ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ (Τ.Ε.Ι.) **ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ**

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (ΠΑΤΡΑ)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΚΤΥΑΚΟΙ ΚΟΜΒΟΙ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΚΑΙ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

ΣΠΟΥΔΑΣΤΡΙΑ: ΚΟΥΤΣΙΚΟΥ ΝΕΚΤΑΡΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Κ. ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΑΛΚΙΟΠΟΥΛΟΣ

ΠΑΤΡΑ - 2016

ΠΡΟΛΟΓΟΣ

Η δημοτικότητα των ιστοτόπων κοινωνικής δικτύωσης έχει αυξηθεί σε εκπληκτικά επίπεδα. Δεν υπάρχει καμία αμφιβολία για την χρησιμότητα των sites όπως το Facebook, το Twitter και το LinkedIn. Μπορούν να χρησιμοποιηθούν για αναζητήσεις επαγγελματικής δικτύωσης και θέσεων εργασίας, ως μέσο για την αύξηση των εσόδων των πωλήσεων, ως ένα εργαλείο για να κρατήσει το κοινό για την ασφάλεια και άλλα θέματα ή ως ένας τρόπος για να επανασυνδεθεί ο χρήστης με τους φίλους του.

Ωστόσο, όπως συμβαίνει με κάθε νέο εργαλείο ή εφαρμογή, είναι πάντα σημαντικό να παρακολουθείται εκ του σύνεγγυς, σχετικά με τις επιπτώσεις ασφάλεια. Κάθε ένα από αυτά τα εργαλεία έρχεται με το δικό του σύνολο ζητημάτων για την ασφάλεια που μπορεί να βάλει συστήματα πληροφοριών ή/και τα προσωπικά δεδομένα σε κίνδυνο. Αυτή η εργασία αναλύει τους κυριότερους από αυτούς τους κινδύνους και προσδιορίζει τις επιπτώσεις και τους μηχανισμούς των επιθέσεων με στόχο να συνεισφέρει στην προστασία των προσωπικών και εταιρικών στοιχείων.

ΠΕΡΙΛΗΨΗ

Οι ιστότοποι κοινωνικής δικτύωσης έχουν γίνει ένας πιθανός στόχος για τους επιτιθέμενους λόγω της διαθεσιμότητας των ευαίσθητων πληροφοριών, καθώς και των εκτενών βάσεων χρηστών. Ως εκ τούτου, τα ζητήματα προστασίας της ιδιωτικής ζωής και της ασφάλειας στα online κοινωνικά δίκτυα αυξάνονται. Αυτή η εργασία αναλύει διαφορετικά θέματα προστασίας της ιδιωτικής ζωής και της ασφάλειας, καθώς και τις τεχνικές που χρησιμοποιούν οι εισβολείς για να ξεπεραστούν οι μηχανισμοί ασφαλείας του κοινωνικού δικτύου, ή να επωφεληθούν από ορισμένες ατέλειες στο site κοινωνικής δικτύωσης.

Λέξεις κλειδιά –ανάλυση κοινωνικών δικτύων, κοινωνικό γράφημα, απόρρητο, ιδιωτικότητα, αρχιτεκτονική εξυπηρετητή-πελάτη, αρχιτεκτονική P2P

ABSTRACT

Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as extensive user base. Therefore, the issues of protection of privacy and security in online social networks are growing. This thesis analyzes different issues of privacy and security, as well as the techniques used by hackers to overcome the security mechanisms of the social network, or take advantage of some defects in the social networking site.

Keywords - social networks analysis, social graph, confidentiality, privacy, identity anonymity, client-server architecture, P2P architecture

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Από τον Ιανουάριο του 2009, η διαδικτυακή εφαρμογή κοινωνικής δικτύωσης Facebook εγγράφει περισσότερα από 175 εκατομμύρια ενεργούς χρήστες. Για να θέσουμε αυτό τον αριθμό σε μια προοπτική, αυτός είναι μόνο ελαφρώς λιγότερος από τον πληθυσμό της Βραζιλίας (190 εκατομμύρια) και πάνω από το διπλάσιο του πληθυσμού της Γερμανίας (80 εκατομμύρια). Την ίδια στιγμή, κάθε λεπτό, 10 ώρες περιεχομένου ανέβηκαν στην πλατφόρμα κοινής χρήσης βίντεο στο YouTube. Και, η ιστοσελίδα φιλοξενίας εικόνων και φωτογραφιών Flickr παρέχει πρόσβαση σε περισσότερα από 3 δισεκατομμύρια φωτογραφίες, καθιστώντας τη παγκοσμίου φήμης συλλογή του Μουσείου του Λούβρου (300.000 αντικείμενα) μικρή συγκριτικά. Σύμφωνα με τη Forrester Research, το 75% των χρηστών του Διαδικτύου χρησιμοποιήσαν τα μέσα κοινωνικής δικτύωσης κατά το δεύτερο τρίμηνο του 2008, με την εγγραφή σε κοινωνικά δίκτυα, ανάγνωση blogs, ή συμβολή με σχόλια σε δικτυακούς τόπους αγορών καταναλωτικών προϊόντων. Παρατηρείται μια σημαντική αύξηση από το 56% το 2007.

Η παραπάνω αύξηση δεν περιορίζεται σε εφήβους, αλλά τα μέλη της Generation X, τώρα 35-44 ετών, καταλαμβάνουν όλο και περισσότερο τις θέσεις των εισερχομένων, θεατών και κριτικών σε ιστοσελίδες κοινωνικής δικτύωσης. Ως εκ τούτου, είναι λογικό να πούμε ότι τα social media αποτελούν μια επαναστατική νέα τάση που θα πρέπει να παρουσιάσει ενδιαφέρον για τις εταιρείες που δραστηριοποιούνται στο διαδικτυακό χώρο - ή οποιοδήποτε χώρο.Σύμφωνα με (EPC, 2015), σε σχέση με το 2014, κατά το 2015 ο παγκόσμιος πληθυσμός αυξήθηκε κατά 1,6% ενώ οι χρήστες του διαδικτύου κατά 21% και οι χρήστες των μέσων κοινωνικής δικτύωσης κατά 12%. Οι μοναδικοί χρήστες κινητών συσκευών αυξήθηκαν κατά 5% ενώ οι χρήστες μέσων κοινωνικής δικτύωσης μέσω κινητών συσκευών αυξήθηκαν κατά 23% (EPC, 2011). Η χρήση των μέσων κοινωνικής δικτύωσης έχει αυξηθεί δραματικά και πλέον δεν αφορά μόνο ιδιωτικούς χρήστες, αλλά και επιχειρήσεις. Πέρα από τα πολλά οφέλη που έχει για τις επιχειρήσεις, υπάρχουν διάφοροι κίνδυνοι και ζητήματα ασφαλείας που εγείρονται.

Οι δικτυακοί τόποι κοινωνικής δικτύωσης στο Internet έχουν δημιουργήσει μια επανάσταση στην κοινωνική συνδεσιμότητα. Ωστόσο, οι απατεώνες, οι εγκληματίες, και άλλοι ανέντιμοι φορείς εκμεταλλεύονται αυτή τη δυνατότητα για φαύλους σκοπούς.

Υπάρχουν κυρίως δύο τακτικές που χρησιμοποιούνται για την εκμετάλλευση στα διαδικτυακά κοινωνικά δίκτυα. Στην πράξη, συχνά συνδυάζονται. Ο πρώτος τρόπος περιλαμβάνει προγράμματα υπολογιστή που ειδικεύονται στην ανάπτυξη και διαχείριση κώδικα υπολογιστή για να αποκτήσουν πρόσβαση ή να εγκαταστήσουν ανεπιθύμητο λογισμικό στον υπολογιστή ή το κινητό του θύματος, και ο δεύτερος τρόπος περιλαμβάνει κακόβουλα άτομα που ειδικεύονται στην εκμετάλλευση των προσωπικών συνδέσεων μέσω των κοινωνικών δικτύων. Οι κοινωνικοί χάκερ, που μερικές φορές αναφέρονται ως κοινωνική μηχανικοί, μπορούν να χειραγωγήσουν τους ανθρώπους μέσω των κοινωνικών αλληλεπιδράσεων (αυτοπροσώπως, μέσω τηλεφώνου, είτε εγγράφως).

Οι άνθρωποι είναι ο αδύναμος κρίκος στην ασφάλεια στον κυβερνοχώρο, και οι χάκερς και κοινωνικοί χειριστές το γνωρίζουν αυτό. Προσπαθούν να ξεγελάσουν τους ανθρώπους ώστε να ξεπεράσουν τους τοίχους ασφαλείας. Σχεδιάζουν τις δράσεις τους για να φαίνονται αβλαβείς και νόμιμοι.

Το να γίνει κανείς θύμα απάτης ή κακόβουλης επίθεσης στο διαδίκτυο, μπορεί να έχει σημαντικές επιπτώσεις για το άτομο θύμα καθώς και για την επιχείρηση στην οποία το άτομο εργάζεται. Οι ιστότοποι κοινωνικής δικτύωσης είναι υπηρεσίες που βασίζονται στο Internet που επιτρέπουν στους ανθρώπους να επικοινωνούν και να μοιράζονται πληροφορίες με μια ομάδα.

Μόλις η πληροφορία πδημοσιεύεται σε ένα site κοινωνικής δικτύωσης, δεν είναι πλέον ιδιωτική. Όσο περισσότερες πληροφορίες δημοσιεύει ένας χρήστης, τόσο πιο ευάλωτος μπορεί να γίνει. Ακόμα και όταν χρησιμοποιεί ρυθμίσεις υψηλής ασφάλειας, οι φίλοι ή οι ιστοσελίδες μπορεί κατά λάθος να διαρρεύσουν πληροφορίες το χρήστη.

Οι προσωπικές πληροφορίες που μοιράζεται ο χρήστης θα μπορούσαν να χρησιμοποιηθούν για τη διεξαγωγή επιθέσεων εναντίον του ίδιου ή των συνεργατών του. Όσο περισσότερες πληροφορίες δημοσιεύονται, το πιο πιθανό είναι κάποιος να μιμηθεί και να ξεγελάσει έναν από τους φίλους σας με στόχο την κοινή χρήση προσωπικών πληροφοριών, το κατέβασμα κακόβουλου λογισμικού, ή την παροχή πρόσβασης σε απαγορευμένες ιστοσελίδες.

1 ΤΟ WEB 2.0 ΚΑΙ ΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

1.1 Η ΑΥΞΗΣΗ ΤΗΣ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το Διαδίκτυο δημιουργήθηκε από το ερευνητικό έργο της ομάδας Agency Research Projects Administration (ARPA) του Υπουργείου Αμύνης των ΗΠΑ τη δεκαετία του 1960, και σχεδιάστηκε ώστε να επιτρέπει στους υπολογιστές να επικοινωνούν μεταξύ τους, σε περίπτωση πυρηνικής επίθεσης. Ένα μεγάλο μέρος της αντοχής του σημερινού συστήματος οφείλεται στις τεράστιες ποσότητες κονδυλίων που επενδύθηκαν προς έρευνα στον τομέα αυτόν. Στην ομάδα ARPA συγκεντρώθηκαν αρκετοί νέοι, φιλόδοξοι επιστήμονες ηλεκτρονικών υπολογιστών, όπως ο Paul Baran, ο οποίος εφηύρε τη μεταγωγή πακέτων, και τις συναφείς καινοτομίες όπως τα νευρωνικά δίκτυα, τη θεωρία ουρών, τη προσαρμοστική δρομολόγηση, και τα πρωτόκολλα μεταφοράς αρχείων. Κατά τη διαδικασία αυτή, η ARPA δημιούργησε ένα δίκτυο αρκετά διαφορετικό από το κεντρικό σύστημα της τηλεφωνικής εταιρείας (δηλαδή, η AT&T), το οποίο στηρίχθηκε σε αναλογικές πληροφορίες. Μάλλον η ψηφιοποίηση διευκόλυνε την δημιουργία ενός αποκεντρωμένου και μετά κατανεμημένου δικτύου. Ο πυρήνας του δικτύου αυτού που ονομάστηκε ARPANET αρχικά συνέδεε τα πανεπιστήμια όπως το Στάνφορντ, UCLA, το Πανεπιστήμιο της Καλιφόρνιας στη Σάντα Μπάρμπαρα, και το Πανεπιστήμιο της Γιούτα. Οι αρχικοί στρατιωτικοί στόχοι σύντομα συμπληρώνονται από πολιτικούς στόχους. Το 1972, ο Ray Tomlinson δημιούργησε προσαρμοσμένα μηνύματα υπολογιστή για προσωπική χρήση, εφευρίσκοντας το email. Από το 1984 έως το 1995, το διαδίκτυο παρεχόταν από το National Science Foundation, το οποίο αναπτύχθηκε για να συνδέσει τους ακαδημαϊκούς υπερυπολογιστές από μια επιλεγμένη σειρά πανεπιστημιουπόλεων στις Ηνωμένες Πολιτείες της Αμερικής (Warf, 2013).

Στη δεκαετία του 1990 ο έλεγχος στο διαδίκτυο ιδιωτικοποιήθηκε μέσω μιας κοινοπραξίας των εταιρειών τηλεπικοινωνιών. Το Διαδίκτυο εμφανίστηκε σε παγκόσμια κλίμακα μέσω της ενσωμάτωσης των υφιστάμενων συστημάτων τηλεφώνου, οπτικών ινών, και δορυφόρων, η οποία κατέστη δυνατή από την τεχνολογική καινοτομία της μεταγωγής πακέτων, το TCP / IP (πρωτόκολλο ελέγχου μετάδοσης / Πρωτόκολλο Διαδικτύου), και την τεχνολογία Ψηφιακού Δικτύου Ενοποιημένων Υπηρεσιών (Integrated Services Digital Network - ISDN), στις οποίες μπορούν να αποσυντεθούν μεμονωμένα μηνύματα, τα συστατικά στοιχεία να μεταδίδονται από διάφορα κανάλια, και στη συνέχεια να επανασυναρμολογούνται, σχεδόν ακαριαία, στον προορισμό (Brandtzægetal., 2011). Στη δεκαετία του 1990, οι γραφικές διεπαφές που αναπτύχθηκαν στην Ευρώπη απλοποίησαν σε μεγάλο βαθμό τη χρήση του Διαδικτύου, γεγονός που οδήγησε στη δημιουργία του Παγκόσμιου Ιστού (World Wide Web).

Σύντομα δημιουργήθηκε και πλήθος ιδιωτικών περιηγητών στο διαδίκτυο (web browsers), όπως οι Netscape, Internet Explorer και Firefox. Ο αριθμός των δικτυακών τόπων αυξήθηκε εκθετικά, από περίπου 1 εκατομμύριο το 1990 σε περισσότερα από 4 δισεκατομμύρια το 2011. Η επανάσταση της μικροηλεκτρονικής είχε ως αποτέλεσμα τεράστιες μειώσεις στο κόστος των υπολογιστών και εκθετικές αυξήσεις στη δύναμη

και τη μνήμη τους. Ως εκ τούτου, η τιμή των προσωπικών υπολογιστών (PCs) συνεχίζει να μειώνεται ραγδαία. Σύμφωνα με τον νόμο του Moore, ο οποίος υποστηρίζει ότι το κόστος των υπολογιστών πέφτει στο μισό κάθε χρόνο, οι ηλεκτρονικοί υπολογιστές έχουν γίνει εμπορικά καταναλωτικά προϊόντα μεγάλης κλίμακας σε πολλές χώρες, και σχετικά τα τερματικά μηχανήματα είναι άμεσα διαθέσιμα για σχετικά μικρά ποσά.

Το Διαδίκτυο έχει εξελιχθεί με τρεις σημαντικούς τρόπους κατά την τελευταία δεκαετία: το περιεχόμενο έχει εξελιχθεί από σχετικά στατικές σελίδες κειμένου και ιστοσελίδες σεπολυμεσικό περιεχόμενο υψηλού εύρους ζώνης που απαιτεί χαμηλή καθυστέρηση μετάδοσης, η χρήσηγίνεται ταχύτατα παγκοσμιοποιημένη και η πρόσβαση έχει μετακινηθεί πέρα από επιτραπέζιους υπολογιστές που χρησιμοποιούν σταθερές συνδέσεις σε μια ποικιλία νέων συσκευών που χρησιμοποιούν κινητές ευρυζωνικές υπηρεσίες. Είναι σημαντικό ότι, η ταχύτητα αυτής της εξέλιξης στην τεχνολογία και η αποδοχή της, είναι μοναδική στην ανθρώπινη ιστορία (Warf, 2013).

Οι υπηρεσίες έχουν εξελιχθεί στο Διαδίκτυο σε δύο κατευθύνσεις που είναι σημαντικές για την ανάπτυξη των παγκόσμιων ροών κυκλοφορίας. Πρώτον, ένας αυξανόμενος αριθμός εφαρμογών υψηλού εύρους ζώνης, κυρίως βίντεο, καθίστανται διαθέσιμος, με αποτέλεσμα τη σημαντική και αυξανόμενη ποσότητα της ζήτησης εύρους ζώνης. Δεύτερον, υπάρχουν όλο και περισσότερο εφαρμογές ευαίσθητες στην καθυστέρηση, όπως το VoIP. Την ίδια στιγμή που οι υπηρεσίες εξελίσσονται, το Διαδίκτυο παγκοσμιοποιείται με ρυθμό επιταχυνόμενο. Η πρόσβαση στο Διαδίκτυο έχει μετακινηθεί από το να επικεντρώνεται στον ανεπτυγμένο κόσμο το 2000, προς το να γίνει όλο και περισσότερο εστιασμένη στις αναπτυσσόμενες χώρες το 2011, ανάλογα με την κατανομή του παγκόσμιου πληθυσμού. Ο τρίτος τρόπος με τον οποίο έχει εξελιχθεί το Διαδίκτυο είναι η αλλαγή στη φύση της πρόσβασης στο Διαδίκτυο: αυτή έχει εξελιχθεί από το να είναι εξαρτημένη από τη σταθερή πρόσβαση, συνήθως μέσω ενός τερματικού στην επιφάνεια εργασίας, με την κινητή πρόσβαση μέσω ενός smartphone ή tablet. Οι κινητές ευρυζωνικές συνδέσεις αυξάνονται με ταχείς ρυθμούς, με ετήσιο ρυθμό ανάπτυξης μεγαλύτερο από τον ετήσιο ρυθμό ανάπτυξης της σταθερής πρόσβασης σε κάθε περιοχή. Σε όλες τις περιοχές, ιδιαίτερα τις αναπτυσσόμενες αγορές, οι κινητές συνδέσεις υπερβαίνουν ήδη τις σταθερές ευρυζωνικές συνδέσεις σε σχέση με τον αριθμό των συνδρομητών. Η διαθεσιμότητα των κινητών ευρυζωνικών μέσω σταθερών συνδέσεων είναι μια σημαντική κινητήρια δύναμη της παγκοσμιοποίησης της πρόσβασης στο Διαδίκτυο στις αναπτυσσόμενες χώρες, και με τη σειρά της η κινητή πρόσβασηαλλάζει τη φύση και τη χρήση της πρόσβασης στο Διαδίκτυο (Warf, 2013).

1.2 Το Web 2.0

Το Web 2.0 είναι το δεύτερο στάδιο του Διαδικτύου, το οποίο χαρακτηρίζεται κυρίως από τη μεταβολή των στατικών ιστοσελίδων σε δυναμικές με περιεχόμενο που παράγεται από τους χρήστες και την ανάπτυξη των μέσων κοινωνικής δικτύωσης (OxfordDictionary, 2016). ToWeb 2.0 είναι ο όρος που χρησιμοποιείται ευρέως για την περιγραφή της νέας προσέγγισης και της χρήσης του διαδικτύου, ως ένα μέρος της δυναμικής αλληλεπίδρασης σε πραγματικό χρόνο, όπου το περιεχόμενο συνεχώς αλλάζει, εμπλουτίζεται και σχολιάζεται από τους χρήστες και τους φορείς

εκμετάλλευσης. Έχει πολύ περισσότερο να κάνει με το τι κάνουν οι άνθρωποι με την τεχνολογία από την ίδια την τεχνολογία, καθώς δεν χρησιμοποιούν πλέον το διαδίκτυο απλώς για την ανάκτηση πληροφοριών, αλλά οι χρήστες έχουν πλέον δημιουργούν και καταναλώνουν το περιέχομενο, και ως εκ τούτου, προστίθεται αξία στις ιστοσελίδες που τους επιτρέπει να το πράξουν (Paquette, 2013).

Ένα σημαντικό χαρακτηριστικό των ιστοσελίδων Web 2.0 είναι η εξ' ορισμού ενσωμάτωση διαφόρων τεχνολογιών και εφαρμογών με στόχο την ενίσχυση της λειτουργικότητας. Αυτή η βελτιωμένη λειτουργικότητα συνδέεται κυρίως με ιστοσελίδες που είναι σε θέση να δημοσιεύσουν και να εμφανίσουν ποικίλο περιεχόμενο,περιεχόμενο που δημιουργήθηκε από τους χρήστες, ή το γεγονός ότιη ιστοσελίδα θα μπορούσε να αντλήσει πληροφορίες συνεργικά από τρίτους (Sambhanthan και Good, 2013).

Αντί για απλή ανάγνωση μιας ιστοσελίδας Web 2.0, ο χρήστης καλείται να συνεισφέρει στο περιεχόμενο της σχολιάζοντας δημοσιεύματα ή με τη δημιουργία ενός λογαριασμού χρήστη ή προφίλ στην ιστοσελίδα, η οποία μπορεί να επιτρέψει αυξημένη συμμετοχή. Αυξάνοντας την έμφαση σε αυτές τις ήδη υφιστάμενες δυνατότητες, οι χρήστες ενθαρρύνονται να στηρίζονται περισσότερο στον browser τους για την διεπαφή χρήστη, το λογισμικό εφαρμογών και τις εγκαταστάσεις αποθήκευσης αρχείου. Το μοντέλο αυτό έχει ονομαστεί «δίκτυο ως πλατφόρμα». Κύρια χαρακτηριστικά του Web 2.0 περιλαμβάνουν τους δικτυακούς τόπους κοινωνικής δικτύωσης, τις πλατφόρμες αυτο-δημοσίευσης, το tagging (ανάθεση ετικετών), τα κουμπιά «Μου αρέσει» και την κοινωνική δικτύωση με τη δημιουργία προφίλ. Οι χρήστες μπορούν να παρέχουν τα δεδομένα που είναι σε μια τοποθεσία Web 2.0 και να ασκούν κάποιο έλεγχο πάνω σε αυτά τα δεδομένα. Αυτές οι ιστοσελίδες μπορεί να έχουν μια «αρχιτεκτονική της συμμετοχής» που ενθαρρύνει τους χρήστες να προσθέτουν αξία στην εφαρμογή, καθώς τη χρησιμοποιούν. Μερικοί μελετητές παραθέτουν το υπολογιστικό νέφος (cloud computing) ως παράδειγμα του Web 2.0, επειδή το υπολογιστικό νέφος προέρχεται από την δυνατότητα υπολογιστικής στο Διαδίκτυο.

