Vulnerabilitatea interacțiunii sociale în spațiul virtual

Dragoş Claudiu FULEA
Serviciul Român de Informații
dfulea870@dcti.ro
Gabriel Angelo MUŞĂTOIU
Serviciul Român de Informații
mangelo870@dcti.ro

Abstract

Due to the technological facilities offered by the information and communication technology (ICT) tools, social media has known an unprecedentedly development.

In the same time, unauthorized data collection is eventually leading to ill-fated consequences affecting individual human rights on intimacy and free, unbiased information.

This article is intended to explain some of the vulnerabilities raised by the social interaction within the cyberspace stressing that, in spite of some naïve and poor precaution measures adopted by users, the naked truth states that in the virtual space there are no secrets but a false sense of security. Therefore, gaining knowledge as well as well-intended advices the way people should protect themselves when harnessing information and communication technology tools, is vital.

Consequently, by diminishing the stress and uncertainty factor of the actions undertaken by inexperienced ICT users, this will lead to a better understanding and an increased integration within the knowledge society of tomorrow.

Keywords: Social media, WEB 2.0, information technology, social networks, blogs, forums, messenger, psychological profile, dominant personality issue, intimacy infiltration, anonymity, passwords.

Dezvoltarea tehnologiilor informaționale de comunicare

Transmiterea informației a cunoscut o puternică transformare, avansând foarte mult în zona digitalizării.

Atunci când se analizează fenomenul de convergență a canalelor de comunicare, cel mai reprezentativ exemplu este platforma Internet care suportă transmisia de date de diverse tipuri: text, audio, foto, video, format electronic.

Ceea ce în anii ’90 era dificil de anticipat dar în prezent a devenit certitudine, se referă la relația de simbioză între apariția şi dezvoltarea Internetului, pe de o parte şi revoluția tehnologiilor informaționale şi de comunicare, pe de altă parte.

Actualmente, în mediul virtual se manifestă preponderent două elemente comunicaționale, respectiv interactivitatea şi presa personalizată (podcasting), care au transformat structura serviciilor oferite de Internet, prin evoluția de la World Wide Web (WEB 1.0) la New Media (WEB 2.0)[1].

Cele două elemente stau la originea „cutremurului” care a zguduit baza fundamentală a comunicării de masă şi a provocat un tsunami în procesul de dezvoltare a tehnologiilor, deşi cu numai trei decenii în urmă ar fi fost considerate subiect de science-fiction.

Interactivitatea reprezintă acțiunea cauzală reciprocă ce defineşte atât relația utilizator-mediu cibernetic, cât şi relația între comunicatori. Tehnologia digitală permite utilizatorilor să-şi editeze propriul conținut comunicațional, după care să-l împărtăşească altor persoane pentru informare şi socializare. Ulterior, informația este consumată şi repoziționată de către vizitatori, proprietarilor de pagini web revenindu-le sarcina de a pune la dispoziție o platformă de comunicare funcțională. *Social media* este cel mai reuşit exponent al interactivității şi, totodată, parte componentă a filozofiei New Media.

Presa personalizată constituie o aplicație derivată din interactivitatea mediului virtual, care permite utilizatorului să preia controlul asupra modului de colectare şi stocare a informației furnizată prin intermediul canalelor de comunicare. Podcasting-ul reprezintă un termen folosit generic pentru a descrie distribuția de conținut multimedia.

Elementele din spațiul virtual reprezentative pentru ceea ce numim New Media[2] se referă la:

- ***Bloguri;***
- ***Forumuri, liste de discuții;***
- ***Rețele de socializare;***
- ***Serviciile de comunicare în timp real, tip messenger***.

Fiecare dintre aceste categorii de surse poate constitui un subiect de preocupare pentru tehnologiile informaționale utilizate de grupurile infracționale specializate în vederea colectării neautorizate de informații

[1] Pakondi Victor, *Dicționar Internet & Tehnologii World Wide Web*, Editura Kondyli, Bucureşti, 2000.

