SECURITATEA CIBERNETICĂ
– MAREA PROVOCARE A SECOLULUI XXI –

Dr. Petru-Viorel ENE
Direcţia pentru Relaţia cu Parlamentul, Ministerul Apărării Naţionale

Securitatea cibernetică este esenţială pentru indivizi, companii, guverne şi naţiuni, în ansamblul lor. Pe măsură ce societatea și economia noastră tind spre digitalizare, tehnologiile utilizate sunt înlocuite, actualizate și modificate constant. Ca răspuns, criminalii cibernetici acordă mai multă atenție modului în care folosesc tehnologia pentru a se implica în activități rău intenționate în mediul digital. În acest context, spațiul cibernetic, aflat în continuă schimbare, generează atât oportunități de dezvoltare, cât și noi provocări. Toate aceste vulnerabilități fac din securitatea cibernetică o prioritate majoră pentru toate entitățile.

Guvernele lumii au decis să investească un volum semnificativ de resurse materiale pentru protecția datelor, deoarece orice investiție inițială este mult mai redusă decât fondurile necesare pentru a înlătura urmările unui atac cibernetic. Pe de altă parte, un incident de securitate cibernetică într-o anumită țară poate foarte bine să aibă impact în afara granițelor țării. Așadar, ce etape trebuie să urmăm?

Cuvinte-cheie: reţea, securitate, ameninţare, digitalizare, vulnerabilitate.

INTRODUCERE

În momentul în care internetul a început să se extindă, multe voci optimiste au prezis beneficiile pe care le implică. În acest context, suntem siguri că acestea sunt absolut fabuloase, dacă luăm în calcul impactul asupra sectorului economic și al volumului de informații la care avem acces.

La nivel european, asistăm la o necesitate acută pentru un spațiu cibernetic mai sigur și, prin urmare, trebuie să susținem eforturile de definire a normelor de conduită în spațiul cibernetic la care toate părțile interesate sunt invitate să adere. În această privință, cetățenii Uniunii Europene trebuie să își respecte obligațiile civile, responsabilitățile sociale și actele normative care reglementează mediul on-line, astfel încât statul să acționeze în conformitate cu normele în vigoare. Dezvoltarea capacităților în domeniul securității cibernetice este o responsabilitate atât pentru sectorul privat, cât și pentru cel public, dar, în același timp, societatea civilă trebuie să ajute la construirea unui spațiu cibernetic sigur.

Totodată, expansiunea mediului on-line, conectivitatea extinsă la nivel global și impactul spațiului cibernetic în lumea fizică au generat nenumărate provocări. În această privință, toate statele trebuie să coopereze, deoarece un incident de securitate cibernetică ce are ca țintă o anumită țară va avea efecte și în afara granițelor acelei țări. Mai mult, furnizorii de servicii de rețea operează, de obicei, la nivelul tuturor țărilor membre aleUniunii Europene și aici ne referim, în special, la companiile de telecomunicații și furnizorii de servicii de internet. Este deosebit de dificil pentru aceștia să își adapteze întregul sistem în concordanță cu cerințele fiecărei țări în parte.

O importantă condiție prealabilă pentru un mediu on-line gratuit, deschis și sigur cu toate beneficiile pe care le presupune pentru societățile din întreaga lume este să se mențină o permanentă cooperare între cei mai relevanți actori interesați de acest domeniu[1]. Aceasta este o prioritate la nivelul comunității europene, după cum reiese din măsurile luate de Agenția Europeană de Apărare, care dezvoltă capacități de apărare în spațiul cibernetic, pentru a consolida dialogul dintre civili și militari în acest domeniu.

În ultimii ani, statele membre ale Uniunii Europene au recunoscut necesitatea de prevenire a incidentelor de securitate și au pornit, spre exemplu, scheme de raportare a incidentelor pentru o mai mare transparență[2].

[1] Jochen Rehrl, *Handbook for decision makers – The common security and defence policy of the European Union,* Imprimerie Centrale, Luxembourg, 2017, p. 164.
[2] https://www.enisa.europa.eu/topics/incident-reporting?tab=details, accesat la 23.08.2019.

Având în vedere că societatea și economia se mută în spațiul digital, răspunsul la nivelul Uniunii Europene debutează cu educarea și însușirea unor anumite abilități a populației, în ansamblul ei. Avem nevoie de un spațiu cibernetic mai sigur, nu doar pentru a ne proteja datele și intimitatea, dar și pentru a preveni abuzurile sau prejudicierea sistemului nostru informatic. În acest cadru, nu doar statele, ci toți utilizatorii au un rol important în menținerea internetului cât mai sigur[3].

Am experimentat deja impactul internetului în această nouă eră digitală și putem susține că urmările acestuia pot fi devastatoare, implicând costuri uriașe, asemenea celor pe care un incident industrial sau un dezastru natural le-ar presupune. Trebuie să tratăm această problemă cu cea mai mare seriozitate și să implicăm în soluționarea ei atât statul și mediul privat, cât și cetățenii.

