AMENINȚĂRI DE TIP SOCIAL ENGINEERING, PRIN INTERMEDIUL REȚELELOR DE SOCIALIZARE

SOCIAL ENGINEERING THREATS THROUGH SOCIAL MEDIA INSTRUMENTS

Drd. Anne Maria DRAGOMIR*

Rețelele de socializare au schimbat fundamental modul în care comunicăm, relaționăm și ne informăm. Beneficiile acestor inovații din domeniul tehnologiei pot fi umbrite de multitudinea de amenințări și de riscuri, pe care utilizarea platformelor social-media le generează atât la nivel individual, cât și la nivel statal sau global. Amenințările de tip social engineering s-au rafinat odată cu instrumentarea resurselor online. Obiectul articolului constă în prezentarea riscurilor online, subiect prea puțin dezbătut în spațiul public românesc, în special în contextul în care una dintre soluțiile eficiente în combaterea acestui tip de amenințări poate veni din informarea utilizatorilor rețelelor de socializare cu privire la riscurile cu care se pot confrunta, în paralel cu educarea acestora în vederea unei utilizări sigure a instrumentelor puse în mișcare, prin intermediul Internetului.

Social Media fundamentally changed the way we communicate, relate and gather our information. The benefits of these technology innovations can be overshadowed by the multitude of threats and risks that social media platforms generate at both individual and governmental levels. Social engineering threats have been refined and have reached a new level by exploiting these online resources. The objective of the present article is to present and raise awareness for a topic that lacks of debate in the Romanian public space, especially considering that one of the effective solutions in combating this type of threats can come from informing Social Media users regarding the risks and educating them in order to secure the use of the tools delivered via Internet.

Cuvinte-cheie: social-media; social-engineering; securitate; amenințări cibernetice.
Keywords*: social-media; social-engineering; security; cyber threats.*

Apariția rețelelor de socializare a schimbat, într-o manieră fundamentală, modul în care comunicăm și ne informăm, marcând toate aspectele vieții cotidiene. Instrumentele puse la dispoziție de social-media au eliminat barierele geografice, lingvistice și culturale. O scurtă analiză a datelor statistice ne conferă o perspectivă clară cu privire la capacitatea de penetrare a rețelelor de socializare și la rolul pe care au ajuns să îl joace în viața noastră, de zi cu zi. Potrivit datelor furnizate de către *We Are Social*, în parteneriat cu Hootsuite, în raportul *Digital in 2018 – Global Overview*, peste 53% din populația globului are acces la Internet, mai precis există peste patru miliarde de utilizatori de Internet[1]. 42% din populație, respectiv 3,195 de miliarde sunt utilizatori activi de social-media[2], dintre care 2,167 de miliarde au conturi de Facebook[3], iar 2,055 miliarde[4] accesează această platformă, prin intermediul dispozitivelor mobile (smartphone sau tabletă). Datele sunt la fel de impresionante și pentru România, unde 70%, respectiv 13,74 milioane, din populație au acces la Internet. Zece milioane de români utilizează rețelele de socializare, 8,9 milioane prin intermediul dispozitivelor mobile[5]. Prin intermediul rețelelor de socializare, utilizatorii fac publice, în mod voluntar, o serie de date și de informații, aparent inofensive, dar care, în mâinile unor entități rău intenționate, pot genera amenințări grave la nivel individual, organizațional, statal sau chiar global.

În perioada 26 decembrie 2009 - 23 ianuarie 2010, Thomas Ryan, specialist în probleme de securitate, a derulat un experiment, cu scopul de a evalua eventualitatea unor scurgeri de informații apărute ca urmare a încrederii în profilurile false de pe rețelele de socializare. În decursul acestei luni,