[2] Manovich, Lev „New Media from Borges to HTML”, The New Media Reader, Ed. Noah Wourdrip-Fruin&Nick Montfort Cambridge, Massachusetts, 2003, 13-25.

privind utilizatorii neavizați. De asemenea, reprezintă un obiectiv al mijloacelor similare uzitate în activitatea de intelligence derulată de diverse entități civile sau guvernamentale. Pentru a înțelege mai ușor sensul acestor precizări, vom puncta succint aspecte descriptive cu relevanță pentru fiecare categorie.

Blogurile reprezintă un tip de site web care utilizează platforme predefinite, oferite gratuit de dezvoltatorii de softuri utilizatorilor personali, în scopul realizării unor proiecte cât mai complexe cu resurse puține.

Conținutul unui blog este afişat cronologic, cel mai nou articol fiind poziționat în partea superioară a paginii. Această structură, precum şi caracterul de cele mai multe ori personal al materialelor a determinat compararea acestui gen de site cu un jurnal.

În timp, această formă de comunicare a cunoscut o popularitate fără precedent, în toate domeniile vieții sociale, fiind considerată cea mai eficientă cale de promovare personală sau, după caz, de informare / dezinformare.

„Blogging-ul" (activitatea de editare a blogurilor) s-a transformat treptat dintr-un simplu hobby, în activitate organizată şi planificată. Articolele postate pe bloguri permit comentarii diverse, nerestricționate, iar acest aspect le conferă interactivitate, un atribut esențial în derularea procesului de comunicare fiind reprezentat de posibilitatea colectării de feed-back din partea publicului-țintă.

Monitorizarea blogging-ului permite colectarea de informații de pe spații geografice în care sursele de informare media fie sunt supuse cenzurii sau puternic politizate, fie sunt insuficient dezvoltate.

Forumurile şi listele de discuții, spre deosebire de bloguri, în cele mai multe situații nu au un proprietar anume, fiind organizate pe teme specifice şi optimizate pentru motoarele de căutare.

În aceste zone ale web-ului se pot obține informații de interes real şi imediat (hărți, scheme, comentarii etc.).

Rețelele de socializare oferă utilizatorilor posibilitatea de a-şi crea o pagină personală conținând fotografii, materiale video, jurnal electronic.

Prezintă interes din punct de vedere al accesului la datele personale ale persoanelor-țintă facilitând inclusiv identificarea, uneori chiar vizualizarea cercului relațional apropiat țintei. Totodată, pot înlesni accesarea secțiunilor de comentarii, așa-numitul jurnal electronic. Deşi datele vehiculate în acest mediu nu au un caracter clasificat, prelucrarea acestora în urma unui proces de analiză asociat exploatării specializate a

surselor deschise, le transformă în informaţii valoroase mai ales în vederea elaborării profilului psihologic.

Serviciile de comunicare în timp real, tip messenger, conferă posibilitatea provocării şi / sau manipulării procesului de comunicare cu un grup extins de persoane, sub protecţia anonimatului.

Având în vedere accelerarea procesului de tehnologizare în domeniul informaticii, se poate emite predicţia conform căreia până la finele acestui deceniu vom asista la cel puţin o revoluţie în procesul de comunicare cibernetică şi la depăşirea unui nou prag tehnologic către WEB 3.0 sau WEB 4.0, cu toate avantajele şi avatarurile implicate de această evoluţie implacabilă.

Riscurile interacţiunii sociale în spaţiul digital

În general, securitatea la nivel instituţional vizează dezvoltarea şi consolidarea unui sistem integrat de protecţie ce implică în mod nemijlocit protecţia personalului. Una dintre acţiunile prioritare pentru realizarea acestui obiectiv strategic constă în evaluarea şi gestionarea riscurilor generate de noile evoluţii tehnologice. Tot mai multe informaţii memorate in fişiere separate devin posibil de corelat prin intermediul unor algoritmi logici care utilizează resursele şi puterea de calcul a unor vaste reţele de calculatoare. Această asociere de date privind persoanele poate conduce către consecinţe nefaste asupra dreptului la intimitate şi a caracterului privat al dreptului la informare.

