Πανεπιστήμιο Πειραιώς

Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

ΠΡΟΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

«Ψηφιακών Συστημάτων»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΤΙΤΛΟ:

« ΜΗΧΑΝΗ ΑΝΑΖΗΤΗΣΗΣ GOOGLE ΚΑΙ ΟΙ ΕΠΙΘΕΣΕΙΣ ΠΟΥ ΕΧΕΙ ΔΕΧΤΕΙ»

ΟΝΟΜΑ :ΚΑΡΑΤΖΑ ΕΛΕΥΘΕΡΙΑ

Α.Μ. Ε/06064

ΔΙΔΑΣΚΩΝ:ΞΕΝΑΚΗΣ Χ.

Πειραιάς 2011

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Μιλώντας κάποιος για «*πληροφοριακό πόλεμο*», "*εννοεί τις επιθετικές και αμυντικές επιχειρήσεις οι οποίες μπορούν να στρέφονται εναντίον των πηγών πληροφοριών και που χαρακτηρίζονται ως τύπου «νίκης-ήττας»*[1]. Ένας από τους λόγους για τους οποίους διεξάγεται ο συγκεκριμένος πόλεμος, συμβαίνει λόγω του γεγονότος ότι οι πηγές αυτές των πληροφοριών παρουσιάζουν ιδιαίτερη σημασία για τους απλούς ανθρώπους και στελέχη των επιχειρήσεων στις μέρες μας.

Σε κάθε φαινόμενο «πληροφοριακού πολέμου» εντοπίζονται τρία βασικά στοιχεία, όπου αυτά είναι οι πηγές των πληροφοριών, οι επιθετικές και αμυντικές επιχειρήσεις αλλά και ο ανθρώπινος παράγοντας ο οποίος εμπλέκεται σε αυτές τις επιχειρήσεις[2]. Είναι γεγονός πως ο «*πληροφοριακός πόλεμος*» σχετίζεται άμεσα με τις επιχειρήσεις και εταιρείες εκείνες, οι οποίες αποσκοπούν στην πλήρη εκμετάλλευση των πηγών των πληροφοριών. Οι πηγές αυτές μπορούν να κατηγοριοποιηθούν σε πέντε βασικές κατηγορίες ως ακολούθως :

- *Φορείς πληροφοριών*
- *Μεταφορείς πληροφοριών*
- *Αισθητήρες πληροφοριών*
- *Καταγραφείς πληροφοριών*
- *Διεκπεραιωτές πληροφοριών*

Οι κατηγορίες αυτές που αναφέρονται παραπάνω δεν σημαίνει ότι ακολουθούν πάντα την συγκεκριμένη αυτή σειρά, καθώς κάθε μια από αυτές μπορεί να επιτελεί περισσότερες από μια λειτουργία. Επιχειρώντας να γίνει μια ανάλυση στις πέντε αυτές κατηγορίες πηγών, θα μπορούσαν να αναφερθούν τα εξής. Οι φορείς πληροφοριών είναι τα μέσα εκείνα τα οποία κατέχουν τις όποιες πληροφορίες. Κάθε αντικείμενο μπορεί να χαρακτηριστεί ως κάτοχος πληροφοριών. Στα αντικείμενα αυτά μπορούν να συμπεριλαμβάνονται η μνήμη των ανθρώπων, κάθε γραπτό μέσο, οι δίσκοι και οι χώροι αποθήκευσης των υπολογιστών, η μνήμη που διαθέτουν καθώς και όποια πληροφορία βρίσκεται αποθηκευμένη σε αυτούς[3].

Οι μεταφορείς πληροφοριών χαρακτηρίζονται ως συστήματα και αντικείμενα επικοινωνιών, τα οποία έχουν την ικανότητα να διακινούν ή να διαβιβάζουν πληροφορίες από ένα συγκεκριμένο

[1] Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA.

[2] Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA.

[3] Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA.

μέρος σε κάποιο άλλο. Στα συστήματα αυτά συμπεριλαμβάνονται τα άτομα τα οποία μεταφέρουν τις πληροφορίες, τα διάφορα οχήματα και γενικά τα μέσα μεταφοράς καθώς και τα διάφορα μέσα μαζικής επικοινωνίας. Σχετικά με τους αισθητήρες πληροφοριών, θα μπορούσε να ειπωθεί πως αυτές είναι συσκευές οι οποίες συλλέγουν πληροφορίες από άλλα αντικείμενα, αλλά και από το περιβάλλον στο οποίο βρίσκονται. Στην κατηγορία αυτή ανήκουν οι ανθρώπινες αισθήσεις, τα scanners, τα ραντάρ και οι φωτογραφικές μηχανές.

Τέλος, ως καταγραφείς των πληροφοριών χαρακτηρίζονται οι συσκευές εκείνες οι οποίες τοποθετούν κάποιες πληροφορίες στους φορείς. Σε αυτές συγκαταλέγονται οι ανθρώπινες ενέργειες, οι οδηγοί δισκετών καθώς και οι εκτυπωτές. Οι αισθητήρες είναι εκείνοι οι οποίοι συλλέγουν τις πληροφορίες από το ευρύτερο περιβάλλον, αυτές κατόπιν εισέρχονται στον υπολογιστή, εκτυπώνονται και μεταβιβάζονται από τα διάφορα τηλεπικοινωνιακά μέσα. Η αλληλοσύνδεση αυτή που υπάρχει, μπορεί να τροφοδοτεί κατάλληλα με πληροφορίες τις επιχειρήσεις του «πληροφοριακού πολέμου»[4].