Universitatea Națională de Apărare „Carol I”
e-mail: *anne.dragomir@gmail.com*

profilul fals creat de către Ryan, sub numele Robin Sage, o tânără cu un parcurs profesional în domeniul securității, a reușit să strângă sute de conexiuni, prin intermediul a cinci instrumente online: Facebook, LinkedIN, Twitter, Google și Blogger. Contactele veneau fie din domeniul securității naționale, angajați ai unor instituții, precum NSA[6] sau DOD[7], fie din corporații. Ryan s-a concentrat, în mod deosebit, pe crearea profilului prin prisma configurării identității personajului. Genul feminin, educația și formarea, asociate cu parcursul profesional și cu rețeaua de prieteni virtuali, i-au conferit personajului fictiv o credibilitate ridicată, facilitând câștigarea încrederii viitoarelor conexiuni pe care le viza. Rezultatele experimentului nu s-au limitat la un banal acces la informațiile împărtășite, în mod public, cu rețelele de contacte, de către cei care i-au acceptat cererile de conectare. Personajul Sage a obținut oferte de muncă, atât în mediul privat, cât și în cadrul instituțiilor de stat și invitații de a susține discursuri la o serie de evenimente, pe teme de securitate[8]. Ryan a reușit să își atingă scopul, aducând în prim plan pericolele generate de încrederea nejustificată a utilizatorilor rețelelor de socializare în persoanele cu care intră în contact, fără a chestiona identitatea sau intențiile acestora din urmă. „Pe parcursul experimentului, care a durat 28 de zile, a devenit evident faptul că propagarea unei identități false, prin intermediul rețelelor de socializare, poate deveni agresivă și virală”[9].

Deși au trecut opt ani de la finalizarea experimentului, amenințările pe care Ryan a reușit să le identifice sunt mai prezente ca oricând, în special din cauza dinamicii caracteristice rețelelor de socializare. Tehnicile de *social-engineering* s-au adaptat și s-au rafinat direct proporțional cu inovațiile continue, în domeniul comunicării și al informațiilor. Pentru a putea înțelege fenomenul, în raport cu mecanismele rețelelor de socializare, vom porni de la prezentarea unor definiții ale conceptului de *social-engineering*.

Pentru că subiectul articolului este spațiul online, am considerat pertinentă utilizarea celui mai popular motor de căutare, Google, pentru a defini, într-o primă etapă, conceptul de *social engineering*. Astfel, în contextul securității informaționale, *social engineering* presupune „utilizarea înșelătoriei pentru a manipula indivizi în a divulga informații personale sau confidențiale, care să poată fi utilizate în scopuri frauduloase”[10]. O explicație similară o întâlnim pe pagina oficială a FBI: „Așadar ce este *social-engineering*? În fond, este un șarlatan care te manipulează să faci ceva ce în mod obișnuit nu ai face”[11]. Mergem mai departe și încercăm să înțelegem modul în care este prezentat fenomenul *social-engineering* de către o companie privată, unul dintre cei mai activi actori pe scena produselor create pentru asigurarea securității în spațiul cibernetic. Kaspersky Lab definește fenomenul ca pe „o formă de tehnici, utilizate de către criminali cibernetici, configurate cu scopul de a ispiti utilizatorii, în transmiterea de date confidențiale, de a le infecta calculatoarele cu malware sau de ai convinge să deschidă pagini web infectate”[12]. Într-una dintre multiplele definiții oferite de către mediul academic se afirmă: „Influențarea și manipularea persoanelor, în vederea divulgării de informații sensibile sau cu scopul de a oferi acces la arii restricționate sunt bine cunoscute ca *social-engineering*”[13].

Așadar, privind fie dintr-o perspectivă academică, fie prin ochii companiilor care au, ca obiect al activității, dezvoltarea de produse, în scopul garantării unei experiențe online în asigurarea securității, *social-engineering* reprezintă, în fond, acele tehnici de manipulare și de înșelătorie, cu scopul de a obține diverse informații, pe care ținta vizată nu le-ar divulga în mod obișnuit, ba mai mult, este foarte posibil ca aceasta din urmă nici măcar să nu conștientizeze faptul că acțiunile sale au condus la un asemenea efect. Niciuna dintre definițiile prezentate mai sus nu face legătura dintre *social-engineering* și rețelele de socializare, însă principalele amenințări, generate de proliferarea social-media, se configurează sub forma manipulării. Astfel, o abordare a fenomenului, prin prisma instrumentării rețelelor de socializare, este o problematică de actualitate.