În acest context, se impune semnalarea necesităţii unui demers la nivel individual şi colectiv în vederea cunoaşterii vulnerabilităţilor existente în relaţiile care guvernează funcţionalitatea binomului utilizator–spaţiu virtual, de natură a se concretiza ulterior în disfuncţii procesuale în demersul de integrare într-o viitoare societate a cunoaşterii.

Societatea nu poate fi responsabilizată pentru lipsa securizării informaţiilor proprii, în situaţia în care nu este informată asupra modalităţilor de protecţie.

În calitate de membru al unei societăţi care a angajat demersuri consistente în plan naţional pentru a accede în era informaţională, orice utilizator din România dispune, în prezent, de libera exercitare a dreptului de a accesa, de a posta şi consuma produsele informaţionale ale spaţiului cibernetic.

Este important ca, mai ales în dubla postură de emitent / destinatar al mesajelor comunicaţionale transmise pe platforma WEB 2.0, internautul român, indiferent de apartenenţa la organizaţiile din sfera civilă sau militară,

să manifeste o conduită bazată pe cunoaşterea şi conştientizarea implicaţiilor interacţiunii sale în mediul cibernetic, în plan personal, iar uneori, în cel al interesului naţional.

Lucrarea nu îşi propune să dezvolte un profil psihologic al utilizatorilor reţelelor sociale on-line, literatura de specialitate abundă de lucrări pe acest subiect, în încercarea de a răspunde la întrebarea de ce majoritatea internauţilor doresc să fie cunoscuţi cum de fapt nu sunt în realitate şi nici nu prezintă implicaţiile juridice ale încălcării drepturilor fundamentale pe parcursul comunicării digitalizate, însă intenţionează să sublinieze un adevăr cert: **în spaţiul virtual nu există secrete**.

Orice activitate derulată în acest mediu – indiferent că este vorba de accesarea unei reţele de socializare sau postarea pe un blog, descărcarea de fişiere sau confecţionarea unei vieţi duble în lumile virtuale –, este uşor de urmărit în baza „amprentei" digitale ataşate fiecărui dispozitiv conectat (desktop, notebook, tabletă PC, smartphone), aşa-numitul IP (Internet Protocol).

Pe de altă parte, conţinutul lucrării nu este axat pe detalii tehnice, dar relevă falsitatea impresiei de securitate deplină în mediul virtual ca urmare a unei aşa-zise protecţii prin parole sau identităţi false confecţionate pe diferite site-uri, accentuând un alt adevăr verificat: **identitatea reală a utilizatorilor nu este secretă decât pentru cei neinteresaţi să o afle**.

Din mai multe perspective, care includ şi interese operaţionale asociate activităţii de intelligence derulate de serviciile de informaţii şi securitate, reţelele de socializare reprezintă o sursă inepuizabilă de informaţii, mai ales în contextul în care, studii sociologice aplicate au relevat faptul că utilizatorii WEB 2.0 au tendinţa de a derula sub umbrela falsă a „anonimităţii" şi „invizibilităţii" pe care o reţea socială le „oferă", acţiuni pe care altfel nu le-ar iniţia niciodată în viaţa reală.

Deşi datele vehiculate nu au neapărat un caracter confidenţial, prelucrarea acestora în urma unui proces de analiză specializat le transformă în informaţii valoroase, mai ales pentru un psiholog specializat. Practic, orice fragment de informaţie despre viaţa personală a unui consumator social media, familia acestuia, prieteni, preferinţe sau pasiuni, poate fi aranjat în mod asemănător realizării unui puzzle pentru creionarea unui profil psihologic. Din punct de vedere comercial şi de marketing, această acţiune se derulează în mod curent, chiar în momentul parcurgerii acestor rânduri, în cazul milioanelor de utilizatori ai motoarelor de căutare aparţinând corporaţiilor multinaţionale precum Google sau Yahoo.