Στην διαδικασία αυτή, εμπλέκεται επίσης και ο όρος «*πληροφοριακή υποδομή*» ο οποίος αναφέρεται σε εκείνες τις πηγές πληροφοριών όπου και εσωκλείονται και τα συστήματα επικοινωνιών. Τα συστήματα αυτά μπορούν να υποστηρίζουν κατάλληλα μια βιομηχανία ή και ένα διεθνές οργανισμό. Χαρακτηριστικό παράδειγμα αποτελεί η πληροφοριακή υποδομή που αποκτούν οργανισμοί και επιχειρήσεις, καθώς και κρατικοί φορείς. Ο χώρος της πληροφορικής αναφέρεται στο σύνολο του στις διάφορες πηγές πληροφοριών και οι οποίες μπορούν να είναι προσιτές σε μια ευρύτερη οντότητα.

Η οντότητα αυτή μπορεί να περιλαμβάνει τα συστήματα των υπολογιστών, τα έγγραφα, τα συστήματα επικοινωνιών αλλά και τις κωδικοποιημένες πληροφορίες. Ως παράδειγμα στην περίπτωση αυτή, μπορεί να αναφερθεί ο χώρος του ίντερνετ ο οποίος περιλαμβάνει ένα μεγάλο σύνολο δικτύων αλλά και ηλεκτρονικών υπολογιστών και ο οποίος καθημερινά δέχεται ένα μεγάλο αριθμό επιθέσεων και ανεπιθύμητων ενεργειών συκοφαντίας και δημιουργίας προβλημάτων ως προς τη λειτουργία των συγκεκριμένων διαδικτυακών καναλιών.

[4] Libicki, G., M., 1995, *"What information is warfare?"*, National Defense University of USA.

Κεφάλαιο 1ο

Η Έννοια της Κρυπτογραφίας και η Προστασία των Πληροφοριών

1.1 *Η Έννοια της Κρυπτογραφίας*

Η κρυπτογραφία αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδόμενων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη ή παραλήπτες. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους[5].

Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε hardware λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου[6].

Η λογισμική κρυπτογραφία είναι φτηνότερη, γεγονός που την κάνει άμεσα αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια, δεν είναι το ίδιο γρήγορη με την εκτέλεση της σε hardware, αλλά η ολοένα αυξανόμενη ανάγκη για διασφάλιση των επικοινωνιών εδραίωσε την χρήση της. Στις ακόλουθες σελίδες θα συζητήσουμε αποκλειστικά για την λογισμική κρυπτογραφία.

Στεγανογραφία είναι η τεχνική της απόκρυψης της ίδιας της ύπαρξης της πληροφορίας. Όπως για την κρυπτογραφία, έτσι και για την στεγανογραφία υπάρχουν δύο τρόποι υλοποίησης της: σε hardware και σε software. Η hardware εκτέλεση της είναι γρήγορη, αλλά πάρα πολύ ακριβή. Χρησιμοποιείται περισσότερο από κυβερνητικές υπηρεσίες και από τον στρατό, καθ' ότι οι τεχνολογίες που χρησιμοποιούνται είναι πολύ ανεπτυγμένες και καθόλου διαδεδομένες. Η εκτέλεση της σε software είναι πιο φθηνή και οι τεχνολογίες που απαιτούνται είναι σαφώς πιο εμπορικές. Στο διαδίκτυο συναντάτε η λογισμική στεγανογραφία για ευνόητους λόγους[7].

Ουσιαστικά κρυπτογραφία *(cryptography)* είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα τον οποίων η λύση είναι δύσκολο να βρεθεί. Κρυπτανάλυση

[5] Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley.

[6] Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley.

[7] Kotler P., 2000, "*Research Methods*", Prentice Hall.

(cryptanalysis) είναι η επίλυση αυτών των προβλημάτων και κρυπτολογία *(cryptology)* είναι ο συνδυασμός της κρυπτογραφίας και της κρυπτολογίας σε ένα ενιαίο επιστημονικό κλάδο[8].

Η εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά[9].

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, την χρήση κάποιας μυστικής πληροφορίας, με άλλα λόγια, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται αλλάζουν. Στις μέρες μας η κρυπτογραφία δεν αφορά μόνο το κομμάτι της κρυπτογράφησης και της αποκρυπτογράφησης. Εκτός από την διασφάλιση του απόρρητου *(privacy)*, η πιστοποίηση ταυτότητας *(authentication)* είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας[10].

Πιστοποιούμε την ταυτότητα μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας[11].

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουροι για το ποιος το έχει γράψει. Επίσης, μια ψηφιακή χρονοσφραγίδα *(digital timestamp)* συνδέει ένα έγγραφο με την ώρα της δημιουργίας του. Τέτοιο μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του διαδικτύου ή ακόμα και για τη σύνδεση με καλωδιακή τηλεόραση.

[8] Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley.

[9] Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley.

[10] Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley.

[11] Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley.

1.2 *Είδη Κρυπτογραφίας*

1.2.1 *Ασύμμετρη Κρυπτογραφία (Public-Key Cryptography)*

Η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα δεν γνωστοποιείται. Η ιδιωτική κλείδα δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα[12]. Η ανάγκη του αποστολέα και του παραλήπτη να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί μ' αυτό και πολλά προβλήματα που θα δούμε παρακάτω.

Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β.

Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Οποιοσδήποτε είναι σε θέση να "ακούσει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Όποιος έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνος που γνωρίζει την ιδιωτική κλείδα. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα[13].

Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό

[12] Kotler P., 2000, "*Research Methods*", Prentice Hall.

[13] Kotler P., 2000, "*Research Methods*", Prentice Hall.

χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Σε αντίθετη περίπτωση η υπογραφή θεωρείται πλαστή ή ότι το μήνυμα έχει τροποποιηθεί[14].

