DIVERSIFICAREA AMENINŢĂRILOR CIBERNETICE ÎN CONTEXTUL EVOLUŢIEI PANDEMIEI DE SARS-CoV-2

DIVERSIFICATION OF CYBER THREATS IN THE CONTEXT OF THE EVOLUTION OF THE SARS-CoV-2 PANDEMIC

Lt.col.drd. Ovidiu-Dumitru RUSU*
Cdor.prof.univ.dr. Sorin TOPOR**

Odată cu declanşarea pandemiei de SARS-CoV-2 provocările în domeniul comunicaţiilor, tehnologiei informaţiei şi securităţii cibernetice au devenit mult mai numeroase şi complexe în acelaşi timp. Continuarea realizării transferului anumitor activităţi cotidiene în spaţiul cibernetic va da naştere la noi provocări majore, cu multe elemente de noutate şi cu multe necunoscute. Este greu de previzionat cum va evolua spaţiul virtual în viitor şi cum va răspunde cerinţelor formulate de societate. Entităţile statale sau nonstatale sunt nevoite să se adapteze rapid la noile cerinţe ale spaţiului cibernetic. Istoria ne-a demonstrat că schimbările majore vor genera inevitabil alte schimbări la care societatea va trebui să găsească soluţiile adecvate care să-i asigure continuitatea. Evoluţia societăţii în pandemia de SARS-CoV-2 ne demonstrează în fiecare zi că dezvoltarea infrastructurii de comunicaţii şi tehnologiei informaţiei, precum şi asigurarea securităţii cibernetice sunt elemente esenţiale, fără de care anumite sectoare de activitate nu pot funcţiona la parametri normali.

With the onset of the SARS-CoV-2 pandemic, the challenges in communications, information technology and cybersecurity have become much more numerous and complex at the same time. The continued transfer of certain daily activities in cyberspace will give rise to new major challenges, with many elements of novelty and unknown. It is difficult to predict how the virtual space will evolve in the future and how it will respond to the requirements formulated by society. State or non-state entities need to adapt quickly to the new demands of cyberspace. History has shown us that major changes will inevitably lead to other changes in which society will have to find the right solutions to ensure its continuity. The evolution of society in the SARS-CoV-2 pandemic shows us every day that the development of communications infrastructure and information technology, as well as ensuring cyber security, are essential elements without which certain sectors of activity cannot function at normal parameters..

Cuvinte-cheie: ameninţări cibernetice; comunicaţii şi tehnologia informaţiei; spaţiul cibernetic; securitate cibernetică; SARS-CoV-2.
Keywords: *cyber threats; communications and information technology; cyberspace; cybersecurity; SARS-CoV-2.*

Pentru prima dată, genomul SARS-CoV a fost identificat în aprilie 2003, ca urmare a declanşării epidemiei cu aceeaşi denumire în state aflate în regiunea asiatică. La acea vreme, SARS-CoV (Severe Acute Respiratory Syndrome CoronaVirus) era privit ca o tulpină de virus care infecta, cu precădere, celulele epiteliale din plămâni.

În urma studiilor efectuate de specialiştii în domeniu, s-a stabilit că această tulpină de virus a fost dezvoltată iniţial de diverse animale (în special civetele de palmier şi liliecii), iar ulterior, SARS-CoV a fost transferat şi la persoane[1].

Bilanţul deceselor înregistrate în anul 2003, ca urmare a dezvoltării pandemiei de SARS-CoV-1 (denumită după declanşarea pandemiei din anul 2020), a fost de circa 774 de persoane[2].

În ceea ce priveşte istoricul SARS-CoV-2, acesta este bine cunoscut, pentru că este un eveniment care a fost declanşat recent şi care încă se află în derulare. Cu toate acestea, dorim să reamintim faptul că SARS-CoV-2 a fost identificat pentru prima oară în 08.12.2019 în localitatea Wuhan, China, iar Organizaţia Mondială a Sănătăţii (OMS) a fost notificată despre existenţa sa în 31.12.2019.