Cu excepția interesului comercial legal, aspect ce implică acordul utilizatorului, obiectivul acestui demers laborios, cronofag şi costisitor (dacă nu deții instrumente de tehnologie informațională adecvate), nu poate fi altul decât documentarea unei palete largi de acțiuni cu scop infracțional, începând cu furtul de identitate până la cele cu accente de violență de gen efracție, răpire sau şantaj. Pe de altă parte, nu se pot exclude operațiunile de colectare şi exploatare informativă derulate de entități civile sau guvernamentale localizate pe diverse spații geografice.

Pentru a înțelege mai bine cum date aparent banale pot fi utilizate în defavoarea utilizatorilor, putem exemplifica situații după cum urmează:

Infiltrarea în cercul familial şi relațional al utilizatorilor. Înmulțirea şi diversificarea platformelor de socializare, a categoriilor de informații vehiculate, precum şi diversitatea consumatorilor, implică o abordare sistemică. În acest scop, entitățile interesate în obținerea de date şi informații despre utilizatori folosesc personal familiarizat în utilizarea eficientă a unor instrumente de colectare şi analiză a datelor, iar țintele care îşi expun în mod neglijent sau din neştiință viața socială (fotografii, scheme de relații structurate pe linii temporale, date personale, montaje audio-video pe YouTube sau „ciripeli" pe Twitter privind evenimente din intimitate) „sprijină", involuntar, 80% din această muncă de documentare.

După caz, acest tip de acțiune derulată cu predilecție pe platforma rețelelor de socializare poate cuprinde următoarele etape:

Monitorizarea permanentă a mediului comunicațional utilizat de țintă. Acest proces presupune un efort complex de cunoaştere detaliată a mediului în care se desfăşoară comunicarea (limbaj, depăşirea barierei lingvistice şi culturale, subiecte de interes etc.).

Elaborarea profilului psihologic comportamental inclusiv din punct de vedere al interacțiunii țintei cu cercul relațional apropiat în scopul determinării celei mai potrivite metode de abordare directă sau indirectă.

Inițierea legăturii on-line, operațiune delicată care presupune un echilibru atent între provocarea comunicării şi atragerea în comunicare.

Exploatarea informativă a țintei, aspect care presupune aplicarea unor tehnici de inginerie socială în vederea obținerii unor date particulare care pot facilita acțiunea infracțională (localizarea exactă a domiciliului şi a locului de muncă, sistemele antiefracție utilizate, ierarhia socială / profesională, situația financiară, parolele de accesare a conturilor bancare etc.).

Identificarea unor vulnerabilități comportamentale generate de exagerarea anumitor pasiuni, prezența unor vicii, frustrări etc., care ar facilita acțiuni de corupere, compromitere ori şantajare[3].

[3] Mitnick Kevin, Simon Williams, Wozniak Steve , T*he Art of Deception*, John Wilwz & Sons, 2002.

Orice viciu sau pasiune expusă prin intermediul rețelelor de socializare înlesneşte nemijlocit identificarea unor potențiale dominante principale de personalitate ale țintei.

În acest sens, este demn de subliniat că platformele comunicaționale de tip messenger, camerele de chat parolate sau forumurile de discuții reprezintă ținte predilecte de colectare a informațiilor privind caracterul şi personalitatea utilizatorilor, preocupări, frustrări, atitudini sau aspecte de intimitate etc.

Metode şi mijloace de protecție în spațiul virtual

Normele de conduită protectivă în mediul on-line derivă din răspunsurile la următoarele întrebări:

- Cu cine se pot împărtăşi informațiile cu caracter personal?
- Ce informații de identificare proprie şi a cercului relațional apropiat sunt permise a fi colectate?
- Ce relevanță prezintă datele personale din perspectiva unei entități infracționale?
- Ce mijloace şi metode de protecție sunt disponibile odată cu diseminarea informațiilor personale în rețelele de socializare? Dar în cazul navigării pe Web?

