SECURITATEA REŢELELOR SOCIALE DIN MEDIUL ONLINE

prof.univ.dr. Ţuţu Pişleag
Universitatea Hyperion
asist.univ.drd. Cătălin Toader
Academia de Poliţie „Alexandru Ioan Cuza”

Abstract:

This article surveys the current state of security issues and available defense mechanisms regarding popular online social networks. It covers a wide variety of attacks and the corresponding defense mechanisms, if available. The authors focuses primarily on security. They offer an in-depth discussion of each category and analyze the connections among the different security issues involved.

Keywords: Security of online social networks; measurement and Analysis of Online Social Networks

Astăzi, o mare parte din utilizatorii reţelelor sociale au ajuns să comunice *cu orice fel de riscuri*, cu toate că se cunoaşte că încă din anul 2010, infractorii online au împânzit aceste reţele. De asemenea, *se ştie că majoritatea oamenilor nu cunoaște măsurile de bază pentru protejarea activităţii lor, a informaţiilor deţinute în propriile computere şi chiar a afacerilor derulate* prin intermediul Internetului. Cei mai mulţi utilizatori sunt fără cunoştinţe avansate în privinţa protecţiei online, accesează reţelele sociale de la adăpostul relativ al propriei case sau de la locul de muncă, crezând astfel că beneficiază de un anonimat care ar oferi un anume grad de siguranţă. Nu în ultimul rând, lipsa unui contact real cu oamenii de pe aceste

reţele este suficientă pentru a ne slăbi propriile măsuri de siguranţă[11]. Tocmai de aceea, majoritatea oamenilor constată într-o bună zi că au împărtăşit informaţii personale unor persoane străine, pe care i-au întâlnit fugar în diferite locuri, sau i-au ales din lista de prieteni a altor cunoştinţe de pe Internet.[12] Ca atare, indiferent de cum ne învaţă literatura de specialitate să ne protejăm pe linia securităţii în cadrul reţelelor sociale, de pericolele *„ascunse”* ale internetului oamenii vor folosi tot mai des aceste servicii via Internet, fie pentru socializare, fie pentru afaceri, conduşi în mare parte atât de propriul bun simţ, cât şi de instinctul de conservare[13].

Conform literaturii de specialitate trebuie să ţinem cont de două mari aspecte cu privire la securitatea în reţelele sociale şi anume:

a)securitatea părţii tehnice

Unde se cunoaşte că serviciile de comunicare şi socializare online permit userilor să intre în contact unii cu alţii mult mai repede şi mai puţin formal decât serviciile clasice de e-mail. Ca atare, reţelele de socializare online permit userilor să trimită file-uri şi attachment-uri cu fotografii, precum şi să folosească programe pentru telefonie sau video-chat, iar odată ce acestea pot fi cunoscute de administratorii de sistem, pot fi filtrate şi chiar blocate dacă se identifică vreo problemă.

b)securitatea personală a userului

Unde reţelele sociale încurajează şi facilitează interacţiunea deschisă între userii care se cunosc între ei sau au preocupări comune, dar astfel legăturile se disipează cumva sau chiar se pierd. Conform experţilor FBI există *două mari tactici* prin care infractorii informatici exploatează reţelele de socializare, cu precizarea că aceste metode sunt folosite împreună. Astfel, rezultă că, ameninţările asupra datelor dvs. pot veni dintr-un mediu *intern* sau *extern*, unde infractorii pot accesa reţelele care nu sunt asigurate într-un mod corect, sau aceştia, deosebit de abili sunt specializaţi în exploatarea vulnerabilităţilor din sistemul dumneavoastră pentru a avea astfel oportunitatea de a vă instala un program nedorit în propriul laptop, P.C. sau

[11]www.cert-ro.eu/ecsm.php

[12]Securitatea în reţelele sociale preocupă tot mai mulţi utilizatori din întreaga lume. Este şi firesc, din moment ce oamenii împărtăşesc o multitudine de informaţii personale, la care au acces nu doar prietenii şi familia, ci şi escrocii, care creează ameninţări tot mai variate. Anul acesta, aproape toţi utilizatorii Facebook au fost expuşi la scam-uri "clasice" de tipul "*ghici cine ţi-a vizualizat profilul*", dar şi la campanii frauduloase care promiteau premii substanţiale.