ÎN ADÂNCUL ATACURILOR CIBERNETICE

În ultimele două decenii, internetul și, mai general, spațiul cibernetic au avut un impact extraordinar asupra întregii societăți. Viața noastră zilnică, drepturile fundamentale, interacțiunile sociale și întreaga economie depind de funcționarea propice a întregului sistem informațional.

Pentru ca mediul cibernetic să rămână deschis, aceleași norme, principii și valori pe care Uniunea Europeană le sprijină în mediul off-line ar trebui să se aplice și în mediul on-line. Drepturile fundamentale, democrația și regulile de drept trebuie să fie protejate în mediul cibernetic. Libertatea și prosperitatea noastră depind, din ce în ce mai mult, de un mediu cibernetic inovativ, care va continua să prospere atât timp cât mediul privat și societatea civilă îi alimentează creșterea. Ceea ce este important de menționat este că libertatea în mediul on-line implică protecția și securitatea tuturor utilizatorilor[4].

Anii recenți ne-au arătat că, în timp ce lumea digitală ne aduce beneficii enorme, aceasta implică și amenințări din ce în ce mai frecvente, complexe și distructive. Uniunea Europeană și membrii săi se confruntă, din ce în ce mai des, cu amenințări neconvenționale ce au caracter global și transfrontalier și un puternic efect distrugător la nivelul comunității. Printre aceste amenințări, propagarea atacurilor cibernetice capabile să distrugă infrastructura critică reprezintă o problemă majoră.

Unele caracteristici definitorii ale amenințărilor neconvenționale sunt reprezentate de faptul că nu sunt executate și nici nu pot fi combătute exclusiv prin mijloace militare și nu se califică pentru a fi încadrate în categoria atacului armat, în sensul

[3] https://www.enisa.europa.eu/media/multimedia/videos/cybersecurity-is-a-shared-responsibility-european-cyber-sec urity-month-2018, accesat la 23.08.2019.

[4] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accesat la 23.08.2019.

prevederilor articolului 5 din Tratatul Atlanticului de Nord[5], ignoră orice graniță, au ca țintă atât persoanele în individualitatea lor, cât și companiile, au un impact psihologic și economic major și necesită informații și capacități distincte pentru a putea fi detectate, prevenite și atribuite.

Aceste caracteristici înseamnă că eforturile pur naționale au un impact limitat, asemenea măsurilor tradiționale referitoare la securitate și apărare națională. În acest context, Uniunea Europeană este într-o postură unică pentru promovarea necesității unei mai profunde sinergii între securitatea internă și cea externă[6].

Uniunea Europeană, dar și statele membre ale NATO au făcut pași importanți în securitate cibernetică, în ultimii ani. Necesitatea consolidării capabilităților și a cooperării în vederea apărării în fața unor astfel de atacuri au fost inițial recunoscute de liderii aliați la Summitul din Praga, din anul 2002[7]. De atunci, securitatea mediului digital a devenit un important obiectiv pe agenda tuturor.

Lipsa granițelor internetului a devenit unul dintre cele mai puternice instrumente pentru procesul globalizării, chiar și fără supraveghere și reglementare din partea guvernelor. În timp ce sectorul privat ar trebui să continue să joace un rol dominant în construcția mecanismelor de utilizare zilnică a internetului, nevoia de transparență, responsabilitatea și securitatea devin din ce în ce mai proeminente. Aceste ultime probleme trebuie să reprezinte o prioritate pentru toate statele și trebuie ca acestea să își ghideze politica de securitate cibernetică în direcția luptei cu toate amenințările care își fac simțită prezența.

Amenințările în acest domeniu sunt lansate de entități ostile, statale sau nestatale, asupra sistemelor informatice de interes strategic ale instituțiilor și companiilor. În această categorie includem, de asemenea, atacurile cibernetice dezvoltate de diferite grupări teroriste. Toate aceste atacuri vor afecta, în mod direct, securitatea țării[8].

Pentru a oferi o privire de ansamblu asupra acestui fenomen, este important să facem o scurtă analiză a amenințărilor cibernetice și a impactului acestora, mai întâi, în România și, apoi, în afara granițelor țării. În acest sens, menționăm un studiu

[5] Părţile convin că un atac armat împotriva uneia sau mai multora dintre ele, în Europa sau în America de Nord, va fi considerat un atac împotriva tuturor părţilor şi, în consecinţă, sunt de acord că, dacă are loc un asemenea atac armat, fiecare dintre ele, în exercitarea dreptului la autoapărare individuală sau colectivă, recunoscut prin art. 51 din Carta Organizaţiei Naţiunilor Unite, va sprijini partea sau părţile atacate, prin realizarea imediată, individual şi împreună cu celelalte părţi, a oricărei acţiuni pe care o consideră necesară, inclusiv folosirea forţei armate, în vederea restabilirii şi menţinerii securităţii în spaţiul Atlanticului de Nord.
Orice astfel de atac armat şi toate măsurile adoptate ca urmare a acestuia vor fi imediat aduse la cunoştinţă Consiliului de Securitate. Aceste măsuri vor înceta după adoptarea de către Consiliul de Securitate a măsurilor necesare pentru restabilirea şi menţinerea păcii şi securităţii internaţionale, https://www.nato.int/cps/en/natolive/official_ texts_17120.htm, accesat la 24.08.2019.