1.2.2 *Συμμετρική Κρυπτογραφία*

Στην συνηθισμένη κρυπτογραφία, ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να κάνει ακριβώς το ίδιο. Αυτή η μέθοδος καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η *Message Authentication Code (MAC)*[15].

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

1.3 *Μειονεκτήματα και Πλεονεκτήματα της Συμμετρικής και Ασύμμετρης Κρυπτογραφίας*

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η **συνεννόηση και ανταλλαγή του κλειδιού**, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσο του διαδικτύου δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί.

Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους[16]. Η

[14] Kotler P., 2000, "*Research Methods*", Prentice Hall.

[15] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

[16] Kotler P., 2000, "*Research Methods*", Prentice Hall.

πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί έχει κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη της.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι γρηγορότερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής ***(non-repudiation)***. Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς ***(Certificate Authority)*** ώστε να διασφαλίζεται η κατοχή στους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη[17].

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλοντα κλειστά, που δεν έχουν σύνδεση με το διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι. Μέχρι τώρα αναφερθήκαμε στα δύο σημαντικότερα κρυπτοσυστήματα που ευρέως εφαρμόζονται σήμερα. Περιγράψαμε τις αρχές που τα διέπουν και το είδος των κλειδιών που χρησιμοποιούν (συμμετρικά ή ασύμμετρα).

1.4 *Τρόποι Άμυνας για τις Μεθόδους «Πληροφοριακού Πολέμου» για Επιχειρήσεις*

Οι τρόποι άμυνας και πρόληψης που χρησιμοποιούνται συνήθως από τις επιχειρήσεις για τις παραπάνω κατηγορίες «*πληροφοριακού πολέμου*», αναφέρονται στις παρακάτω εξής περιπτώσεις :

---

[17] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

- *Πρόληψη*
- *Αποτροπή*
- *Ενδείξεις και προμηνύματα*
- *Ανακάλυψη*
- *Προετοιμασία για επείγοντα περιστατικά*
- *Απάντηση*

Οι συγκεκριμένες κατηγορίες είναι αλληλένδετες μεταξύ τους και ορισμένοι από τους μηχανισμούς χρησιμοποιούνται σε περισσότερες από μια κατηγορίες. Εξαίρεση αποτελεί η περίπτωση όπου εντοπίζονται τα περισσότερα έξοδα και τα οποία επιβάλλονται για την λήψη των κατάλληλων και απαιτούμενων μέτρων. Φυσικά δύναται να υπάρξουν περισσότερα έξοδα και τα οποία είναι λίγο δύσκολο να προσδιοριστούν αναλόγως.

Ο πρώτος τρόπος αντιμετώπισης των μεθόδων «πληροφοριακού πολέμου», είναι εκείνος της Πρόληψης. Ο συγκεκριμένος τρόπος αποβλέπει στην αποφυγή μιας εκδήλωσης επίθεσης η οποία αιωρείται ουσιαστικά στον επιτιθέμενο μια πρόσβαση στην πηγή των πληροφοριών. Ο μηχανισμός που εμπλέκεται σε αυτόν τον τρόπο άμυνας, περιλαμβάνει την απόκρυψη σημαντικών πληροφοριών, τον έλεγχο εισόδου από τους χρήστες αλλά και την πιστοποίηση τους. Ουσιαστικά, η απόκρυψη των πηγών πληροφοριών στοχεύει στην κοινολόγηση των πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα[18]. Οι σχετικοί αυτοί μηχανισμοί εσωκλείουν συστήματα ασφαλείας και διαχωρισμούς των πληροφοριών. Η πιστοποίηση που απαιτείται, έχει ως στόχο την διαπίστωση της ταυτότητας των χρηστών μέσω της χρήσης κωδικών πρόσβασης και επαλήθευσης.

Ο δεύτερος τρόπος αντιμετώπισης, είναι εκείνος που αναφέρεται στην Αποτροπή. Η συγκεκριμένη μέθοδος στοχεύει στην τοποθέτηση αντιμετώπισης μιας μη ελκυστικής επίθεσης για ανάκτηση πηγών πληροφοριών. Στην κατηγορία αυτή εσωκλείονται οι νόμοι, οι ποινές που επέρχονται από αυτούς αλλά και οι αποζημιώσεις που μπορούν να προκύψουν. Ο έλεγχος ασφαλείας που μπορεί να λάβει χώρα σε αυτή την περίπτωση, διεξάγεται προληπτικά αφού ένας πιθανός επιτιθέμενος μπορεί να διαπιστώσει πως ενδεχομένως δεν χρειάζεται να εισχωρήσει σε κάποιο σύστημα και να κινδυνέψει για αυτό, αφού οι πληροφορίες που θα ανακτήσει ίσως να μην είναι αρκετά σημαντικές. Βέβαια, κάθε στοιχειώδης έλεγχος που θα διεξαχθεί, το μόνο που θα προσφέρει είναι βοήθεια και πρόληψη ενάντια στις μεθόδους «πληροφοριακού πολέμου».

Ο τρίτος τρόπος αντιμετώπισης τέτοιων φαινομένων, είναι οι Ενδείξεις και τα Προμηνύματα. Ο τρόπος αυτός λειτουργεί ως εργαλείο αναγνώρισης μιας επίθεσης από έναν απρόσμενο και ανεπιθύμητο παράγοντα. Μέσω αυτού του εργαλείου, μπορούν να παρθούν συγκεκριμένα μέτρα και

[18] Pfleeger, C., P., 1997.