[13] http://www.descoperă.ro/capcanele-internetului/protect-securitatea-în-reţelele-sociale, Nicu Pârlog - 2012.

telefon mobil de ultimă generaţie.[14] De asemenea, hoţii pot sparge biroul dumneavoastră şi fura echipamente, iar personalul ar putea extrage date pe medii externe portabile.[15]

Ca atare, ameninţările interne sunt cu mult mai greu de anticipat şi pot fi la fel de devastatoare pentru afacerea dumneavoastră. Personalul poate fura datele din greşeală sau intenţionat, din diverse motive. În altă ordine de idei, datele sunt foarte uşor de extras din birou cu ajutorul CD-uri inscriptibile, stickuri USB, MP3 playere sau telefoane mobile. Toate aceste dispozitive pot deţine cantităţi mari de date şi sunt un mod discret în care un angajat ar putea copia datele şi pleca de la birou[16]. Cu privire la securitatea dispozitivelor (a laptopurilor sau altor dispozitive portabile), nu există nici o garanţie că acestea nu vor fi furate sau pierdute. În timp ce furtul în sine este frustrant şi aduce multe neplăceri, pierderea de informaţii ar putea avea consecinţe pe termen lung pentru afacerea ori datele cu caracter personal ale fiecăruia dintre noi. Dispozitivele portabile sunt destinate transportării uşoare de informaţii şi utilizării în afara biroului. Din aceste considerente sunteţi obligaţi să asiguraţi dispozitivele, la fel şi informaţiile care sunt conţinute în aceste dispozitive[17].

De asemenea, se cunoaşte că, odată ce o informaţie a fost postată online, ea şi-a pierdut caracterul privat, iar cu cât sunt postate mai multe informaţii despre o anumită persoană cu atât mai mult acea persoană devine din ce în ce mai vulnerabilă. În timp, infractorii, posedând aceste informaţii, au posibilitatea să-ţi spargă contul, tău sau al prietenilor ori asociaţilor, să-ţi instaleze virusuri sau troieni cu care la final poţi fi păgubit. Mulţi atacatori fac parte din grupuri de infractori care sunt motivaţi şi bine organizaţi, dispuşi să investească timp şi bani în vederea realizării obiectivelor infracţionale. După cum se vede interesul infractorilor este pe termen lung şi

[14]Idem

[15]Trebuie să analizaţi cu atenţie unde să stocaţi datele şi cum să le securizaţi fizic si electronic, să specificaţi cine are acces la acestea şi ce dispozitive sunt permise personalului să se conecteze la reţeaua dvs. de computere.

[16]http://cert.gov.md/resurse/furtul-de-date.html.

[17]Dispozitive mobile, cum ar fi laptop-urile şi telefoanele mobile ar trebui să fie criptate şi protejate cu o parolă. Există diverse programe pentru a cripta hard disk-ul din calculator pentru împiedica accesarea acestuia în cazul furtului. Criptarea este o conversie a datelor într-un cod secret pentru transmisterea datelor prin internet. Criptarea fişierelor vă asigură că persoane terţe nu pot vizualiza datele chiar dacă au acces la dispozitiv. Un astfel de program este folosit de regulă, pentru protejarea informaţiilor sensibile, cum ar fi proprietate intelectuală, politici ale companiei, date confidenţiale ale persoanelor, etc.

se folosesc de reţelele sociale, pentru că sunt cât de cât într-un mediu protejat.[18] Specialiştii în domeniu cunosc că infractorii exploatează popularitatea reţelelor sociale în scopul de a distribui spam-ul, malware-ul, precum şi atacurile de tip phishing, aceasta fiind o tehnică destul de comună în aceste zile.