Desigur, fenomenul nu este nici pe departe nou. Poate nu întâmplător unul dintre cei mai cunoscuți viruși, Calul troian, poartă numele cadoului mitic oferit de către greci troienilor, cu scopul de a-i determina, fără a fi conștienți de urmările acțiunilor lor, să deschidă porțile cetății și să permită armatei grecești să câștige războiul troian. Grecii au utilizat, în Antichitate, aceeași armă a înșelăciunii, care este una dintre amenințările majore la adresa securității, în zilele noastre. Însă instrumentarea rețelelor de socializare, în acest sens, a dus tehnicile de *social - engineering* la un nou nivel, soluțiile pentru a

combate aceste amenințări părând imposibil de configurat, într-un spațiu nedeterminat de nicio barieră geografică, nereglementat și caracterizat de o viteză incredibilă de propagare a mesajelor.

Candid Wüest, Senior Software Engineer al companiei Symantec, identifică opt amenințări de tip *social-engineering*, instrumentate prin intermediul rețelelor de socializare: momeli (baits) ascunse, sub forma unor sugestii de tip *trends*, care îi determină pe utilizatori să acceseze o serie de linkuri capcană, în ideea de a fi la curent cu noutăți din diverse domenii-înșelătorii, generate de dorința utilizatorilor de a-și lărgi aria de conexiuni. Există site-uri care oferă posibilitatea cumpărării efective de like-uri pe Facebook și urmăritori pe Twitter – cu riscul expunerii datelor de conectare la conturile personale; pagini false ale unor personalități publice, cu scopul distribuirii de informații eronate; distribuirea de mesaje răuvoitoare, prin preluarea conturilor personale; virusul Kooface, identificat a fi primul atac masiv de tip *malware*, instrumentat de obișnuința utilizatorului de a deschide linkuri, fără a filtra informația; phishing – crearea de copii ale platformelor bine cunoscute, în scopul extragerii de informații-înșelătorii, în vederea obținerii de beneficii materiale; utilizarea în mod tendențios a unor informații vehiculate intenționat în mediul online, în vederea preluării conturilor personale, câștigării încrederii unei plaje largi de utilizatori[14].

Desigur, pericolele sunt multiple și se pot prezenta sub diverse forme, în funcție de scopul pe care inițiatorul unor astfel de înșelătorii îl vizează. În ceea ce privește o scurtă caracterizare a tipologiei inițiatorului tehnicilor de *social-engineering*, „acest personaj este adeseori prietenos, volubil, silindu-te să fii recunoscător că l-ai întâlnit”[15], „în majoritatea cazurilor, inginerii acestor tehnici au abilități de comunicare cu oamenii. Sunt șarmanți, politicoși, ușor de plăcut – trăsături sociale necesare în vederea obținerii unei relaționări rapide și a încrederii. Un astfel de personaj este capabil să obțină orice informație țintită, utilizând tehnici și tactici specifice profesiei sale”[16].

Kevin Mitnick și-a câștigat notorietatea în anul 1995, când a fost arestat, ca urmare a unor infracțiuni multiple din spațiul cibernetic. Actualmente, Mitnick este consultant în domeniul securității IT și autorul unei ample lucrări pe tema *social engineering*. Acesta a schițat un ciclu al atacurilor de tip social engineering. Un asemenea atac pornește de la o componentă de cercetare care conduce către dezvoltarea de conexiuni, prin câștigarea încrederii acestora. Odată câștigată încrederea, aceasta este exploatată în vederea obținerii și utilizării de informații, care le instrumentează pentru noi cercetări[17].

Cu privire la spațiul românesc, în anul 2017 CERT-RO[18] a lansat două alerte, în ceea ce privește amenințări de tipul *social-engineering*, venite din mediul rețelelor de socializare. Două dintre cele mai populare și utilizate aplicații de mesagerie instant, WhatsApp și Facebook Messenger, erau instrumentate în mod vicios, cu scopul de a înșela încrederea utilizatorilor.