Cu toate că, la începutul pandemiei de SARS-CoV-2, multe state erau reticente în ceea

***Universitatea Naţională de Apărare „Carol I”**
e-mail: *rusuodumitru@yahoo.com*
****Universitatea Naţională de Apărare „Carol I”**
e-mail: *sorin_topor@yahoo.com*

ce privește efectele și rapiditatea de răspândire a acestui virus, la 11.03.2020, Organizația Mondială a Sănătății a declarat SARS-CoV-2 pandemie mondială. Efectele dezastruoase provocate de SARS-CoV-2, precum și răspândirea fulgerătoare a SARS-CoV-2 au determinat statele lumii să adopte de urgență o serie de măsuri fără precedent, care au condus, inevitabil, la o schimbare radicală a modului de viață al cetățenilor. Măsurile întreprinse pentru combaterea pandemiei de SARS-CoV-2 au fost graduale și au condus, în final, la o închidere aproape totală, dar temporară, a activităților desfășurate pe întreg mapamondul (transporturi, învățământ, comerț, turism etc.). Aceste restricții impuse de instituțiile guvernamentale au generat o serie de modificări majore în modul de viață al cetățenilor. Una dintre măsurile cele mai eficiente, impuse pentru evitarea răspândirii SARS-CoV-2, a fost respectarea distanțării sociale a persoanelor, care a determinat un transfer al multor activități în spațiul virtual.

Nu era chiar un element de noutate, pentru că deja multe activități se desfășurau în spațiul virtual (comerțul electronic, învățământul la distanță prin platforme de tip e-learning etc.), însă ceea ce a surprins a fost faptul că infrastructura existentă nu era pregătită să suporte un transfer atât de mare de informații. Capacitatea informațiilor și serviciile solicitate în spațiul virtual au atins niveluri la care infrastructura de comunicații și tehnologia informației le-a făcut față cu anumite limitări.

Treptat, infrastructura de comunicații și tehnologia informației au început să funcționeze la parametri normali, însă nu oricum, ci cu investiții masive. Însă, pentru ca activitățile în spațiul virtual să se desfășoare într-un mod normal și sigur, au fost și încă sunt necesare investiții care să permită dezvoltarea infrastructurilor de comunicații și tehnologiei informației.

Chiar dacă, înaintea declanșării pandemiei de SARS-CoV-2, dezvoltarea infrastructurilor de comunicații și tehnologia informației constituiau deja obiective prioritare, planificate într-un anumit orizont de timp, odată cu apariția COVID-19, termenele au trebuit să fie devansate astfel încât oamenii să poată desfășura anumite activități în condiții de siguranță și de securitate cibernetică.

Măsurile anti-SARS-CoV-2 au scos la iveală dependența funcționării anumitor sectoare de activitate (și nu puține) de infrastructura de comunicații și tehnologia informației, și a determinat alocarea de fonduri suplimentare pentru a putea dezvolta și extinde spațiul virtual în condiții de securitate cibernetică.

Pandemia de SARS-CoV-2, prin restricțiile impuse, a arătat faptul că lipsa competențelor digitale, într-o lume în care spațiul virtual a devenit vital, generează o serie de probleme, care pot fi remediate cu greu.

Această pandemie de SARS-CoV-2 a generat o serie de noi provocări care au determinat și vor determina statele lumii să adopte măsuri fără precedent, care vor impune un nou mod de viață dependent de spațiul virtual.

Atacuri cibernetice în contextul SARS-CoV-2

Transferul multor activități din mediul obișnuit către spațiul virtual a generat în mod inevitabil și o creștere a amenințărilor, vulnerabilităților și implicit a riscurilor la care persoanele care folosesc spațiul virtual sunt expuse.

În acest sens, la 22.10.2020, șeful Departamentului de securitate cibernetică Cyberint, din cadrul Serviciului Român de Informații (SRI), Anton Rog, a declarat că „pandemia SARS-CoV-2 a creat un mediu special de care atacatorii cibernetici au profitat, în special din cauza lipsei de informații cu care ne confruntăm toți, mai ales în luna martie 2020, când am semnalat public faptul că numărul și complexitatea atacurilor cibernetice au crescut, principalul subiect folosit de atacatori fiind un presupus tratament miraculos”[3].