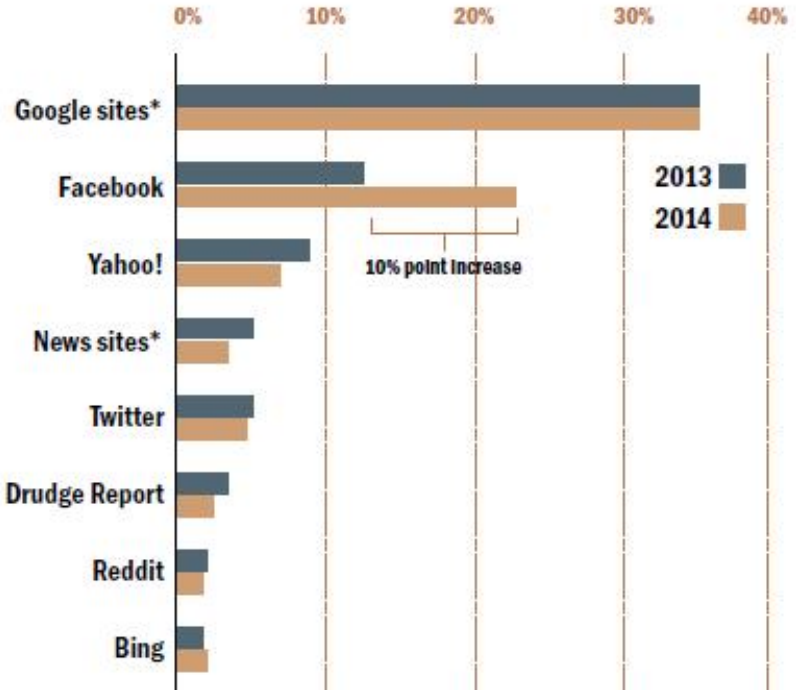
Το Web 2.0 προσφέρει σε όλους τους χρήστες την ίδια ελευθερία να συνεισφέρουν. Ενώ το γεγονός αυτό δίνει τη δυνατότητα για σοβαρή συζήτηση και συνεργασία, επίσης αυξάνει τη συχνότητα εμφάνισης των «spamming» από κακόβουλους χρήστες. Η αδυναμία θέσης εκτός από την ομάδα των μελών που δεν συμβάλλουν στην παροχή αγαθών από την ανταλλαγή των κερδών δημιουργεί την πιθανότητα τα σοβαρά μέλη να προτιμήσουν να μην συμβάλλουν και να αποδέχονται μόνο τη δωρεάν συμβολή των άλλων. Αυτό απαιτεί αυτό που μερικές φορές ονομάζεται ριζική εμπιστοσύνη από τη διοίκηση της ιστοσελίδας. Σύμφωνα με τον Best, τα χαρακτηριστικά του Web 2.0 είναι: πλούσια εμπειρία του χρήστη, η συμμετοχή των χρηστών, το δυναμικό περιεχόμενο, μεταδεδομένα, τα πρότυπα Ιστού, και η επεκτασιμότητα. Περαιτέρω χαρακτηριστικά, όπως η διαφάνεια, η ελευθερία και η συλλογική νοημοσύνη μέσω της συμμετοχής των χρηστών, μπορούν επίσης να θεωρηθούν ως βασικά χαρακτηριστικά του Web 2.0.

Τα βασικά χαρακτηριστικά του Web 2.0 περιλαμβάνουν (O'Reilly, 2005):

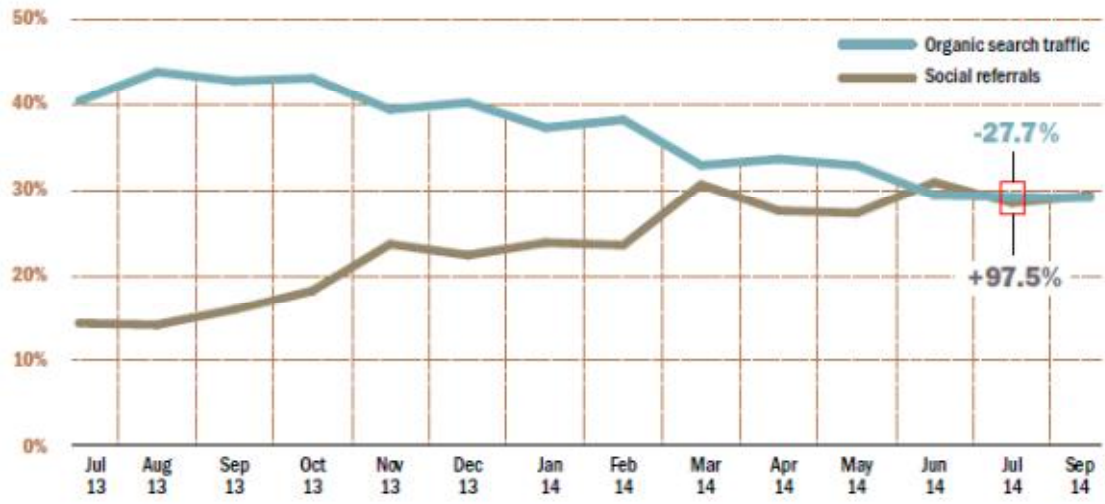
- Ελεύθερη κατηγοριοποίηση των δεδομένων που επιτρέπει στους χρήστες να ταξινομούν και να βρίσκουν πληροφορίες συλλογικά (π.χ. tagging)

- Πλούσια εμπειρία του χρήστη - το δυναμικό περιεχόμενο που ανταποκρίνεται στα σχόλια των χρηστών
- Συμμετοχή χρήστη - Η ροή πληροφοριών γίνεται σε δύο κατευθύνσεις, μεταξύ του ιδιοκτήτη της ιστοσελίδας και του χρήστη του ιστοτόπου μέσω της αξιολόγησης, αναθεώρησης και του σχολιασμού. Οι χρήστες του ιστοτόπου προσθέτουν περιεχόμενο σε αυτόν το οποία είναι προσβάσιμο και από άλλους χρήστες.
- Λογισμικό ως υπηρεσία – Οι ιστοσελίδες Web 2.0 αναπτύσσουν APIs που επιτρέπουν την αυτοματοποιημένη χρήση, όπως από μια εφαρμογή ή mashup
- Μαζική συμμετοχή - Καθολική πρόσβαση στο διαδίκτυο οδηγεί σε διαφοροποίηση των ανησυχιών από την παραδοσιακή βάση χρηστών Διαδικτύου

1.3 ΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (SOCIALMEDIA)



Εικόνα 1-1 Κίνηση που δημιουργούν τα μέσα κοινωνικής δικτύωσης προς ιστοσελίδες, σε σύγκριση με άλλες πηγές (EPC, 2015).



Εικόνα 1-2κίνηση σε ιστοσελίδες από αναφορές στα μέσα κοινωνικής δικτύωσης σε σύγκριση με την κίνησης που προκύπτει από οργανική αναζήτηση (EPC, 2015).

Η Εικόνα 1-1 παρουσιάζει τη κίνηση που δημιουργούν τα μέσα κοινωνικής σε ιστοσελίδες που έχουν καταγραφεί στη λίστα του Parse.ly (EPC, 2015). Παρατηρούμε ότι μεταξύ 2013-2014 η κίνηση που δημιουργεί το Facebook αυξήθηκε κατά 10% ενώ άλλα σημαντικά μέσα κοινωνικής δικτύωσης όπως το Twitterπαρουσίασαν ελάχιστη μείωση. Στην Εικόνα 1-2 παρουσιάζεται διάγραμμα που περιγράφει την πηγή της κίνησης στις ιστοσελίδες της λίστας του Parse.ly (EPC, 2015). Παρατηρούμε ότι ενώ το 2013 η κίνηση που δημιουργούταν από τα μέσα κοινωνικής δικτύωσης υπολειπόταν κατά 25 ποσοστιαίες μονάδες αυτή που δημιουργούταν από τις μηχανές αναζήτησης, αυτό το ποσοστό έχει εξισορροπηθεί από τον Ιούνιο του 2014 και τα μέσα κοινωνικής είναι υπεύθυνα για το 30% της κίνησης που κατευθύνεται στις ιστοσελίδες.

Ωστόσο, δεν είναι υπερβολικά πολλές οι επιχειρήσεις που φαίνεται να ενεργούν με άνεση σε έναν κόσμο όπου οι καταναλωτές μπορούν να μιλήσουν τόσο ελεύθερα μεταξύ τους και οι επιχειρήσεις έχουν ολοένα και λιγότερο έλεγχο πάνω τις διαθέσιμες πληροφορίες σχετικά με αυτές στον κυβερνοχώρο. Σήμερα, αν ένας χρήστης πληκτρολογεί στο Internet το όνομα μιας επιχείρησης στην αναζήτηση Google, ανάμεσα στα πέντε κορυφαία αποτελέσματα συνήθως περιλαμβάνεται όχι μόνο η εταιρική ιστοσελίδα, αλλά και η αντίστοιχη καταχώρηση στη διαδικτυακή εγκυκλοπαίδεια Wikipedia. Εδώ, για παράδειγμα, οι πελάτες μπορούν να διαβάσουν ότι το τάδε προϊόν μπορεί να φέρει και μειονεκτήματα ή ελαττώματα. Ιστορικά, οι εταιρείες ήταν σε θέση να ελέγχουν τις διαθέσιμες πληροφορίες σχετικά με αυτές, με στρατηγικά τοποθετημένα ανακοινώσεις στον Τύπο και μέσω των Δημοσίων Σχέσεων. Σήμερα, ωστόσο, οι επιχειρήσεις υποβιβάζονται ολοένα και περισσότερο στο στο περιθώριο ως απλοί παρατηρητές, που δεν έχει ούτε τη γνώση, ούτε την πιθανότητα - ή, μερικές φορές, ακόμη και το δικαίωμα - να αλλάξουν όσα σχόλια αναρτώνται δημοσίως τα οποία παρέχονται από τους πελάτες τους. Η Wikipedia, για παράδειγμα, απαγορεύει ρητά τη συμμετοχή των επιχειρήσεων σε απευθείας σύνδεση με τη κοινότητα (Kende, 2012).

Μια τέτοια εξέλιξη δεν μπορεί να προκαλεί έκπληξη. Το Διαδίκτυο ξεκίνησε ως τίποτα περισσότερο από ένα γιγαντιαίο σύστημα Bulletin Board (BBS) που επέτρεπε

στους χρήστες να ανταλλάσσουν λογισμικό, δεδομένα, μηνύματα και ειδήσεις μεταξύ τους. Στα τέλη της δεκαετίας του 1990 υπήρξε αυξημένη δημοτικότητα σε ιστοσελίδες, στις οποίες μέσοι χρήστες μπορούσαν να ανταλλάσσουν πληροφορίες σχετικά με την ιδιωτική τους ζωή (σημερινό ισοδύναμο θα ήταν το weblog ή blog). Η εποχή των εταιρικών ιστοσελίδων και του ηλεκτρονικού εμπορίου (e-commerce) ξεκίνησε σχετικά πρόσφατα με την έναρξη των Amazon και eBay το 1995, και εξελίχθηκε ραγδαία 6 χρόνια αργότερα, με τις ιστοσελίδες dot-com το 2001. Η τρέχουσα τάση προς τα μέσα κοινωνικής δικτύωσης μπορεί ως εκ τούτου, να θεωρηθεί ως εξέλιξη στις ρίζες του Διαδικτύου, δεδομένου ότι μεταμορφώνει τον Παγκόσμιο Ιστό σε σχέση με την αρχική του μορφή ως πλατφόρμα για τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ των χρηστών. Οι τεχνολογικές πρόοδοι που έχουν γίνει κατά τη διάρκεια των τελευταίων 20 ετών επιτρέπει πλέον μια μορφή εικονικής κοινής χρήσης περιεχομένου που είναι θεμελιωδώς διαφορετική και πιο ισχυρή από το BBS στα τέλη της δεκαετίας του 1970 (Warf, 2013).

Στη συνέχεια θα δώσουμε τον ορισμό και την ταξινόμηση των μέσω κοινωνικής δικτύωσης κοιτάζοντας ιστορικές ρίζες τους, τις τεχνικές ιδιαιτερότητες, και διαφορές από άλλους φορείς, όπως το Web 2.0 και το Περιεχόμενο Παραγόμενο από Χρήστες. Η συγκεκριμένη ανάλυση θα επικεντρωθεί σε έξι τύπους των μέσων κοινωνικής δικτύωσης - συνεργατικά έργα, blogs, κοινότητες διαμοιρασμού περιεχομένου, ιστότοποι κοινωνικής δικτύωσης, εικονικά παιχνίδια, και εικονικά κοινωνικά δίκτυα - και θα παρουσιάσει τους τρόπους με τους οποίους οι επιχειρήσεις μπορούν να επωφεληθούν από τη χρήση των εφαρμογών αυτών (Kende, 2012).

1.3.1 Ορισμός

Ο επίσημος ορισμός του όρου «μέσα κοινωνικής δικτύωσης» απαιτεί πρώτα τον διαχωρισμό του από δύο συναφείς έννοιες που συχνά συγχέονται με αυτόν: Web 2.0 και Περιεχόμενο Παραγόμενο από Χρήστες (Usergeneratedcontent – UGC). Το Web 2.0 είναι ένας όρος που χρησιμοποιήθηκε για πρώτη φορά το 2004 για να περιγράψει ένα νέο τρόπο με τον οποίο οι προγραμματιστές λογισμικού και οι τελικοί χρήστες άρχισαν να χρησιμοποιούν τον Παγκόσμιο Ιστό, δηλαδή, ως πλατφόρμα στην οποία το περιεχόμενο και τις εφαρμογές δεν δημιουργούνται και δημοσιεύονται πλέον από τα άτομα, αλλά, αντίθετα, τροποποιούνται συνεχώς από όλους τους χρήστες σε μια συμμετοχική και συνεργατική διαδικασία. Ενώ οι εφαρμογές, όπως προσωπικές ιστοσελίδες, και η ιδέα της δημοσίευσης του περιεχομένου ανήκουν στην εποχή του Web 1.0, αυτά αντικαθίστανται από τα blogs, τα wikis, και συνεργατικά έργα στο Web 2.0. Παρά το γεγονός ότι το Web 2.0 δεν αναφέρεται σε κάποια συγκεκριμένη τεχνική ενημέρωση του Παγκοσμίου Ιστού, υπάρχει μια σειρά από βασικές λειτουργίες που είναι απαραίτητες για τη λειτουργία του. Μεταξύ αυτών είναι το Adobe Flash (μια δημοφιλής μέθοδος για την προσθήκη animation, διαδραστικότητας, και ήχου / βίντεο συνεχούς ροής σε ιστοσελίδες), το RSS (Really Simple Syndication), μια οικογένεια μορφών τροφοδοσίας του Παγκόσμιου Ιστού που χρησιμοποιείται για τη δημοσίευση περιεχομένου που ενημερώνεται συχνά, όπως καταχωρίσεις σε blog ή ειδήσεις, σε τυποποιημένη μορφή, και το AJAX (Asynchronous Java Script), μια τεχνική για την ανάκτηση δεδομένων από τους ασύγχρονους διακομιστές του Διαδικτύου, που επιτρέπει την ενημέρωση του περιεχομένου χωρίς να παρεμβαίνει με την εμφάνιση και τη συμπεριφορά ολόκληρης

της σελίδας. Όπως σύντομα αναφέρθηκε και προηγουμένως, θεωρούμε το Web 2.0 ως πλατφόρμα για την εξέλιξη των μέσων κοινωνικής δικτύωσης (Haenleinand Kaplan, 2009).

Εφόσον το Web 2.0 αποτελεί την ιδεολογική και τεχνολογική βάση, το περιεχόμενο που δημιουργείται από τους χρήστες (UGC) μπορεί να θεωρηθεί ως το άθροισμα όλων των τρόπων με τους οποίους οι άνθρωποι κάνουν χρήση των μέσων κοινωνικής δικτύωσης. Με τον όρο αυτόν, που χρησιμοποιείται ευρέως από το 2005, περιγράφονται οι διάφορες μορφές του περιεχομένου πολυμέσων που είναι διαθέσιμες στο κοινό και δημιουργείται από τους τελικούς χρήστες. Το UGC πρέπει να πληροί τρεις βασικές προϋποθέσεις προκειμένου να θεωρηθεί ως Περιεχόμενο Παραγόμενο από Χρήστες: Πρώτον, θα πρέπει να δημοσιεύεται είτε σε δημόσια προσβάσιμο δικτυακό τόπο ή σε μια σελίδα κοινωνικής δικτύωσης με πρόσβαση από επιλεγμένη ομάδα ανθρώπων. Δεύτερον, χρειάζεται να υπάρχει ορισμένη έκταση δημιουργικής προσπάθειας και τέλος, χρειάζεται να έχει δημιουργηθεί εκτός του πλαισίου επαγγελματικών μεθόδων εργασίας και πρακτικών. Η πρώτη προϋπόθεση αποκλείει το περιεχόμενο που ανταλλάσσεται στα e-mail ή τα άμεσα μηνύματα, η δεύτερη αποκλείει τις επαναλήψεις του ήδη υπάρχοντος περιεχομένου και η τρίτη, όλο το περιεχόμενο που έχει δημιουργηθεί υπό ένα εμπορικό πλαίσιο αγοράς. Παρά το γεγονός ότι το UGC ήταν διαθέσιμο πριν από το Web 2.0, ο συνδυασμός των τεχνολογικών εξελίξεων (π.χ., αυξημένη ευρυζωνική διαθεσιμότητα και δυναμικότητα του υλικού), των οικονομικών παραγόντων (π.χ., αυξημένη διαθεσιμότητα των εργαλείων για τη δημιουργία UGC), και διαφόρων κοινωνικών παραγόντων, κάνουν το UGC σήμερα ριζικά διαφορετικό από αυτό που παρατηρήθηκε στις αρχές του 1980. Με βάση αυτές τις διευκρινίσεις για το Web 2.0 και UGC, είναι πλέον εύκολο να δώσουμε έναν πιο λεπτομερή ορισμό του τι εννοούμε με τον όρο μέσα κοινωνικής δικτύωσης (KaplanandHaenlein, 2010).

Τα μέσα κοινωνικής δικτύωσης είναι μια ομάδα του διαδικτυακών εφαρμογών που στηρίζονται στις ιδεολογικές και τεχνολογικές βάσεις του Web 2.0, και που επιτρέπουν τη δημιουργία και την ανταλλαγή περιεχομένου που παράγεται από χρήστες. Μέσα σε αυτό το γενικό ορισμό, υπάρχουν διάφοροι τύποι μέσων κοινωνικής δικτύωσης που πρέπει να διακριθούν περαιτέρω. Ωστόσο, αν και οι περισσότεροι άνθρωποι θα μπορούσαν πιθανότατα να συμφωνήσουν ότι τα Wikipedia, YouTube και Facebook είναι όλα μέρος αυτής της μεγάλης ομάδας, δεν υπάρχει συστηματικός τρόπος με τον οποίο μπορούν να ταξινομηθούν διαφορετικές εφαρμογές μέσων κοινωνικής δικτύωσης. Επίσης, νέες ιστοσελίδες εμφανίζονται στον κυβερνοχώρο κάθε μέρα, έτσι είναι σημαντικό ότι κάθε σύστημα ταξινόμησης λαμβάνει υπόψη τις επικείμενες εφαρμογές.

1.3.2 Χρήση – Ιδιωτική και Εταιρική

Τα μέσα κοινωνικής δικτύωσης θεωρούνται συχνά ως ένα εργαλείο προσωπικής επικοινωνίας. Από τη προσωπική οπτική γωνία του χρήστη, τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται ως μέσο επικοινωνίας με φίλους και συγγενείς, είτε ως αντικατάσταση ή επέκταση των υφιστάμενων μεθόδων επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο. Η ευκολία με την οποία οι ιστότοποι κοινωνικής δικτύωσης επιτρέπουν στους ανθρώπους να διατηρήσουν επαφή με γνωστά του άτομα και να επανασυνδεθούν με παλιούς φίλους, παρέχει κάποια στοιχεία σχετικά

με τη δημοτικότητα αυτού του μέσου επικοινωνίας. Εκτός από τις καθαρά προσωπικές χρήσεις, μερικές ιστοσελίδες έχουν αξιοποιηθεί για τις επαγγελματικές ανάγκες των χρηστών και για να βοηθήσουν τα άτομα να χτίσουν και να διατηρήσουν ένα επαγγελματικό δίκτυο. Αυτές οι δυνατότητες έχουν αλλάξει τους τρόπους με τους οποίους τα άτομα συνδέονται με τους συμμαθητές ή τα άτομα που αφορούν την επαγγελματική τους συμπεριφορά. Λόγω της εντυπωσιακής υιοθέτησης των μέσων κοινωνικής δικτύωσης από το ευρύ κοινό, οι επιχειρήσεις συνειδητοποιούν ότι αυτό το μέσο μπορεί να προσφέρει επιχειρηματικά οφέλη. Με τη σύνδεση με τους υπάρχοντες και μελλοντικούς πελάτες, οι επιχειρήσεις απλά μεταφέρουν τις δραστηριότητες τους μέσα στο εικονικό περιβάλλον - τοποθεσία, τοποθεσία, τοποθεσία. Η επικοινωνία με και η παροχή υπηρεσιών προς τους πελάτες χωρίς τη φυσική μεταφορά τους, επιτρέπει την πρόσβαση, την έγκαιρη επικοινωνία, και την ελπίδα για μια καλύτερη και προσαρμοσμένη εμπειρία του πελάτη (BITS, 2011).

Με την ανάπτυξη των μέσων κοινωνικής δικτύωσης, κάθε αλληλεπίδραση είναι μέρος μιας νέας συνεργασίας μεταξύ της εταιρείας και των πελατών: ένα ζωτικό μέρος της διαχείριση πελατειακών σχέσεων 2.0. Τα social media απλά δημιουργούν ευκαιρίες για τις επιχειρήσεις να πουν τις δικές τους ιστορίες. Ο στόχος των επιχειρήσεων είναι η επιθυμία από τις εταιρείες να αυξήσουν την εμπειρία των πωλήσεων και τη βελτίωση των σχέσεων με τους πελάτες. Για τους επαγγελματίες που επέλεξαν να συμμετέχουν στα μέσα κοινωνικής δικτύωσης, τα οφέλη δεν είναι απλώς η ανταλλαγή πληροφοριών αλλά ένας τρόπος για να οικοδομήσουν και να αποκτήσουν ευκαιρίες σταδιοδρομίας και εισόδημα. Ο Paquette (2013) δίνει έμφαση στη σημασία των μέσων κοινωνικής δικτύωσης ως εργαλείο μάρκετινγκ, λόγω της ικανότητάς τους να παρέχουν σύνδεση μεταξύ των εμπορικών σημάτων και των καταναλωτών, προσφέροντας ένα προσωπικό κανάλι για το χρήστη με επίκεντρο τη δικτύωση και την κοινωνική αλληλεπίδραση. Η έρευνα για τα κίνητρα και τη συμπεριφορά των καταναλωτών είναι πολύ σημαντική προκειμένου να εξασφαλιστεί η απόδοση της προώθησης μέσω των μέσων κοινωνικής δικτύωσης, καθώς αυτά έχουν ενισχύσει την ικανότητα των επιχειρήσεων να συγκεντρώσουν δεδομένα σε σχέση με τη συμπεριφορά των καταναλωτών και των κινήτρων τους (Chu, 2011). Επίσης, τα μέσα κοινωνικής δικτύωσης επηρεάζουν θετικά τα κίνητρα των καταναλωτών (Paquette, 2013). Η επικοινωνία μεταξύ των επιχειρήσεων και των καταναλωτών μέσω των επηρεάζει διάφορες πτυχές της συμπεριφοράς των καταναλωτών. Πιο συγκεκριμένα, η χρήση των μέσων κοινωνικής δικτύωσης συμβάλλει στην αύξηση της ευαισθητοποίησης, την απόκτηση των πληροφοριών στη διαμόρφωση στάσεων, απόψεων και συμπεριφορών αγοράς και την επικοινωνία μετά την πώληση και την αξιολόγηση (Mangold και Faulds, 2009). Η ανάπτυξη και η διατήρηση της αφοσίωσης στην επιχείρηση αποτελεί κεντρικό στόχο των στρατηγικών μάρκετινγκ (Erdogmus και Cicek, 2012).

Για την αλληλεπίδραση μέσα από διαδικτυακές πλατφόρμες, τα μέσα κοινωνικής δικτύωσης εξαρτώνται τεχνολογίες κινητής και σταθερής διαδικτυακής επικοινωνίας, μέσω των οποίων τα άτομα και μετέχουν σε κοινότητες, συν-δημιουργούν, συζητούν και τροποποιοιούν το περιεχόμενο που δημιουργείται από χρήστες. Με τον τρόπο αυτό, οι επιχειρήσεις, οι κοινότητες και τα άτομα μοιράζονται τα δεδομένα σε ένα καινοτόμο κανάλι επικοινωνίας (Kietzman και Hermkens, 2011). Ο Kaplan (2012) ορίζει ως mobile marketing κάθε εμπορική δραστηριότητα που διεξάγεται μέσω ενός παγκοσμίου δικτύου με το οποίο οι καταναλωτές είναι συνεχώς συνδεδεμένοι χρησιμοποιώντας μια προσωπική συσκευή κινητής τηλεφωνίας. Οι Yadav et al. (2015) υποστηρίζουν ότι η επικοινωνία μάρκετινγκ μέσω κινητών μέσων κοινωνικής

δικτύωσης μπορούν να κατηγοριοποιηθούν σε δύο τύπους. Ο πρώτος τύπος είναι η επικοινωνία B2C / B2B και ο δεύτερος είναι το περιεχόμενο που παράγεται από χρήστες.