Pe 4 mai 2017, CERT-RO prevenea utilizatorii de WhatsApp, din România, cu privire la o campanie de tip phishing. „Recent, utilizatorii binecunoscutei aplicații de mesagerie WhatsApp sunt vizați de o campanie de phishing, al cărei scop este de a-i determina pe aceștia să se aboneze la diferite servicii taxate prin SMS, să instaleze malware pe dispozitivul mobil sau să comande anumite ‹‹produse minune›› de slăbit în timp record”[19].

Prin intermediul aplicației de mesagerie, a circulat, pe durata câtorva zile, la începutul lunii mai, următorul mesaj: „!!! Aplicația WhatApp va costa 0.01 $, pentru fiecare mesaj trimis. Trebuie să confirmați profilul pentru a continua să îl utilizați GRATUIT! Activați profilul dvs. aici http://whatapp.us/Activati/Romania/”[20].

Sunt vizibile câteva elemente care ar fi trebuit să determine ignorarea automată a mesajului de către utilizatori. Numele aplicației este scris greșit atât la începutul mesajului, cât și în URL. Formatul mesajului ar fi putut trage un alt semnal de alarmă. După cum putem observa în figura 1, acesta se prezenta sub forma unui spam, fiind compus dintr-o serie de elemente, configurate de așa natură încât să

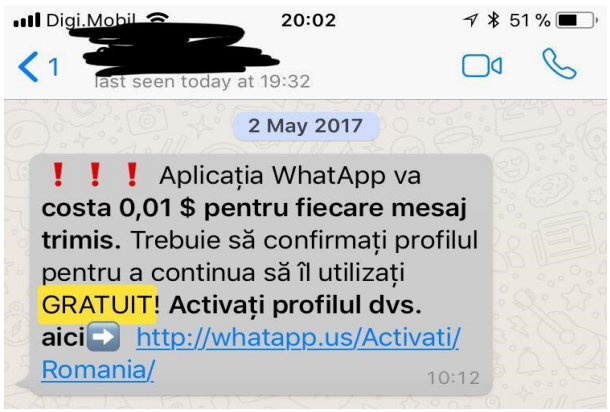

Fig. 1 *Campanie de tip phishing, prin intermediul aplicației de mesagerie instant WhatsApp*

atragă atenția, trei semne de întrebare de culoarea roșie, cuvinte îngroșate sau chiar marcate cu o culoare distinctă, scrise cu majuscule.

CERT-RO consideră, de asemenea, că un semn de întrebare ar fi trebuit să îl ridice și faptul că mesajul venea fie de la un număr de mobil normal, fie chiar de la un contact din agendă. Din punctul meu de vedere, un mesaj primit de la un contact al utilizatorului, o persoană cunoscută de acesta, poate credibiliza conținutul, și nu invers. Recomandările CERT-RO, în vederea prevenirii unor asemenea amenințări, pornesc de la premisa că utilizatorii sunt conștienți de pericolele care vin din această zonă și se concentrează pe verificarea surselor. Adevărata problemă însă este generată de lipsa instruirii utilizatorilor cu privire la toate aspectele pe care le implică interconectivitatea, ce guvernează toate aspectele vieții noastre de zi cu zi.

Lipsa unei educații în siguranța utilizării Internetului și a platformelor de socializare și-a spus încă o dată cuvântul, în luna august, când instrumentul a fost platforma de mesagerie instant a gigantului Facebook. Conform CERT-RO: „În ultimele zile, utilizatorii binecunoscutei aplicații de mesagerie Facebook Messenger sunt vizați de o campanie de răspândire de malware, prin intermediul unor mesaje, care îi îndeamnă pe aceștia să acceseze un link (URL) către un așa-zis video al unui prieten”[21]. Accesarea linkului poate genera o serie de riscuri la adresa utilizatorului platformei de mesagerie, de la livrarea de informații cu privire la obișnuințele de consum online ale acestuia, trimiterea în mod automat a unor mesaje de tip malițios către rețeaua de conexiuni, până la preluarea de parole și de date de conectare la diverse conturi, inclusiv la cele bancare.