Tot cu privire la *securitatea reţelelor sociale*, se poate spune că atacurile de spam prin intermediul reţelelor, a crescut vertiginos în ultimul timp.[19] Astfel, conform unui raport de cercetare publicat în 2013 de analiză a spamului în reţelele sociale (numai pentru reţelele Facebook, Twitter şi YouTube, cu privire la atacuri de spam în reţele între lunile aprilie şi iunie 2011) a dus la realizarea graficului de mai jos în care se prezintă atacurile pe cele trei reţele sociale şi procentajul spamului calculat pentru cele trei luni.[20] Se poate spune că cele mai multe spam-uri provin de la botnet. În cazul în care IP-urile originare au fost analizate (aşa cum se arată în graficul de mai jos), s-a constatat că 53% din spam-ul trimis în reţeaua socială îşi are originea în Statele Unite. Un alt 19% provine din diferite ţări europene.

[18]http://zeltser.com/computer-attacks-defenses.

[19]Unul dintre modelele evidente observate în raportul de cercetare, constă în creşterea numărului de atacuri de pe un site de social networking, apoi o cădere bruscă şi apoi o schimbare la următorul site social, ca şi în cazul în care ar urma unui model ciclic. S-a observat o creştere bruscă a numărului de atacuri pe Facebook, (un vârf), iar apoi un declin drastic. În timp ce atacurile de pe Facebook s-au redus, s-a observat o creştere a atacurilor de pe Twitter, care apoi a diminuat treptat, urmat de un val de atacuri pe YouTube. Durata medie de viaţă a fiecărui atac spam-ul în reţeaua socială este cuprins între 15 şi 20 de zile.

[20]http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf

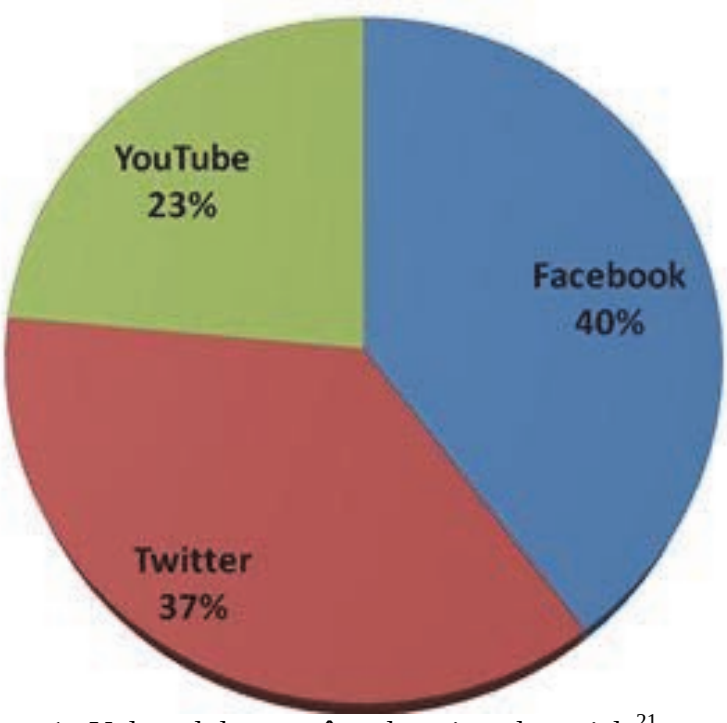

Figura 1. Volumul de spam în cele trei reţele sociale[21]

Cele mai multe dintre aceste adrese IP au fost pe lista neagră de tehnologie bazată pe o reputaţie negativă, din cauza implicării lor în trimiterea de spam.