De asemenea, cu aceeași ocazie, șeful Departamentului de securitate cibernetică Cyberint, din cadrul Serviciului Român de Informații, a precizat că principalele atacuri cibernetice înregistrate în perioada pandemiei de SARS-CoV-2 au fost cele de tip *ransomware* și înșelăciune. Aceste două tipuri de atacuri cibernetice au vizat, cu precădere, instituții din sistemul de sănătate, din sistemul bancar, din sistemul administrațiilor locale și centrale, precum și din sistemul de învățământ.

Într-o declarație anterioară, publicată la 14.08.2020, Anton Rog a dezvăluit faptul că, în timpul pandemiei de SARS-CoV-2, anumite entități statale (fără a preciza identitatea acestora) au desfășurat atacuri și operații cibernetice în scop de spionaj cibernetic[4]. În opinia sa, atacatorii cibernetici au utilizat tehnici de inginerie socială prin intermediul unor e-mailuri, care au fost

diseminate către anumite persoane angajate în instituțiile statului român. Conținutul mesajelor se referea, în principal, la aspecte legate de pandemia de SARS-CoV-2 (cum trebuie să te protejezi, statistici legate de numărul de infectați etc.). În același timp, oficialul din cadrul Serviciului Român de Informații a mărturisit că una dintre țintele principale ale atacatorilor cibernetici a constituit-o sistemul sanitar, prin instituțiile sale aferente[5].

În Buletinul special CYBERINT în contextul COVID-19, publicat de Serviciul Român de Informații, sunt detaliate principalele tipuri de atacuri cibernetice înregistrate la nivel mondial.

Astfel, specialiștii în domeniul cibernetic din cadrul Serviciului Român de Informații apreciază că, de la începutul declanșării pandemiei de SARS-CoV-2 și până în prezent, au fost înregistrate, cu precădere, următoarele tipuri de atacuri cibernetice:

- ransomware (Covidlock, Netwalker, Maze, Nemty);
- web defacement;
- troian bancar (Cerberus android banker, Qbot)[6].

Covidlock este un atac cibernetic de tip ransomware care se transmite prin intermediul aplicației mobile COVID-19 Tracker. Prin această aplicație, este blocat dispozitivul și conform caracteristicilor tipurilor de atacuri ransomware, se solicită achitarea unei sume de bani în format digital, pentru a permite accesul proprietarului terminalului la propriile informații.

Netwalker a fost identificat pentru prima dată în anul 2019 și a fost creat de un grup de criminalitate cibernetică, autointitulat ”Circus spider”. Principalele caracteristici ale acestui tip de atac ransomware sunt următoarele:

- acționează pe dispozitive care au instalat sistemul de operare Windows 10;
- are ca țintă predilectă dispozitivele folosite în scop personal;
- dispune de capabilități specifice, care-i permit să evite sistemele antivirus.

De asemenea, Maze aparține categoriei atacurilor cibernetice de tip ransomware și folosește, ca vectori de propagare, mesaje de tip phishing sau vulnerabilități ale protocoalelor de comunicații la distanță. Tehnicile utilizate de atacatorii cibernetici sunt cele clasice, identificarea unor credențiale slabe sau transmiterea unor documente cu extensia .docx, pentru accesare.

Nemty reprezintă un alt tip de atac cibernetic care aparține familiei ransomware. Acesta a fost identificat în august 2019 de către specialiștii în domeniul cibernetic ai companiei americane de programe informatice McAffe. Nemty acționează în scopul blocării accesului proprietarului dispozitivului la informații, prin criptarea acestora, procedând, în același timp, la ștergerea copiilor de rezervă ale datelor și informațiilor.

La 20.10.2020, The European Union Agency for Cybersecurity (ENISA) a publicat *List of top 15 threats from January 2019 to April 2020*, unde sunt prezentate în mod detaliat principalele amenințări cibernetice înregistrate în perioada menționată. În acest document complex, specialiștii în domeniul securității cibernetice au analizat în amănunt fiecare amenințare, prezentând, cu precădere, vectorii de propagare, tendințele actuale și viitoare ale amenințărilor și vulnerabilităților, precum și principalele măsuri de prevenție și securitate cibernetică.