Όσον αφορά τον τρόπο με τον οποίο οι επιχειρήσεις χρησιμοποιούν τα social media σε προωθητικές ενέργειες, πολλές εταιρείες προωθούν τα προϊόντα και τις υπηρεσίες μέσω δημοφιλών blogs, προκειμένου να κερδίσουν την αποδοχή και τα θετικά σχόλια από τους καταναλωτές (Heinonen, 2011). Τα blogs είναι τώρα μέρος του μίγματος μάρκετινγκ, δεδομένου ότι είναι μάλλον αποτελεσματικά από πλευράς κόστους, μεγάλης προβολής και υψηλής επίδρασης στους καταναλωτές. Τα προϊόντα μπορούν να προωθηθούν και οι ενδιαφερόμενοι αναγνώστες των άρθρων μπορεί να γίνουν πραγματικοί πελάτες ή υπάλληλοι της εταιρείας (Kaplan και Haenlein, 2010). Η ζωντανή κριτική σε ένα blog για ένα προϊόν ή μια υπηρεσία ή ακόμη και για μια εταιρεία, μπορεί να καταστρέψει τη φήμη της όταν προέρχεται από έναν εργαζόμενο ή συνεργάτη της εταιρείας. Η κατηγορία των blogs αυξάνεται με ταχείς ρυθμούς και μπορούν επίσης να ταξινομηθούν σε υποκατηγορίες, λόγω των διαφορετικών στόχων τους.

Οι κοινότητες περιεχομένου, όπως το YouTube, είναι πολύ δημοφιλείς και πολλές εταιρείες τις χρησιμοποιούν για να προωθήσουν τα προϊόντα και τις υπηρεσίες τους με έμμεσο τρόπο. Επιπλέον, τις χρησιμοποιούν για να δημοσιεύουν και να διαμοιράζονται τις εκστρατείες τους, προκειμένου να προσελκύσουν ομάδες-στόχους μέσω στοχοθετημένων δραστηριοτήτων (Kaplan και Haenlein, 2010). Ο ρόλος της διαφήμισης Viral Video ενισχύεται μέσα από την ανάδειξη του YouTube (Huang et al., 2012). Η διαφήμιση μέσω viral βίντεο έχει μοναδικά χαρακτηριστικά, αφού η προβολή βίντεο ενεργοποιεί τις δραστηριότητες κοινής χρήσης του βίντεο και της επεξεργασίας πληροφοριών της εταιρείας ή του προϊόντος (Huang et al., 2012).

1.3.3 Κατηγορίες

Η θεωρία της κοινωνικής παρουσίας αναφέρει ότι τα μέσα διαφέρουν ως προς το βαθμό της κοινωνικής παρουσίας, που ορίζεται ως η ακουστική, οπτική και φυσική επαφή με την οποία μπορεί να επιτευχθεί, η οποία μπορεί να προκύψει μεταξύ των δύο εταίρων επικοινωνίας. Η κοινωνική παρουσία επηρεάζεται από την οικειότητα την αμεσότητα (ασύγχρονη εναντίον σύγχρονη) του μέσου, και μπορεί να αναμένεται χαμηλότερη για τη μεσολάβηση (π.χ., τηλεφωνική συνομιλία), τη διαπροσωπική (π.χ., συζήτηση πρόσωπο με πρόσωπο) και την ασύγχρονη (π.χ., e- mail), από ό, τι για τη σύγχρονη επικοινωνία (π.χ., live chat). Όσο υψηλότερη είναι η κοινωνική παρουσία, τόσο μεγαλύτερη είναι η κοινωνική επιρροή που οι εταίροι της επικοινωνίας έχουν στη συμπεριφορά του άλλου. Στενά συνδεδεμένη με την ιδέα της κοινωνικής παρουσίας είναι η έννοια του πλούτου των μέσων ενημέρωσης. Η θεωρία του πλούτου βασίζεται στην υπόθεση ότι ο στόχος κάθε επικοινωνίας είναι η ανάλυση της ασάφειας και η μείωσης της αβεβαιότητας. Αναφέρει ότι τα μέσα ενημέρωσης διαφέρουν ως προς το βαθμό του πλούτου που κατέχουν, δηλαδή τη ποσότητα των πληροφοριών που επιτρέπουν να μεταδοθεί σε ένα δεδομένο χρονικό διάστημα - και ότι, ως εκ τούτου ορισμένα μέσα είναι πιο αποτελεσματικά από άλλα στην επίλυση της ασάφειας και της αβεβαιότητας. Όσον αφορά την κοινωνική διάσταση των μέσων κοινωνικής δικτύωσης, η έννοια της αυτο-παρουσίασης δηλώνει ότι σε κάθε είδος κοινωνικής αλληλεπίδρασης των ανθρώπων υπάρχει η επιθυμία να ελεγχθούν οι

εντυπώσεις των άλλων για το ίδιο το άτομο. Από τη μία πλευρά, αυτό γίνεται με στόχο το άτομο να επηρεάσει τους άλλους και να κερδίσει ανταμοιβές, και από την άλλη πλευρά οδηγείται από την επιθυμία να δημιουργήσει μια εικόνα που είναι συνεπής με την προσωπική ταυτότητα του ατόμου. Ο βασικός λόγος για τον οποίο οι άνθρωποι αποφασίζουν να δημιουργήσουν μια προσωπική ιστοσελίδα είναι, για παράδειγμα, η επιθυμία να παρουσιάσουν τον εαυτό τους στον κυβερνοχώρο. Συνήθως, μια τέτοια παρουσίαση γίνεται μέσω της αυτο-αποκάλυψης, δηλαδή, της συνειδητής ή ασυνείδητης αποκάλυψη προσωπικών πληροφοριών που είναι συνεπής με την εικόνα που το άτομο θα ήθελε να δώσει. Η αυτο-αποκάλυψη είναι ένα κρίσιμο βήμα για την ανάπτυξη στενών σχέσεων αλλά μπορεί επίσης να παρατηρηθεί μεταξύ αγνώστους(Schau και Gilly, 2003).

Όσον αφορά την κοινωνική παρουσία και τον πλούτο των μέσων, εφαρμογές όπως συνεργατικά έργα (π.χ. Wikipedia) και blogs έχουν χαμηλότερο επίπεδο, δεδομένου ότι συχνά βασίζονται σε κείμενο και ως εκ τούτου, επιτρέπουν μόνο για μια σχετικά απλή ανταλλαγή πλκηροφοριών. Στο επόμενο επίπεδο βρίσκονται κοινότητες περιεχομένου (π.χ. YouTube) και οι ιστότοποι κοινωνικής δικτύωσης (π.χ. Facebook), οι οποίοι, εκτός από την επικοινωνία που βασίζεται σε κείμενο, επιτρέπουν την κοινή χρήση φωτογραφιών, βίντεο και άλλων μορφών μέσων επικοινωνίας. Στο υψηλότερο επίπεδο είναι το εικονικό παιχνίδι και τα κοινωνικά εικονικά δίκτυα (π.χ., το World of Warcraft, το Second Life), τα οποία προσπαθούν να αναπαράγουν όλες τις διαστάσεις της αλληλεπίδρασης πρόσωπο με πρόσωπο σε ένα εικονικό περιβάλλον. Όσον αφορά την αυτο-παρουσίαση και την αυτο-αποκάλυψη, τα blogs συνήθως είναι σε χαμηλότερο επίπεδο από ό, τι τα συνεργατικά έργα, καθώς τείνουν να επικεντρώνονται σε συγκεκριμένους τομείς περιεχομένου. Σε παρόμοιο πνεύμα, οι ιστότοποι κοινωνικής δικτύωσης επιτρέπουν μεγαλύτερο βαθμό αυτο-αποκάλυψης από τις κοινότητες περιεχομένου. Τέλος, τα εικονικά κοινωνικά δίκτυα απαιτούν υψηλότερο επίπεδο αυτο-αποκάλυψης από τα εικονικά παιχνίδια, καθώς τα τελευταία διαθέτουν αυστηρές κατευθυντήριες γραμμές που αναγκάζουν τους χρήστες να συμπεριφέρονται με ένα συγκεκριμένο τρόπο (π.χ., ως πολεμιστές σε ένα φανταστικό κόσμο).

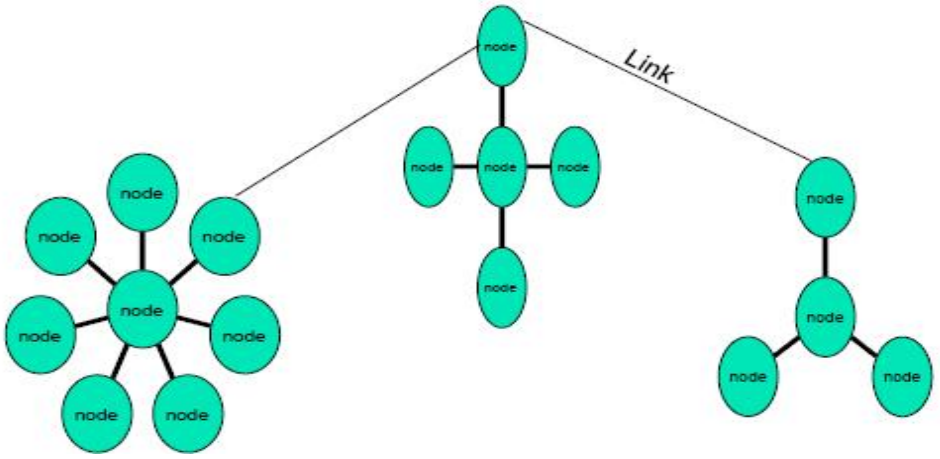
Κοινωνική παρουσία – Πλούτος του μέσου				
Αυτό-παρουσίαση, Αυτό - αποκάλυψη		***Υψηλή***	***Μέση***	***Χαμηλή***
	Υψηλή	blogs	Σελίδες κοινωνικής δικτύωσης όπως το Facebook	Εικονικά κοινωνικά δίκτυα (SecondLife)
	Χαμηλή	Συνεργατικά έργα όπως η Wikipedia	Κοινότητες Περιεχομένου όπως το YouTube	Εικονικά παιχνίδια

Πίνακας 1-1 Κατηγοριοποίηση μέσων κοινωνικής δικτύωσης

2 ΑΝΑΛΥΣΗ ΜΕΣΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

2.1 ΔΙΚΤΥΑΚΟΙ ΚΟΜΒΟΙ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Γενικά, ένα δίκτυο είναι μια αλληλοσυνδεόμενη ομάδα ή σύστημα, όπως για παράδειγμα ένα δίκτυο επιχειρήσεων, ένα δίκτυο ξενοδοχείων ή ένα κοινωνικό δίκτυο. Η Εικόνα 2-1 παρουσιάζει τη συσχέτιση των οντοτήτων (κόμβων – nodes) σε ένα δίκτυο.



Εικόνα 2-1 Δίκτυο και κόμβοι δικτύου (ΕΜΠ, 2011)

Στην Εικόνα 2-1 παρατηρούμε ότι υπάρχουν πολλοί κόμβοι οι οποίοι συνδέονται μεταξύ τους σε μικρότερες και μεγαλύτερες ομάδες. Κάθε κόμβος για να ανήκει στο δίκτυο θα πρέπει να συνδέεται με τουλάχιστον έναν άλλο κόμβο. Στα κοινωνικά δίκτυα, οι κόμβοι είναι άτομα ή επιχειρήσεις οι οποίοι συνδέονται μεταξύ τους με έναν ή περισσότερους τύπους αλληλεξάρτησης, όπως αξίες, οράματα, ιδέες, οικονομικές συναλλαγές, φιλία, συγγένεια, αντιπάθεια, συγκρούσεις, σεξουαλικές επαφές, μεταφορά μολυσματικών ασθενειών ή επιγραμμικές (web) επαφές (ΕΜΠ, 2011).

Ο όρος κοινωνικό δίκτυο αναφέρεται στη σύναψη μιας κοινωνικής σχέσης μεταξύ ατόμων, οικογενειών, νοικοκυριών, κοινοτήτων, περιοχών, επιχειρήσεων κ.ά. Κάθε ένας από τους συμμετέχοντες, μπορεί να έχει διπλό ρόλο, δρώντας ως μονάδα – κόμβος ενός κοινωνικού δικτύου, ή δράστης (socialactor). Οι σχέσεις μεταξύ των κόμβων σε ένα κοινωνικό δίκτυο μπορεί να είναι συγγένειας ή να δημιουργούνται μέσω της καθημερινής επικοινωνίας, των πολιτιστικών δραστηριοτήτων (για παράδειγμα, η φιλία). Σε ένα κοινωνικό δίκτυο η σχέση μεταξύ των κόμβων μπορεί να είναι και αρνητική. Επομένως, οι κόμβοι μπορεί να είναι διαφορετικοί, δηλαδή να εκπροσωπούν ένα άτομο, μια κοινότητα ή μια επιχείρηση, αλλά έχουν ένα κοινό χαρακτηριστικό, τη σύναψη ή μη σύναψη μιας δυαδικής σχέσης με κάποιον άλλον κόμβο. Επίσης, αν υπάρχει μια σύνδεση-σχέση μεταξύ δύο κόμβων, είναι αβάσιμο να θεωρήσουμε ότι αυτή έχει μόνο μια κατεύθυνση, καθώς οι σχέσεις στα κοινωνικά

δίκτυα δεν είναι απαραιτήτως συμμετρικές. Στα κοινωνικά δίκτυα η ασύμμετρες σχέσεις είναι όσο κοινές είναι και οι συμμετρικές. Λόγω αυτής της ιδιότητας, τα κοινωνικά δίκτυα δεν μπορούν να συγχέονται με τις κοινωνικές ομάδες. Όσον αφορά τις κοινωνικές ομάδες, υπάρχουν δύο προσεγγίσεις, η ρεαλιστική και η νομιναλιστική. Η ρεαλιστική προσέγγιση ορίζει την κοινωνική ομάδα ως μονάδα που αποτελείται από κόμβους που διαχωρίζονται από τους υπόλοιπους και διατηρούνται σχέσεις επικοινωνίας, συναισθηματικές και συμπεριφορικές μεταξύ των κόμβων. Επομένως δημιουργείται ένα συναίσθημα συνειδητότητας μεταξύ των κόμβων και δημιουργούνται κάποιοι περιορισμοί όσον αφορά τη συμπεριφορά, τους κανόνες και τους ρόλους της αλληλεπίδρασης των κόμβων. Η νομιναλιστική προσέγγιση, από την άλλη πλευρά, επιτρέπει τον επαναπροσδιορισμό των ορίων και περιορισμών που καθορίζουν την συμμετοχή ενός κόμβου σε μια κοινωνική ομάδα (Jangetal., 2010).

Τα κοινωνικά δίκτυα αναπαρίστανται με τη βοήθεια διγράφων (digraphs) ή γράφων, αν η σύνδεση μεταξύ των κόμβων δεν έχει κατεύθυνση, οι οποίοι παρέχουν τη χαρτογράφηση των δεσμών μεταξύ των κόμβων του δικτύου. Η συμπεριφορά των χρηστών των διαδικτυακών μέσων κοινωνικής δικτύωσης καλύπτει διάφορες κοινωνικές δραστηριότητες που οι χρήστες μπορούν να κάνουν σε απευθείας σύνδεση, όπως η δημιουργία φιλίας, δημοσίευση περιεχομένου, περιήγηση προφίλ, μηνύματα, και ο σχολιασμός. Αξίζει να σημειωθεί ότι, οι δραστηριότητες αυτές μπορεί να είναι θετικές ή κακόβουλες. Η κατανόηση της συμπεριφοράς των χρηστών των διαδικτυακών μέσων κοινωνικής δικτύωσης είναι σημαντική για τους διάφορες συμμετέχοντες του Διαδικτύου σε διάφορες πτυχές (Jinetal, 2013):

- Για τους παρόχους υπηρεσιών διαδικτύου την υπηρεσία Internet παρόχους (ISPs), καθώς η κίνηση στα μέσα κοινωνικής δικτύωσης αυξάνεται με ταχείς ρυθμούς και γίνεται σημαντική, οι οποίοι θέλουν να μάθουν την εξέλιξη του είδους κίνησης αυτής. Αυτό μπορεί να τους καθοδηγήσει ώστε να λάβουν μέτρα που σχετίζονται με την υποδομή του δικτύου (π.χ., βελτιστοποίηση της κυκλοφορίας στο δίκτυο).
- Για τους παρόχους υπηρεσιών διαδικτυακών μέσων κοινωνικής δικτύωσης, οι οποίοι επιθυμούν να κατανοήσουν τη στάση των πελατών τους προς διαφορετικές λειτουργίες, ειδικά για ορισμένες πειραματικές λειτουργίες. Επιπλέον, από τη σκοπιά των επενδύσεων σε έργα υποδομής, όπως η επιλογή των γεωγραφικών θέσεων που είναι πιο αποδοτικές για την κατασκευή των κέντρων δεδομένων ή του δικτύου διανομής περιεχομένου (CDN) που θα μπορούσε να λειτουργήσει ως μοχλός για την παροχή δεδομένων συχνής πρόσβασης, η κατανόηση της γεωγραφικής κατανομής των χρηστών και της δραστηριότητα της κυκλοφορίας είναι ζωτικής σημασίας.
- Για τους χρήστες των διαδικτυακών μέσων κοινωνικής δικτύωσης, η μελέτη της συμπεριφοράς είναι σημαντική για την ενίσχυση της εμπειρίας του χρήστη. Για παράδειγμα, υπάρχουν πολλοί κακόβουλοι λογαριασμοί ΛΤΔ. Οι λογαριασμοί αυτοί παράγουν ανεπιθύμητα μηνύματα προς νόμιμους χρήστες. Ως εκ τούτου, ο εντοπισμός και το κλείδωμα κακόβουλων χρηστών έχουν μεγάλη σημασία για την εξασφάλιση της καλής εμπειρίας του χρήστη.

2.2 ΓΙΑΤΙ ΝΑ ΑΝΑΛΥΣΟΥΜΕ ΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Τα μέσα κοινωνικής δικτύωσης είναι ήδη στο επίκεντρο μερικών πολύ δημοφιλών τοποθεσιών στο διαδίκτυο. Καθώς η τεχνολογία ωριμάζει, περισσότερες εφαρμογές είναι πιθανό να προκύψουν. Είναι επίσης πιθανό ότι η κοινωνική δικτύωση θα διαδραματίσει σημαντικό ρόλο στη μελλοντική διαδικτυακή προσωπική και εμπορική αλληλεπίδραση, καθώς και τη θέση και την οργάνωση της πληροφορίας και της γνώσης. Παραδείγματα περιλαμβάνουν τα πρόσθετα (plug-ins) των περιηγητών στο διαδίκτυο (browser) που ανακαλύπτουν πληροφορίες που είναι ορατές από τους φίλους, και τα συνεργατικά εργαλεία αναζήτησης Ιστού που βασίζονται σε κοινωνικά δίκτυα. Ακόμη και μεγάλες εταιρείες αναζήτησης στο Διαδίκτυο αναπτύσσουν υπηρεσίες που αξιοποιούν τα κοινωνικά δίκτυα, όπως το MyWeb Yahoo! και το Google Co-op. Στη συνέχεια θα περιγραφούν μερικοί από τους τρόπους με τους οποίους η κατανόηση της δομής των διαδικτιακών μέσων κοινωνικής δικτύωσης θα οφελήσουν τον σχεδιασμό νέων συστημάτων και θα βοηθήσει στην κατανόηση της επίδρασης των κοινωνικών δικτύων στο μέλλον του Διαδικτύου. Επιπλέον, τα δεδομένα που προκύπτουν από την ανάλυση των μέσων κοινωνικής δικτύωσης μπορεί να έχει ενδιαφέρον σε άλλα ερευνητικά πεδία (Wilsonetal., 2009).

2.2.1 Κοινό ενδιαφέρον και εμπιστοσύνη

Οι γειτονικοί χρήστες σε ένα κοινωνικό δίκτυο τείνουν να εμπιστεύονται ο ένας τον άλλο. Ένας αριθμός ερευνητικών συστημάτων έχουν προταθεί για την αξιοποίηση αυτής της εμπιστοσύνης. Η SybilGuard χρησιμοποιεί ένα κοινωνικό δίκτυο για την ανίχνευση επιθέσεων Sybil σε κατανεμημένα συστήματα, αξιοποιώντας το γεγονός ότι οι χρήστες Sybil δεν θα είναι σε θέση να δημιουργήσουν πολλές έμπιστες συνδέσεις με τους χρήστες μη-Sybil. Η εφαρμογή Re αξιοποιεί την εμπιστοσύνη μεταξύ των χρηστών ηλεκτρονικού ταχυδρομείου για να βοηθήσει στην ταξινόμηση των spam από λευκές λίστες μηνυμάτων από τους φίλους και τους φίλους- φίλων. Η βαθύτερη κατανόηση της υποκείμενης τοπολογίας είναι ένα ουσιαστικό πρώτο βήμα στο σχεδιασμό και την ανάλυση ισχυρών συστημάτων μετρήσεων της εμπιστοσύνης (Dunnetal, 2012).

Οι γειτονικοί χρήστες σε ένα κοινωνικό δίκτυο τείνουν επίσης να έχουν κοινά συμφέροντα. Οι χρήστες περιηγούνται σε γειτονικές περιοχές του κοινωνικού δικτύου τους, επειδή είναι πιθανό να βρουν το περιεχόμενο που τους ενδιαφέρει. Συστήματα όπως το Yahoo! Web, Google Co-op και PeerSpective χρησιμοποιούν τα κοινωνικά δίκτυα για να ταξινομήσουν τα αποτελέσματα αναζήτησης του Διαδικτύου σε σχέση με τα συμφέροντα της γειτονιάς ενός χρήστη στο κοινωνικό δίκτυο. Τα συστήματα αυτά παρατηρούν τις εμφανίσεις περιεχομένου και τα κλικ των αποτελεσμάτων αναζήτησης από τα μέλη ενός κοινωνικού δικτύου για να ταξινομήσουν καλύτερα τα αποτελέσματα των μελλοντικών αναζητήσεων του χρήστη. Η κατανόηση της δομής των διαδικτυακών μέσων κοινωνικής δικτύωσης, καθώς και οι διαδικασίες που τη διαμορφώνουν, είναι σημαντικοί παράγοντες για αυτές τις εφαρμογές. Θα ήταν χρήσιμο να έχουμε αποδοτικούς αλγορίθμους που θα βρίσκουν το πραγματικό βαθμό των κοινών συμφερόντων μεταξύ δύο χρηστών, ή την αξιοπιστία ενός χρήστη (όπως γίνεται αντιληπτή από άλλους χρήστες). Όσον αφορά την ασφάλεια, είναι σημαντικό να κατανοήσουμε την ευρωστία των εν λόγω δικτύων σε εσκεμμένες προσπάθειες χειραγώγησης (Jinetal., 2013).

2.2.2 Επιπτώσεις στο μέλλον του Διαδικτύου

Τα κοινωνικά δίκτυα υπάρχουν στις βάσεις δεδομένων των διαδικτυακών τόπων κοινωνικής δικτύωσης. Ωστόσο, τα άλλα διαδικτυακά κοινωνικά δίκτυα υλοποιούντια ως υπερκείμενα δίκτυα. Για παράδειγμα, η γραφική παράσταση που σχηματίζεται από τους ανθρώπους που ανταλλάσσουν email, ή το γράφημα που σχηματίζεται από το τους χρήστες του Skype που περιλαμβάνουν ο ένας τον άλλο στις λίστες επαφών τους μπορεί να θεωρηθεί ως ένα άλλο κοινωνικό δίκτυο στην κορυφή του Διαδικτύου. Αν τα μελλοντικά κατανεμημένα διαδικτυακά μέσα κοινωνικής δικτύωσης είναι δημοφιλή και απαιτούν μεγάλο εύρος ζώνης, μπορούν να έχουν σημαντικές επιπτώσεις στην κίνηση στο Διαδίκτυο, όπως ακριβώς κάνουν τα υφιστάμενα δίκτυα peer-to-peer διανομής περιεχομένου. Η κατανόηση της δομής των διαδικτυακών μέσων κοινωνικής δικτύωσης δεν είναι μόνο ζωτικής σημασίας για την κατανόηση της ευρωστίας και την ασφάλειας των κατανεμημένων κοινωνικών δικτύων, αλλά και για την κατανόηση των επιπτώσεών τους στο μέλλον του Διαδικτύου (Dunnetal., 2012).