νόμοι προκειμένου να αποτραπεί ή να καταστεί αδύνατη η επίθεση από αυτούς τους ανεπιθύμητους παράγοντες. Συνήθως οι κυβερνήσεις είναι αυτές που εφαρμόζουν τα μέτρα αυτά και ζητούν πληροφορίες από επιχειρήσεις και οργανισμούς που παρακολουθούν τέτοιου είδους επιθέσεις.

Ο τέταρτος τρόπος αντιμετώπισης, είναι εκείνος Ανακάλυψης. Η ανακάλυψη έχει και εκείνη σχεδόν τον ίδιο σκοπό με τις Ενδείξεις και τα Προμηνύματα και την στενή παρακολούθηση μιας επίθεσης μετά την έναρξη της. Τα εργαλεία που χρησιμοποιούνται σε αυτό τον τρόπο αντιμετώπισης, έχουν την ικανότητα να λειτουργούν μεθόδους, οι οποίες μπορούν να εντοπίζουν επιβλαβείς ή ψευδείς πληροφορίες και εν συνεχεία να επεξεργάζονται τις εισερχόμενες πληροφορίες[19]. Οι μηχανισμοί αυτοί, περιλαμβάνουν επίσης κάποιες κρυφές κάμερες προστασίας αλλά και συστήματα ασφαλείας τα οποία χρησιμοποιούνται σε ηλεκτρονικούς υπολογιστές για τον εντοπισμό καταστρεπτικών ιών και βλαβερών ουσιών μέσα σε αυτούς.

Η πέμπτη κατηγορία αντιμετώπισης των μεθόδων «πληροφοριακού πολέμου», είναι αυτή της Προετοιμασίας για επείγοντα περιστατικά. Ο τρόπος αυτός σχετίζεται άμεσα με την δυνατότητα ενός συστήματος για ανάκαμψη μετά την επίθεση που θα δεχθεί αλλά και την απάντηση του σε αυτό. Στην κατηγορία αυτή συγκαταλέγονται και η λήψη των αντιγράφων αλλά και η διόρθωση μιας βλάβης μετά από μια ισχυρή επίθεση. "Με αυτόν τον τρόπο όμως δεν θεωρείται πιθανή η πρόβλεψη ή η πρόληψη κάθε επίθεσης. Ο αμυντικός «πληροφοριακός πόλεμος» σχετίζεται άμεσα με την σωστή διαχείριση των κινδύνων αλλά όχι με την αποφυγή τους, σε οποιοδήποτε κόστος κάτι τέτοιο θα είναι αποδεκτό[20].

1.5 *Μορφές και Ενέργειες Επιθετικού «Πληροφοριακού Πολέμου»*

Σε ορισμένες χώρες ανά τον κόσμο, η πρόσβαση σε έναν ηλεκτρονικό υπολογιστή θεωρείται παράνομη. Όλες οι πληροφορίες οι οποίες βρίσκονται αποθηκευμένες στον υπολογιστή αυτό ή στον σκληρό του δίσκο, δεν μπορούν να χρησιμοποιηθούν από άτομα τα οποία δεν διαθέτουν την κατάλληλη εξουσιοδότηση. Στην περίπτωση όπου κάποιος αναφέρεται στον επιθετικό «πληροφοριακό πόλεμο», γίνεται λόγος για τις εισβολές σε ηλεκτρονικούς υπολογιστές αλλά και στις ενέργειες στις οποίες επιδίδονται οι διάφοροι «χάκερς» και εισβολείς συστημάτων[21].

Οι συγκεκριμένες αυτές πράξεις αποτελούν αντικείμενο κλοπής και απάτης, αφού αυτές εκτελούνται με την μορφή «υπερκείμενης απάτης» και διεξάγονται εις βάρος του πραγματικού

[19] Pfleeger, C., P., 1997.

[20] Kesler, R., 1988.

[21] Adams, J., 1998.

χρήστη του ηλεκτρονικού υπολογιστή. Φυσικά οι απώλειες οι οποίες μπορούν να προκύψουν, ίσως είναι δραματικές αφού σημαντικά δεδομένα μπορούν να διαγραφούν ή να υποκλαπούν.

Η συνήθης μέθοδος η οποία ακολουθείται σε αυτές τις περιπτώσεις, θεωρείται απλή και ιδιαιτέρως κατανοητή από τους διάφορους «χάκερς». Μέσω της χρησιμοποίησης ενός λογαριασμού πρόσβασης, ο κάθε εισβολέας ή υποκλοπέας μπορεί να προβεί σε ενέργειες οι οποίες θα τον καταστήσουν ικανό να αποκτήσει πρόσβαση σε συγκεκριμένα και σημαντικά δεδομένα. Η πρόσβαση που θα αποκτήσει ένας μη εξουσιοδοτημένος σε κάποιον υπολογιστή, μπορεί να του επιτρέψει την ανάγνωση πληροφοριών, καταστροφή διαφόρων αρχείων, επεξεργασία ηλεκτρονικών μηνυμάτων αλλά και καταγραφή αξιόπιστων πηγών για μια επιχείρηση ή κυβερνητικό οργανισμό.

Οι ζημιές βέβαια που μπορούν να προκύψουν, εξαρτώνται κάθε φορά από την πρόσβαση αλλά και τις ενέργειες στις οποίες μπορεί να προβεί ο μη εξουσιοδοτημένος χρήστης. Για το λόγο αυτό πολλές εταιρείες παροχής υπηρεσιών στο διαδίκτυο, διατηρούν διάφορους λογαριασμούς συνδρομητών με σκοπό την παροχή συγκεκριμένων και μεμονωμένων υπηρεσιών σε κάθε μέλος ή συνδρομητή αυτών των υπηρεσιών. Ένας εισβολέας θα μπορέσει να αποκτήσει πρόσβαση σε έναν ηλεκτρονικό υπολογιστή μέσω ενός λογαριασμού ίντερνετ είτα μέσω μιας δικτυακής σύνδεσης.