[6] European Political Strategy Centre, *The Defense-Security Nexus – Towards an EU Collective Security*, 2017.

[7] https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm, accesat la 24. 08.2019

[8] *Strategia națională de apărare a țării pentru perioada 2015-2019*, București, 2015, p. 14.

efectuat de Bitdefender, cea mai mare companie ce are ca obiect de activitate securitatea cibernetică și un lider în materie de programe antivirus, oferind protecție pentru mai bine de 500 de milioane de sisteme în peste 150 de țări.

Conform reprezentanților acestei companii, România este țara cea mai afectată de Scranos, o amenințare informatică agresivă, ce compromite activitatea victimelor și sustrage toate parolele și informațiile bancare ale acestora. Bitdefender a alertat autoritățile cu privire la această amenințare care își are originea în China și care a fost descoperită în luna aprilie a acestui an, când s-a răspândit agresiv în Europa și în Statele Unite, contaminând dispozitivele cu sistem de operare Windows și Android și accesând datele personale ale victimelor[9].

Kaspersky Lab, un alt imens furnizor de servicii de securitate, ne informează că România ocupă locul al șaselea în topul țărilor amenințate de viruși de tip ransomware. Aceștia au rolul de a cripta fișierele din dispozitivele victimelor și de a transmite acesteia modalitatea de răscumpărare a informației criptate. Observăm că România este o țară atractivă pentru crimele cibernetice, iar amenințările asupra dispozitivelor mobile au evoluat în mod constant nu doar în ceea ce privește cantitatea programelor cu grad de periculozitate, ci și în ceea ce privește modul în care banii și informațiile valoroase pot fi însușite utilizând dispozitivele mobile[10].

Cercetătorii Kaspersky Lab au observat că numărul atacurilor ce au ca obiect infectarea dispozitivelor mobile cu programe compromise s-a dublat în doar un singur an. În 2018, au avut loc 116.5 milioane de atacuri, comparativ cu 66.4 milioane în anul 2017, cu o creștere semnificativă în ceea ce privește utilizatorii unici care sunt afectați[11]. Deși un program mobil este puțin probabil să pună în pericol securitatea sistemului nostru militar, trebuie să luăm în considerare faptul că, pe de o parte, asistăm la un permanent și sistematic atac și, pe de altă parte, numărul în continuă creștere al atacurilor trebuie să fie un semnal de alarmă pentru a demara o abordare meticuloasă cu obiectivul de a securiza mediul on-line.

Am arătat că fiecare cetățean poate fi ținta unui atac cibernetic, dar aceasta este, de asemenea, o problemă permanentă pentru guverne și sectorul privat. În acest scop, statele membre ale Uniunii Europene au simțit nevoia să reglementeze această problemă sensibilă, născându-se, astfel, Strategia Națională de Securitate Cibernetică, atât la nivelul Comunității, cât și al statelor membre.

În ceea ce privește țara noastră, scopul Strategiei Naționale de Securitate Cibernetică a României este de a menține un mediu virtual sigur, cu un înalt grad de reziliență și de încredere, bazat pe infrastructurile cibernetice naționale,

[9] https://www.bitdefender.ro/news/romania-cea-mai-afectata-tara-din-lume-de-amenintarea-informatica-a-momentului-3666.html, accesat la 26.08.2019.

[10] https://securelist.com/mobile-malware-evolution-2018/89689/, accesat la 26.08.2019.

[11] https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies, accesat la 26.08.2019.

care să constituie un important suport pentru securitatea națională și buna guvernare, pentru maximizarea beneficiilor cetățenilor, mediului de afaceri și al societății românești, în ansamblul ei[12]. Acest principiu este îmbrățișat la nivelul Uniunii Europene, de vreme ce viziunea întregii comunități este de a clarifica rolul și responsabilitățile fiecăruia, de a dezvolta o protecție efectivă și de a promova drepturile cetățenilor prin salvgardarea mediului cibernetic, oferind libertate deplină și securitate tuturor beneficiarilor[13].

Rezultă din cele de mai sus că, la nivelul Uniunii Europene și al statelor membre, prioritățile planului de acțiune sunt similare. Scopul este acela de a menține securitatea mediului cibernetic, astfel încât toți cetățenii să se poată bucura de valorile democrației și de un domeniu virtual sigur atât pentru satisfacerea nevoilor personale, dar, în același timp, și pentru menținerea securității la nivelul mediului de afaceri. În acest din urmă caz, o breșă de securitate va conduce, cel mai probabil, la pagube semnificative, cu consecințe devastatoare.