Fără a avea pretenția unei abordări comprehensive a subiectului privind metodele de protecție în spațiul virtual este dezirabil ca membrii unei societăți informaționale, îndeosebi cei care activează în domeniul intelligence, să aibă în vedere respectarea următorului decalog:

1. Nu se împărtăşesc informații familiale în rețelele de socializare. Nu se postează în nici o împrejurare fotografii sau montaje audio-video cu caracter personal sau din intimitate.

Dezvoltarea programelor de recunoaştere facială permite identificarea în timp real a unei persoane în condițiile existenței unei conexiuni de mare viteză şi a unei fotografii personale.

În condițiile în care, inclusiv rețeaua de socializare Facebook[4], dispune de un software specializat intitulat Facr, regăsirea unei persoane care şi-a postat fotografia devine o formalitate.

2. Nu se comunică în rețeaua de socializare date privind activitatea profesională sau viața privată.

Informațiile plasate de către utilizatorii neglijenți în rețelele de socializare sunt arhivate în baze de date cu structură complexă (conversații,

[4]www.bloomberg.com/news/2012-06-18/facebook-buys-face-com-adds-facial-recognition-software.html.

discuții, documente, texte etc.) care acceptă cumpărarea drepturilor de consultare şi extragere de informații de către terțe părți.

3. Nu se comunică în spațiul virtual date privind situația financiară

Neglijența privind gestionarea datelor financiare reprezintă un factor ce favorizează infracțiunile de fraudare a conturilor bancare. Un exemplu reprezentativ recent este cel al prestigioasei firmei de consultanță în domeniul exploatării surselor deschise STRATFOR, a cărei neglijență inexplicabilă în adoptarea unor măsuri de protecție a bazelor de date proprii a permis diseminarea neautorizată pe Internet a datelor financiare complete ale clienților şi fraudarea conturilor bancare ale acestora[5].

4. Serviciile de localizare permanentă prin GPS, disponibile atât în sistemul de operare Android (smartphone şi tablete PC), cât şi pe platformele de socializare trebuie dezactivate.

Cel puțin pentru personalul serviciilor de informații şi securitate, monitorizarea şi anticiparea deplasărilor în teren prin compromiterea securității on-line, se poate constitui într-un factor de risc (exemplu, activarea opțiunilor „Latitude" din Google Maps sau „Places" din Facebook[6]).

În plus, odată stabilită locația, tehnologia actuală permite activarea de la distanță a microfonului încorporat în terminalul mobil, în scopul realizării unor interceptări ambientale ilegale, cu condiția „infectării" în prealabil a dispozitivului cu un program software disponibil pe platformele comerciale on-line (protocolul „raving bug").

Trebuie subliniat că înlăturarea bateriei din telefonul mobil nu înlătură decât parțial pericolul unei interceptări ambientale ilegale, întrucât grație tehnologiei RFID[7], un microfon inert poate recepționa energie şi se poate activa de la o sursă externă aflată la distanță (2-200 metri) în urma „bombardării" cu unde de înaltă frecventă (3,1-10 GHz).

5. Opțiunea de transmitere de date prin aplicațiile Bluetooth sau WiFi trebuie dezactivată.

Datele stocate într-un terminal mobil tip smartphone, mai ales agenda telefonică, calendarul personal de evenimente şi fotografiile realizate pot fi accesate cu uşurință prin intermediul aplicației Bluetooth sau printr-o conexiune WiFi nesecurizată. De asemenea, facilitează transmiterea prin unde radio a programelor de tip „spy phone" către telefonul persoanei țintă.

[5] www. cryptome.org.
[6] http://apps.facebook.com/viewmycalendar.
[7] Radio Frequency Identification.

6. Identitatea dispozitivului cu care se accesează resursele mediului cibernetic (coincide în 90 % din cazuri cu identitatea utilizatorului) trebuie protejată în cursul navigării pe Web, prin anonimizare[8].

Comportamentul şi preferinţele unei ţinte pot fi stabilite printr-un proces de analiză a traficului de date şi a frecvenţei de accesări a unui domeniu anume. Indiferent dacă este vorba de reţele mobile (Vodafone, Orange) sau fixe (Romtelecom, DIGI NET), cel mai indicat mod de navigare este cel anonim.