În altă ordine de idei, literatura de specialitate indică principalele metode de a ataca *userii*, după cum urmează:[22]

a)Spoofing: un atac de spoofing, este o situaţie, în care o persoană sau program, este mascat cu success de un alt program, *prin falsificarea datelor* în scopul de a obţine un avantaj nelegitim.[23]

b)Pharming: este un atac cybernetic destinat pentru a redirecţiona userul de la un site legitim spre unul fals, cu scopul de a extrage datele persoanei.[24]

[21] Idem

[22] Catalogate ca incidente cu privire la securitatea reţelelor sociale.

[23]Spoofing-ul via e-mail se foloseşte de o adresă falsă de e-mail sau simulează o adresă reală. Spoofing-ul tip IP este folosit pentru a ascunde adresa IP reală a computerului infractorului.

[24] http://en.wikipedia.org/wiki/Pharming.

c)Phreaking: constă în obţinerea accesului neautorizat în sistemele de telecomunicaţii, cum ar fi echipamente şi sisteme, conectate la reţelele publice de telefonie. Atunci când reţelele de telefonie au devenit computerizate, phreaking-ul a devenit strâns legat de pirateria informatică. *Phreak, phreaker,* sau *Phreak telefon* sunt denumiri folosite de persoanele fizice care participă la *phreaking,* iar identităţile lor sunt, de obicei, mascate. Acest lucru este uneori numit cultura H / P (H *picioare* pentru *hacking* şi *P în picioare* pentru *phreaking).*[25]

d)Elicitation: constă în folosirea strategică a conversaţiilor pentru a extrage informaţii fără ca victima să îşi dea seama că de fapt este supusă unui interogatoriu. Nefind conştienţi de aceste tactici, răspundeţi la anumite întrebări aparent nevinovate, cu informaţii despre propria persoană, despre familie şi cercul de prieteni, precum şi despre alte lucruri ce îl interesează pe suspect. ***Elicitation*** poate folosi o poveste de acoperire pentru orice subiect de conversaţie şi de asemenea de ce se cer anumite întrebări.[26] Acesta (suspectul) poate apărea oriunde, la adunări culturale, pe reţelele de socializare, la conferinţe, la telefon, pe stradă, ori în casa cuiva când faceţi o vizită. Un *elicitor* instruit înţelege anumite predispoziţii şi înclinaţii umane sau culturale şi utilizează anumite tehnici pentru a exploata informaţiile.[27]

c)Doxing: este o formă de furt, exercitată printr-un proces de culegere sau deducere de informaţii ale altor persoane, cum ar fi numele, vârsta, e-mailul, adresa, numărul de telefon, fotografii etc. folosind surse accesibile publicului, cum ar fi Internetul. Cu alte cuvinte, doxingul, este metoda de a folosi internetul pentru a căuta detalii personale despre cineva.[28] Majoritatea

---

[25]Bruce Sterling, McLean, ,,Hacker represiunii" Virginia: IndyPublish.com. ISBN 1-4043-0641-2 . 2002.

[26] http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques.

[27]De exemplu, aţi planificat vreodată o petrecere surpriză pentru cineva şi trebuia să se ştie programul de desfăşurare, lista cu alimentele care le plac sau displac sau alte informaţii, fără ca persoana să afle de ce s-au colectat aceste informaţii sau în ce scop.

[28]Doxing se face iniţial prin luarea unei porţiuni (bucată) de informaţii (cum ar fi "nume" sau "adresa de e-mail") şi este menţinut ca o bază pentru a afla alte detalii posibile despre acea persoană. Termenul "doxing" este derivat din cuvântul "document de urmărire", care înseamnă a prelua documentele cu privire la o anumită persoană sau societate de orice natură, în scopul de a afla mai multe despre ei. De asemenea este o strategie utilizată de către grupuri de hacking, cum ar fi Anonymous şi LulzSec spinoffs sale şi AntiSec. Astăzi, reţelele sociale prin Internet au crescut la o asemenea dimensiune încât acesta conţine aproape orice