Uniunea Europeană și statele membre au nevoie de o legislație puternică și care să se plieze pe specificul problematicii, deoarece evoluția tehnicilor de atac cibernetic a cunoscut o rapidă dezvoltare și, în această situație, instituțiile care au ca obiectiv aplicarea legii nu pot să combată criminalitatea din mediul on-line prin mijloace desuete. Din fericire, la nivelul Uniunii Europene, ne bazăm în continuare pe suportul instituțiilor pentru identificarea minusurilor, dar și a punctelor forte în ceea ce privește investigarea și combaterea criminalității cibernetice.

Cu toate acestea, conceptul de securitate cibernetică implică și dimensiunea apărării cibernetice. Pentru a mări durabilitatea sistemelor informaționale care se află în sprijinul acțiunilor de apărare a statelor membre și a securității lor naționale, capacitatea de apărare cibernetică trebuie să se concentreze pe detectarea, răspunsul și refacerea după un atac cibernetic sofisticat.

Așa cum am arătat mai sus, România înfruntă, în momentul de față, nenumărate amenințări la adresa infrastructurii sale. Aceasta se datorează interdependenței în continuă creștere între infrastructura cibernetică și infrastructura clasică, mai ales în arii precum sectorul bancar, transporturile, sectorul energetic și cel al apărării naționale. Observăm că există o necesitate extraordinară de acțiune în această arie, tocmai pentru a soluționa problemele care apar.

Cele mai multe organizații au dezvoltat capabilități de răspuns la incidentele cibernetice. Totuși, aceste capabilități, care de cele mai multe ori se axează pe răspunsuri pe termen scurt și probleme de IT, pot eșua în a controla impactul atacurilor. Evitarea unei crize cibernetice se rezumă, de obicei, la modul de gestionare a un incident înainte, în timpul și imediat ce acesta își produce efectele.

[12] Anexa 1 art. 2 din HG. 271/2013 pentru aprobarea *Strategiei de Securitate Cibernetică a României* și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică.

[13] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accesat la 26.08.2019.

În acest context, trebuie să aducem în discuție importanța pașilor de urmat pentru a securiza datele din mediul digital și pentru a veni cu un răspuns puternic în cazul unui astfel de atac. În această direcție, experții în domeniu vorbesc despre managementul riscurilor, în trei faze, cu oportunități uriașe de a proteja organizația în fața riscurilor și a costurilor ce însoțesc aceste breșe și de a pregăti structura pentru un răspuns conform cu dimensiunea atacului.

Disponibilitatea este faza care implică menținerea unei echipe bine pregătite, multifuncționalem care poate oricând să soluționeze toate aspectele incidentului de securitate. Pe timpul desfășurării acestei faze, este important să punem la dispoziție infrastructura necesară pentru desfășurarea unor exerciții pe tema incidentelor cibernetice, esențiale pentru stimularea cooperării între instituțiile statului și mediul privat. Bineînțeles că acest curs de acțiune implică un număr mare de experți în domeniul securității cibernetice. Din nefericire, se așteaptă o creștere a locurilor de muncă vacante în domeniu de peste 3,5 milioane, la nivel mondial[14]. Este limpede că o cooperare puternică între autoritățile competente și sectorul privat depinde de capacitatea noastră de a asigura școlarizarea necesară.

Un *răspuns nesatisfăcător*, deși are ca obiectiv înlăturarea amenințării, poate genera o criză. Răspunsurile coordonate pot limita pierderea timpului, a resurselor, dar și reputației autorității vizate. Managementul de răspuns la amenințări trebuie să asigure permanenta comunicare în media, dar și pe site-urile de socializare, astfel încât părțile interesate să aibă certitudinea că răspunsul organizației este perfect creat pentru a răspunde amenințărilor cibernetice apărute.

Etapa de *recuperare post-incident* este deosebit de importantă. Pașii de urmat pentru a reveni la un mediu de lucru firesc și limitarea pagubelor produse organizației și tuturor partenerilor își găsesc aplicabilitatea imediat după incident. Aceste măsuri includ evaluarea cauzelor și a managementului de răspuns în cazul incidentelor sau al crizelor cibernetice, ca și analizarea lecțiilor învățate în urma respectivului atac.

Un management eficient al crizelor nu se oprește la pregătirea pentru un eveniment anume, ci merge până la dezvoltarea unor capabilități flexibile care să poată oferi răspunsul potrivit la o gamă largă de evenimente de varii dimensiuni. Riscul pe care un incident de securitate îl aduce reputației unei organizații subliniază necesitatea de a contura un plan de răspuns la crize eficient, înainte ca evenimentul respectiv să aibă loc[15]. Astfel, prevenirea crimelor cibernetice este cheia pentru păstrarea acestui fenomen sub control. Însă, aceste acte ilegale prezintă particularități în ceea ce privește modul de prevenire, fiind necesară adaptarea măsurilor la specificul amenințării. Aceste particularități includ omniprezența și accesibilitatea dispozitivelor mobile, ceea ce conduce la un număr de posibile

[14] https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/, accesat la 27.08.2019.
[15] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf, accesat la 27.08.2019

victime în continuă expansiune; posibilitatea de anonimat și disimulare; natura transnațională a multora dintre crimele cibernetice și rapiditatea în inovare.