Λόγω όμως του γεγονότος πως για πρόσβαση μέσω ίντερνετ απαιτείται ένας κωδικός, οι «χάκερς» χρησιμοποιούν κάποιους τους οποίους μπορούν να τους μαντέψουν. Οι κωδικοί αυτοί μπορούν να φέρουν τα μικρά τους ονόματα ή τα επώνυμα τους ή ακόμα και το όνομα της αγαπημένης τους ομάδας. Σε σχετική έρευνα που διεξήχθη από την εταιρεία ηλεκτρονικών υπολογιστών Compaq Inc. το 1990, διαπιστώθηκε πως το 82% των μη εξουσιοδοτημένων χρηστών, χρησιμοποιούσαν εύκολους κωδικούς για την αυθαίρετη χρήση ηλεκτρονικών υπολογιστών[22].

1.7 «Κυβερνομικρόβια» και Επιθετικός «Πληροφοριακός Πόλεμος»

Στους ανθρώπους της πληροφορικής, είναι ιδιαιτέρως γνωστά τα επονομαζόμενα «*κυβερνομικρόβια*». Τα συγκεκριμένα προγράμματα ηλεκτρονικών υπολογιστών, έχουν την ικανότητα να μιμούνται με άριστο τρόπο τις διάφορες μορφές ζωής μέσα σε έναν υπολογιστή. Μπορούν να δημιουργούν αντίγραφα πληροφοριών και να κινούνται με ευελιξία μέσα στην «χώρα» ενός ηλεκτρονικού υπολογιστή. Τα συγκεκριμένα «*κυβερνομικρόβια*» μπορούν να προκαλέσουν σοβαρές βλάβες και να λειτουργήσουν ως ωρολογιακές βόμβες.

[22] Branscomb, A. W., 1994.

Μπορούν επίσης να αποκρύπτονται για αρκετό καιρό και να εκδηλωθούν στον κατάλληλο χρόνο. Θα πρέπει επίσης να αναφερθεί πως εφόσον αυτά έχουν εισβάλλει σε έναν ηλεκτρονικό υπολογιστή, έχουν την ικανότητα να διαγράψουν ή να καταστρέψουν συγκεκριμένα δεδομένα ή να αποστείλουν τα δεδομένα αυτά στους υπολογιστές των «*χάκερς*» ή υποκλοπείς.

Ως εργαλείο «πληροφοριακού πολέμου», τα κυβερνομικρόβια μπορούν να καταστρέφουν την ακεραιότητα των δικτύων υπολογιστών και να οδηγούν σε άρνηση της παροχής συγκεκριμένων υπηρεσιών. Ακόμα και αν δεν καταστρέφουν σκοπίμως τα διάφορα δεδομένα ή δεν απενεργοποιούν συστήματα ηλεκτρονικών υπολογιστών, οι μολυσμένοι από αυτά υπολογιστές θα είναι καλύτερο να τεθούν εκτός λειτουργίας και να μην εκτελούν όλα όσα πρέπει να κάνουν κατά την διάρκεια που θα καταβάλλεται προσπάθεια για να απομακρυνθούν αυτοί οι ιοί από το σύστημα[23].

Μηχανισμός Block Ciphers

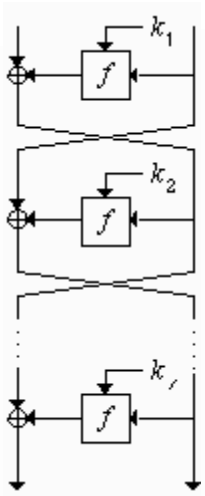
Block cipher είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης που μετατρέπει ένα block μη κρυπτογραφημένου καθορισμένου μήκους κειμένου ***(plaintext)***, σε block κρυπτογραφημένου του ίδιου μήκους κειμένου ***(ciphertext)***. Αυτός ο μετασχηματισμός πραγματοποιείται με την βοήθεια ενός μυστικού κλειδιού που χορηγείται από τον χρήστη. Η αποκρυπτογράφηση γίνεται με την εφαρμογή του αντίστροφου μετασχηματισμού στο κρυπτογραφημένο κείμενο χρησιμοποιώντας το ίδιο μυστικό κλειδί. Το καθορισμένο μήκος καλείται ***block size*** και για πολλούς ciphers είναι 64 bits. Στα μελλοντικά χρόνια το μήκος θα αυξηθεί στα 128 bits καθώς οι υπολογιστές γίνονται πιο ικανοί. Κάθε κείμενο δίνει διαφορετικό ciphertext.

Οι block ciphers λειτουργούν επαναληπτικά, κρυπτογραφώντας ένα block διαδοχικά αρκετές φορές. Σε κάθε γύρο, ο ίδιος μετασχηματισμός εφαρμόζεται στα δεδομένα χρησιμοποιώντας ένα ***subkey***. Το σύνολο των subkeys προέρχεται από το μυστικό κλειδί που χορήγησε ο χρήστης, με ειδική συνάρτηση. Το σύνολο των subkeys καλείται ***key schedule***[24].

Ο αριθμός των επαναλήψεων του επαναληπτικού cipher εξαρτάται από το επίπεδο της επιθυμητής ασφάλειας και την απόδοση του συστήματος. Στις περισσότερες περιπτώσεις, ο αυξημένος αριθμός επαναλήψεων βελτιώνει την προσφερόμενη ασφάλεια, αλλά για μερικούς ciphers ο αριθμός των επαναλήψεων για να επιτευχθεί ικανοποιητική ασφάλεια θα είναι πολύ μεγάλος για να πραγματοποιηθεί.

[23] Adams, J., 1998.