utilizatorilor de Internet se dovedesc a fi activi pe social media, prin site-urile de reţele sociale cum ar fi Facebook şi LinkedIn, care oferă o mină de aur virtuală cu informaţii necesare pentru a efectua *doxing.* Pentru că majoritatea utilizatorilor nu sunt conştienţi de problemele de securitate on-line şi au setările de confidenţialitate slabe pentru profilul lor, acest lucru este mai uşor pentru atacatori pentru a obţine acces la informaţiile personale, cum ar fi fotografii, numele reale, localizare, locuri de muncă, partenerul de viaţă, nume prieteni, rude, etc.[29] Consecinţele furtului de date prin doxing pot fi nebănuit de periculoase, în cazul în care informaţiile obţinute cum ar fi activităţile zilnice ale vreunei persoane publice, istoricul medical, preferinţele sexuale şi alte informaţii cu caracter personal sunt făcute publice. Acest lucru poate constitui o ameninţare gravă la adresa sănătăţii, nivelului de trai sau relaţiei victimei în societate.[30]

e)Cross-Site Scripting (XSS)[31]*:* este o tehnică de atac, care constă în *injectarea unui cod nociv* pe un site inofensiv, site care la prima vedere prezintă foarte multă încredere. Acest atac informatic de tip Stored XSS are loc atunci când codul infestant ajunge să fie instalat permanent pe un server, ceea ce va duce la *"infectarea"* oricărui computer care foloseşte serverul respectiv. Un alt tip de atac de tip Reflected XSS are loc atunci când un user care nu bănuieşte nimic dă click pe un link infectat, iar codul-problemă ajunge în server, de unde este retrimis înapoi în browserul victimei. Ca atare computerul victimei crede că acel cod este unul venit dintr-o sursă sigură şi de încredere.[32]

f)Baiting: (momeala), este atunci când cineva îţi înmânează un dispozitiv USB sau orice alt dispozitiv de stocare care este infestat cu un malware care va ajunge în computerul tău şi-i va oferi gratis tot ce deţii în el. Pentru a preveni infectarea este recomandabil să se scaneze toate device-urile electronice înainte de a accesa informaţia de pe ele[33].

g) Click-jacking: este tot o tehnică malware, care constă în a păcăli un utilizator de Web prin trimiterea de hyperlink-uri ascunse abil sub un link legitim şi pe care dai click fără ca victima să poată prevedea ceva.[34] După

---

informaţie pe care am fi putut-o imagina vreodată. Tot ce trebuie să faci este să utilizezi tehnici de doxing pentru a căuta ceea ce vrei.

[29] http://www.gohacking.com/what-is-doxing-and-how-it-is-done.

[30] Idem.

[31] Universal Cross Site Scripting (UXSS, sau Universal XSS).

[32] http://en.wikipedia.org/wiki/Cross-site_scripting.

[33] http://en.wikipedia.org/wiki/Scam_baiting

[34]Termenul "Clickjacking" a fost inventat de către Ieremia Grossman şi Robert Hansen în 2008.

accesare, un malware s-a instalat deja în computerul tău, sau ID-ul tău a ajuns deja la un site al celui (celor) care ţi-au trimis malware-ul. De regulă capcanele sunt instalate sub butoane virtuale pe care scrie "Like" sau "Share" de pe reţelele sociale.[35] Clickjacking este posibil deoarece caracteristici aparent inofensive ascunse abil pe pagini de web HTML pot fi utilizate pentru a efectua acţiuni neaşteptate, pentru a-ţi fura datele personale. Alte tehnici de malware asemănătoare ***click-jacking-ului,*** **sunt** *likejacking-ul şi cursorjacking* (o tehnică de redresare folosită pentru a schimba cursorul de la locaţia utilizatorului, sau pentru ascunderea lui).[36]