2.2.3 Αντίκτυπος σε άλλα ερευνητικά πεδία

Επιπλέον, η ανάλυση των διαδικτυακών μέσων κοινωνικής δικτύωσης έχει ενδιαφέρον σε πεδία πέρα από την επιστήμη των υπολογιστών. Για τους κοινωνικούς επιστήμονες, τα διαδικτυακά κοινωνικά δίκτυα προσφέρουν μια άνευ προηγουμένου ευκαιρία να μελετηθούν τα κοινωνικά δίκτυα σε μεγάλη κλίμακα. Οι κοινωνιολόγοι μπορούν να εξετάσουν τα δεδομένα για να δοκιμάσουν τις υπάρχουσες θεωρίες στα διαδικτυακά κοινωνικά δίκτυα, καθώς και να αναζητήσουν νέες μορφές συμπεριφοράς στο διαδικτυακά κοινωνικά δίκτυα (Jinetal, 2013).

Η μελέτη της δομής των διαδιακτυακών μέσων κοινωνικής δικτύωσης μπορεί να συμβάλει στη βελτίωση της κατανόησης των διαδικτυακών εκστρατειών μάρκετινγκ και viralμάρκετινγκ. Οι πολιτικές εκστρατείες έχουν συνειδητοποιήσει τη σημασία των blogs στις εκλογές. Παρομοίως, οι ειδικοί του μάρκετινγκ πειραματίζονται με το viral marketing με στόχο την καλύτερη προώθηση των προϊόντων και των επιχειρήσεων. Ανεξάρτητα από τη στάση του ατόμου σε αυτά τα φαινόμενα, μια καλύτερη κατανόηση της δομής των κοινωνικών δικτύων είναι πιθανό να βελτιώσει την κατανόησή για τις ευκαιρίες, τους περιορισμούς και τις απειλές που συνδέονται με αυτές τις ιδέες.

2.3 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΝΑΛΥΣΗΣ ΚΟΙΝΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

2.3.1 Κοινωνικά δίκτυα και Δίκτυα υπολογιστών

Τα δίκτυα μπορούν να ταξινομηθούν σύμφωνα με την τοπολογία, η οποία είναι η γεωμετρική διάταξη ενός συστήματος ηλεκτρονικού υπολογιστή. Κοινές τοπολογίες περιλαμβάνουν το πρωτόκολλο starή ring που καθορίζει ένα κοινό σύνολο κανόνων και σημάτων που ακολουθούν οι υπολογιστές στο δίκτυο. Οι αρχιτεκτονικές δικτύου μπορούν γενικά να ταξινομηθούν είτε ως peer-to-peerήclient / server. Οι υπολογιστές σε ένα δίκτυο μερικές φορές ονομάζονται κόμβοι. Οι υπολογιστές και οι συσκευές που διαθέτουν τους πόρους για ένα δίκτυο, ονομάζεται servers. Υποστηρίζεται ότι τα κοινωνικά δίκτυα διαφέρουν από τους περισσότερους άλλους τύπους δικτύων, συμπεριλαμβανομένων των τεχνολογικών και βιολογικών δικτύων, με δύο σημαντικούς τρόπους. Κατ' αρχάς, έχουν μη τετριμμένη ομαδοποίηση ή μεταβατικότητα δικτύου και δεύτερον, δείχνουν θετικές συσχετίσεις μεταξύ των βαθμών των παρακείμενων κορυφών. Τα κοινωνικά δίκτυα συχνά χωρίζονται σε ομάδες ή κοινότητες, και έχει πρόσφατα προταθεί ότι αυτή η διαίρεση θα μπορούσε να εξηγήσει την παρατηρούμενη ομαδοποίηση. Επιπλέον, η δομή της ομάδας στα δίκτυα μπορεί επίσης να ευθύνεται για το βαθμό των συσχετίσεων. Ως εκ τούτου, η ανάμειξη με βάση τα κοινά χαρακτηριστικά σε τέτοια δίκτυα με μια διακύμανση των μεγεθών των ομάδων παρέχει το προβλεπόμενο επίπεδο και ταιριάζει καλά με αυτό που παρατηρείται στα δίκτυα του πραγματικού κόσμου (Abraham, 2012).

2.3.2 Ιστότοποι κοινωνικής δικτύωσης

Οι ιστότοποι κοινωνικής δικτύωσης είναι ιστοσελίδες που επιτρέπουν στους χρήστες να εγγραφούν, να δημιουργήσουν τη δική τους σελίδα προφίλ (πραγματική ή εικονική) που περιέχει πληροφορίες για τον εαυτό τους, προκειμένου να καθιερώσουν συνδέσεις «φίλων» με άλλα μέλη και να επικοινωνούν με άλλα μέλη. Η επικοινωνία παίρνει συνήθως τη μορφή των ιδιωτικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, δημόσια σχόλια γραμμένα σε άλλες σελίδες προφίλ, blog ή εικόνες, ή instant messaging (Kim&Leskovec, 2011).

Οι ιστότοποι κοινωνικής δικτύωσης όπως το Facebook και το MySpace είναι μεταξύ των δέκα πιο δημοφιλών ιστοσελίδων στον κόσμο. Οι ιστότοποι κοινωνικής δικτύωσης είναι πολύ δημοφιλείς σε πολλές χώρες και περιλαμβάνουν τις Orkut (Βραζιλία), Cyworld (Κορέα), και Mixi (Ιαπωνία).

Η ανάπτυξη των ιστότοπων κοινωνικής δικτύωσης φαίνεται να έχει ενισχυθεί από τη νεολαία, με το Facebook να προέρχονται από μια ιστοσελίδα κολλεγίου και το MySpace έχει μέση ηλικία μελών στα 21 έτη. Ωστόσο, ένα αυξανόμενο ποσοστό μεγαλύτερων ηλικιών χρησιμοποιούν επίσης αυτά τα sites. Το βασικό κίνητρο για τη χρήση των ιστότοπων κοινωνικής δικτύωσης είναι η κοινωνικότητα, ωστόσο, το γεγονός αυτό δείχνει ότι μερικοί τύποι ανθρώπων δεν μπορούν ποτέ να χρησιμοποιούν ιστότοπους κοινωνικής δικτύωσης εκτενώς. Επιπλέον, φαίνεται ότι η εξωστρέφεια είναι ευεργετική στους ιστοτόπους κοινωνικής δικτύωσης και ότι οι γυναίκες χρήστες του MySpace φαίνεται να είναι πιο εξωστρεφείς και πιο πρόθυμες

να αυτο-αποκαλύψουν πληροφορίες για τον εαυτό τους από τους άνδρες χρήστες, γεγονός που δείχνει ότι η επικοινωνία μπορεί να είναι πιο αποτελεσματική σε αυτό το περιβάλλον (Abraham, 2012).

Οι ιστότοποι κοινωνικής δικτύωσης έχουν πολύ ενδιαφέρον, επειδή υποστηρίζουν τις δημόσιες συζητήσεις μεταξύ φίλων και γνωστών. Τα προφίλ κοινωνικής δικτύωσης είναι γνωστά ως χώροι για την έκφραση της ταυτότητας των μελών και τα δημόσια σχόλια που εμφανίζονται σε αυτά τα προφίλ, μπορούν επίσης να αποτελούνται ή να ερμηνευθούν από τη σκοπιά της έκφρασης ταυτότητας και όχι απλώς ως εκτέλεσης μιας καθαρά επικοινωνιακής λειτουργίας. Την ίδια στιγμή, οι δημόσιες συζητήσεις έχουν ενδιαφέρον, διότι η ιστοσελίδα περιέχει εκατομμύρια των άτυπων δημόσιων μηνυμάτων στα οποία οι ερευνητές μπορούν να έχουν πρόσβαση και να αναλύσουν. Η διαθεσιμότητα των δημογραφικών πληροφοριών σχετικά με τον αποστολέα και τον παραλήπτη στις σελίδες προφίλ, καθιστά αυτές τις πληροφορίες πιο ενδιαφέρουσες και χρήσιμες, αλλά ορισμένα ηθικά ζητήματα μπορούν να προκύψουν (σε αντίθεση με τα τυποποιημένα πρωτόκολλα συνέντευξης ή ερωτηματολογίου). Ωστόσο, εάν τα δεδομένα έχουν τοποθετηθεί στο πιο δημόσιο χώρο ώστε να μπορούν να βρεθούν από την αναζήτηση της Google, τότε η χρήση τους δεν αποτελεί κανενός είδους παραβίωση της ιδιωτικής ζωής (Kim&Leskovec, 2011).

Ένα ηθικό ζήτημα προκύπτει μόνο αν δίνεται ανατροφοδότηση στους συντάκτες κειμένου, ή αν δημιουργηθεί επαφή. Η έρευνα εξόρυξης δεδομένων στο MySpace ήταν περισσότερο εμπορικά προσανατολισμένη και όχι προς τους στόχους της κοινωνικής επιστήμης, αλλά στη συνέχεια η μελέτη της IBM έδειξε τον τρόπο με τον οποίο μπορεί να δημιουργηθεί κατάταξη των μουσικών με βάση τις απόψεις που εξορύσσονται από τα σχόλια στο MySpace, και μια ομάδα της Microsoft ανέπτυξε ένα σύστημα πίνακα κατάταξης για ταινίες με την εξαγωγή καταλόγων από το προφίλ MySpace, χωρίς τη ρητή ανάλυση συναισθήματος (Abraham, 2012).

2.3.3 Κοινωνικά Δίκτυα: Μετρήσεις Ανάλυσηςκαι Απόδοση

Αυτή η ενότητα περιγράφει τα διάφορα μέτρα απόδοσης που συναντώνται κατά τη διάρκεια οποιασδήποτε ανάλυσης δικτύων, προκειμένου να κατανοήσουμε τις βασικές έννοιες. Οι τέσσερις πιο σημαντικές έννοιες που χρησιμοποιούνται στην ανάλυση του δικτύου είναι η εγγύτητα, η πυκνότητα του δικτύου, η κεντρικότητα, η ενδιαμεσότητα και ο συγκεντρωτισμός. Εκτός από αυτά, υπάρχουν τέσσερα άλλα μέτρα της απόδοσης του δικτύου που περιλαμβάνουν: την ευρωστία, την αποδοτικότητα, την αποτελεσματικότητα και την ποικιλομορφία. Η πρώτη δέσμη μέτρων αφορά τη δομή, ενώ η δεύτερη δέσμη αφορά τη δυναμική και, επομένως, εξαρτώνται από μια θεωρία που εξηγεί γιατί ορισμένοι παράγοντες κάνουν ορισμένα πράγματα, προκειμένου να έχουν πρόσβαση στις πληροφορίες (Abraham, 2012).

Εγγύτητα

Η εγγύτητα αναφέρεται στο βαθμό με τον οποίο ένα άτομο είναι πιο κοντά σε όλους τους άλλους σε ένα δίκτυο, είτε άμεσα είτε έμμεσα. Περαιτέρω, αντανακλά τη δυνατότητα πρόσβασης σε πληροφορίες μέσω της «αμπέλου» των μελών του δικτύου. Με τον τρόπο αυτό, η εγγύτητα θεωρείται ότι είναι το αντίστροφο του

αθροίσματος της μικρότερης απόστασης (που μερικές φορές ονομάζεται γεωδαισιακή απόσταση) μεταξύ κάθε ατόμου και όλων των άλλων διαθέσιμων στο δίκτυο.

Πυκνότητα δικτύου

Η πυκνότητα του δικτύου είναι ένα μέτρο της συνεκτικότητας σε ένα δίκτυο. Η πυκνότητα ορίζεται ως ο πραγματικός αριθμός των δεσμών σε ένα δίκτυο, που εκφράζεται ως ποσοστό του μέγιστου δυνατού αριθμού δεσμών. Είναι ένας αριθμός που κυμαίνεται μεταξύ 0 και 1,0. Όταν η πυκνότητα είναι κοντά στο 1,0, το δίκτυο λέγεται ότι είναι πυκνό, διαφορετικά είναι αραιό. Όταν ασχολούμαστε με κατευθυνόμενους δεσμούς, ο μέγιστος δυνατός αριθμός των ζευγαριών χρησιμοποιείται αντ' αυτού. Το πρόβλημα με το μέτρο της πυκνότητας είναι ότι είναι ευαίσθητο στον αριθμό των κόμβων του δικτύου. Ως εκ τούτου, δεν μπορεί να χρησιμοποιηθεί για τις συγκρίσεις μεταξύ των δικτύων που διαφέρουν σημαντικά ως προς το μέγεθος.

Κεντρικότητα: Τοπική και Παγκόσμια

Η έννοια της κεντρικότητας περιλαμβάνει δύο επίπεδα: τοπικό και παγκόσμιο. Ένας κόμβος λέγεται ότι έχει τοπική κεντρικότητα, όταν έχει υψηλότερο αριθμό δεσμών με άλλους κόμβους, αλλιώς αναφέρεται ως παγκόσμια κεντρικότητα. Λαμβάνοντας υπόψη ότι η τοπική κεντρικότητα θεωρεί μόνο τους άμεσους δεσμούς (οι δεσμοί που συνδέονται άμεσα με αυτόν τον κόμβο), η παγκόσμια κεντρικότητα θεωρεί επίσης τους έμμεσους δεσμούς (που δεν είναι άμεσα συνδεδεμένοι με αυτόν τον κόμβο). Για παράδειγμα, σε ένα δίκτυο με μια δομή «αστεριού», στο οποίο, όλοι οι κόμβοι έχουν δεσμούς με έναν κεντρικό κόμβο, η τοπική κεντρικότητα του κεντρικού κόμβου είναι ίση με 1,0. Ενώ τα τοπικά μέτρα κεντρικότητας εκφράζονται σε σχέση με τον αριθμό των κόμβων στους οποίους είναι συνδεδεμένος ένας κόμβος, η παγκόσμια κεντρικότητα εκφράζεται σε όρους των αποστάσεων μεταξύ των διαφόρων κόμβων. Δύο κόμβοι συνδέονται με μια διαδρομή, εάν υπάρχει μια αλληλουχία διακριτών δεσμών που τους συνδέουν, και το μήκος της διαδρομής είναι απλά ο αριθμός των δεσμών που το συνθέτουν. Η συντομότερη απόσταση μεταξύ δύο σημείων στην επιφάνεια της γης βρίσκεται κατά μήκος της γεωδαιτικής που τους συνδέει, και, κατ' αναλογία, η συντομότερη διαδρομή μεταξύ οποιουδήποτε συγκεκριμένου ζεύγους κόμβων σε ένα δίκτυο ονομάζεται γεωδαιτικό. Ένας κόμβος είναι συνολικά κεντρικός εάν βρίσκεται σε μικρή απόσταση από πολλούς άλλους κόμβους. Ένας τέτοιος κόμβος λέγεται ότι είναι "κοντά" σε πολλούς από τους άλλους κόμβους του δικτύου, μερικές φορές η παγκόσμια κεντρικότητα ονομάζεται επίσης κεντρικότητα εγγύτητας. Η τοπική και παγκόσμια κεντρικότητα εξαρτώνται κυρίως από το μέγεθος του δικτύου, και ως εκ τούτου δεν μπορούν να συγκριθούν, όταν τα δίκτυα διαφέρουν σημαντικά ως προς το μέγεθος.

Ενδιαμεσότητα

Ως ενδιαμεσότητα ορίζεται ο βαθμός στον οποίο ένας κόμβος βρίσκεται μεταξύ άλλων κόμβων στο δίκτυο. Εδώ, η συνδεσιμότητα των γειτόνων του κόμβου λαμβάνεται υπόψη προκειμένου να παρέχει μια υψηλότερη τιμή για τους κόμβους που γεφυρώνουν νησίδες. Αυτή η μέτρηση αντιπροσωπεύει τον αριθμό των ανθρώπων που συνδέονται έμμεσα μέσω απευθείας συνδέσεων. Η ενδιαμεσότητα ενός κόμβου μετρά το βαθμό στον οποίο ένας πράκτορας (εκπροσωπείται από έναν κόμβο) μπορεί να παίξει το ρόλο ενός χρηματιστή ή φύλακα με δυναμικό έλεγχο πάνω στους άλλους. Μεθοδολογικά, η ενδιαμεσότητα είναι το πιο περίπλοκο

υπολογιστικά από τα μέτρα της κεντρικότητας και πάσχει επίσης από τα ίδια μειονεκτήματα, όπως η τοπική και η παγκόσμια κεντρικότητα.

Συγκέντρωση

Η συγκέντρωση υπολογίζεται ως ο λόγος του αριθμού των συνδέσεων για κάθε κόμβο προς το μέγιστο δυνατό άθροισμα των διαφορών. Η συγκέντρωση παρέχει ένα μέτρο του βαθμού στον οποίο ένα ολόκληρο δίκτυο έχει μια συγκεντρωτική δομή. Λαμβάνοντας υπόψη ότι η συγκέντρωση περιγράφει το βαθμό στον οποίο αυτή η συνεκτικότητα είναι οργανωμένη γύρω από συγκεκριμένους εστιακούς κόμβους, η πυκνότητα περιγράφει το γενικό επίπεδο της σύνδεσης σε ένα δίκτυο. Η συγκέντρωση και η πυκνότητα, ως εκ τούτου, είναι σημαντικά συμπληρωματικά μέτρα. Ενώ ένα κεντρικό δίκτυο θα έχει πολλούς από τους δεσμούς του διεσπαρμένα γύρω από ένα ή λίγους κόμβους, το αποκεντρωμένο δίκτυο είναι ένα δίκτυο στο οποίο υπάρχει μικρή διαφορά μεταξύ του αριθμού των συνδέσεων που διαθέτει κάθε κόμβος. Η γενική διαδικασία που εμπλέκεται με οποιοδήποτε μέτρο της συγκέντρωσης του δικτύου είναι να δούμε τις διαφορές μεταξύ του βαθμού κεντρικότητας του πιο κεντρικού κόμβου και εκείνες όλων των άλλων κόμβων. Βασικά, η συγκέντρωση μπορεί να απεικονιστεί με τρεις τρόπους - ένα για κάθε μία από τα τρία μέτρα κεντρικότητας: τοπική, παγκόσμια και ενδιαμεσότητα Και τα τρία μέτρα συγκέντρωσης κυμαίνονται από 0 έως 1,0. Το μηδέν αντιστοιχεί σε ένα δίκτυο στο οποίο όλοι οι κόμβοι συνδέονται με όλους τους άλλους κόμβους, ενώ η τιμή 1,0 επιτυγχάνεται σε όλα τα μέτρα για δίκτυα τύπου "αστέρι". Ωστόσο, η πλειοψηφία των πραγματικών δικτύων βρίσκεται μεταξύ αυτών των δύο άκρων. Μεθοδολογικά, οι επιλογές του ενός από αυτά τα τρία μέτρα συγκέντρωσης εξαρτάται από το σε ποια συγκεκριμένα διαρθρωτικά χαρακτηριστικά θέλει να εστιάσει ο ερευνητής.

Απόδοση Κοινωνικών Δικτύων

Μόλις ολοκληρωθεί η ανάλυση του δικτύου, η δυναμική του δικτύου μπορεί να προβλέψει την απόδοση του δικτύου, η οποία μπορεί να αξιολογηθεί ως συνδυασμός: (1) της ευρωστίας του δικτύου στην απομάκρυνση των δεσμών ή / και των κόμβων, (2) της αποτελεσματικότητας του δικτύου από την άποψη της απόστασης από τον ένα κόμβο στον άλλο και του μη πλεοναστικού μεγέθους του, (3) την αποτελεσματικότητα του δικτύου όσον αφορά τα οφέλη των πληροφοριών που διατίθενται στους κεντρικούς κόμβους και, τέλος, (4) τη ποικιλομορφία του δικτύου όσον αφορά την ιστορία του καθενός από τους κόμβους (Kim&Leskovec, 2011).

Ευρωστία

Οι αναλυτές κοινωνικών δικτυών τονίζουν τη σημασία της δομής του δικτύου σε σχέση με την ευρωστία του δικτύου. Η ευρωστία μπορεί να αξιολογηθεί με βάση το πώς κατακερματίζεται όταν ένα αυξανόμενο ποσοστό των κόμβων αφαιρεθεί. Η ανθεκτικότητα μετριέται ως εκτίμηση της τάσης των ατόμων στα δίκτυα να σχηματίσουν τοπικές ομάδες ή ομάδες ατόμων με τους οποίους μοιράζονται παρόμοια χαρακτηριστικά, δηλαδή, ομαδοποίηση. Για παράδειγμα, εάν τα άτομα X, Y, και Z είναι εμπειρογνώμονες του υπολογιστή και αν το X γνωρίζει το Y και το Y ξέρει το Z, τότε είναι πολύ πιθανό ότι το X θα γνωρίσει το Z χρησιμοποιώντας τον κανόνα της αλυσίδας. Εάν το μέτρο της ομαδοποίησης των ατόμων είναι υψηλό για ένα δεδομένο δίκτυο, τότε η ευρωστία του εν λόγω δικτύου αυξάνεται - μέσα σε ένα σύμπλεγμα / ομάδα.

Αποδοτικότητα

Η αποδοτικότητα του δικτύου μπορεί να μετρηθεί με βάση τον αριθμό των κόμβων που μπορούν να έχουν άμεση πρόσβαση σε ένα μεγάλο αριθμό διαφορετικών κόμβων - πηγές της γνώσης, κατάσταση - μέσα από ένα σχετικά μικρό αριθμό δεσμών. Αυτοί οι κόμβοι αντιμετωπίζονται ως μη πλεονάζουσες επαφές. Για παράδειγμα, με δύο δίκτυα ίσου μεγέθους, αυτό με περισσότερες μη-πλεονάζουσες επαφές προσφέρει περισσότερα οφέλη από ό, τι το άλλο. Επίσης, είναι προφανές ότι το κέρδος από μια νέα επαφή που είναι πλεονάζουσα σε σχέση με τις υπάρχουσες επαφές θα είναι ελάχιστο. Ωστόσο, καλό είναι να καταναλώνεται χρόνος και ενέργεια στην δημιουργία μιας νέας επαφής προς ανθρώπους που δεν έχουν προσεγγιστεί. Ως εκ τούτου, οι αναλυτές κοινωνικών δικτυών μετρούν την αποδοτικότητα με τον αριθμό των μη-πλεοναζουσών επαφών και τον μέσο αριθμό των δεσμών που πρέπει να διασχίσει ένα εγώ (ego) για να έχει πρόσβαση σε κάθε alter, ο αριθμός αυτός αναφέρεται ως το μέσο μήκος διαδρομής. Όσο μικρότερο είναι το μέσο μήκος διαδρομής σε σχέση με το μέγεθος του δικτύου και όσο χαμηλότερος ο αριθμός των πλεοναζόντων επαφών, τόσο πιο αποδοτικό είναι το δίκτυο.

Αποτελεσματικότητα

Η αποτελεσματικότητα στοχεύει το σύμπλεγμα των κόμβων που μπορεί να επιτευχθεί μέσω των μη πλεοναζουσών επαφών. Σε αντίθεση, η απόδοση στοχεύει στη μείωση του χρόνου και της ενέργειας που δαπανάται για τις πλεονάζουσες επαφές. Κάθε σύμπλεγμα επαφών είναι μια ανεξάρτητη πηγή πληροφοριών. Ένα σύμπλεγμα γύρω έναν μη πλεονάζοντα κόμβο, ανεξαρτήτως του πλήθους των μελών του, είναι μόνο μια πηγή πληροφοριών, επειδή οι άνθρωποι που συνδέονται μεταξύ τους τείνουν να γνωρίζουν τα ίδια πράγματα την ίδια στιγμή. Για παράδειγμα, ένα δίκτυο είναι πιο αποτελεσματικό όταν το όφελος των πληροφοριών που παρέχονται από πολλαπλές συστάδες επαφών είναι ευρύτερο, παρέχοντας την καλύτερη διαβεβαίωση ότι θα ενημερωθεί ο κεντρικός κόμβος. Επιπλέον, επειδή οι μη-πλεονάζουσες επαφές συνδέονται μόνο μέσω του κεντρικού κόμβου, ο κεντρικός κόμβος είναι εξασφαλισμένα ο πρώτος που θα δει τις νέες ευκαιρίες που δημιουργούνται από τις ανάγκες σε μια ομάδα που θα μπορούσε να εξυπηρετείται από τις δεξιότητες άλλης ομάδας.