[24] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.



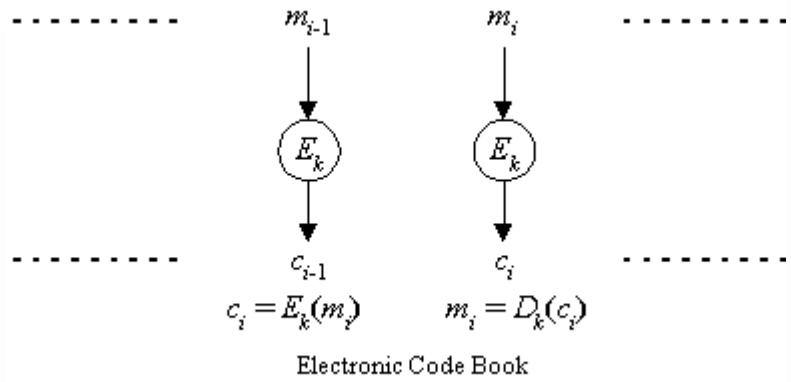
Οι Feistel ciphers είναι ειδικές περιπτώσεις επαναληπτικών ciphers όπου το κρυπτογραφημένο κείμενο υπολογίζεται ως εξής: το κείμενο χωρίζεται στο μισό. Η συνάρτηση *f* εφαρμόζεται στο ένα μισό με χρήση ενός subkey και η έξοδος της *f* περνάει από λογική πράξη X-OR με το άλλο μισό. Έπειτα, το αποτέλεσμα της λογικής πράξης γίνεται είσοδος της *f* και το προηγούμενο μισό το οποίο μετασχηματίστηκε γίνεται μία από τις εισόδους της επόμενης X-OR. Η άλλη είσοδος της X-OR είναι το αποτέλεσμα του δεύτερου μετασχηματισμού, ο οποίος χρησιμοποιεί νέο subkey. Ο αλγόριθμος συνεχίζεται με το ίδιο τρόπο. Στο τέλος της τελευταίας επανάληψης, τα δύο κρυπτογραφημένα μισά συνενώνονται.

Ένα σημαντικό χαρακτηριστικό του Feistel είναι ότι η αποκρυπτογράφηση είναι δομικά ταυτόσημη με την κρυπτογράφηση. Τα subkeys χρησιμοποιούνται σε αντίστροφη σειρά στην αποκρυπτογράφηση. Οι Feistel ciphers καλούνται και *DES-like* ciphers[25].

Τρόποι Λειτουργίας

Ένας αλγόριθμος τύπου block cipher έχει διάφορους τρόπους λειτουργίας. Κάθε τρόπος λειτουργίας μπορεί να έχει τις δικές του ιδιότητες εκτός από αυτές που κληρονομεί από τον βασικό cipher. Οι βασικοί τρόποι λειτουργίας είναι: ο *Electronic Code Book (ECB),* ο *Cipher Block Chaining (CBC),* ο *Cipher Feedback (CFB)* και ο *Output Feedback (OFB)*.

[25] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.



Electronic Code Book

Σε ECB mode, το κείμενο χωρίζεται σε ισομήκη block. Κάθε μη κρυπτογραφημένο block κρυπτογραφείται ανεξάρτητα από την συνάρτηση του βασικού block cipher. Μειονέκτημα αυτού του τρόπου είναι ότι ομοιότητες του plaintext δεν καλύπτονται. Τα plaintext block που είναι ταυτόσημα, δίνουν ταυτόσημα ciphertext block και το κείμενο μπορεί εύκολα να τροποποιηθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη των όμοιων ciphertext block. Η ταχύτητα της κρυπτογράφησης κάθε plaintext block είναι ίδια με την ταχύτητα του block cipher. Ο ECB επιτρέπει την παράλληλη παραγωγή των ciphertext blocks για καλύτερη απόδοση[26].

Σε CBC mode, κάθε μη κρυπτογραφημένο block συνδυάζεται μέσω της λογικής πράξης X-OR με το πρωτύτερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη X-OR πράξη που καλείται *Initialization Vector*, c_0. Τα όμοια plaintext blocks καλύπτονται με την χρήση της λογικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρ' όλο που η αποκρυπτογράφηση μπορεί[27].

Σε CFB mode, το προηγούμενο ciphertext block κρυπτογραφείται και το αποτέλεσμα που παράγεται συνδυάζεται με το επόμενο plaintext block με χρήση μιας X-OR. Η έξοδος της X-OR αποτελεί το νέο ciphertext block που θα κρυπτογραφηθεί, συνεχίζοντας την διαδικασία. Γίνεται η ποσότητα που χρησιμοποιείται για ανάδραση ***(feedback)*** να μην είναι ένα πλήρες block.Απαιτείται ένας Initialization Vector c_0 για την πρώτη X-OR πράξη.

Με αυτόν τον τρόπο καλύπτονται πιθανές ομοιότητες στα plaintext blocks μέσω της X-OR. Γίνεται, όμως, στην πλήρη ανάδραση τα c_i και c_{i-1} να είναι ταυτόσημα. Σαν συνέπεια και το επόμενο ζεύγος κρυπτογραφημένων block θα είναι ταυτόσημα μεταξύ τους. Αυτό το πρόβλημα λύνεται με την χρήση μερικής ανάδρασης. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher και δεν επιτρέπεται παράλληλη επεξεργασία.