h) Scam[37]: atunci când suspecţii, în ingeniozitatea lor, fac tranzacţii şi afaceri false care conving userii să furnizeze sume de bani, informaţii personale sau diverse servicii în schimbul unor beneficii foarte mari. Dacă cineva de pe o rețea de socializare vă propune o afacere prea bună pentru a fi adevărată, mai mult ca sigur că sunteţi pe cale de a deveni victima unei tentative de scam. Ciber-infractorii se folosesc deseori de link-uri cu ştiri de mare impact sau evenimente sportive sau artistice drept momeli pentru persoanele care dau astfel click şi ajung pe site-uri infectate. Tot în categoria scam se încadrează escrocheriile online în urma cărora oamenii sunt păcăliţi să doneze sume de bani către organizaţii de caritate false.[38]

i)CryptoLocker Ransomware: ***este un fişier de criptare.***[39] **Corporaţiile şi firmele, primesc e-mailuri cu presupuse plângeri din partea clienţilor care conţin o ataşare care, atunci când este deschisă, apare ca o fereastră şi este, de fapt, un downloader malware. Acest downloader apoi se descarcă şi instalează malware-ul cunoscut astăzi sub numele de CryptoLocker. Deci malware-ul infectează fişierele importante care au fost criptate folosind o cheie publică unică generată de calculator. Pentru a decripta fişierele, aveţi nevoie de asistenţă şi ajutor pentru a obţine cheia privată. O copie a cheii private se află pe un server de la distanţă, care va distruge cheia după timpul specificat afişat în fereastră.** Însă, **atacatorii cer o răscumpărare de 300 dolari ca plată, în scopul de a decripta fişierele. Ceea ce utilizatorul nu ştie este că, şi după plată, decriptarea nu este fezabilă, iar acest malware nu**

[35]Fredrick Lane, "Web Surfers Face Dangerous New Threat: 'Clickjacking'". newsfactor.com. Retrieved 2008-10-08.

[36] http://en.wikipedia.org/wiki/Clickjacking.

[37] Fraudă, înşelătorie.

[38] http://en.wikipedia.org/wiki/Confidence_trick.

[39]CryptoLocker, este un Ransomware troian care vizează computerele care rulează cu aplicaţia Microsoft Windows şi a apărut prima dată în septembrie 2013, detectat de serverele F.B.I.

părăseşte calculatorul, punându-l la îndemâna tuturor. Soluţia constă în formatarea şi reinstalarea hard disk-ului şi restaurarea fişierelor distruse de pe o copie de rezervă.[40] *După cum se observă,* escrocii folosesc tehnici, metode şi sisteme inteligente, pentru a înşela milioane de oameni şi a obţine informaţii cu care păcălesc victimele să le trimită bani sau alte foloase necuvenite[41].

Ca o *concluzie,* se constată că ,,Riscurile ce frânează încă dezvoltarea explozivă a domeniului sunt agresarea spaţiului intim, privat şi lipsa de încredere în necunoscuţi. Călcâiul lui Ahile este teama că alţi străini din publicul larg vor afla care ne sunt valorile private, iar oamenii nu vor să împărtăşească informaţii personale sau cunoştinţe acumulate greu şi prin efort cu persoane necunoscute. Ultimul zid ce trebuie depăşit pentru a combina perfect tehnologia cu interacţiunea umană este problema confidenţialităţii şi respectării dreptului la siguranţă şi viaţă privată prin acceptarea în comunităţile online doar a persoanelor invitate, selectate, ce fac parte din acelaşi grup de interese".[42]

Ca atare, securitatea în reţelele sociale, este necesară pentru a asigura siguranţa tuturor proceselor informaţionale, iar aceasta nu se poate realiza fără anumite politici sau regulamente care să ofere un proces transparent, prin care orice persoană să fie informată despre cerinţele de utilizare şi să permită specialiştilor să monitorizeze şi să verifice practicile de securitate. Securitatea în reţelele sociale, poate ajuta orice beneficiar al reţelelor de socializare să reducă numărul încălcărilor normelor de securitate şi pierderea datelor, ajutând orice angajat prin respectarea practicilor de securitate sigure de utilizare a computerului.[43]

---

[40]http://en.wikipedia.org/wiki/CryptoLocker.