În acest scenariu, structurile implicate trebuie să reflecte asupra necesității cooperării regionale și internaționale în prevenirea crimelor cibernetice. Metodele trebuie să ofere o imagine de ansamblu asupra fenomenului, actualizată permanent, și abordările trebuie să implice în mare măsură părțile interesate și, în special, sectorul privat, care deține infrastructura necesară și operează cu preponderență în mediul on-line[16].

Atacurile cibernetice sunt variate și țintesc o multitudine de instituții publice ori private. Aceste atacuri au în vizor de la date din domeniul medical, ale cardurilor bancare, date de identificare personală, de naștere, adrese de e-mail ori numere de telefon, până la date referitoare din aria administrației publice sau fiscale, instalații nucleare sau chiar, după cum am observat, procese electorale.

Începând cu alegerile prezidențiale ce au avut loc în anul 2016, în Statele Unite ale Americii, marcate de implicarea Rusiei în procesul electoral, teama de atacuri cibernetice s-a răspândit extrem de repede. Totuși, Uniunea Europeană a recunoscut importanța securității cibernetice cu câțiva ani în urma atacurilor cibernetice din timpul campaniei electorale din SUA.

În anul 2017, Comisia Europeană a venit cu recomandări suplimentare de îmbunătățire a securității cibernetice și de încurajare a statelor membre pentru a demara investițiile necesare. Începând din acel an, o serie de măsuri au fost aplicate pentru a consolida rezistența și abilitatea de răspuns la un atac cibernetic major. Aceste măsuri includ constituirea unui Centru de Răspuns la Incidente de Securitate (CERT), care are responsabilitatea de a crea o abordare coordonată a problematicii și de a dezvolta certificate de securitate produselor și serviciilor de pe teritoriul Uniunii.

Având în vedere faptul că, recent, am experimentat un eveniment politic major la nivelul Uniunii Europene, alegerile privind Parlamentul European, trebuie să facem mențiunea că, pe lângă un atac cibernetic direct, există o amenințare acută de dezinformare ce emană de la alte state, în acest fel amestecându-se în procesul legislativ. Din nefericire, este o cale simplă și relativ frecventă de a influența, în mod indirect, opinia publică a alegătorilor. Este, de asemenea, mult mai simplu și mai sigur pentru un potențial atacator să folosească dezinformarea decât să organizeze un atac cibernetic major. Totuși, nu sunt multe de făcut în acest sens, cu excepția educării cetățenilor pentru o gândire critică[17].

Întorcându-ne la analiza începută, așa cum am menționat, în anul 2018, numărul atacurilor cibernetice s-a dublat comparativ cu o statistică din anul 2017,

[16] United Nations Office on Drugs and Crime, *Comprehensive study on Cybercrime,* New York, 2013, p. 226.
[17] https://www.esjnews.com/are-european-elections-vulnerable-to-cyber-attacks, accesat la 27.08.2019.

dar ceea ce este și mai înfricoșător este faptul că rata acestor crime cibernetice se așteaptă să fie în continuă creștere. Criminalii cibernetici găsesc modalități din ce în ce mai inteligente și mai diabolice pentru a fura date. În acest context, costul anual al daunelor produse de crime cibernetice este așteptat să atingă pragul de cinci miliarde de dolari, în anul 2020[18].

Înființat în Washington D.C. acum mai bine de 50 de ani, Centrul pentru Studii Strategice și Internaționale menționează, într-un studiu actualizat până în luna august, că mai bine de 60 de atacuri cibernetice majore au avut loc până acum[19]. Acest studiu a analizat atacurile cibernetice asupra agențiilor guvernamentale, apărare și companii *high tech* precum și crimele economice cu un cost peste pragul de un milion de dolari. Acum, putem să ne creionăm o idee despre magnitudinea acestei probleme de securitate.

Trebuie să fim conștienți de faptul că, pe lângă aceste amenințări îndreptate împotriva guvernului și a diferitelor companii private, ne confruntăm cu un risc imens în termenii securității digitale pentru cetățeni. De aceea, în Strategia de Securitate Cibernetică a Uniunii Europene și în cea a României sunt enumerate o serie de măsuri ce au ca scop promovarea unei culturi a securității în spațiul virtual. În acest sens, observăm că, pe lângă aceste măsuri ce privesc securitatea la nivel guvernamental, există o constantă necesitate de informare a populației despre riscurile și vulnerabilitățile specifice utilizării spațiului cibernetic. Mai mult, pregătirea profesională concretă și de calitate a persoanelor care lucrează în domeniul securității cibernetice și promovarea certificării reale în această arie sunt considerate elemente- cheie în procesul de consolidare a culturii cibernetice a cetățenilor[20].