Totuşi, este important de reţinut faptul că anonimizarea nu este sinonimă cu invizibilitatea, aspect perfect cunoscut de către persoanele specializate în colectarea de informaţii din spaţiul cibernetic.

7. Nu se deschid mesaje cu ataşamente primite de la persoane necunoscute cu care se interacţionează pe forumuri de discuţii sau pe aplicaţii gen messenger.

Deschiderea unor ataşamente recepţionate de la persoane necunoscută implică crearea unei breşe de securitate prin infectarea dispozitivelor conectate la spaţiul virtual (smartphone, laptop, desktop) urmată de extragerea, transmiterea iar ulterior distrugerea, tuturor informaţiilor stocate.

8. Comunicarea prin trafic E-mail cu persoanele din cercul relaţional apropiat trebuie securizată.

Securizarea comunicării prin criptarea poştei electronice blochează documentarea de către terţe părţi interesate, până la un orizont temporal la care informaţia devine irelevantă şi perimată[9].

9. Utilizarea unui program antivirus performant şi a unor programe de identificare a protocolului de spionare raving bug este obligatorie.

Întrucât socializarea on-line constituie o sursă potenţială de atacuri cibernetice asupra confidenţialităţii datelor proprii, utilizarea unui program antivirus minimalizează pericolul dar nu îl înlătură. În cazul terminalelor mobile infectate cu programe de spionare, procesul este ireversibil în majoritatea cazurilor. În consecinţă, se va proceda la resetarea telefonului.[10]

---

[8] Klander Lars, *Anti–Hacker,Ghidul securităţii reţelelor de calculatoare*, Editura All Educaţional, Bucureşti,1998.

[9] Băjenărescu Titu, *Progresele informaticii, criptografiei şi telecomunicaţiilor în secolul XX*, Ed. Matrix Rom, Bucureşti, 2003.

[10] www.KasperskyLab.com; www.Bitdefender.com.

10. Este recomandabil ca parolele utilizate pe site-urile de socializare să fie diferite şi schimbate lunar.

Pentru a oferi un minimum de protecție, parolele trebuie să fie complicate şi lungi, compuse din litere şi cifre aleatoare.

În privința arsenalului mijloacelor de protecție, profilul unui internaut precaut, mai ales din perspectiva unui angajat din domeniul intelligence, poate fi creionat după cum urmează:

- navighează pe Internet prin utilizarea unor programe de anonimizare eficiente (recomandăm software-ul TOR[11] sau JonDonym);
- foloseşte o căsuță poştală electronică criptată (recomandăm Hushmail);
- utilizează programe de criptare pentru datele sensibile din calculatorul personal (recomandăm TrueEncrypt).

Bibliografie

1. Băjenărescu Titu, *Progresele informaticii, criptografiei şi telecomunicațiilor în secolul XX*, Editura Matrix Rom, Bucureşti, 2003.

2. Goncalves Marcus, *Internet Strict Secret*, Editura Teora, Bucureşti, 2000.

3. Klander Lars, *Anti–Hacker. Ghidul securității rețelelor de calculatoare*, Editura All Educațional, Bucureşti,1998.

4. Manovich Lev, „New Media from Borges to HTML", The New Media Reader. Ed. Noah Wourdrip-Fruin&Nick Montfort Cambridge, Massachusetts, 2003.

5. Mitnick Kevin, Simon Williams, Wozniak Steve, *The Art of Deception*, John Wilwz & Sons, 2002.

6. Pakondi Victor, *Dicționar Internet & Tehnologii World Wide Web*, Editura Kondyli, Bucureşti, 2000.

Surse Internet

1. http://en.wikipedia.org/wiki/New_media
2. http://en.wikipedia.org/wiki/Facebook
3. http://apps.facebook.com/viewmycalendar
4. www.KasperskyLab.com
5. www.Bitdefender.com
6. www.cryptome.org
7. www.torproject.org

[11] www.torproject.org.