[41]Prevenirea atacurilor informatice se dovedeşte a fi soluţia cea mai bună şi are la bază conştientizarea, de către user, a pericolelor interactivităţii pe reţelele sociale. Este foarte bine să fii prevăzător/prevăzătoare, să poţi anticipa anumite consecinţe. Conform specialiştilor în domeniu, s-a constatat că Internetul are o putere de fascinaţie colosală în privinţa eliberării de inhibiţiile personale. De asemenea, nu tasta online ceva care, la un moment dat, s-ar putea întoarce împotriva ta sau prin intermediul căruia poţi fi atacat, mai ales că pe reţeaua de socializare poate fi un recidivist periculos sau un individ cu mari probleme comportamentale. Mediul online devine mai sigur atunci când sunt respectate câteva reguli de bază şi când cunoaştem riscurile comunicării pe calea Internetului.

[42]Mircea Mitruţiu, citat ,,*Analiza reţelelor sociale"* Pdf, Timişoara 2005, pag 20

[43]O politică de securitate în reţelele sociale, ar trebui să includă un şir de instrucţiuni pentru personal, pentru a putea răspunde la orice întrebare a acestora, inclusiv şi la întrebarea: la ce foloseşte această politică de securitate? Motivul

Ca propunere de ***lege ferenda*** la acest articol**, ar trebui implementată mai ales la nivel naţional o procedură de raportare a încălcărilor de securitate, ori elaborarea unui *cod de conduită* pentru pentru utilizatorii reţelelor sociale**[44]. Odată ce politica de securitate în reţelele de socializare este implementată, ea trebuie să devină o parte a activităţii unde fiecare trebuie să fie informat despre problemele de securitate actuale, astfel încât politica de securitate elaborată în prezent să fie actuală. Actualizarea politicii de securitate este o activitate de zi cu zi pentru fiecare dintre noi, cum ar fi verificarea poştei electronice împotriva viruşilor şi deconectarea computerului de la Internet, la sfârşitul zilei. De asemenea, trebuie monitorizată şi testată politica de securitate şi identificate problemele potenţiale şi reale de securitate înainte ca acestea să devină probleme care pot costa timp şi bani[45].

Bibliografie selectivă:

Bruce Sterling, McLean, ,,Hacker represiuni" Virginia: IndyPublish.com. ISBN 1-4043-0641-2 . 2002;

Fredrick Lane, "Web Surfers Face Dangerous New Threat: 'Clickjacking'". newsfactor.com. Retrieved 2008-10-08;

Mircea Mitruţiu, ,,*Analiza reţelelor sociale"* Pdf, Timişoara 2005, pag 20

Resurse internet:

www.cert-ro.eu/ecsm.php;

http://www.descoperă.ro/capcanele-internetului/protect-securitatea-în-reţelele-sociale, Nicu Pârlog – 2012;

http://cert.gov.md/resurse/furtul-de-date.html;

http://zeltser.com/computer-attacks-defenses;

http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf;

http://en.wikipedia.org/wiki/Pharming;

http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques;

http://cert.gov.md/resurse/politica-de-securitate.html.

---

principal pentru a implementa o politică de securitate constă în necesitatea de a informa toţi angajaţii despre metodele corecte de utilizare a calculatoarelor şi nu numai,cât şi de a informa cum să reacţioneze în cazurile unor incidente.

[44]Se cunoaşte că deseori angajaţilor le este dificil să vorbească în mod deschis. Dacă se oferă un astfel de mecanism de raportare, este o probabilitate că ei mai repede vor raporta despre ceea ce-i îngrijorează. Au existat o serie de cazuri mediatizate în care angajaţii au discutat opiniile cu colegii în reţele socializate cu privire la locul de muncă şi normele de conduită.

[45]http://cert.gov.md/resurse/politica-de-securitate.html