilizatori, apare necesitatea unei pregătiri de bază a utilizatorului în vederea familiarizării acestuia cu conceptul de securitate cibernetică, cu responsabilitatea pe care o poartă în acest sens, precum şi cu principalele instrumente folosite, indiferent de domeniul de activitate al utilizatorului sau al competenţelor deţinute.

Până la contactul cu strategiile organizaţionale axate pe securitate şi programele de instruire ale companiilor, utilizatorii pot beneficia de o serie de informaţii din alte surse. În acest sens, crearea unor programe educaţionale axate pe securitatea cibernetică, care să poată fi introduse în schemele de învăţământ universitar, dar şi la nivelul programelor de specializare în diverse domenii, reprezintă pentru societatea modernă o nevoie în creştere, ce rezidă dintr-o altă nevoie, respectiv cea de

[7] Merill W et al, 2020. *Using the security triad to assess blockchain technology in public sector applications*. International Journal of Information Management, 2020, vol. 52, p. 3.

conştientizare a securităţii cibernetice şi a efectului acţiunilor fiecărui individ în acest sens.

Concluzii

Expansiunea rapidă a mediului virtual şi intensificarea procesului de digitalizare vor determina, cu siguranţă, o intensificare a atacurilor cibernetice pe toate planurile, de la cel individual, la cel economic şi guvernamental. Pandemia COVID-19 a accelerat nu doar transferul multiplelor activităţi cotidiene în mediul virtual, dar şi creşterea importanţei securităţii cibernetice ca punct central al siguranţei companiilor.

Încă din perioada pre-pandemică, studiile au evidenţiat faptul că cel mai mare risc în apariţia unui atac cibernetic este utilizatorul sistemului informatic sau resursa umană, acest aspect fiind din nou demonstrat odată cu intensificarea fenomenului de „lucru de la distanţă", când tot mai multe birouri ale companiilor au fost transferate „virtual" în locuinţele angajaţilor.

În acest context, înţelegerea faptului că elementul uman al securităţii cibernetice este la fel de important precum componenta tehnică reprezintă primul pas în construirea unor protocoale sustenabile care să ţină cont, pe lângă evoluţia tehnologică şi de punctele forte şi de punctele slabe ale fiecărui individ. Companiile pot astfel opta pentru implementarea unei strategii de apărare cibernetică axată şi pe instruirea angajaţilor, în vederea dezvoltării unei abordări preventive şi de conştientizare a propriilor acţiuni sau inacţiuni.

Însă, conştientizarea comportamentului în domeniul securităţii cibernetice poate debuta mult mai devreme prin crearea de programe educaţionale la nivel universitar care să furnizeze informaţiile de bază în materie de securitate, punând accentul pe diferite contexte şi domenii de specializare. Astfel, educaţia în domeniu securităţii cibernetice poate dobândi un caracter continuu (mediu academic – mediu organizaţional), fiind direcţionată, acţionabilă, realizabilă şi putând oferi feedback la fiecare nivel.

BIBLIOGRAFIE

AL-GHAMDI M.I., *Effects of knowledge of cyber security on prevention of attacks. Materials Today:* Proceedings, disponibil la https://doi.org/ 10.1016/j.matpr.2021.04.098, accesat la 18.08.2021;

ALHARBI T., TASSADDIQ, A., *Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data and Cognitive Computing*, 5(23), 2021, pp. 1-15;

AL-MUHTADI J. et al,. *A lightweight cyber security framework with context-awareness for pervasive computing environments. Sustainable Cities and Society*, 2021;

ESET. *Cyberchology the Human Element*, disponibil la https://-workplaceinsight.net/wp-content/uploads/2020/ 11/ESET_Cyberchology.pdf, accesat la 25.08.2021

GRAYSON, K., *Improve employees' cyber security awareness*. Computer Fraud & Security, August 2019, vol. 8, 2019, pp. 12-13;

IBM, *Cost of Data Breach Report*, p. 47, disponibil la https://liangroup.-net/¬blog¬/-wpcontent/uploads/2021/ 07/ Cost-of-a-Data-Breach-Report-2021.pdf, accesat la 25.08.2021;

KRITZINGER E., VON SOLMS S.H., *Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security*, 29, 2021, pp. 840-847;

MERILL, W. et al, *Using the security triad to assess blockchain technology in public sector applications*, International Journal of Information Management, 2020, vol. 52, p. 3;

National Institute of Standards and Technology, 1998. NIST Special Publication 800-16, p. 15, disponibil la https://nvlpubs.-nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.-pdf, accesat la 25.08.2021;

NOBLES, C., Shifting the Human Factors Paradigm in Cybersecurity, NIST,2018, disponibil la https://csrc.nist.gov/CSRC/media/-Events/Federal-Information-Systems-Security-Educators-As/documents/17.pdf, accesat la 26.08.2021;

ORACLE, 2018. Security in the Age of AI, disponibil la https://www.oracle.com/a/ocom/docs/data-security-report.-pdf, accesat în data de 26.08.2021.