Ποικιλομορφία

Ενώ η απόδοση έχει ως στόχο έναν μεγάλο αριθμό (μη-πλεοναζουσών) κόμβων, η ποικιλομορφία ενός κόμβου, προτείνει αντίθετα μια κρίσιμη απόδοση όταν οι κόμβοι είναι διαφορετικοί ως προς τη φύση, δηλαδή, η ιστορία του κάθε κόμβου εντός του δικτύου είναι σημαντική. Είναι ιδιαίτερα αυτή η πτυχή που μπορεί να εξερευνηθεί μέσω μελετών περίπτωσης, η οποία είναι ένα θέμα έντονης συζήτησης μεταξύ των αναλυτών κοινωνικών δικτύων. Φαίνεται να δείχνει ότι οι κοινωνικοί επιστήμονες θα πρέπει να προτιμούν και να χρησιμοποιούν την ανάλυση του δικτύου σύμφωνα με το πρώτο σκέλος της σκέψης που αναπτύχθηκε από τους αναλυτές κοινωνικών δικτύων, αντί των λογαριασμών με βάση τη διαφορετικότητα του κάθε κόμβου.

3 ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

3.1 ΤΑ ΛΕΙΤΟΥΡΓΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΜΕΣΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Τα διαδικτυακά κοινωνικά δίκτυα (ΔΚΔ), όπως τα Facebook, MySpace, και Twitter επιτρέπουν στους ανθρώπους να μείνουν σε επαφή με τις επαφές τους, να επανασυνδεθούν με παλιούς γνωστούς, και να δημιουργήσουν νέες σχέσεις με άλλους ανθρώπους με βάση κοινές λειτουργίες όπως οι κοινότητες, τα χόμπι , τα ενδιαφέροντα, και επικαλύψεις σε κύκλους φιλίας. Τα τελευταία χρόνια έχουν δει πρωτοφανή ανάπτυξη στην εφαρμογή των ΔΚΔ, με περίπου 300 συστήματα ΔΚΔ να συλλέγουν πληροφορίες για περισσότερους από μισό δισεκατομμύριο εγγεγραμμένους χρήστες. Ως αποτέλεσμα, τα ΔΚΔ αποθηκεύουν ένα τεράστιο ποσό ενδεχομένως ευαίσθητων και ιδιωτικών πληροφοριών σχετικά με τους χρήστες και τις αλληλεπιδράσεις τους. Αυτές οι πληροφορίες είναι συνήθως ιδιωτικές και προορίζονται μόνο για ένα συγκεκριμένο κοινό. Ωστόσο, η δημοτικότητα των ΔΚΔ προσελκύει όχι μόνο τους πιστούς χρήστες, αλλά και άτομα ή επιχειρήσεις με μάλλον κακόβουλα συμφέροντα. Η διαφοροποίηση και η πολυπλοκότητα των σκοπών και των τρόπων χρήσης των ΔΚΔ αναπόφευκτα εισάγει κινδύνους παραβίασης της ιδιωτικής ζωής σε όλους τους χρήστες ΔΚΔ, ως αποτέλεσμα της ανταλλαγής πληροφοριών και της κοινής χρήσης του Διαδικτύου. Επομένως, δεν αποτελεί έκπληξη το γεγονός ότι οι ιστορίες για παραβιάσεις της ιδιωτικής ζωής από το Facebook και το MySpace εμφανίζονται κατ' επανάληψη στα mainstream μέσα ενημέρωσης (Zhang&Sun, 2010).

Ανεξάρτητα από το σκοπό των ΔΚΔ, ένα από τα βασικά κίνητρα ώστε οι χρήστες του διαδικτύου να συμμετάσχουν σε ένα ΔΚΔ, να δημιουργήσουν ένα προφίλ και να χρησιμοποιήσουν διαφορετικές εφαρμογές που προσφέρονται από το ΔΚΔ, είναι η δυνατότητα να μοιραστούν εύκολα τις πληροφορίες με επιλεγμένες επαφές ή το κοινό, και να διευκολυνθεί η κοινωνική αλληλεπίδραση μεταξύ των χρηστών του ΔΚΔ. Η αποκάλυψη προσωπικών πληροφοριών στα ΔΚΔ είναι ένα δίκοπο μαχαίρι. Από τη μία πλευρά, η έκθεση πληροφοριών είναι συνήθως ένα συν, ίσως και υποχρεωτική, αν οι άνθρωποι θέλουν να συμμετέχουν στις κοινωνικές κοινότητες. Η ορατότητα των προφίλ χρηστών και η δημόσια επίδειξη των συνδέσεων (λίστες φίλων) είναι αναγκαία για την εφαρμογή βασικών λειτουργιών των ΔΚΔ όπως η κοινωνική αναζήτηση και η κοινωνική διάσχιση. Από την άλλη πλευρά, η διαρροή των προσωπικών πληροφοριών, ειδικά της ταυτότητας του ατόμου, μπορεί να προκαλέσει κακόβουλες επιθέσεις από τον πραγματικό κόσμο και τον κυβερνοχώρο, όπως η καταδίωξη, η συκοφαντία, εξατομικευμένο spamming, και phishing. Παρά τους κινδύνους, πολλοί από τους μηχανισμούς προστασίας της ιδιωτικής ζωής και του ελέγχου της πρόσβασης στα σύγχρονα ΔΚΔ είναι σκόπιμα αδύναμοι ώστε να διευκολυνθεί η ένταξη στα ΔΚΔ και η ανταλλαγή πληροφοριών. Πιστεύουμε ότι οι πιο αποτελεσματικοί και ευέλικτοι μηχανισμοί ασφαλείας, ως εκ τούτου απαιτούνται για την ασφάλεια των χρηστών ΔΚΔ.

Δεδομένου ότι το κίνητρο της έρευνάς μας είναι η διερεύνηση των ζητημάτων που υποβιβάζουν την προστασία της ιδιωτικής ζωής και την ασφάλειας στα ΔΚΔ, τα

επιθυμητά χαρακτηριστικά των παραδοσιακών ΔΚΔ και οι πιθανές εφαρμογές τους αναλύονται αρχικά.

Χωρίς αμφιβολία, υπάρχει μεγάλη ποικιλομορφία μεταξύ των ΔΚΔ σε όλες τις διαστάσεις. Ωστόσο, είναι ευρέως αποδεκτό ότι όλα τα ΔΚΔ έχουν κάποια βασικά χαρακτηριστικά. Ένα ΔΚΔ χαρακτηρίζεται ως εξής. Ένα ΔΚΔ είναι μια ψηφιακή αναπαράσταση των χρηστών του και (ένα υποσύνολο) κοινωνικών συνδέσεων / σχέσεων τους στο φυσικό ή εικονικό κόσμο, καθώς και υπηρεσίες για την ανταλλαγή μηνυμάτων και την κοινωνικοποίηση μεταξύ των χρηστών του δικτύου. Παρέχει μια πλατφόρμα που(Zhang&Sun, 2010):

- Επιτρέπει στους χρήστες να κατασκευάσουν ψηφιακές αναπαραστάσεις του εαυτού τους (συνήθως γνωστές ως προφίλ χρήστη) και να δημιουργήσουν κοινωνικές συνδέσεις με άλλους χρήστες (δηλαδή, λίστες επαφών).
- Υποστηρίζει τη συντήρηση και βελτίωση των προϋπάρχουσων κοινωνικών σχέσεων μεταξύ των χρηστών στο φυσικό ή εικονικό κόσμο.
- Βοηθά στη δημιουργία νέων συνδέσεων με βάση τα κοινά συμφέροντα, την τοποθεσία, τις δραστηριότητες, και ούτω καθεξής.

Με βάση τον παραπάνω ορισμό, ένα ΔΚΔ θα πρέπει να παρέχει τις ακόλουθες λειτουργίες για τη διευκόλυνση της αυτο-αναπαράστασης των χρηστών και των διαδικτυακών κοινωνικών αλληλεπιδράσεων.

3.1.1 Διαχείριση προσωπικού χώρου

Ένα ΔΚΔ πρέπει να υποστηρίξει το χρήστη στη:

- Δημιουργία και διαγραφή λογαριασμού χρήστη (δηλαδή, εγγραφή χρήστη ή απόσυρσης)
- Δημιουργία και επεξεργασία του προφίλ του χρήστη
- Ανέβασμα και επεξεργασία περιεχομένου που παράγεται από το χρήστη (δηλαδή, το blog-όπως αποσπάσεις, ενημέρωση κατάστασης)

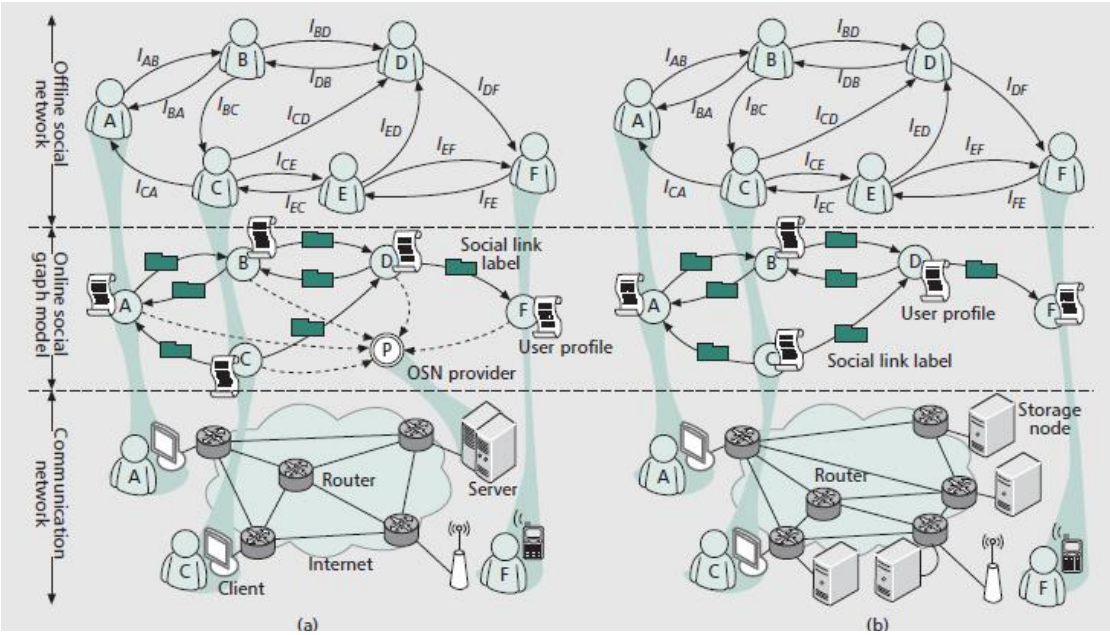
Ας σημειωθεί ότι στα περισσότερα ΔΚΔ, οι ενέργειες ενός χρήστη στον προσωπικό χώρο του θα αναφερθούν στις κοινωνικές επαφές του αυτόματα. Ως αποτέλεσμα, το περιεχόμενο που δημιουργείται από το ανέβασμα του χρήστη και την επεξεργασία, χρησιμεύει ως ένα σημαντικό αρχέτυπο επικοινωνίας μεταξύ ενός χρήστη και των επαφών του.

3.1.2 Διαχείριση Κοινωνικής Σύνδεσης

Ένα ΔΚΔ συνδέει τους ανθρώπους με την παροχή επίσημων μέσων ώστε οι χρήστες να δημιουργήσουν σχέσεις με άλλους χρήστες (π.χ. λίστες φίλων). Εκτός από την εκπροσώπηση των υφιστάμενων κοινωνικών δεσμών, ένα ΔΚΔ μπορεί να χρησιμοποιηθεί για να αποκαταστήσει τις χαμένες κοινωνικές συνδέσεις αν είναι χρήστες του ίδιου ΔΚΔ. Οι κοινωνικοί δεσμοί μπορεί επίσης να έχουν δημιουργηθεί πρόσφατα, για παράδειγμα, όταν οι χρήστες βρίσκουν και μοιράζονται κοινά

ενδιαφέροντα. Ως εκ τούτου, ένα ΔΚΔ θα πρέπει να υποστηρίζει τους χρήστες στη δημιουργία, διατήρηση και ανάκληση μιας κοινωνικής σχέσης (Zhang&Sun, 2010).

Χρησιμοποιούμε ένα απλό επισημασμένο διάγραμμα (δηλαδή, σε ένα διαδικτυακό κοινωνικό γράφημα) με το υπόδειγμα όλων των δεδομένων που είναι αποθηκευμένα σε ένα ΔΚΔ, το οποίο απεικονίζεται στην Εικόνα 3-1. Εδώ, οι κορυφές-κόμβοι μοντελοποιούν μεμονωμένους χρήστες σε ένα ΔΚΔ, ενώ τα άκρα- συνδέσεις μοντελοποιούν τις κοινωνικές συνδέσεις μεταξύ των χρηστών. Κάθε κόμβος διατηρεί το αντίστοιχο προφίλ χρήστη, καθώς και κάθε σύνδεσμος έχει επισημανθεί με ετικέτα κοινωνικού συνδέσμου. Μερικά ΔΚΔ επιτρέπουν στους χρήστες όχι μόνο να καθορίσουν τους τύπους των κοινωνικών συνδέσεων (π.χ., τους φίλους ή τους συναδέλφους), αλλά και να δημιουργήσουν σχέσεις εμπιστοσύνης, που εκφράζουν το πόσο εμπιστεύονται τα άλλα μέλη, είτε σε σχέση με ένα συγκεκριμένο θέμα (τοπική εμπιστοσύνη) ή γενικά (απόλυτη εμπιστοσύνη). Μπορούμε να μοντελοποιήσουμε όλες αυτές τις περιγραφές και τις προδιαγραφές για μια κοινωνική σύνδεση με την ετικέτα του αντίστοιχου κοινωνικού συνδέσμου στο διαδικτυακό κοινωνικό γράφημα. Η συλλογή των προφίλ ενός συγκεκριμένου χρήστη και των συνδεδεμένων κοινωνικών δεσμών ονομάζεται ψηφιακός προσωπικός χώρος (προσωπικός χώρος για συντομία). Η συλλογή των προσωπικών χώρων από όλους τους εγγεγραμμένους χρήστες ενός ΔΚΔ ονομάζεται ψηφιακός κοινωνικός χώρος.



Εικόνα 3-1 Μία περιγραφή τριών επιπέδων των διαδικτυακών κοινωνικών δικτύων: α) client-server αρχιτεκτονική, β) peer-to-peer αρχιτεκτονική (Zhang&Sun, 2010)

3.1.3 Μέσα Επικοινωνίας

Η επικοινωνία με τους άλλους είναι το κεντρικό χαρακτηριστικό που προσφέρεται από τις υπηρεσίες ΔΚΔ. Υπάρχουν αρκετά πιθανά κανάλια επικοινωνίας μεταξύ των χρηστών. Πρώτον, μπορεί κανείς να αφήσει δημόσια μηνύματα (π.χ., blogging), με τη μορφή τ κειμένων, βίντεο, ήχου, φωτογραφιών, και ούτω καθεξής, χρησιμοποιώντας

προσωπικό χώρο. Επιπλέον, μπορεί κανείς να στείλει προσωπικά μηνύματα, που είναι μια άλλη μορφή της ασύγχρονης επικοινωνίας, σε αντίθεση με τη σύγχρονη επικοινωνία όπως το instant messaging, άμεσα διαθέσιμο σε όλα σχεδόν τα ΔΚΔ. Ένα ελκυστικό χαρακτηριστικό των ΔΚΔ είναι ότι είναι ανοικτά σε εφαρμογές τρίτων. Ενώ πολλές από αυτές τις εφαρμογές παρέχουν εναλλακτικά μέσα των σύγχρονων επικοινωνιών, υπάρχουν επίσης εφαρμογές που επιτρέπουν στους χρήστες να συμμετάσχουν σε δραστηριότητες σε πραγματικό χρόνο, όπως online παιχνίδια.

3.1.4 Εξερεύνηση του Ψηφιακού Κοινωνικού Χώρου

Το ΔΚΔ δεν περιορίζονται στις αλληλεπιδράσεις με τις υπάρχουσες επαφές, και ενθαρρύνει τους χρήστες να δημιουργήσουν νέες κοινωνικές συνδέσεις (κοινωνικοποίηση). Ως εκ τούτου, η υποστήριξη για την αναζήτηση ή τη διάσχιση στο ψηφιακό κοινωνικό χώρο είναι ένα κρίσιμο συστατικό των ΔΚΔ. Η περιήγηση στο προσωπικό χώρο ενός νέου χρήστη έχει λάβει άδεια λειτουργίας σε δύο στάδια. Υπάρχουν δύο τρόποι με τους οποίους μπορεί να προσπελαστεί ο προσωπικός χώρος ενός άγνωστου χρήστη:

3.1.4.1 Παγκόσμια Αναζήτηση λέξης (ή Κοινωνικής Αναζήτηση)

Το πρώτο μέσο για να βρεθεί ένας άγνωστος χρήστης είναι να διεξαχθεί μια παγκόσμια αναζήτηση λέξεων-κλειδιών. Μια επιτυχής αναζήτηση θα παράγει για την πρόσβαση του χρήστη τα θέση στη λίστα αναζήτησης ενός χρήστη-στόχου. Ένας χρήστης μπορεί να καθορίσει μια πολιτική αναζήτησης για να επιτρέψει μόνο ένα υποσύνολο των χρηστών να είναι σε θέση να φτάσουν την καταχώρισή αναζήτηση της μέσα από μια παγκόσμια αναζήτηση ονόματος.

3.1.4.2 Διάσχιση Κοινωνικού Γραφήματος (ή κοινωνική διάσχιση)

Ένας δεύτερος τρόπος για να φτάσει ένας χρήστης στη λίστα αναζήτησης του χρήστη στόχου για να φτάσει μια λίστα αναζήτησης είναι η διάσχιση του online κοινωνικού γραφήματος. Ένας χρήστης μπορεί να διασχίσει αυτό το γράφημα με την εξέταση των καταλόγων φίων των άλλων χρηστών. Πιο συγκεκριμένα, η λίστα των φίλων του χρήστη είναι ουσιαστικά το σύνολο των λιστών αναζήτησης από τους φίλους του. Ένας χρήστης μπορεί να περιορίσει την διάσχιση καθορίζοντας μια πολιτική διάσχισης, η οποία καθορίζει το σύνολο των χρηστών που επιτρέπεται να εξετάσουν τη λίστα φίλων του μετά την πρόσβαση στη λίστα αναζήτησης. Για να επιτευχθούν οι στόχοι των παραδοσιακών ΔΚΔ, όπως η χρηστικότητα και η κοινωνικότητα, πρέπει να στηρίξουμε όλες τις λειτουργίες που αναφέρονται παραπάνω στο σχεδιασμό νέων ασφαλών ΔΚΔ που σέβονται την ιδιωτική ζωή των χρηστών. Υπάρχουν και άλλοι στόχοι, όπως η αποδοτικότητα και παραμετροποίηση.

3.2 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΣΥΣΤΗΜΑΤΟΣ

Υπάρχουν δύο παραδείγματα της εφαρμογής ενός ΔΚΔ στη βιβλιογραφία, η αρχιτεκτονική client-server και η αρχιτεκτονική peer-to-peer (P2P), η οποία αποφέρει κεντρικά και κατανεμημένα συστήματα, αντίστοιχα (Zhang&Sun, 2010).

3.2.1 Αρχιτεκτονική Client-Server

Τα σύγχρονα ΔΚΔ είναι συγκεντρωτικά και βασίζονται στους διαδικτυακούς διακομιστές. Όλες οι λειτουργίες, όπως η αποθήκευση, η συντήρηση, καθώς και η πρόσβαση σε υπηρεσίες ΔΚΔ, προσφέρονται από τους εμπορικούς παρόχους ΔΚΔ όπως το Facebook Inc., LinkedIn Corp., και XING AG. Αυτή η παραδοσιακή αρχιτεκτονική έχει το πλεονέκτημα ότι είναι απλή και εύκολη στην εφαρμογή, ενώ πάσχει από όλα τα μειονεκτήματα των κεντρικών συστημάτων. Για παράδειγμα, κάθε κεντρικός φορέας μπορεί εύκολα να είναι ένα ενιαίο σημείο αποτυχίας, ένας ενιαίος στόχος για άρνηση υπηρεσίας denial-of-service (DoS), καθώς επίσης και μια δυσχέρεια για την απόδοση του δικτύου.

3.2.2 P2P Αρχιτεκτονική

Υπάρχει μια ισχυρή τάση για τον σχεδιασμό μιας αρχιτεκτονικής P2P για τα ΔΚΔ επόμενης γενιάς. Η υιοθέτηση μιας αποκεντρωμένης αρχιτεκτονικής βασίζεται στη συνεργασία ανάμεσα σε μια σειρά ανεξάρτητων φορέων οι οποίοι είναι επίσης οι χρήστες των ΔΚΔ. Οι προσωπικοί χώροι των χρηστών αποθηκεύονται και διατηρούνται κατανεμητικά. Με την υποστήριξη της άμεσης ανταλλαγής πληροφοριών μεταξύ των συσκευών, μεταξύ των χρηστών που έχουν συναντηθεί πριν ή μεταξύ γειτονικών κόμβων ενός δικτύου πλέγματος της πόλης, μια αρχιτεκτονική P2P μπορεί να ωφελήσει τη γεωγραφική εγγύτητα των πραγματικών κοινωνικών δικτύων με την υποστήριξη των τοπικών υπηρεσιών, όταν η πρόσβαση στο Internet είναι διαθέσιμη. Αλλά για την αρχιτεκτονική P2P, η προσφορά κάποιων υπηρεσιών (π.χ., η παγκόσμια αναζήτηση) των ΔΚΔ με ένα κατανεμημένο τρόπο, είναι ένα δύσκολο πρόβλημα.

Η Εικόνα 3-1 απεικονίζει δύο είδη των αρχιτεκτονικών για τα ΔΚΔ, όπου η αρχιτεκτονική client-server απαιτεί σύνδεση στο Internet ώστε οι χρήστες να επικοινωνούν μέσω του απομακρυσμένου κεντρικού server, και το P2P ομόλογό υποστηρίζει επικοινωνίες μέσω τοπικής συνδεσιμότητας δεδομένου ότι ο ρόλος του κεντρικού διακομιστή κατανέμεται σε κάθε κόμβος εγκατάστασης αποθήκευσης. Ας σημειωθεί ότι για την αρχιτεκτονική client-server, στο αντίστοιχο διαδικτυακό μοντέλο κοινωνικό γράφημα, προστίθεται μια νέα οντότητα που ονομάζεται πάροχος ΔΚΔ, και κάθε χρήστης ΔΚΔ έχει μια κοινωνική (π.χ., εμπιστοσύνη) σχέση μαζί του.

3.3 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

3.3.1 Εμπιστευτικότητα ή προστασία προσωπικών δεδομένων

Η προστασία προσωπικών δεδομένων είναι υψίστης σημασίας στα ΔΚΔ, δεδομένου ότι η παράνομη αποκάλυψη και ανάρμοστη χρήση των ιδιωτικών πληροφοριών των χρηστών μπορεί να προκαλέσει ανεπιθύμητες ή βλαβερές συνέπειες στη ζωή των ανθρώπων.