[26] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

[27] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

Σε OFB mode, η διαδικασία είναι παρόμοια με αυτήν του CFB mode, με την διαφορά ότι η ποσότητα που συνδυάζεται με X-OR με κάθε plaintext block παράγεται ανεξάρτητα από τα plaintext και ciphertext. Ένας Initialization Vector s_0 χρειάζεται για να ξεκινήσει την διαδικασία και κάθε block s_i προκύπτει από την κρυπτογράφηση του προηγούμενου s_{i-1}. Η κρυπτογράφηση plaintext block γίνεται με τον συνδυασμό κάθε plaintext block μέσω μιας X-OR, με το κρυπτογραφημένο *s*.

Η ανάδραση με block χωρίς να είναι πλήρες δεν συνιστάται για λόγους ασφάλειας. Ο OFB mode έχει το εξής πλεονέκτημα σε σχέση με τον CFB. Τα πιθανά λάθη μετάδοσης δεν πολλαπλασιάζονται κατά την αποκρυπτογράφηση και έτσι δεν την επηρεάζουν. Το κείμενο, όμως, μπορεί εύκολα να αλλοιωθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη όμοιων ciphertext block. Δεν είναι δυνατή η παράλληλη επεξεργασία, αλλά η διαδικασία μπορεί να επιταχυνθεί με την παραγωγή των κρυπτογραφημένων *s* πριν τα δεδομένα να είναι διαθέσιμα για κρυπτογράφηση.

Μηχανισμός Steam Ciphers

Stream cipher είναι ένας τύπος αλγόριθμου συμμετρικής κρυπτογράφησης. Είναι εξαιρετικά ταχύς αλγόριθμοι, κατά πολύ ταχύτεροι από τους block ciphers. Σε αντίθεση με τους block ciphers που λειτουργούν με μεγάλα κομμάτια δεδομένων ***(blocks)***, οι stream ciphers τυπικά λειτουργούν με μικρότερες μονάδες απλού κειμένου, συνήθως με bits. Η κρυπτογράφηση ενός συγκεκριμένου κειμένου με έναν block cipher θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Με έναν stream cipher, ο μετασχηματισμός των μικρότερων αυτών μονάδων θα ποικίλει, ανάλογα με πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης[28].

Ένας stream ciphers παράγει μια ακολουθία από bits που χρησιμοποιείται σαν κλειδί και καλείται keystream. Η κρυπτογράφηση επιτυγχάνεται με τον συνδυασμό του keystream με το plaintext, συνήθως μέσω X-OR πράξης. Η παραγωγή του keystream μπορεί να είναι ανεξάρτητη του plaintext και του ciphertext ***(synchronous stream cipher)*** ή μπορεί να εξαρτάται από αυτά ***(self-synchronizing stream cipher)***. Οι περισσότεροι stream ciphers είναι synchronous.

Οι stream ciphers βασίζονται στις θεωρητικές ιδιότητες ενός one-time pad. One-time pads (καμιά φορά καλούνται και Vernam ciphers) είναι ciphers που χρησιμοποιούν μια ακολουθία bits ***(keystream)*** που παράγεται τελείως στην τύχη. Το keystream είναι του ίδιου μήκους με το μη κρυπτογραφημένο κείμενο και συνδυάζεται μέσω μιας X-OR πράξης με το αυτό για την παραγωγή του ciphertext. Επειδή του keystream είναι τελείως τυχαίο και είναι του ίδιου μήκους με το plaintext, η εύρεση του κειμένου είναι αδύνατη ακόμα και με την διάθεση τεράστιας υπολογιστικής ισχύς.

Ένας τέτοιος cipher εξασφαλίζει άκρα μυστικότητα και ασφάλεια και έχει χρησιμοποιηθεί σε καιρό πολέμου για μεγάλα χρονικά διαστήματα για την διασφάλιση διπλωματικών καναλιών. Το

[28] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

γεγονός, όμως, ότι το μυστικό κλειδί (δηλαδή το keystream), που χρησιμοποιείται μόνο μία φορά, είναι του ίδιου μήκους με το μήνυμα, δημιουργεί σημαντικό πρόβλημα στην διαχείριση του κλειδιού. Παρ' όλη την ασφάλεια που προσφέρει, ο one-time pad δεν μπορεί να εφαρμοστεί στην πράξη[29].

Οι stream ciphers αναπτύχθηκαν σαν μια προσέγγιση της λειτουργίας ενός one-time pad. Βέβαια δεν είναι σε θέση παρέχουν την θεωρητική ασφάλεια ενός time-pad είναι τουλάχιστον πρακτικοί. Ο πιο ευρέως χρησιμοποιούμενος stream cipher είναι ο RC4. Ενδιαφέρον παρουσιάζει το γεγονός ότι συγκεκριμένοι τρόποι λειτουργίας ενός block cipher προσομοιάζουν ένα stream cipher όπως για παράδειγμα ο DES σε CFB και OFB modes. Ακόμα και έτσι, οι αυθεντικοί stream ciphers είναι αρκετά ταχύτεροι[30].

Ένας μηχανισμός για την παραγωγή του keystream είναι ο ***Linear Feedback Shift Register (LFSR)***. Ο καταχωρητής αποτελείται από μία σειρά κελιών ***(cells)*** το καθένα από τα οποία αποτελείται από ένα bit. Τα περιεχόμενα των κελιών καθορίζονται από ένα Initialization Vector που λειτουργεί σαν το μυστικό κλειδί. Το keystream δεν αποτελεί πλέον το μυστικό κλειδί (όπως στους one-time pads) λόγω του μεγέθους του. Η συμπεριφορά του καταχωρητή ρυθμίζεται από ένα ρολόι και σε κάθε χρονική στιγμή τα bits μετακινούνται μία θέση δεξιά, την στιγμή που το X-OR αποτέλεσμα μερικών από αυτών τοποθετείται στο αριστερότερο κελί. Κάθε αλλαγή του ρολογιού δίνει ένα bit εξόδου[31].

[29] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

[30] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

[31] Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books.