Pentru utilizatorii de Internet din România, CERT-RO se poate dovedi o resursă extrem de valoroasă în vederea dobândirii de cunoștințe, în ceea ce privește complexitatea acestor interacțiuni atât de banale, în aparență, în mediul virtual. Însă, pentru a putea exploata această resursă, utilizatorul trebuie să aibă deja un interes cu privire la subiect și să caute, în mod activ, informații. Din cei 10 milioane de utilizatori ai rețelelor de socializare, doar 8.230[22] urmăresc pagina de Facebook a CERT-RO, reprezentând un procent de 0,083. Procentul insignifiant nu este determinat de o lipsă generală de interese a utilizatorilor cu privire la siguranța lor în spațiul online, ci mai degrabă o lipsă de conștientizare a amenințărilor, în paralel cu un număr infim de informații legate de acest subiect, în spațiul public.

Concluzii

Utilizatorii se pot proteja împotriva tehnicilor de *social-engineering*, instrumentate prin mecanismele rețelelor de socializare, atunci când conștientizează pericolele la care se expun, și devin un pic mai rezervați, în momentul inițierii unor conexiuni noi în spațiul virtual. O doză de scepticism este bine-venită, în egală măsură, și atunci când sunt angajați în diverse acțiuni de către persoane pe care le cunosc, le au în lista de prieteni, dar care inițiază un tip de discuție similară unui spam. Încrederea pe care un utilizator al rețelelor de socializare o are într-o persoană în viața reală nu ar trebui să fie transpusă automat, în aceeași măsură, și în mediul virtual. Datele de conectare la conturile personale pot fi mult mai ușor de obținut de către terți, decât ne putem imagina. În acest sens, utilizatorii ar trebui să își configureze parole puternice, formate din mai multe tipuri de caractere, pe care să le schimbe periodic. De asemenea, accesul la rețele de socializare diferite ar trebui să se facă prin parole diferite. O înregistrare, pe terțe pagini, cu profilul de pe o platformă de socializare, precum Facebook, Twitter sau LinkedIn, ar trebui să presupună, anterior, o verificare a site-ului în cauză, pentru a se convinge că această solicitare nu este doar un mijloc, prin care persoane cu intenții răuvoitoare să aibă acces la profilurile de social-media. Poate primul pas ar trebui să fie stăpânirea setărilor legate de securizarea conturilor. O atenție mai ridicată cu privire la informațiile pe care le împărtășim, prin intermediul rețelelor de socializare, ne poate proteja atât pe noi, cât și pe apropiații noștri.

Instituțiile cu prerogative în domeniul securității ar trebui să acorde o atenție deosebită acestui fenomen, atât prin instruirea angajaților cu privire la amenințările generate de prezența pe platformele de socializare, cât și prin asistarea lor, într-o utilizare sigură a spațiului online, prin elaborarea de ghiduri și de manuale de conduită. Acțiunile individuale ale angajaților instituțiilor statului pot genera amenințări la adresa colegilor, a instituției sau chiar a securității, prin scurgeri de informații involuntare, în lipsa unei cunoașteri comprehensive a tuturor fațetelor rețelelor de socializare.

Fie că vorbim despre utilizatorul obișnuit, fie despre angajați ai instituțiilor statului, există o necesitate ridicată de informare și de educare cu

privire la utilizarea instrumentelor puse la dispoziție de mediul online. Conștientizarea riscurilor este un prim pas fundamental în vederea utilizării în siguranță a Internetului.

NOTE:

1 *We Are Social – Digital in 2018 Global Overview*, slide 28, https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338, accesat la 13 februarie 2018.

2 *Ibidem,* slide 51.

3 *Ibidem,* slide 59.

4 *Ibidem,* slide 67.