Η προστασία της ιδιωτικής ζωής στο πλαίσιο των ΔΚΔ έχει αρκετές ευρείες κατηγορίες (Zhang&Sun, 2010):

- Ανωνυμία ταυτότητας χρήστη. Η προστασία των αλλαγών της ταυτότητας ενός χρήστη σε διαφορετικούς τύπους ΔΚΔ. Σε ιστοσελίδες κολεγίου, όπως το Facebook, ενθαρρύνεται η χρήση των πραγματικών ονομάτων για την παρουσίαση του προφίλ του λογαριασμού με το υπόλοιπο ΔΚΔ. Δεν υπάρχει ανωνυμία ταυτότητας χρήστη, επειδή οι περισσότερες εφαρμογές στο Facebook στηρίζονται σε σύνδεση των προφίλ των χρηστών με τη δημόσια ταυτότητά τους. Σε dating sites όπως το Friendster, μια ασθενής ψευδωνυμία δημιουργείται κάνοντας μόνο το πρώτο όνομα του συμμετέχοντος ορατό στους άλλους, και όχι το επίθετό του. Σε dating sites που λειτουργούν με ψευδώνυμα όπως το Match.com, αποθαρρύνεται η χρήση των πραγματικών ονομάτων και προσωπικών στοιχείων επικοινωνίας. Ένα τυχαίο αναγνωριστικό χρησιμοποιείται για την προστασία της δημόσιας ταυτότητας ενός ατόμου.
- Προστασία του προσωπικού χώρου του χρήστη - Η προβολή του προφίλ χρήστη διαφέρει επίσης μεταξύ των διαφόρων τύπων των ΔΚΔ. Από προεπιλογή, τα προφίλ στο Friendster και Tribe.net ανιχνεύονται από τις μηχανές αναζήτησης, που τα καθιστά ορατά σε όλους, ανεξάρτητα από το αν ή όχι ο θεατής έχει ένα λογαριασμό. Τα ΔΚΔ όπως το MySpace επιτρέπουν στους χρήστες να επιλέξουν αν θέλουν το προφίλ τους να είναι δημόσιο ή ορατό μόνο σε φίλους. Το Facebook έχει μια διαφορετική προσέγγιση: από προεπιλογή, οι χρήστες οι οποίοι είναι μέρος του ίδιου υποδικτύου μπορούν να δουν τα προφίλ των άλλων, εκτός αν ένας ιδιοκτήτης προφίλ έχει αποφασίσει να αρνηθεί την άδεια σε εκείνους που βρίσκονται στο υποδίκτυο του. Για τα περισσότερα ΔΚΔ, μια λίστα φίλων είναι ορατή σε όποιον έχει τη δυνατότητα να δει το προφίλ του, αν και υπάρχουν εξαιρέσεις. Για παράδειγμα, ορισμένοι χρήστες του MySpace έχουν χακάρει τα προφίλ τους για να κρύψουν τους καταλόγους φίλων τους, και το LinkedIn επιτρέπει στους χρήστες να επιλέξουν την απόκρυψη του καταλόγου φίλων.
- Προστασία επικοινωνίας χρήστη - Εκτός από τα προσωπικά στοιχεία που γνωστοποιούνται στον ψηφιακό χώρο του χρήστη, ο χρήστης ΔΚΔ μπορεί επίσης να αποκαλύψει προσωπικές πληροφορίες στο χειριστή του δικτύου ή τον πάροχο ΔΚΔ χρησιμοποιώντας το ίδιο το δίκτυο: τα δεδομένα όπως είναι ο χρόνος και το μήκος των συνδέσεων, η τοποθεσία (διεύθυνση IP) της σύνδεσης, τα προφίλ άλλων χρηστών που επισκέπτεται, τα μηνύματα που αποστέλλονται και λαμβάνονται, και ούτω καθεξής. Ως εκ τούτου, επιπλέον, η προστασία της επικοινωνίας πρέπει να τηρείται.

Για να συνοψίσουμε, η απαίτηση προστασίας της ιδιωτικής ζωής του χρήστη είναι διττή. Κατ' αρχάς, μη εξουσιοδοτημένες οντότητες (οι οποίοι δεν έχουν πρόσβαση στα ιδιωτικά στοιχεία) δεν πρέπει να μάθουν το περιεχόμενο των ιδιωτικών δεδομένων που αποκαλύπτει πληροφορίες ταυτοποίησης του κατόχου των δεδομένων (του χρήστη). Αυτή η πτυχή της ιδιωτικής ζωής των δεδομένων προϋποθέτει την εμπιστευτικότητα των δεδομένων και την ανωνυμία του ιδιοκτήτη, και άμεσα οδηγεί στην ανάγκη για έλεγχο πρόσβασης. Η πρόσβαση σε πληροφορίες για ένα χρήστη μπορεί να χορηγηθεί μόνο από το χρήστη άμεσα, και ο έλεγχος της πρόσβασης πρέπει να είναι όσο λεπτομερής, ώστε οι πληροφορίες κάθε ιδιωτικού στοιχείου πρέπει να είναι ξεχωριστά διαχειρίσιμες. Δεύτερον, οι μη εξουσιοδοτημένες οντότητες δεν πρέπει να είναι σε θέση να συνδέσουν πολλαπλά αρχεία ιδιωτικών δεδομένων στο προφίλ του ιδιοκτήτη, που σημαίνει ότι η εμφάνιση των αποθηκευμένων ή μεταδιδόμενων ιδιωτικών δεδομένων θα πρέπει να είναι τυχαία και να μην διαρρέει καμία χρήσιμη πληροφορία. Η πτυχή αυτή είναι ουσιαστικά η απαίτηση Μη-συνδεσιμότητας.

3.3.2 Ταυτότητας και ακεραιότητα δεδομένων

Αν και υπάρχουν εξαιρέσεις, τα περισσότερα ΔΚΔ υποστηρίζουν κυρίως προϋπάρχουσες κοινωνικές σχέσεις στην πραγματική ζωή. Ως εκ τούτου, σε ιδανικές περιπτώσεις ένα ΔΚΔ είναι απλά μια ψηφιακή αναπαράσταση ενός offline κοινωνικού δικτύου (ονομάζεται επίσης κοινωνικό δίκτυο πραγματικής ζωής [RSN]). Εφόσον τα δεδομένα που είναι αποθηκευμένα σε ένα ΔΚΔ μπορούν να μοντελοποιηθούν ως ένα online κοινωνικό γράφημα, υπάρχει μια χαρτογράφηση ένας-προς-έναν από το RSN στο online κοινωνικό γράφημα (Εικ. 3-1). Η ακεραιότητα των δεδομένων στο πλαίσιο του ΔΚΔ σημαίνει ότι αυτή η συνέπεια πρέπει να διατηρηθεί. Δηλαδή, κάθε απόπειρα απόκλισης σε ένα online κοινωνικό γράφημα από το αντίστοιχο RSN του είναι ένα είδος επίθεσης, και θα πρέπει να εντοπιστεί και να διορθωθεί με κατάλληλους μηχανισμούς (Gunatilaka, 2016).

Προφανώς, υπάρχουν δύο τύποι των επιθέσεων στα onlineκοινωνικά γραφήματα: η σφυρηλάτηση κόμβων και ταυτοτήτων και η σφυρηλάτηση κοινωνικών δεσμών και συνδέσεων. Η σφυρηλάτηση ενός κόμβου (π.χ. κλοπή ταυτότητας) είναι ένα θεμελιώδες πρόβλημα στα ΔΚΔ και βρίσκεται στη ρίζα πολλών άλλων προβλημάτων ασφαλείας. Για παράδειγμα, ένας εισβολέας μπορεί να δημιουργήσει ψεύτικο προφίλ στο όνομα γνωστών προσωπικοτήτων ή επιχειρηματικών επωνυμιών, προκειμένου να συκοφαντήσει τους ανθρώπους ή τα κέρδη από τη φήμη τους. Επίσης, ένας εισβολέας μπορεί να δημιουργήσει πολλαπλές πλαστές ταυτότητες για να διαταράξει τα ψηφιακά συστήματα φήμης στα ΔΚΔ. Ως εκ τούτου, απαιτείται ότι οι οντότητες που επικοινωνούν (π.χ., οι χρήστες ΔΚΔ) πρέπει να είναι σίγουρες για την νομιμότητα του άλλου (δηλαδή, τα κλειδιά που χρησιμοποιούνται για τον έλεγχο ταυτότητας να έχουν πράγματι ανατεθεί από αξιόπιστη αρχή) και την αυθεντικότητα (δηλαδή, μια οικονομική οντότητα πρέπει να έχει στην κατοχή της την ταυτότητα που χρησιμοποιεί).

3.3.3 Άλλες

Επειδή ορισμένα ΔΚΔ χρησιμοποιούνται ως επαγγελματικά εργαλεία για να ενισχύσουν τις επιχειρήσεις ή τη σταδιοδρομία των επαγγελματιών - μελών τους, πρέπει επίσης να πληρούνται άλλες απαιτήσεις ασφάλειας, συμπεριλαμβανομένης της διαθεσιμότητας (δηλαδή, στοιχεία που δημοσιεύονται από τους χρήστες πρέπει να είναι συνεχώς διαθέσιμα) και της λογοδοσίας (δηλαδή, η ανάρμοστη συμπεριφορά των χρηστών θα πρέπει να είναι ανιχνεύσιμη).

3.4 ΣΧΕΔΙΑΣΤΙΚΑ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

3.4.1 Εξερεύνηση κοινωνικού χώρου

Για την υποστήριξη της κοινωνικής αναζήτησης και διάσχισης, αποκαλύπτονται απαραιτήτως κάποιες πληροφορίες σχετικά με τα προφίλ και τις λίστες φίλων των χρηστών. Για την κοινωνική έρευνα, προφανώς, περισσότερα δεδομένα προσωπικού χαρακτήρα πρέπει να δημοσιοποιούνται, προκειμένου να υποστηριχθεί πιο αποτελεσματικά και με ακρίβεια η αναζήτηση στο ψηφιακό κοινωνικό χώρο. Ως εκ τούτου, υπάρχει ένα trade-off μεταξύ των δυνατοτήτων αναζήτησης και της προστασίας της ιδιωτικής ζωής. Συγκεκριμένα, η υψηλότερη απόδοση αναζήτησης σημαίνει επίσης μεγαλύτερη πιθανότητα παραβίασης της ιδιωτικής ζωής (Zhang&Sun, 2010).

Για την κοινωνική διάσχιση, η δημόσια επίδειξη των κοινωνικών συνδέσεων επηρεάζει επίσης την ιδιωτική ζωή των χρηστών. Κατ' αρχάς, οι κοινωνικές επαφές αντιπροσωπεύουν από μόνες τους ευαίσθητες, προσωπικές πληροφορίες που μπορεί να χρησιμοποιηθούν καταχρηστικά. Για παράδειγμα, το γεγονός ότι δύο επαγγελματίες που απασχολούνται από αντίπαλες εταιρείες είναι φίλοι μπορεί να προκαλέσει υποψίες. Δεύτερον, τα στοιχεία της κοινωνικής επαφής μπορεί να χρησιμοποιηθούν για να συμπεράνουμε περισσότερες ιδιωτικές πληροφορίες. Για παράδειγμα, ας υποθέσουμε ότι το προφίλ του χρήστη Bob κρυπτογραφείται και είναι προσβάσιμο μόνο από τους φίλους του, ενώ οι λίστες φίλων όλων των χρηστών είναι ανοικτές, προκειμένου να διευκολυνθεί η κοινωνική διάσχιση. Σε αυτή την περίπτωση τα προσωπικά δεδομένα του Bob μπορεί να συναχθούν έμμεσα από τους αντιπάλους. Διαισθητικά, οι φίλοι τείνουν να μοιράζονται κοινά χαρακτηριστικά. Για παράδειγμα, συμμαθητές του δημοτικού σχολείου έχουν παρόμοια ηλικία και την ίδια πατρίδα. Ως εκ τούτου, για να συμπεράνουμε την ηλικία κάποιου ή τα προσωπικά συμφέροντα, μπορούμε να ελέγξουμε τις τιμές αυτών των χαρακτηριστικών από τους συμμαθητές του ή τους φίλους του. Σημειώστε ότι από την άλλη πλευρά η γνωστοποίηση πληροφοριών για την κοινωνική επαφή παρέχει επίσης πολλούς νέους τρόπους για την προστασία στα μέσα κοινωνικής δικτύωσης. Για παράδειγμα, τα μονοπάτια σε ένα online κοινωνικό γράφημα είναι χρήσιμα για να εκφράσουν τους αξιόπιστους χρήστες: οι κοντινοί χρήστες-κόμβοι σε ένα online κοινωνικό γράφημα συχνά λαμβάνουν ένα υψηλότερο επίπεδο εμπιστοσύνης. Επίσης, τα μονοπάτια σε ένα online κοινωνικό γράφημα μπορεί να παρέχουν μια βάση για τους μηχανισμούς ελέγχου πρόσβασης, όπου οι χρήστες καθορίζουν τους εξουσιοδοτημένους χρήστες με βάση την απόστασή τους από τον εαυτό τους στο κοινωνικό γράφημα (Abraham, 2012).

3.4.2 Αλληλεπίδραση μεταξύ χρηστών

Η διευκόλυνση της κοινωνικής αλληλεπίδρασης είναι η κύρια λειτουργία όλων των ΔΚΔ. Ωστόσο, αυτό μπορεί να οδηγήσει σε διαρροή πληροφοριών της ιδιωτικής ζωής με ανεξέλεγκτο τρόπο για τους χρήστες ΔΚΔ. Για παράδειγμα, ο Bob είναι καθηγητής Λυκείου και μέλος του συλλόγου όπλων, που θέλει να κρατήσει την προσωπική και επαγγελματική του ζωή ξεχωριστή. Έτσι συμμετέχει σε δύο ΔΚΔ: ΠροσωπικόΔΚΔ (P-ΔΚΔ) για τους προσωπικούς του φίλους και την ΔΚΔ Εργασία (W-ΔΚΔ) για όλες τις επαγγελματικές επαφές του. Η Αλίκη και η Κάρολ είναι στις λίστες φίλων του P-ΔΚΔ και W-ΔΚΔ, αντίστοιχα. Στην αρχή, ο Bob P-ΔΚΔ και W-ΔΚΔ είναι εντελώς διαφορετικοί. Ωστόσο, λίγες μέρες αργότερα, η Κάρολ βρίσκει την συμμαθήτρια τηςΑλίκη στο δίκτυο, και η Αλίκη καλεί την Κάρολ για να ενταχθεί στο P-ΔΚΔ. Η Κάρολ θέλει να βρει συμμαθητές με τους οποίους έχει χάσει επαφή με την εξέταση της λίστας των φίλων της Αλίκη στη P-ΔΚΔ, και διαπιστώνει ότι ο συνάδελφός της, ο Μπομπ είναι συλλέκτης όπλων. Όταν ο Bob έχει επίγνωση αυτής της αλλαγής, τα μέρη των προσωπικών του πληροφοριών έχουν ήδη γίνει γνωστά στις επαφές του στο W-ΔΚΔ.

Στο προηγούμενο παράδειγμα, οι πληροφορίες για την ταυτότητα του Bob αποκαλύπτεται τόσο μέσω του P-ΔΚΔόσο και του W-ΔΚΔ. Ακόμα και αν ο Bob δεν αποκαλύπτει καμία από τις προσωπικές του πληροφορίες, άλλοι μπορούν να το πράξουν κατά τη διάρκεια των κοινωνικών αλληλεπιδράσεων. Ας υποθέσουμε ότι ο Bob χρησιμοποιεί το ψευδώνυμο 5473625 για να προστατεύσει την ταυτότητά του, και όλα τα προσωπικά στοιχεία του κρυπτογραφούνται και είναι προσβάσιμα μόνο για τους φίλους του. Η Αλίκη, ένας φίλος του Μπομπ, μπορεί ακόμα να αποκαλύψει την ηλικία, το επάγγελμα, και ακόμη και το πραγματικό όνομα του Bob κατά τη διάρκεια των αλληλεπιδράσεών τους με τους εξής τρόπους (Balduzzietal, 2010):

- Η Αλίκη μπορεί να φορτώσει μια φωτογραφία που τραβήχτηκε με τον Μπομπστα λευκώματα της. Μπορεί επίσης να σχολιάσει τη φωτογραφία «Μπομπ και η Αλίκη στο Διαστημικό Κέντρο Κένεντι» και να συνδέσει τη φωτογραφία στο προφίλ του χρήστη 5473625 του. Η δράση αυτή θα αποκαλύψει το πλήρες όνομα του χρήστη 5473625, τη πραγματική ταυτότητα (μέσω της αναγνώρισης προσώπου), καθώς και το γεγονός ότι ο Μπομπ και η Αλίκη είναι φίλοι.
- Ας υποθέσουμε ότι η Αλίκη συνιστά επίσης τον Μπομπ ως «ο καλύτερος δάσκαλος στο Ορλάντο» στη δική της σελίδα, και ως εκ τούτου αποκαλύπτει κατά λάθος το επάγγελμα του Μπομπ και την πόλη όπου ζει. Έτσι, η Αλίκη μπορεί ακούσια να αποκαλύψει ένα μεγάλο αριθμό πληροφοριών σχετικά με Μπομπ χωρίς τη γνώση του. Με άλλα λόγια, οι προσπάθειες του Μπομπ να προστατεύσει την ταυτότητά του μπορεί εύκολα να εξουδετερωθούν από τη συμπεριφορά των άλλων στις κοινωνικές αλληλεπιδράσεις τους. Επιπλέον, είναι δύσκολο για τον Μπομπ να ανιχνεύσει περιστατικά τέτοιων διαρροών ιδιωτικής ζωής λόγω της κατανεμημένης φύσης τους.

3.4.3 Εξόρυξη δεδομένων

Τα δεδομένα που συλλέγονται από τους παρόχουςΔΚΔ ή aggregators δεδομένων είναι μια σημαντική πηγή για την κοινωνική ανάλυση και το μάρκετινγκ, η οποία μπορεί να παρέχει χρήσιμες πληροφορίες για την εξέλιξη μιας κοινωνικής κοινότητας, τη συνεργατική επίλυση προβλημάτων, και ούτω καθεξής. Επιπλέον, μπορούν επίσης να χρησιμοποιηθούν για τη βελτιστοποίηση των υπηρεσιών ΔΚΔ και της προσαρμογής τους σε σχέση με τις προτιμήσεις και τα ενδιαφέροντα των χρηστών. Ωστόσο, ενδέχεται να προκύψουν πιθανές συγκρούσεις μεταξύ εξόρυξης κοινωνικών δεδομένων και των απαιτήσεων προστασίας της ιδιωτικής ζωής ΔΚΔ. Ένας αντίπαλος μπορεί να εισβάλλει στην ιδιωτική ζωή των χρηστών ΔΚΔ με τα δημοσιευμένα στοιχεία ΔΚΔ και κάποια γνώση του υποβάθρου. Ακόμη και μετά την απόκρυψη των ταυτοτήτων των χρηστών αντικαθιστώντας τα αντίστοιχα ονόματα χρήστη με τυχαία αναγνωριστικά (δηλαδή, ανωνυμοποίηση του κόμβου), έχει αποδειχθεί ότι, οι αντίπαλοιμπορούν να ανακτήσουν το μεγαλύτερο μέρος τωνταυτότητωντων χρηστών. Προφανώς, υπάρχει ένας συμβιβασμός ανάμεσα στην ποιότητα του αποτελέσματος της εξόρυξης δεδομένων και των απαιτήσεων προστασίας της ιδιωτικής ζωής των χρηστών ΔΚΔ.

3.4.4 Αρχιτεκτονικές client-server και P2P

Μια αρχιτεκτονική client-server παρουσιάζει αρκετά πλεονεκτήματα σε σχέση με την αρχιτεκτονική P2P στην εκπλήρωση των παραδοσιακώνστόχων τωνΔΚΔ. Για παράδειγμα, οι χρήστες ΔΚΔ δεν περιορίζονται στις αλληλεπιδράσεις με τους φίλους που έχουν ήδη, αλλά μπορούν να αποκαταστήσουν χαμένες κοινωνικές συνδέσεις, αν οι άνθρωποι αυτοί είναι, επίσης, μέλη στο ΔΚΔ. Όταν ένας χρήστης ψάχνει για παλιούς συμμαθητές σε ψηφιακό κοινωνικό χώρο με παγκόσμια έρευνα του ονόματος ή διάσχιση του κοινωνικού γραφήματος, μια κεντρική ιστοσελίδα μπορεί να προκαλέσει την έκθεση πιο εύκολα. Επίσης, οι χρήστες θέλουν να βρουν άλλους με παρόμοια ενδιαφέροντα, τοποθεσίες ή οργάνωση. Με την εξόρυξη δεδομένων, μπορούν να βρεθούν οι ομάδες συγγένειας. Η εξόρυξη δεδομένων είναι τόσο πιο αποδοτική και πιο αποτελεσματική σε ένα κεντρικό αποθετήριο. Ωστόσο, με την αρχιτεκτονική client-server τα πλήρη στοιχεία, άμεσα ή έμμεσα, που παρέχονται από όλους τους χρήστες, συλλέγονται και αποθηκεύονται μόνιμα στις βάσεις δεδομένων του παρόχουΔΚΔ, οι οποίες ενδεχομένως να γίνονται ένας μεγάλος αδελφός, ικανός να αξιοποιήσει αυτά τα δεδομένα με πολλούς τρόπους που μπορεί να παραβιάζουν τη προστασία της ιδιωτικής ζωής των μεμονωμένων χρηστών. Αυτά τα ιδιωτικά δεδομένα μπορούν επίσης να πέσουν υπό τον έλεγχο των χάκερ (Balduzzietal, 2010).

3.5 ΚΙΝΔΥΝΟΙ

3.5.1 Ζητήματα προστασίας προσωπικών δεδομένων

Τα ζητήματα που εμπίπτουν σε αυτή τη κατηγορία σχετίζονται κυρίως με την ανωνυμία και την ταυτότητα. Σε πολλούς δικτυακούς τόπους κοινωνικής δικτύωσης, οι χρήστες χρησιμοποιούν το πραγματικό τους όνομα για να εκπροσωπήσουν τους λογαριασμούς τους. Έτσι, η ταυτότητά τους εκτίθεται δημοσίως σε άλλους χρήστες κοινωνικών δικτύων, καθώς και όλους τους άλλους στον online κόσμο. Επίσης, ο λογαριασμός του χρήστη κοινωνικού δικτύου μπορεί να αναπροσαρμόζεται από μηχανή αναζήτησης και συνήθως εμφανίζεται στην κορυφή της κατάταξης των αποτελεσμάτων αναζήτησης. Σε αυτή την περίπτωση, αν οι επιτιθέμενοι γνωρίζουν το όνομα των θυμάτων, μπορούν εύκολα να ψάξουν το προφίλ του θύματος, ή μπορούν να το αναζητήσουν μέσα από ιστοσελίδες κοινωνικής δικτύωσης για να αποκτήσουν νέα θύματα. Εκτός από την απλή χρήση του πραγματικού του ονόματος ως το όνομα του λογαριασμού, υπάρχουν επίσης και άλλες τεχνικές που μπορούν να χρησιμοποιηθούν για να εκθέσουν την ανωνυμία του χρήστη κοινωνικού δικτύου. Οι δύο μέθοδοι που θα συζητηθούν είναι επίθεση αποανωνυμοποίησης και η γειτονική επίθεση (Gunatilaka, 2016).

3.5.1.1 Η επίθεση αποανωνυμοποίησης

Με τη χρήση της τεχνικής κλοπής των πληροφοριών μελών της ομάδας και του ιστορικού, οι επιτιθέμενοι θα μπορούσαν να αποκαλύψουν την ανωνυμία των χρηστών του κοινωνικού δικτύου.

Σε αυτήν την τεχνική, οι επιτιθέμενοι πρέπει να μάθουν σε ποια ομάδα του κοινωνικού δικτύου ανήκουν τα θύματα (ομάδα χρηστών που μοιράζεται κοινά ενδιαφέροντα ή ομάδα ανθρώπων με το ίδιο υπόβαθρο π.χ. πήγαν στο ίδιο σχολείο ή εργάζονται στο ίδιο μέρος). Η ομάδα του κοινωνικού δικτύου επικεντρώνεται δεδομένου ότι ο αριθμός των μεμονωμένων χρηστών ενός κοινωνικού δικτύου είναι πολύ μεγαλύτερος από τον αριθμό των ομάδων στα κοινωνικά δίκτυα. Ως εκ τούτου, είναι ευκολότερο να επικεντρωθούν πρώτα στην ομάδα, και στη συνέχεια να χρησιμοποιήσουν την ομάδα ώστε να αποκτήσουν πρόσβαση σε κάθε χρήστη. Οι επιτιθέμενοι θα χρησιμοποιήσουν τη μέθοδο της κλοπής ιστορικού για να μάθουν ποιες ποια URLs (ιστοσελίδες) έχουν επισκεφθεί τα θύματα στο παρελθόν με στόχο να μάθουν την ομάδα του θύματος.

Υπάρχουν δύο τύποι των συνδέσμων στην ιστοσελίδα κοινωνικής δικτύωσης. Μια στατική σύνδεση είναι η ίδια για όλους τους χρήστες των κοινωνικών δικτύων. Χρησιμοποιείται για την εμφάνιση της αρχικής σελίδας του χρήστη, καθώς και μια δυναμική σύνδεση που περιέχει κάποιες πληροφορίες μοναδικές για κάθε χρήστη ή κάθε ομάδα (Krishnamur&Willis, 2008).