SECURITATEA CIBERNETICĂ – O RESPONSABILITATE COMUNĂ

Acasă, la muncă, la școală, dependența de tehnologie, aflată în continuă creștere, solicită o mai mare securitate on-line. Cetățenii sunt prima linie de apărare împotriva acestui tip de riscuri. Din acest motiv, securitatea cibernetică este o responsabilitate comună, solicitând conștientizare și vigilență din partea fiecăruia dintre noi.

Guvernul Marii Britanii, într-un studiu recent, afirmă că patru din 10 companii (43%) și două din 10 organizații neguvernamentale (19%) au experimentat breșe cibernetice sau atacuri în ultimele 12 luni. Această statistică se modifică notabil când vine vorba de companiile mari (72%) și de organizațiile neguvernamentale cu venituri de peste cinci milioane de lire (73%). Breșele au fost identificate mai des

[18] https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/, accesat la 27.08.2019.
[19] https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents, accesat la 27.08.2019.
[20] Anexa 1 cap. III art. 3 din HG. 271/2013 pentru aprobarea *Strategiei de Securitate Cibernetică a României* și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică.

în companiile care dețin date cu caracter personal, acolo unde angajații folosesc diferite dispozitive în timpul programului de lucru sau utilizează sistemul de stocare *cloud*[21].

În conformitate cu un studiu realizat de Kaspersky, jumătate dintre companiile ce au făcut obiectul acestei analize consideră că lipsa cunoștințelor, nepăsarea sau răutatea din partea angajaților pot conduce la atacuri cibernetice. Cercetări adiționale arată că 84% dintre victimele unui atac cibernetic atribuie rezultatul, cel puțin în parte, erorii umane. În consecință, ei confirmă un alt studiu ce a fost desfășurat în anul 2016 de compania IBM și care a subliniat, în Indexul de Securitate Cibernetică din 2016, că eroarea umană este un factor major în apariția acestor breșe de securitate și vina se îndreaptă, în mare parte din cazuri, spre propriii angajați. De la e-mail-uri trimise unui alt destinatar până la expedierea datelor confidențiale unui sistem nesigur, greșelile pot fi foarte costisitoare[22].

Ca răspuns la aceste provocări, când vine vorba de acțiunea de prioritizare a atacurilor cibernetice, observăm că mare parte dintre companii consideră că înfruntă o problemă majoră. Riscurile sunt înțelese și, ca urmare, terenul de acțiune este pregătit. Un procent de 77% dintre companii consideră securitatea cibernetică o problemă foarte importantă, în timp ce 21% o consideră o problemă minoră, iar 2% nu o consideră o prioritate[23].

Pericolul din mediul on-line există pentru fiecare dintre noi. În acest domeniu al securității cibernetice, se menționează frecvent faptul că risc zero nu există. Oamenii obișnuiesc să considere că progresul tehnologic este singurul factor care le certifică securitatea, această viziune fiind clar greșită. Deși companiile mari, în mod obișnuit, alocă o mare atenție regulamentelor în această arie, breșele apar în mod inevitabil. Indiferent de câte resurse sunt alocate ori de cât timp este investit în securitatea sistemului, breșele vor continua să apară. Unul dintre motivele pentru care se întâmplă acest lucru este acela că nimic, nici chiar în această explozie tehnologică, nu poate înlocui cel mai important actor – omul[24].

Cu scopul de a sublinia rolul omului în securitatea dispozitivelor și a internetului în ansamblul său, trebuie să menționăm necesitatea pentru un constant și eficient antrenament în domeniul securității cibernetice pentru fiecare angajat în parte, deoarece, câteodată, chiar și cel mai bine intenționat angajat poate comite o greșeală care lasă întreaga organizație vulnerabilă la atacuri cibernetice.

[21] Department for Digital, Culture, Media & Sport, *Cyber Security Breaches Survey: Statistical Release,* 2018, p. 1.
[22] https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company, accesat la 28.08.2019.
[23] https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf, accesat la 28.08.2019.
[24] *People's Role in Cyber Security: Academics' Perspective,* 2014, https://www.crucial.com.au/pdf/, accesat la 28.08.2019.

În acest cadru, asigurarea securității cibernetice este o responsabilitate atât pentru stat, cât și pentru individ. Utilizatorii joacă un rol crucial în asigurarea securității rețelei: ei trebuie să fie conștienți de riscurile pe care le înfruntă în mediul on-line și să aibă capacitatea de a urma pași simpli pentru a se proteja împotriva acestor atacuri. Câteva inițiative au fost dezvoltate în ultimii ani, în acest sens. ENISA (Agenția Europeană pentru Securitate Cibernetică) a fost implicată într-o campanie de conștientizare prin publicarea unor rapoarte, organizarea unor întâlniri cu experți în domeniu și dezvoltarea parteneriatelor public-privat. Europol, Eurojust și autoritățile ce au ca scop securitatea datelor la nivel național sunt, de asemenea, permanent active în ceea ce privește aceste campanii.