Conform *List of top 15 threats from January 2019 to April 2020*, principalele 15 amenințări cibernetice identificate au fost următoarele: malware, web based attack, phishing, web application attack, spam, DDOS, identity theft, data break, insider threat, botnets, physical manipulation, information leakage, ransomware, cyberspionage and cryptojacking. La o primă analiză a documentului, observăm că cele 15 amenințări cibernetice identificate în cadrul acestui document sunt aceleași celor publicate, în ianuarie 2019, în Threat Landscape Report 2018 ENISA, cu mici modificări în ceea ce privește ordinea în clasament.

Necesitatea asigurării securităţii cibernetice în spaţiul virtual

Declanșarea pandemiei de SARS-CoV-2 și adoptarea unor măsuri restrictive pentru diminuarea efectelor generate de aceasta au condus în mod inerent la modificări majore în ceea ce privește modul de viață al cetățenilor.

În urma măsurilor adoptate de instituțiile guvernamentale ale statelor, foarte multe activități au migrat din mediul lor obișnuit către spațiul cibernetic. Necesitatea de a comunica, de a învăța, de a munci etc., într-un cuvânt, „nevoia de a trăi”, este dependentă din ce în ce mai mult de spațiul virtual.

Investițiile masive în tehnologizarea infrastructurii de comunicații și tehnologiei informației reprezintă o condiție necesară, însă nu și suficientă. Pentru a transfera o parte din modul nostru de viață din mediul actual către spațiul cibernetic, avem nevoie de certitudinea că acesta este sigur, stabil, accesibil și eficient. Cu siguranță că există și alte condiții pe care spațiul cibernetic trebuie să le asigure utilizatorilor în vederea desfășurării unor activități virtuale normale, fără riscuri asumate.

Într-un articol, publicat, în anul 2020, de compania Harvey Nash (furnizor global de servicii de consultanță în recrutare și externalizare IT) se menționează că, de la începutul pandemiei de SARS-CoV-2, companiile intervievate au cheltuit sume uriașe pentru dezvoltarea infrastructurii de comunicații și tehnologiei informației și, de asemenea, pentru asigurarea securității cibernetice. Cu toate acestea, în același articol se subliniază că aceste investiții nu au putut să stopeze atacurile cibernetice. În sondajul efectuat, la care au participat circa 4.200 de specialiști în domeniul tehnologiei informației, 4 din 10 lideri IT au declarat că, în perioada pandemiei, au înregistrat o creștere a atacurilor cibernetice. Cele mai importante amenințări cibernetice au fost de tip phishing și malware[7].

Apreciem că unul dintre factorii care au contribuit la creșterea amenințărilor cibernetice în perioada pandemiei de SARS-CoV-2 a fost faptul că o bună parte din populația activă a început să lucreze de acasă, fiind mult mai expusă atacurilor cibernetice tocmai din cauza măsurilor minime sau, uneori, inexistente de securitate cibernetică. Printre acestea, am dori să menționăm lipsa unei culturi adecvate de securitate, dotarea cu echipamente și programe care nu asigură securitatea cibernetică, informarea din surse neoficiale etc.

În acest context, afirmăm că investițiile vor trebui să vizeze atât infrastructura de comunicații și tehnologia informației, cât și asigurarea cu resurse a securității cibernetice.

Lipsa securității cibernetice în spațiul virtual poate avea consecințe grave atât asupra securității actorilor statali sau nonstatali, cât și asupra securității cetățenilor.

Concluzii

Pandemia de SARS-CoV-2, prin măsurile întreprinse și efectele generate, a dezvăluit lumii întregi un nou mod de viață, simbioza absolut necesară dintre om și spațiul cibernetic. Activitățile umane sunt tot mai dependente de spațiul virtual, ceea ce ne face și mai responsabili în ceea ce privește realizarea securității cibernetice. Un spațiul virtual securizat generează în mod automat un confort pentru cetățenii care desfășoară diverse activități cotidiene. Adresându-ne o singură întrebare: *Cum am fi trăit în pandemie fără existența spațiului cibernetic?*, ne dăm seama că variabilele într-o astfel de ecuație ar fi fost cu totul altele.