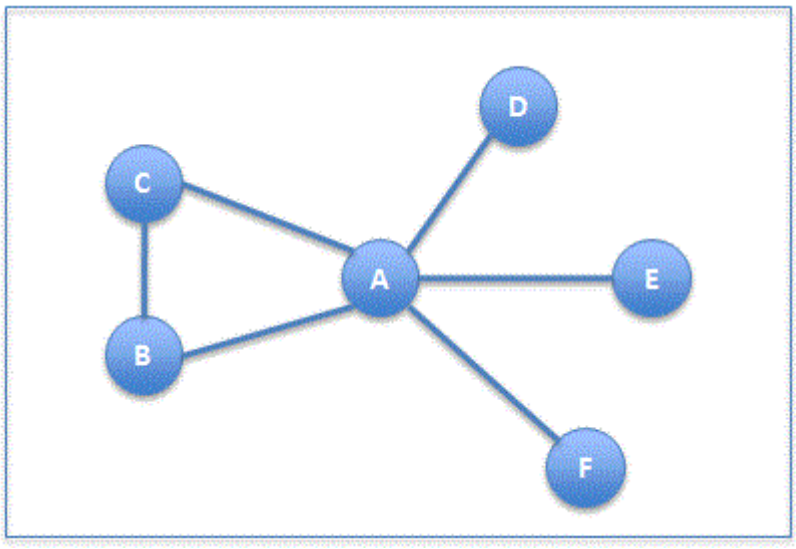
Στην κλοπή ιστορικού, οι επιτιθέμενοι παρασύρουν τους χρήστες στις ιστοσελίδες τους, και στη συνέχεια προσπαθούν να εξαγάγουν το ιστορικό περιήγησης του χρήστη στέλνοντας μία λίστα από URL, δηλαδή URL της ομάδας κοινωνικού δικτύου που οι χρήστες ενδεχομένως να είναι μέλη. Αυτές οι διευθύνσεις URL μπορούν να ληφθούν εύκολα μέσω του καταλόγου της ομάδας που παρέχεται από δικτυακούς τόπους κοινωνικής δικτύωσης. Στη συνέχεια, οι εισβολείς θα κάνουν το πρόγραμμα

περιήγησης του θύματος να ελέγξει αν μια διεύθυνση URL στη λίστα έχει δεχθεί επίσκεψη από το θύμα ή όχι κοιτάζοντας το ιστορικό περιήγησης των θυμάτων. Στη συνέχεια, οι πληροφορίες ιστορικού περιήγησης αποστέλλονται πίσω στους επιτιθέμενους. Η εξόρυξη του ιστορικού περιήγησης του χρήστη μπορεί να γίνει χρησιμοποιώντας τη λογική υπό όρους στο CSS (Cascading Style Sheet) ή με τη χρήση client-side script όπως το JavaScript (Huberetal, 2011).

Ως εκ τούτου, χρησιμοποιώντας τη κλοπή ιστορικού, οι επιτιθέμενοι μπορούν να αποκτήσουν το ιστορικό περιήγησης του θύματος, και στη συνέχεια να χρησιμοποιήσουν αυτήν τη λίστα για να φιλτράρουνι τις διευθύνσεις URL που σχετίζονται με τη δραστηριότητα του κοινωνικού δικτύου του θύματος, ιδιαίτερα τις δυναμικές συνδέσεις κοινωνικού δικτύου που περιέχουν κάποιο μοναδικές πληροφορίες σχετικά με τους χρήστες ή τις ομάδες. Σε γενικές γραμμές, πολλές ομάδες κοινωνικής δικτύωσης παρέχουν τη λίστα των μελών της ομάδας. Έτσι, οι επιτιθέμενοι μπορούν να χρησιμοποιούν τα ληφθέντα μηνύματα ηλεκτρονικού ταχυδρομείου για να ψάξουν τις ταυτότητας (προφίλ) των θυμάτων.

Γειτονική επίθεση

Τα κοινωνικά δίκτυα μπορούν να αναπαρασταθούν με κοινωνικό γράφημα, όπου ένας κόμβος αντιπροσωπεύει ένα χρήστη κοινωνικού δικτύου, και μια άκρη αντιπροσωπεύει τη σχέση μεταξύ δύο χρηστών κοινωνικών δικτύων. Η γειτονική επίθεση βασίζεται στην ιδέα ότι, αν οι επιτιθέμενοι γνωρίζουν τους γείτονες του κόμβουτων θυμάτων, καθώς και τη σχέση μεταξύ τους, τότε οι επιτιθέμενοι μπορούν να εντοπίσουν τον κόμβο του θύματος. Για παράδειγμα, αν ένας εισβολέας γνωρίζει ότι ο A έχει πέντε φίλους, δύο από τους φίλους του A (B, C) είναι φίλοι μεταξύ τους και οι άλλοι τρεις (D, E, F) δεν είναι φίλοι, η Εικόνα 3-2 παριστάνει το γειτονικό γράφημα του κόμβου A. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν αυτό το γράφημα για να προσδιορίσουν τον A, καθώς το γειτονικό γράφημα είναι μοναδικό για κάθε κόμβο στο κοινωνικό δίκτυο (Gunatilaka, 2016)..



Εικόνα 3-2 Γειτονικό γράφημα του κόμβου A (Gunatilaka, 2016).

3.5.1.2 Προφίλ χρήστη και προσωπικές πληροφορίες

Όπως και ο λογαριασμός του χρήστη, τα προφίλ χρηστών του κοινωνικού δικτύου περιέχουν κυρίως πραγματικές πληροφορίες σχετικά με τους χρήστες. Ευαίσθητες πληροφορίες, όπως το πλήρες όνομα του χρήστη, στοιχεία επικοινωνίας, την κατάσταση της σχέσης, την ημερομηνία γέννησης, την προηγούμενη και την τρέχουσα εργασία και το ιστορικό εκπαίδευσης, προσελκύουν τους επιτιθέμενους. Ως εκ τούτου, το κύριο θέμα του προφίλ χρήστη είναι η διαρροή του προφίλ και των προσωπικών πληροφοριών. Πηγές της διαρροής του προφίλ των χρηστών είναι οι εξής (Krishnamur&Willis, 2008):

Διαρροή πληροφοριών μέσω ελλιπών ρυθμίσεων απορρήτου: Οι περισσότεροι χρήστες των κοινωνικών δικτύων δεν είναι προσεκτικοί σχετικά με τις ρυθμίσεις απορρήτου τους. Πολλοί ανοίγουν το προφίλ τους στο κοινό, ώστε ο καθένας μπορεί να έχει πρόσβαση και να δει τις πληροφορίες τους. Επίσης, οι προεπιλεγμένες ρυθμίσεις προστασίας σε πολλές ιστοσελίδες κοινωνικής δικτύωσης δεν είναι ακόμη ασφαλείς, όπως το Facebook, όπου ένας φίλος ενός φίλου που ο χρήστης δεν γνωρίζει, μπορεί ακόμα να δει τις πληροφορίες του. Ωστόσο, ακόμη και με τις πιο ασφαλείς ρυθμίσεις για την προστασία της ιδιωτικής ζωής, εξακολουθούν να υπάρχουν αδυναμίες που επιτρέπουν στους επιτιθέμενους να έχουν πρόσβαση σε πληροφορίες του χρήστη.

Διαρροή πληροφοριών για εφαρμογές τρίτων: Πολλές ιστοσελίδες κοινωνικής δικτύωσης όπως το Facebook παρέχουν ένα API (Application Programming Interface) για εφαρμογές τρίτων, ώστε να δημιουργήσουν εφαρμογές που μπορούν να τρέχουν στην πλατφόρμα της. Αυτές οι εφαρμογές τρίτων είναι πολύ δημοφιλείς μεταξύ των χρηστών κοινωνικών δικτύων. Μόλις οι χρήστες προσθέτουν και επιτρέψουν στις εφαρμογές τρίτων την πρόσβαση στις πληροφορίες τους, αυτές οι εφαρμογές μπορούν να έχουν πρόσβαση στα δεδομένα του χρήστη αυτόματα. Είναι επίσης ικανές να δημοσιεύσουν στον χώρο του χρήστη ή σε χώρο φίλων του χρήστη, ή μπορούν να έχουν πρόσβαση σε πληροφορίες άλλου χρήστη εν αγνοία του χρήστη (Gunatilaka, 2016)..

Διαρροή πληροφοριών προς τρίτους: Πολλές ιστοσελίδες κοινωνικής δικτύωσης χρησιμοποιούν την υπηρεσία domaintρίτων, για να παρακολουθούν τις δραστηριότητες των χρηστών του κοινωνικού δικτύου, ή να επιτρέπουν στη διαφήμιση συνεργάτη την πρόσβαση και την συγκέντρωση δεδομένων των χρηστών του κοινωνικού δικτύου για εμπορικό όφελος (Krishnamur&Willis, 2008).

3.5.2 Υποκλοπή ταυτότητας

Η κλοπή ταυτότητας είναι μια πράξη κλοπής της ταυτότητας ή ευαίσθητων πληροφοριών κάποιου, και στη συνέχεια προσποίηση ότι είναι το πρόσωπο αυτό, ή

χρήση αυτής της ταυτότητας με κακόβουλο τρόπο. Τα κοινωνικά δίκτυα είναι καλοί στόχοι που προσελκύουν επιτιθέμενους αφού περιέχουν έναν τεράστιο αριθμό των διαθέσιμων πληροφοριών χρήστη. Μία τεχνική της κλοπής ταυτότητας είναι η κλωνοποίηση του προφίλ. Στην τεχνική αυτή, οι επιτιθέμενοι εκμεταλλεύονται την εμπιστοσύνη μεταξύ των φίλων, και ότι οι άνθρωποι δεν είναι προσεκτικοί όταν δέχονται αιτήματα φίλων. Το κοινωνικό phishing είναι μια άλλη μέθοδος που μπορεί να χρησιμοποιηθεί για να κλέψουν την ταυτότητά του χρήστη κοινωνικού δικτύου.

Κλωνοποίηση Προφίλ

Μια τεχνική για την κλοπή ταυτότητας ενός χρήστη κοινωνικού δικτύου ονομάζεται κλωνοποίηση προφίλ. Οι κύριοι στόχοι της κλωνοποίησης προφίλ είναι οι χρήστες που καθορίζουν το προφίλ τους να είναι δημόσιο. Το δημόσιο προφίλ επιτρέπει στους επιτιθέμενους να αποκτήσουν τις πληροφορίες του προφίλ εύκολα, και ως εκ τούτου μπορεί να αναπαραγάγουν ή να αντιγράψουν πληροφορίες του προφίλ τους για να δημιουργήσουν μια ψεύτικη ταυτότητα. Υπάρχουν δύο τύποι κλωνοποίησηςπροφίλ: η κλωνοποίηση υφιστάμενου προφίλ και η κλωνοποίηση προφίλ Cross-Site (Gunatilaka, 2016).

- Κλωνοποίηση Υφιστάμενου Προφίλ: Σε αυτή τη τεχνική, οι επιτιθέμενοι δημιουργούν ένα προφίλ των ήδη υπαρχόντων χρηστών χρησιμοποιώντας το όνομά τους, τα προσωπικά στοιχεία, καθώς και εικόνα για την αύξηση της εξάρτησης, και στη συνέχεια την αποστολή των αιτήσεων φιλίας σε φίλους του ίδιου του χρήστη. Αυτή η ενέργεια είναι επιτυχής δεδομένου ότι οι περισσότεροι χρήστες αποδέχονται αιτήματα φιλίας από το πρόσωπο που ξέρουν ήδη, χωρίς να κοιτάζουν μέσα στον χώρο του προσεκτικά. Επίσης, είναι πιθανό ότι ένα άτομο μπορεί να έχει πολλαπλούς λογαριασμούς. Αν το θύμα αποδεχθεί τα αιτήματα φίλων, στη συνέχεια, οι εισβολείς θα είναι σε θέση να έχουν πρόσβαση στις πληροφορίες του.

- Κλωνοποίηση Προφίλ Cross-Site: Σε αυτή τη τεχνική, οι εισβολείς κλέβουν το προφίλ του χρήστη από ένα site κοινωνικής δικτύωσης που οι χρήστες έχουν καταχωρήσει ένα λογαριασμό, και στη συνέχεια δημιουργούν το προφίλ ενός νέου χρήστη σε ένα άλλο site κοινωνικής δικτύωσης που ο χρήστης δεν έχει εγγραφεί στο παρελθόν. Μετά από αυτό, οι επιτιθέμενοι χρησιμοποιούν τη λίστα επαφών των χρηστών από το εγγεγραμμένο site κοινωνικής δικτύωσης για να στείλουν αιτήματα φιλίας σε όλες αυτές τις επαφές της λίστας φίλων σε ένα άλλο site κοινωνικής δικτύωσης. Σε αυτή την περίπτωση, είναι πιο πειστικοί από την πρώτη περίπτωση, δεδομένου ότι υπάρχει μόνο ένας λογαριασμός για το συγκεκριμένο χρήστη. Στη συνέχεια, αν οι επαφές δεχτούν το αίτημα φιλίας, οι επιτιθέμενοι μπορούν να έχουν πρόσβαση στο προφίλ τους.

Κοινωνικό Phishing

Στην επίθεση phishing, οι επιτιθέμενοι παρέχουν μια πλαστή ιστοσελίδα που μοιάζει αυθεντική για να δελεάσουν τα θύματα να παρέχουν ευαίσθητες πληροφορίες, όπως τον κωδικό πρόσβασης, οικονομικές πληροφορίες, ή τον αριθμό αναγνώρισης στον ιστότοπο. Η επίθεση Phishing μαζί με προσωπικές πληροφορίες από τα κοινωνικά δίκτυα κάνουν τις επιθέσεις να γίνονται όλο και πιο επιτυχημένες. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τη μέθοδο της κοινωνικής μηχανικής με τη συλλογή δεδομένων από τους χρήστες του κοινωνικού δικτύου και στη συνέχεια να εκτελέσουν την αυτοματοποιημένη εξαγωγή των δεδομένων για την απόκτηση πληροφοριών πλαισίου που είναι χρήσιμες για να ξεγελάσουν τους χρήστες στο site phishing. Για παράδειγμα, οι επιτιθέμενοι μπορούν να στείλουν μια ιστοσελίδα phishing στα θύματα χρησιμοποιώντας ονόματα φίλων του θύματος (Huberetal, 2011).

3.5.3 Διάδοση κακόβουλου λογισμικού

Το malware, ή αλλιώς κακόβουλο λογισμικό, είναι λογισμικό σχεδιασμένο για να βλάψει το σύστημα του υπολογιστή χωρίς συναίνεση ή τη γνώση του ιδιοκτήτη. Το λογισμικό θεωρείται ως κακόβουλο λογισμικό με βάση την αντίληψη της πρόθεσης του δημιουργού, και όχι με βάση τα ιδιαίτερα χαρακτηριστικά του. Ο κώδικας λογισμικό περιλαμβάνει ιούς, worms και ιούς trojan. Το malware θα αξιοποιήσει δημοφιλή εργαλεία επικοινωνίας, όπως τα worms μέσω e-mail και τα άμεσα μηνύματα, trojan από ιστοσελίδες μολυσμένες με ιό, τα αρχεία που μοιράζονται από peer to peer συνδέσεις. Το λογισμικό επιδιώκει να εκμεταλλευτεί τις υπάρχουσες ευπάθειεςστα συστήματα, δηλαδή τα προβλήματα στο λογισμικό των υπολογιστών που δημιουργούν αδυναμίες, κάνοντας την είσοδό του εύκολη και διακριτική.

Σύμφωνα με μια έκθεση που δημοσιεύθηκε από την Sophos, το 2010, το κακόβουλο λογισμικό είναι σε άνοδο σε κοινωνικά δίκτυα όπως το Facebook, Twitter, LinkedIn και το MySpace. Κατά το παρελθόν έτος, το 36% των χρηστών ανέφεραν για την αποστολή malware μέσω της ιστοσελίδας κοινωνικής δικτύωσης, μια αύξηση της τάξης του 70% από το προηγούμενο έτος. Η Sophos ερεύνησε πάνω από 500 επιχειρήσεις, και το 72% πιστεύει ότι τα κοινωνικά δίκτυα αποτελούν κίνδυνο για την εταιρεία. Εξήντα τοις εκατό των οργανισμών δήλωσε ότι το Facebook αποτελεί τον μεγαλύτερο κίνδυνο για την ασφάλεια, και ακολουθούν το MySpace, το Twitter και το LinkedIn.

Η διασπορά κακόβουλου λογισμικού, μέσω των κοινωνικών δικτύων αποτελεί κίνδυνο για την ασφάλεια στα χρηματοπιστωτικά ιδρύματα, για του εξής λόγους (Gunatilaka, 2016):

- Δυνητικά αυξανόμενες απειλές κακόβουλου λογισμικού επιτίθενται στις υποδομές και τα δεδομένα του οργάνου λόγω της χρήσης των κοινωνικών δικτύων από τους εργαζόμενους στην ιδιοκτησία της εταιρείας και μέσω συσκευών απομακρυσμένης πρόσβασης.

- Απειλή της εμπιστοσύνης των καταναλωτών στα μέτρα ασφαλείας του ιδρύματος και το χειρισμό των προσωπικών και οικονομικών πληροφοριών τους.

Δεδομένου ότι η κύρια έννοια των κοινωνικών δικτύων βασίζεται στη σχέση μεταξύ των χρηστών στα συστήματα, το κακόβουλο λογισμικό μπορεί εύκολα να μεταδοθεί μέσω αυτής της διασύνδεσης. Επιπλέον, πολλές ιστοσελίδες κοινωνικής δικτύωσης εξακολουθούν να στερούνται των μηχανισμών που καθορίζουν αν οι διευθύνσεις URL ή ενσωματωμένες συνδέσεις είναι κακόβουλες ή όχι. Ως εκ τούτου, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτό το ελάττωμα. Ένα κακόβουλο link μπορεί να ανακατευθύνει τα θύματα σε κακόβουλες ιστοσελίδες, και στη συνέχεια να στείλει κακόβουλο κώδικα στον υπολογιστή του θύματος για να κλέψει πληροφορίες, ή να χρησιμοποιήσει τον υπολογιστή του θύματος για να επιτεθεί σε άλλους.

Ψεύτικο προφίλ

Οι επιτιθέμενοι μπορούν να δημιουργήσουν ένα ψεύτικο προφίλ για να δελεάσουν άλλους χρήστες του κοινωνικού δικτύου ώστε να συνδεθούν μαζί τους και να δουν το προφίλ τους. Το ψεύτικο προφίλ μπορεί να είναι υπό τη μορφή του προφίλ μιας διασημότητας που προσελκύει τα θύματα στο να επικοινωνήσουν μαζί τους. Σε αυτή την περίπτωση, υπάρχουν πολλοί πιθανοί τρόποι με τους οποίους οι επιτιθέμενοι μπορεί να εξαπλώσουν malware στα θύματα. Ένας τρόπος είναι να δελεάσουν τα θύματα να κάνουν κλικ για να δουν τα προφίλ τους.

API κοινωνικών δικτύων

Οι εφαρμογές τρίτων μπορεί να είναι η πηγή της διαρροής πληροφοριών των χρηστών του κοινωνικού δικτύου. Σε αυτήν την περίπτωση, αυτές οι εφαρμογές είναι επίσης πιθανές πηγές malware δεδομένου ότι όλοι οι χρήστες μπορούν εύκολα να αποκτήσουν πρόσβαση στην εφαρμογή. Κατά την άποψη του χρήστη, οι εφαρμογές αυτές μπορεί να φαίνονται αυθεντικές, και φαίνεται να λειτουργούν όπως πρέπει, αλλά στο εσωτερικό θα μπορούσαν να κρύβουν ένα κακόβουλο link που παίρνει τους χρήστες σε κακόβουλες ιστοσελίδες, και εξαπλώνεται το κακόβουλο λογισμικό για τους χρήστες (Huberetal, 2011).

Drive-by επίθεση λήψης

Αυτό το είδος της επίθεσης χρησιμοποιεί τη διαφήμιση ως μέσο για τη διάδοση malware στα κοινωνικά δίκτυα. Είναι επίσης γνωστή ως κακόβουλες διαφημίσεις επίθεση. Οι επιτιθέμενοι δημοσιεύσετε κακόβουλο διαφήμιση στον τοίχο ή ένα μήνυμα του σκάφους χρήστη κοινωνικού δικτύου. Όταν οι χρήστες κάνουν κλικ σε διαφημίσεις, θα κατευθυνθούν προς τις κακόβουλες ιστοσελίδες που στη συνέχεια θα ζητήσει από τα θύματα να κατεβάσετε κακόβουλο κώδικα, όπως η Java ή ActiveX περιεχόμενο στο πρόγραμμα περιήγησής τους. Στη συνέχεια, οι υπολογιστές τους θα πάρουν μολυνθεί με κακόβουλο λογισμικό (Gunatilaka, 2016).

Σύντομοι και κρυφοί σύνδεσμοι

Η συντόμευση URL υπήρξε μια δημοφιλής μέθοδος που επιτρέπει στους ανθρώπους να μειώσουν το μέγεθος των διευθύνσεων URL τους, δεδομένου ότι πολλές διευθύνσεις URL είναι πολύ μεγάλες. Οι άνθρωποι μπορούν εύκολα να έχουν πρόσβαση σε αυτό το είδος της υπηρεσίας. Αυτό που έχουν να κάνουν είναι να υποβάλουν την αρχική διεύθυνση URL. Η υπηρεσία στη συνέχεια θα δημιουργήσει τη σύντομη εκδοχή του URL που θα ανακατευθύνει στην αρχική διεύθυνση URL όταν χρησιμοποιείται. Σύμφωνα με την έρευνα της Symantec για τα κακόβουλα σύντομα URLs σε ιστότοπους κοινωνικής δικτύωσης, «το 65% των κακόβουλων URLs για τα κοινωνικά δίκτυα έχουν σύντομες διευθύνσεις URL, και το 88% αυτών των διευθύνσεων URL χτυπήθηκαν από τους χρήστες του κοινωνικού δικτύου». Με τις σύντομες διευθύνσεις URL, οι χρήστες των κοινωνικών δικτύων δεν μπορούν να προσδιορίσουν την ιστοσελίδα προορισμού. Οι επιτιθέμενοι μπορούν να δημιουργήσουν δημοφιλείς ιστοσελίδες, και στη συνέχεια, αντί να χρησιμοποιούν την πραγματική σύνδεση, να χρησιμοποιούν τη ψεύτικη συντομευμένη διεύθυνση URL για να ξεγελάσουν τους χρήστες. Επιπλέον, βασίζονται στην εμπιστοσύνη μεταξύ των χρηστών σε κοινωνικά δίκτυα, οι χρήστες του κοινωνικού δικτύου εμπιστεύονται συνήθως το σύνδεσμο που έχει αναρτηθεί στον πίνακα μηνυμάτων του φίλου τους. Αυτό αυξάνει το click-through rate του κακόβουλου συνδέσμου (Balduzzietal, 2010).

Επίθεση Cross-Site Scripting

Το Cross-site scripting (XSS) είναι ένα από τα τρωτά σημεία της διαδικτυακής εφαρμογής που τρέχει σε ένα πρόγραμμα περιήγησης στο web. Το Cross-site scripting τροφοδοτεί το JavaScript στο πρόγραμμα περιήγησής του θύματος. Ένας εισβολέας μπορεί να γράψει δυναμικό κώδικα HTML για να κάνει το πρόγραμμα περιήγησης στο Web να στέλνει τα cookies του θύματος στο διακομιστή του εισβολέα.

Ο XSS Worm είναι ένας ιός που μπορεί να μεταδοθεί αυτόματα μεταξύ των χρηστών που έχουν πρόσβαση σε κακόβουλες ιστοσελίδες. Χρησιμοποιεί τον web browser για να εξαπλωθεί το κακόβουλο λογισμικό σε άλλους χρήστες και να κλέψει τα στοιχεία του χρήστη. Επειδή τα κοινωνικά δίκτυα βασίζονται στη συνδεσιμότητα μεταξύ των χρηστών, είναι μια καλή πλατφόρμα για την εξάπλωση του XSS Worm. Η διαδικασία της μόλυνσης έχει ως εξής: οι επιτιθέμενοι θα επιλέξουν τον κόμβο-πηγή, ο οποίος είναι ένας χρήστης του κοινωνικού δικτύου, που θα ξεκινήσει την εξάπλωση του κακόβουλου λογισμικού. Μόλις το αρχείο ο κόμβος-πηγή εισέλθει στην ιστοσελίδα κοινωνικής δικτύωσης, το κακόβουλο λογισμικό θα αναλάβει τον έλεγχο του προγράμματος περιήγησης και την εντολή για να εκτελέσει κάποιες εργασίες. Για παράδειγμα, οι επιτιθέμενοι μπορούν να λειτουργήσουν ως κάτοχος του λογαριασμού με την ταχυδρόμηση ή αποστολή μηνύματος σε άλλους χρήστες κοινωνικών δικτύων, να προσθέσουν εφαρμογές στο λογαριασμό του χρήστη, ή να κλέψουν τη λίστα επαφών. Στη συνέχεια ο κόμβος-πηγή θα εξαπλώσσει malware σε άλλους χρήστες κοινωνικών δικτύων που συνδέονται με αυτόν. Η μόλυνση θα εξαπλωθεί ως μια αλυσίδα από έναν κόμβο σε άλλους κόμβους (Gunatilaka, 2016).