Dar, aceste măsuri nu sunt suficiente pentru a reduce magnitudinea problemei. Toate aceste activități dispuse de guverne, de agenții internaționale ori internaționale rămân fără efectul scontat dacă organizația ori compania respectivă nu va face tot ceea ce este posibil pentru a educa personalul în vederea respectării regulilor pentru un spațiu cibernetic sigur.

Având în vedere faptul că, în România, există o imensă lipsă de experți în acest domeniu, este esențial ca o masă de specialiști să fie creată, sens în care guvernul, sectorul privat și mediul academic trebuie să colaboreze pentru dezvoltarea unor scheme de pregătire pentru specialiștii în domeniul IT[25]. Pe aceeași linie de acțiune, campaniile de conștientizare trebuie să fie organizate la nivel național.

Sistemul European de Schimb de Informații și Alertare, de exemplu, adună informații și materiale educaționale de la computerele echipelor de răspuns la situații de urgență din țările Uniunii. Materialele sunt, apoi, adaptate pentru diferite grupuri de cetățeni și pentru companii mici și mijlocii. Informațiile sunt diseminate prin utilizarea *social media*, a site-urilor web și prin email.

Companiile din domeniul IT, dar și organizațiile nonprofit au demarat, de asemenea, acest tip de campanii. Campania *Bine de știut* a gigantului american Google, de exemplu, a fost dezvoltată în peste 40 de limbi diferite începând cu anul 2011. Reclamele din ziare, reviste, mediul on-line și din transportul public oferă sfaturi de securitate și explică câteva noțiuni de bază, cum ar fi noțiunile de *cookie*[26] sau *adresă IP*[27]. Institutul pentru securitatea on-line a familiei a colaborat, de asemenea, cu companii din domeniul IT pentru a asigura resurse educaționale pentru părinți, copii și educatori, pe *platforma lor pentru un website bun.* Pentru o audiență mai tânără, Disney a condus, în anul 2012, o campanie de securitate cibernetică atât la TV, cât și on-line, care s-a îndreptat spre 100 de milioane de copii și părinți în Europa, Orientul Mijlociu și Africa[28].

[25] Serviciul Român de Informații, *Buletin Cyberint,* semestrul 1-2019, p. 11.
[26] Fișiere care stochează informații despre utilizator și comportamentul său pe internet. Ele sunt fișiere foarte mici păstrate pe dispozitivul utilizatorului, ce pot fi folosite de situri sau de aplicații pentru a ajusta experiența on-line.
[27] Este un protocol care asigură un serviciu de transmitere a datelor, fără conexiune permanentă.
[28] United Nations Office on Drugs and Crime, *Comprehensive study on Cybercrime,* New York, 2013, p. 227.

Așadar, dacă la nivelul unor companii uriașe există măsuri concrete, la nivel instituțional, ce pași trebuie să urmăm pentru a creiona un spațiu cibernetic mai sigur, care sunt cele mai comune erori umane și cum le putem combate?

Primul pas este acela de a investi resurse și timp în pregătirea angajaților în ceea ce privește pericolul iminent. Doar atunci când angajații sunt educați în acest sens pot lua măsuri pentru a evita o greșeală ce se poate transforma rapid într-un incident major. De cele mai multe ori, ne vin în minte probleme legate de informațiile ce au ca obiect cardurile de credit, dar, ceea ce nu luăm în considerare, sunt informațiile de pe adresa de mail. Anul trecut au avut loc multiple compromiteri de date personale, activitate ce va continua și în acest an, dar și în viitor și care este considerată ca fiind unul dintre riscurile majore pentru companii și pentru consumatori.

Apoi, în afara rețelelor de socializare, adresa de e-mail este unul dintre modalitățile de top pe care le folosim pentru a comunica în mediul on-line. Adresa de email a unui utilizator este, practic, identitatea lui în mediul digital. Gândiți-vă la informațiile pe care oamenii le expediază pe această cale: adrese, informații bancare, documente medicale, informații cu caracter juridic etc. Urmărirea acestor mijloace de comunicare electronică este o modalitate de securizare a adresei de mail pentru a avea certitudinea că mesajele expediate ajung la persoana dorită[29]. Angajații nu trebuie să acceseze mesaje electronice, atașamente ori diferite link-uri de la persoane pe care nu le cunosc.

Parolele repetitive ce conțin informații personale, de pildă, porecle ori nume de străzi, reprezintă o problemă majoră. 81% dintre adulți utilizează aceeași parolă pentru fiecare cont pe care îl dețin. Așadar, este necesar să fie conturate reguli clare, care să impună angajaților să utilizeze parole unice, complexe și să le schimbe de fiecare dată când consideră că au fost compromiși.

Studiile arată că majoritatea companiilor oferă angajaților cursuri în domeniul securității cibernetice. Este un exemplu foarte bun de urmat pentru sectorul public, pentru a oferi informații utile, anual, fiecărui angajat, deoarece oamenii vor fi întotdeauna la celălalt capăt al unui sistem automat, al unui telefon ori al unui mesaj electronic[30]. Apărarea on-line împotriva atacurilor reprezintă educarea personalului sau, altfel spus, antrenamente de conștientizare a importanței securității cibernetice.