Progresul omenirii obținut și datorită existenței infrastructurii de comunicații și tehnologiei informației nu poate fi negat, ci trebuie recunoscut, susținut, continuat și folosit în scopuri nobile.

În virtutea celor prezentate anterior, pentru asigurarea unei infrastructuri moderne de comunicații și tehnologiei informației, cu o securitate cibernetică performantă, în contextul evoluției pandemiei de SARS-CoV-2, propunem următoarele:

- alocarea de fonduri suficiente pentru dezvoltarea infrastructurii de comunicații și tehnologiei informației;
- asigurarea unui spațiu virtual normal și sigur prin implementarea unor soluții eficiente de securitate cibernetică;
- continuarea pregătirii și susținerea unei resurse umane calificate care să realizeze securitatea cibernetică a infrastructurii de comunicații și tehnologiei informației;
- asigurarea accesului la Internet pentru toți cetățenii, astfel încât aceștia să-și poată desfășura activitățile în spațiul cibernetic;
- asigurarea alfabetizării digitale a tuturor cetățenilor prin organizarea de programe dedicate în acest sens.

NOTE:

1 https://www.chinadaily.com.cn/china/2006-11/23/content_740511.htm, accesat la 29.12.2020.

2 https://romania.europalibera.org/a/coronavirus-de-ce-%C3%AEn-epidemia-de-sars-%C3%AEn-2003-au-murit-mult-mai-pu%C8%9Bini-oameni/30545956.html, accesat la 29.12.2020.

3 https://economie.hotnews.ro/stiri-telecom-24369538-oficiali-din-guvern-sri-confruntam-adevarata-pandemie-spatiul-cibernetic-victime-fost-romania-semnalul-alarma-privinta-securitatii-5g.htm, accesat la 29.12.2020.

4 *Ibidem*.

5 https://www.digi24.ro/interviurile-digi24-ro/cine-sunt-spionii-din-telefon-si-din-calculator-interviu-cu-

directorul-cyberint-anton-rog-1352811, accesat la 30.12.2020.

6 [Serviciul Român de Informații], *Buletinul special CYBERINT în contextul COVID-19*, pp. 5-6, 2020.

7 https://home.kpmg/xx/en/home/media/press-releases/2020/09/covid-19-forces-one-of-the-biggest-surges-in-technology-investment-in-history-finds-worlds-largest-technology-leadership-survey.html, accesat la 30.12.2020.

BIBLIOGRAFIE

*** *Threat Landscape – Cyber espionage*, ENISA, 2020.

*** *Threat Landscape – List of top 15 threats*, ENISA, 2020.

*** *Strategia naţională de apărare a României pentru perioada 2020-2024*, București, 2020.

[Ministerul Apărării Naționale], *Carta albă a apărării*, București, 2020.

[Serviciul Român de Informații], *Buletinul CYBERINT*, semestrul I, 2020.

[Serviciul Român de Informații], *Buletinul special CYBERINT în contextul COVID-19*, 2020.

https://home.kpmg/.html

https://www.defense.ro

https://www.sri.ro

https://certmil.ro

https://www.chinadaily.com.cn/china/2006-11/23/content_740511.htm

https://romania.europalibera.org/a/coronavirus-de-ce-%C3%AEn-epidemia-de-sars-%C3%AEn-2003-au-murit-mult-mai-pu%C8%9Bini-oameni/30545956.html

https://economie.hotnews.ro/stiri-telecom-24369538-oficiali-din-guvern-sri-confruntam-adevarata-pandemie-spatiul-cibernetic-victime-fost-romania-semnalul-alarma-privinta-securitatii-5g.htm.

https://www.digi24.ro/interviurile-digi24-ro/cine-sunt-spionii-din-telefon-si-din-calculator-interviu-cu-directorul-cyberint-anton-rog-1352811