Clickjacking

Το Clickjacking είναι μια τεχνική στην οποία εισβολείς ξεγελούν τα θύματα για να κάνουν κλικ σε ένα κουμπί ή ένα στοιχείο. Στη συνέχεια, ο κρυφός κωδικός θα ενεργοποιείται για να εκτελέσει κάποια κακόβουλη ενέργεια. Για παράδειγμα, υπάρχει το Facebook likejacking, όπου σε αυτή την περίπτωση οι χρήστες των κοινωνικών δικτύων, παρουσιάζονται με ένα video player που μοιάζει με βίντεο από το YouTube. Όταν κάνουν κλικ στο βίντεο, αντί να παίξει το βίντεο, ενεργοποιείται κουμπί Facebookliketου περιεχομένου. Ως εκ τούτου, οι χρήστες ξεγελάστηκαν για να κάνουν like στη σελίδα, έτσι ώστε η σελίδα να γίνει πιο δημοφιλής. Επιπλέον, ορισμένα από αυτά τα ψεύτικα βίντεο μπορεί να ωθήσουν τους χρήστες να εισάγουν κάποιες προσωπικές πληροφορίες πριν από την προβολή του βίντεο, έτσι ώστε οι επιτιθέμενοι να μπορούν να λάβουν περισσότερες πληροφορίες για το θύμα (Gunatilaka, 2016).

3.5.4 Κοινωνική μηχανική

Η κοινωνική μηχανική είναι μια συλλογή από τεχνικές που χρησιμοποιούνται για να χειραγωγήσουν τους ανθρώπους σε εκτέλεση ενεργειών ή αποκάλυψη εμπιστευτικών πληροφοριών, δηλαδή την μη εξουσιοδοτημένη απόκτηση ευαίσθητων πληροφοριών ή προνομίων ακατάλληλης πρόσβασης από μια πιθανή πηγή κινδύνου. Ο όρος ισχύει κατά κανόνα για την εκμετάλλευση της εμπιστοσύνης ή την κατασκευή μιας ακατάλληλης σχέσης εμπιστοσύνης με έναν νόμιμο χρήστη, τη δημιουργία ή την εκμετάλλευση της εμπιστοσύνης ή τη ματαιοδοξία ενός κακόβουλου χρήστη να συγκεντρώσει πληροφορίες ή να επηρεάσει τις ενέργειες του άλλου ατόμου ή οντότητας για τη συλλογή πληροφοριών ή την πρόσβαση στο σύστημα του υπολογιστή.

Ο στόχος της κοινωνικής μηχανικής είναι να ξεγελάσει κάποιον στην παροχή πληροφοριών που διαφορετικά δεν θα μοιραστεί ή δεν θα αποκαλύψει. Οι τεχνικές κοινωνικής μηχανικής που χρησιμοποιούνται συνήθως περιλαμβάνουν: pretexting Phishing ή SMiSHing Pharming Vishing ή Phishingμέσω τηλεφώνου.

3.5.5 Αποκάλυψη δεδομένων πνευματικής ιδιοκτησίας ή άλλων ευαίσθητων δεδομένων

Τα κοινωνικά δίκτυα και μέσα μαζικής ενημέρωσης σχετίζονται όλα με την κοινή χρήση πληροφοριών. Δυστυχώς, οι χρήστες των social media μπορούν να μοιραστούν με πρόθεση ή ακούσια πληροφορίες που θεωρούνται ευαίσθητες ή αποκλειστικές από την πλευρά των επιχειρήσεων (Balduzzietal, 2010).

Ο κίνδυνος αυτός συνεπάγεται τυχαία ή σκόπιμη αποκάλυψη των μυστικών της εταιρείας, στρατηγικών ή άλλων στοιχείων ενεργητικού και, ενδεχομένως, πληροφοριών κατοχυρωμένων με δίπλωμα ευρεσιτεχνίας μέσω ενός site κοινωνικής δικτύωσης, καθώς και ιδιωτικές πληροφορίες σχετικά με πελάτες ή άλλους εξωτερικούς χρήστες και ενδιαφερόμενα μέρη. Αυτό θα μπορούσε να περιλαμβάνει:

μυστικούς τύπους (όπως η πρόσφατη δημοσιότητα γύρω από τη συνταγή της Coca-Cola), στρατηγικές κώδικα προγραμματισμού για την εμπορία, την ανάπτυξη των επιχειρήσεων ή πληροφορίες εξαγορών πελάτη: αριθμοί πιστωτικών καρτών ή κοινωνικής ασφάλισης, ημερομηνιες γέννησης, διευθύνσεις, κλπ κάθε είδους αποκάλυψη που μπορεί να θέσει την εταιρεία σε μειονεκτική θέση στον ανταγωνισμό ή θα μπορούσε να εκθέσει τα άτομα σε κίνδυνο κλοπής ταυτότητας ή παραβίασης της ιδιωτικής ζωής. Τέτοιες καταστάσεις θέτουν μια εταιρεία σε κίνδυνο αστικής νομικής δράσης γύρω από την αποτυχία στην προστασία των δεδομένων αυτών, ρυθμιστικές κυρώσεις, ακόμα και απώλεια της φήμης.

3.5.6 Διαχείριση πρόσβασης

Με τόσα πολλά νομικά ζητήματα και απειλές για την ασφάλεια, που σχετίζονται με τη χρήση των κοινωνικών μέσων δικτύωσης, είναι σημαντικό ότι τα χρηματοπιστωτικά ιδρύματα διαχειρίζονται προσεκτικά την πρόσβαση των εργαζομένων σε ιστότοπους κοινωνικής δικτύωσης. Ο περιορισμός της πρόσβασης στα κοινωνικά μέσα δικτύωσης μόνο σε εκείνους τους εργαζόμενους που έχουν νόμιμη επιχειρηματική ανάγκη θα κάνει τον έλεγχο πολύ πιο εύκολο. Η πρακτική αυτή βοηθά στο να διασφαλιστεί ότι οι ιστότοποι κοινωνικής δικτύωσης χρησιμοποιούνται μόνο για τις επιχειρήσεις, και οι εργαζόμενοι με πρόσβαση είναι κατάλληλα εκπαιδευμένοι σε όλες τις πολιτικές για τα μέσα κοινωνικής δικτύωσης της εταιρείας. Αυτές οι πολιτικές εφαρμόζονται για την προστασία της εταιρείας από ανεπιθύμητους κινδύνους.

Ορισμένοι κίνδυνοι από την ανεξέλεγκτη πρόσβαση στα μέσα κοινωνικής δικτύωσης περιλαμβάνουν:

- Κίνδυνος δυσφήμισης.
- Κίνδυνος απάτης και ασφάλειας των πληροφοριών (social engineering και phishing που μπορεί να οδηγήσει σε δεδομένα στην κλοπή δεδομένων και ταυτότητας, επιθέσεις malware από hackers και spammers, και διαρροή των ιδιοκτησιακών και εμπιστευτικών πληροφοριών της εταιρείας).
- Η ευθύνη για τις αρνητικές δηλώσεις ενός εργαζομένου για ένα άλλο πρόσωπο ή ανταγωνιστή σε μια ιστοσελίδα ή blog.
- Αποκάλυψη εμπιστευτικών πληροφοριών, εμπορικών μυστικών ή παραβίαση πνευματικής ιδιοκτησίας από έναν υπάλληλο.
- Κατηγορίες για απάτη τίτλων που προκύπτουν από ψευδείς δηλώσεις σε υλικό δημοσιεύτηκε από τον υπάλληλο.
- Αγωγές κατά της γλώσσας που χρησιμοποιεί ο υπάλληλος ή της δραστηριότητας που είναι ενοχλητική, κάνει διακρίσεις, απειλητική ή υποτιμητική.
- Απώλεια της παραγωγικότητας των εργαζομένων. Οι εργαζόμενοι που έχουν πρόσβαση στο Facebook, το Twitter ή άλλους δικτυακούς τόπους κοινωνικής δικτύωσης κατά τη διάρκεια των ωρών γραφείου χάνουν περίπου δεκαπέντε λεπτά έως δύο ώρες κάθε μέρα. Αυτό οδηγεί σε μια πτώση σε επίπεδο της συνολικής παραγωγικότητας των εργαζομένων της τάξης του 1,5%. Μια έρευνα που ολοκληρώθηκε από Nucleus Research έδειξε ότι μόνο το 13% των εργαζομένων που αναφέρουν την πρόσβαση σε μέσα κοινωνικής δικτύωσης

κατά τη διάρκεια των ωρών εργασίας θα μπορούσαν να προσδιορίσουν εταιρικό στόχο και λόγο για τη πρόσβαση, με αποτέλεσμα να βγαίνει το συμπέρασμα ότι η πλειοψηφία των εργαζομένων έχει πρόσβαση για προσωπικούς λόγους.

3.5.7 Έλλειψη κεντρικής διακυβέρνησης

Με δεδομένη την μόνιμη, γρήγορη κίνηση και την καθολική φύση των κοινωνικών μέσων μαζικής ενημέρωσης, η κακή χρήση αυτών των εργαλείων, εκ προθέσεως ή όχι, μπορεί να οδηγήσει σε δυσφήμηση, οικονομική ή νομική βλάβη σε μια εταιρεία. Μια σαφής δομή διακυβέρνησης για την παρακολούθηση και το συντονισμό δραστηριότητας των μέσων κοινωνικής δικτύωσης, που επιτρέπει στους εργαζόμενους να συντονίσουν στενά τις δραστηριότητές τους στις επιχειρήσεις και να έχουν μια σαφή κατανόηση της δομής της διοίκησης και της λογοδοσίας, θα εξασφαλίσει τη συνέπεια των μηνυμάτων και τη διατήρηση της ασφάλειας των δεδομένων.

Η έλλειψη διακυβέρνησης θα μπορούσε να οδηγήσει σε μια σειρά από θέματα, όπως (Balduzzietal, 2010):

Φυσική ασφάλεια:

- Απώλεια δεδομένων
- Παραβίαση της ασφαλείας της τεχνολογίας

Φήμη και Μάρκα:

- Έλλειψη προτύπων πολιτικήςσε εταιρικό επίπεδο, της στρατηγικής και του περιεχομένου
- Ασυνεπής διαδικασία για την εξακρίβωση / έγκριση των αιτήσεων χρήσης των social media
- Ασυνεπή μηνύματα
- Σύγχυση σχετικά με τη διαδικασία και τη λογοδοσία, τόσο εσωτερικά όσο και εξωτερικά
- Ασυνεπής σχεδιασμός της κρίσης και των επικοινωνιών

Νομική / Συμμόρφωση:

- Κανονιστικές παραβιάσεις
- Αστικές αγωγές επί του περιεχομένου

Ανθρώπινο δυναμικό:

- Παραβίαση των κανονισμών εργασίας / νόμων
- Ανάγκη για πειθαρχικά μέτρα κατά των καταχρήσεων των εργαζομένων

3.5.8 Φυσικός κίνδυνος για την ασφάλεια των ατόμων

Εκτός από τις ηλεκτρονικές απειλές που ενδέχεται να συναντήσουν οι χρήστες των κοινωνικών δικτύων, η φυσική απειλή είναι ένα άλλο θέμα που πρέπει να αφορά τους χρήστες των κοινωνικών δικτύων. Φυσική απειλή είναι σωματική βλάβη σε πρόσωπο, ή στην ιδιοκτησία ενός ατόμου, όπως η κλοπή, καταδίωξη, εκβιασμός, ή σωματική παρενόχληση. Με τα χαρακτηριστικά και τις δυνατότητες που παρέχονται στις ιστοσελίδες κοινωνικής δικτύωσης, οι χρήστες του κοινωνικού δικτύου βρίσκονται σε κίνδυνο τέτοιων απειλών.

Το πρώτο χαρακτηριστικό είναι ότι η πραγματική ταυτότητα του χρήστη κοινωνικού δικτύου δεν είναι γνωστή. Ως εκ τούτου, ένας χρήστης δεν γνωρίζει πραγματικά με ποιον συνδέεται. Το δεύτερο είναι η προσωπική πληροφορία που έχει αναρτηθεί στις ιστοσελίδες κοινωνικής δικτύωσης που περιλαμβάνουν στοιχεία χρήστη επαφής, τα ενδιαφέροντα και οι συνήθειες. Αυτά επιτρέπουν στους εγκληματίες να μάθουν εύκολα για το πώς θα προσεγγίσουν τα θύματα τους. Επιπλέον, πολλά από τα προηγούμενα ζητήματα που αναφέρονται μπορεί επίσης να οδηγήσουν σε φυσικές απειλές. Για παράδειγμα, το κοινωνικό phishing μπορεί να επιτρέψει σε έναν εισβολέα να έχει φυσική πρόσβαση σε τραπεζικό λογαριασμό του θύματος, και να εκτελέσει κάποιες συναλλαγές. Τα θέματα προστασίας της ιδιωτικής ζωής είναι επίσης μια άλλη απειλή που μπορεί να οδηγήσει σε σωματική απειλή. Αν οι εγκληματίες μπορούν να έχουν πρόσβαση σε κάποιες ευαίσθητες πληροφορίες, όπως μια ευαίσθητη εικόνα ή ένα βίντεο, μπορούν να τα χρησιμοποιήσουν για να εκβιάσουν τα θύματα.

Επιπλέον, πολλές λειτουργίες κοινωνικής δικτύωσης επιτρέπουν στους εγκληματίες να είναι σε θέση να παρακολουθούν τη συμπεριφορά και τη θέση του θύματος. Για παράδειγμα, οι υπηρεσίες location-based για έξυπνα τηλέφωνα όπως το Google Latitude ή Foursquare, επιτρέπει στους χρήστες του κοινωνικού δικτύου να κάνουν check-in με την τρέχουσα θέση τους στο μήνυμα που δημοσιεύεται στον τοίχο τους. Επίσης, αν οι χρήστες των κοινωνικών δικτύων κάνουν χρήση της εφαρμογής κοινωνικής δικτύωσης για smart phones για να δημοσιεύσουν κάτι, θα αναρτηθεί από προεπιλογή και η θέση τους. Επιπλέον, ένα άλλο χαρακτηριστικό, όπως η γεωγραφική ετικέτα που επιτρέπει στους χρήστες να επισημάνουν τη θέση τους σχετικά με την εικόνα που δημοσιεύουν, μπορεί επίσης να εκθέσει την τοποθεσία του χρήστη, έτσι ένας εγκληματίας θα μάθει εύκολα που βρίσκονται τα θύματα του, και μπορεί να τα πλησιάσει (Gunatilaka, 2016)..

Ένα άλλο χαρακτηριστικό των κοινωνικών δικτύων που θα μπορούσε να βοηθήσει τους εγκληματίες να μάθουν για τα θύματα τους ευκολότερα, είναι το χρονοδιάγραμμα(timeline)του Facebook. Το χρονοδιάγραμμα του Facebook είναι ένα νέο χαρακτηριστικό που επιτρέπει στους χρήστες του Facebook να παρουσιάσουν το προφίλ τους με τρόπο που μοιάζει σε μια ιστορία. Το χρονοδιάγραμμα θα ενθαρρύνει τους χρήστες του Facebook να δημοσιεύσουν τις φωτογραφίες και τα βίντεο που αντιστοιχούν σε σημαντικά γεγονότα της ζωής τους. Ως εκ τούτου, οι επιτιθέμενοι μπορούν να μάθουν για τη ζωή του θύματος και παλαιότερες δραστηριότητες. Με αυτό το χαρακτηριστικό, ο εγκληματίας μπορεί να μάθει τις συνήθειες και τις δραστηριότητες των θυμάτων πιο εύκολα από ό, τι στο παρελθόν. Δεδομένου ότι οι πληροφορίες και παλαιότερες δραστηριότητες του θύματος είναι ήδη τοποθετημένες

με χρονολογική σειρά, οι εγκληματίες δεν πρέπει να καταβάλουν προσπάθεια για την εξεύρεση παλαιών πληροφοριών (Balduzzietal, 2010).

4 ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι ιστότοποι κοινωνικής δικτύωσης έχουν γίνει ένας πιθανός στόχος για τους επιτιθέμενους λόγω της διαθεσιμότητας των ευαίσθητων πληροφοριών, καθώς και των εκτενών βάσεων χρηστών. Ως εκ τούτου, τα ζητήματα προστασίας της ιδιωτικής ζωής και της ασφάλειας στα online κοινωνικά δίκτυα αυξάνονται. Αυτή η εργασία ανέλυσε διαφορετικά θέματα προστασίας της ιδιωτικής ζωής και της ασφάλειας, καθώς και τις τεχνικές που χρησιμοποιούν οι εισβολείς για να ξεπεραστούν οι μηχανισμοί ασφαλείας του κοινωνικού δικτύου, ή να επωφεληθούν από ορισμένες ατέλειες στο site κοινωνικής δικτύωσης.

Το ζήτημα της προστασίας της ιδιωτικής ζωής είναι μία από τις κύριες ανησυχίες, δεδομένου ότι πολλοί χρήστες των κοινωνικών δικτύων δεν είναι προσεκτικοί σχετικά με την απόκρυψη πληροφοριών στο διάστημα που συμμετέχουν στα μέσα κοινωνικής δικτύωσης. Το δεύτερο ζήτημα είναι η κλοπή ταυτότητας, οι επιτιθέμενοι κάνουν χρήση των λογαριασμών των κοινωνικών δικτύων για να κλέψουν την ταυτότητά του θύματος. Το τρίτο ζήτημα είναι το κακόβουλο λογισμικό καθώς οι επιτιθέμενοι χρησιμοποιούν τα κοινωνικά δίκτυα ως δίαυλο για τη διάδοση malware, δεδομένου ότι μπορεί να εξαπλωθεί πολύ γρήγορα μέσω της συνδεσιμότητας μεταξύ των χρηστών. Οι ιστότοποι κοινωνικής δικτύωσης αντιμετωπίζουν πάντα νέα είδη κακόβουλου λογισμικού. Τέλος, φυσικές απειλές, οι οποίες είναι οι πιο επιβλαβείς αναφέρθηκαν και αναλύθηκαν. Λόγω κάποιων από τα χαρακτηριστικά της κοινωνικής δικτύωσης, όπως η υπηρεσία με βάση την τοποθεσία, είναι πιο εύκολη η παρακολούθηση των θυμάτων από τους εγκληματίες.

Οι ιστότοποι κοινωνικής δικτύωσης προσπαθούν να εφαρμόσουν διαφορετικούς μηχανισμούς ασφαλείας για την πρόληψη τέτοιων ζητημάτων, καθώς και την προστασία των χρηστών τους, αλλά οι επιτιθέμενοι βρίσκουν πάντα νέες μεθόδους για να σπάσουν αυτές τις άμυνες. Ως εκ τούτου, οι χρήστες των κοινωνικών δικτύων θα πρέπει να είναι ενήμεροι για όλες αυτές τις απειλές, και να είναι πιο προσεκτικοί κατά τη χρήση τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

O'Reilly, T., 2005. What is Web 2.0. Design Patterns and Business Models for the Next Generation of Software.

Paquette, H. (2013). Social Media as a Marketing Tool: A Literature Review. http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1001&context=tmd_major_papers

Sambhanthan, A., & Good, A. (2013). Strategic advantage in web tourism promotion: an e-commerce strategy for developing countries. arXiv preprint arXiv:1302.5195.

Oxford Dictionary, (2016) Web 2.0 definition. Online: http://www.oxforddictionaries.com/definition/english/web-2.0 [Retrieved February 29, 2016]

BITS (2011). Social media risks and mitigation.Division of the Financial Services Roundtable.

Haenlein, M., & Kaplan, A. M. (2009). Flagship brand stores withinvirtual worlds: The impact of virtual store exposure on real lifebrand attitudes and purchase intent. Rechercheet Applicationsen Marketing 24(3).

Haenlein, M., & Kaplan, A. M. (2010). Users of the world, unite! The challenges andopportunities of Social Media. Business Horizons (2010) 53, 59—68.

Heinonen, K. (2011). "Consumer activity in social media: Managerial approaches to consumers' social media behavior." Journal of Consumer Behavior 10: 356-364.

Huang et al. (2013). Attitude Toward the Viral Ad: Expanding Traditional Advertising Models to

Erdogmus and Cicek (2012). The impact of social media marketing on brand loyalty.Procedia - Social and Behavioral Sciences 58 (2012) 1353 – 1360

Chu, S. (2011). "Viral advertising in social media: Participation in Facebook groups and responses among college-aged users." Journal of Interactive Advertising 12: 30-43.

Kietzmann, J.H., Hermkens, K., McCarthy, I.P. and Silvestre, B.S. (2011), "Social media? Get serious! Understanding the functional building blocks of social media", Business Horizons, Vol. 54 No. 3, pp. 241-251.

Schau, H. J., &Gilly, M. C. (2003). We are what we post? Self-presentation in personal web space. Journal of Consumer Research, 30(3), 385—404.

Warf, B. (2013) Global Geographies of the Internet, Springer Briefs in Geography, DOI: 10.1007/978-94-007-1245-4_2

Brandtzæg, P., Heim, J., &Karahasanovic, A. (2011). Understanding the new digital divide—A typology of internet users in Europe. International Journal of Human-Computer Studies,69(3), 123–138.

EPC, (2015). Global Social Media Trends. Part of the EPC global media trends book series. European Publishers Council.

Kende, M. (2012). How the Internet continues to sustain growth and innovation. Report for the Internet Society. Ref: 35128-362

Jin, L., Chen, Y., Wnag, T. and Hui, P. (2013). Understanding User Behavior inOnline Social Networks: A Survey. IEEE Communications Magazine.

Wilson C. et al., (2009). User Interactions in Social Networks and Their Implications.Proc. EuroSys.

Jiang J. et al., (2010). Understanding Latent Interactions inOnline Social Networks. Proc. IMC.

Dunn C. W. et al., (2012). Navigation Characteristics of OnlineSocial Networks and Search Engines Users.Proc.WOSN.

ΕΜΠ, (2011). (Κοινωνικάδίκτυα &ΑνάλυσηΚοινωνικώνΔικτύων(Social Networking & Social Network Analysis). ΣημειώσειΕΜΠ, http://imu.ntua.gr/static/courses/strategicISmanagement/lectures/11-Social%20Networks.pdf

Gunatilaka, D. (2016). A Survey of Privacy and Security Issues in Social Networks. Washington University in St. Lewis.

Balduzzi, M. Platzer, C. Holz, T. Kirda, E. Balzarotti, D. and Kruegel C. (2010).AbusingSocial Networks for Automated User Profiling. Symposium on Recent Advances inIntrusion Detection (RAID), 6307, 422-441.

Krishnamurthy B., Wills, C. (2008). Characterizing Privacy in OnlineSocial Networks," WOSN '08 Proceedings of the first workshop on Online socialnetworks. 37-42.

Huber, M. Mulazzani, M. Weippl, E. Kitzler, G. and Goluch, S. (2011). Friend-in-the-MiddleAttacks: Exploiting Social Networking Sites for Spam.Internet Computing, IEEE,15(3), 28-34.

Zhang, C., Sun, J. (2010). Privacy and Security for Online SocialNetworks: Challenges and Opportunities. IEEE Network, July/August 2010

Boyd D. M. and Ellison N. B. (2007). Social Network Sites: Definition, History, andScholarship," J. Comp.-Mediated Commun., 13(1), 210–30.

Carminati, B. Ferrari, E. and Perego, A. (2009). Enforcing Access Control in Web-Based Social Networks. ACM Trans. Info. Sys. Security, 13(1), 1–38.

Kim, M. &Leskovec, J. (2011). Modeling Social Networks with Node Attributes using theMultiplicative Attribute Graph Model. Stanford University

A. Abraham (ed.), Computational Social Networks: Mining and Visualization,DOI 10.1007/978-1-4471-4054-2 1, Springer-Verlag London 2012