Pregătirea în securitate presupune, uneori, testări aleatorii. De asemenea, include discuții despre managementul parolelor, modul de utilizare a dispozitivelor mobile, email-urile ce nu trebuie accesate și diferite alte exemple concrete cu care organizația s-a confruntat.

[29] https://digitalguardian.com/blog/cybersecurity-risks-2019, accesat la 29.08.2019.
[30] https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability, accesat la 29.08.2019.

După un asemenea tip de activitate, organizația trebuie să măsoare eficiența acțiunilor întreprinse prin criterii obiective și să verifice dacă procesul de învățare a inspirat angajații să aplice ceea ce le-a fost prezentat. Acest tip de antrenament, la nivelul întregului personal al organizației, trebuie să răspundă la două întrebări: Au transpus în practică, la locul de muncă, tot ceea ce au învățat? A avut antrenamentul rezultatul scontat?[31]

Cultura în domeniul securității cibernetice trebuie să se axeze mai mult pe integrarea securității on-line de la început în fiecare structură și, totodată, trebuie să fie percepută ca o chestiune de o importanță extraordinară, ca un concept ce aparține nouă, tuturor.

CONCLUZII

Securitatea cibernetică este, acum, una dintre cele mai bune afaceri, dar, în același timp, poate fi o arie foarte sensibilă și care are potențialul de a produce unei organizații pagubele cele mai însemnate. Gestionarea acestei probleme trebuie să se alinieze la nivelul de dezvoltare tehnologică, pentru a găsi cele mai bune soluții în vederea menținerii securității spațiului virtual.

Soluțiile în ceea ce privește provocările ce apar ca urmare a pregătirii personalului în domeniul securității necesită o abordare interdisciplinară și o permanentă cooperare între sectoarele public și privat. Sănătatea și securitatea la locul de muncă reprezintă, acum, norma și rareori această normă este considerată ca fiind altceva decât un standard obligatoriu.

Securitatea cibernetică este o problemă globală și suntem toți parte din aceasta. Nu ne putem aștepta ca un atacator singuratic, ce stă într-o anumită țară și lansează atacuri multiple, să reprezinte o amenințare izolată. În această situație, toți actorii implicați trebuie să coopereze, să comunice pentru a crea un răspuns închegat și flexibil în orice situație ivită.

Trebuie să ne amintim permanent că securitatea aparține fiecăruia dintre noi, de la nivelul cel mai înalt de conducere până la ultima funcție de execuție. Fiecare deține o parte din ceea ce semnifică securitatea unei companii, deoarece nu poate fi altfel garantă protecție atât timp cât persoanele își neglijează responsabilitățile în acest domeniu de o importanță covârșitoare.

Securitatea cibernetică este o luptă continuă. O soluție decisivă cu aplicabilitate permanentă pentru această problemă nu va fi, probabil, identificată sau, chiar dacă va fi găsită, aceasta nu se va întâmpla curând. Având în vedere circumstanțele enumerate, trebuie să ne concentrăm atenția pe măsuri concrete, să lansăm soluții sustenabile și proceduri cu aplicabilitate în acest domeniu sensibil.

[31] Society for Human Resource Management, *Implementing effective cyber security training for end users of computer networks,* Virginia, 2015, p. 13.

BIBLIOGRAFIE:

1. ***, *Buletin Cyberint*, Serviciul Român de Informaţii, semestrul I, 2019.
2. ***, *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime, New York, 2013.
3. ***, *Cyber Security Breaches Survey: Statistical Release*, Department for Digital, Culture, Media & Sport, 2018.
4. ***, *Hotărârea Guvernului nr. 271/2013 pentru aprobarea Strategiei de Securitate Cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică.*
5. ***, *Implementing effective cyber security training for end users of computer networks*, Society for Human Resource Management, Virginia, 2015.
6. ***, *People's Role in Cyber Security: Academics' Perspective*, 2014.
7. Jochen Rehrl, *Handbook for decision makers – The common security and defence policy of the European Union*, Imprimerie Centrale, Luxembourg, 2017.

WEBOGRAFIE:

1. https://www.bitdefender.ro/news/romania-cea-mai-afectata-tara-din-lume-de-amenintarea-informatica-a-momentului-3666.html
2. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
3. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/
4. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf
5. https://digitalguardian.com/blog/cybersecurity-risks-2019
6. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
7. https://www.enisa.europa.eu/topics/incident-reporting?tab=details
8. https://www.enisa.europa.eu/media/multimedia/videos/cybersecurity-is-a-shared-responsibi lity-european-cyber-security-month-2018
9. https://www.esjnews.com/are-european-elections-vulnerable-to-cyber-attacks
10. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company
11. https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies
12. https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf
13. https://www.nato.int/cps/en/natolive/official_texts_17120.htm
14. https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability
15. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
16. https://securelist.com/mobile-malware-evolution-2018/89689/.