5 *We Are Social – 2018 Digital Yearbook*, slide 188, https://www.slideshare.net/wearesocial/2018-digital-yearbook-86862930/91, accesat la 13 februarie 2018.

6 *National Security Agency*, traducere din limba engleză: Agenția Națională de Securitate a Statelor Unite.

7 *Department of Defense*, traducere din limba engleză: Departamentul Apărării al Statelor Unite.

8 Ryan Thomas, Getting in Bed with Robin Sage, *Through this 28-day experiment, it became evident that the propagation of a false identity via social networking websites can be rampant and viral*, p. 2, https://www.privacywonk.net/download/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf, accesat la 12 februarie 2018.

9 *Ibidem,* p. 2.

10 *Social engineering (in the context of information security*): the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purpose. (Google Dictionary)

11 Beth Anne Steele, *FBI Tech Tuesday: Digital Defense Against Social Engineering*, FBI Portland, 20 iunie 2017, https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday-digital-defense-against-social-engineering, accesat la 12 februarie 2018.

12 *Social engineering is a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites*, https://usa.kaspersky.com/resource-center/definitions/social-engineering. (KasperskyLab)

13 Sven Uebelacker, Susanne Quiel, *The Social Engineering Personality Framework*, Hamburg University of Technology Security in Distributed Applications, ”Influencing and manipulating persons to reveal sensitive information or granting access to restricted areas is widely known as Social Engineering (SE)”, https://pdfs.semanticscholar.org/86c1/d56dc8fbe55f0f95a6633ce5d9206e00292c.pdf

14 WÜEST, Candid The Risks of Social Networking, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

15 Kevin Mitnick, William L. Simon, *THE ART OF DECEPTION Controlling the Human Element of Security*, ”This character is often so friendly, glib, and obliging that you’re grateful for having encountered him”, p. 13 http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

16 *Ibidem,* ”In most cases, successful social engineers have strong people skills. They’re charming, polite, and easy to like-social traits needed for establishing rapid rapport and trust. An experienced social engineer is able to gain access to virtually any targeted information by using the strategies and tactics of his craft”, p. 16.

17 François Mouton, Mercia Malan, Louise Leenen, *Social Engineering Attack Framework*, https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework

18 *Centrul Național de răspuns la incidente de securitate cibernetică*.

19 https://www.CERT-RO, Campanie de tip phishing prin intermediul WhatsApp, 8/vv https://cert.ro/citeste/campanie-phishing-whatsapp

20 Am recepționat acest mesaj în data de 1 și de 2 mai 2017, de la trei persoane cunoscute, ale căror numere de mobil le aveam în agenda telefonului mobil.

21 Campanie de răspândire malware, prin intermediul aplicației de mesagerie Facebook Messenger, 25 august 2017, https://cert.ro/citeste/campanie-malware-facebook-messenger

22 https://www.facebook.com/CERT.RO/

BIBLIOGRAFIE

Hadnagy Christopher *Social Engineering The Art of Human Hacking,* Wiley Publishing, 2011, http://zempirians.com/ebooks/The_Art_of_Human_Hacking.pdf

Mitnick D. Kevin & Simon L. William, Foreword by Steve Wozniak, *THE ART OF DECEPTION Controlling the Human Element of Security*, http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

Nohlberg M., Kowalski S., *The Cycle of Deception - A Model of Social Engineering Attacks*, Defences and Victims Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008), https://www.cscan.org/openaccess/?id=50

Mouton François, Malan Mercia și Leenen Louise & Venter H.s., *Social Engineering Attack Framework*, 2014, https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework

Uebelacker Sven, Quiel Susanne, *The Social Engineering Personality Framework*, Hamburg University of Technology Security in Distributed Applications, https://pdfs.semanticscholar.org/86c1/d56 dc8fbe55f0f95a6633ce5d9206e00292c.pdf

CERT-UK, National Cyber Security Center, *An introduction to social engineering*, https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Introduction-to-social-engineering.pdf

https://www.cert.ro

https://KasperskyLab, www.kaspersky.com

https://Symantec, www.symantec.com