Κεφάλαιο 2ο

Η Έννοια και η Σημασία του Διαδικτύου στις Μέρες μας

2.1 *Ποια είναι η Έννοια του Διαδικτύου*

Το διαδίκτυο στην ευρύτερη σημασία του, αποτελείται από έναν σεβαστό αριθμό υπολογιστών που ενώνονται μεταξύ τους, δημιουργώντας ένα δίκτυο το οποίο στη συνέχεια συνδέεται με άλλα δίκτυα. Η αγγλική ορολογία του διαδικτύου προέρχεται από την ένωση δύο λέξεων (inter-network)[32]. Το διαδίκτυο που είναι η δημιουργία ενός αξιόλογου αριθμού μικρότερων συνδέσεων υπολογιστών, χρησιμοποιεί μια σειρά από ελεύθερα πρωτόκολλα για τη διανομή μιας γκάμας διαδικτυακών υπηρεσιών. Δεν είναι δυνατόν, να περιοριστεί, να ελεγχτεί και να διαμορφωθεί από κάποιον.

Κατά τον Μπαμπινιώτη, πρόκειται για ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών, που ενώθηκαν με μικρότερα ή και μεγαλύτερα δίκτυα ανά την υφήλιο με στόχο τη μεταφορά, την επεξεργασία και την ανταλλαγή δεδομένων για λόγους ψυχαγωγίας, ενημέρωσης, εμπορίας προϊόντων και υπηρεσιών[33].

Την δυνατότητα εισόδου στο διαδίκτυο μπορεί να έχει κανείς από κάθε υπολογιστή όταν αυτός έχει δημιουργήσει συνδρομή με κάποια εταιρεία παροχής υπηρεσιών διαδικτύου. Οι χρήστες του, μπορούν να του δώσουν αξία ανεβάζοντας νέο υλικό στις ιστοσελίδες που το απαρτίζουν (mp3, video, φωτογραφίες σχόλια σε forums κ.λ.π.). Δεν περιορίζεται σε γεωγραφικούς τόπους, σε χρονικά πλαίσια, σε μέγεθος και σε είδος δεδομένων. Κατέχει μια συνεχή και ανανεωτική τάση που δεν είναι ελέγξιμη, εξυπηρετώντας αφιλοκερδώς επικοινωνιακούς, ψυχαγωγικούς σκοπούς και κάθε είδους διακίνηση πληροφοριών.

Στις μέρες μας, οι συνδέσεις των χρηστών στο διαδίκτυο ανέρχονται στις 4,3 δισεκατομμύρια, σε ποσοστό του 85% των δυνατοτήτων του δικτύου (web). Σύμφωνα με τους ειδικούς σε τρία έτη το ποσοστό αυτό θα φτάσει το 100%.

---

[32] Κωνσταντίνου, Μ., (2000), Αρθρο "Διαφήμιση στο Ελληνικό ιντερνέτ - impressions ή χρονοχρέωση", Περιοδικό e-market.

[33] Κωνσταντίνου, Μ., (2000), Αρθρο "Διαφήμιση στο Ελληνικό ιντερνέτ - impressions ή χρονοχρέωση", Περιοδικό e-market.

2.2 *Διαδικτυακά Κανάλια και Συστήματα Προσέλκυσης Νέων Χρηστών*

Υπάρχουν συστήματα τα οποία αποτελούν μια νέα προσέγγιση στο χώρο του Μάρκετινγκ και προσφέρουν ένα σημαντικό ανταγωνιστικό πλεονέκτημα στα διαδικτυακά κανάλια που τα χρησιμοποιούν και δραστηριοποιούνται μέσω αυτού. Τα συστήματα αυτά προσφέρουν την δυνατότητα στους διαδικτυακούς χώρους να χρησιμοποιούν τις δυνατότητες της σημερινής τεχνολογίας των ηλεκτρονικών υπολογιστών και των τηλεπικοινωνιών, οδηγώντας προγράμματα προσανατολισμένα στον πελάτη –χρήστη με έναν διαπροσωπικό, σαφή και αποδοτικό κοινωνικό τρόπο. Στηρίζονται στην τεχνολογία της συλλογής, επεξεργασίας και χρήσης χρήσιμων πληροφοριών για πραγματικούς ή δυνητικούς πελάτες (διαχείριση γνώσης χρηστών).

Η πρώτη και αρκετά σημαντική δραστηριότητα που απαιτεί τη βοήθεια της τεχνολογίας είναι η λειτουργία των διαδικτυακών καναλιών τα οποία απευθύνονται σε διάφορες κοινωνικές πτυχές της ζωής των χρηστών. Από την εφαρμογή ενός αντίστοιχου συστήματος, το κάθε διαδικτυακό κανάλι μπορεί και συγκεντρώνει πληθώρα προσωπικών και κοινωνικών στοιχείων που αφορούν στη δραστηριότητα των χρηστών, τις επιθυμίες, τις ανάγκες αλλά και τα προβλήματα τους. Η μελέτη, για παράδειγμα, των δεδομένων από τη λειτουργία ενός διαδικτυακού κέντρου μπορεί να δείξει στο κανάλι αν οι χρήστες εξυπηρετούνται σωστά ή όχι, αν οι χρόνοι παραμονής τους σε αυτά είναι ικανοποιητικοί, τι είδους αιτήματα υποβάλλονται και κατά πόσο το κανάλι είναι έτοιμο να ανταποκριθεί στα αιτήματα αυτά.

Η επεξεργασία όλων των προσωπικών στοιχείων που προκύπτουν από ένα διαδικτυακό κανάλι, αλλά και γενικότερα όλων των στοιχείων που αφορούν στις σχέσεις του με τους χρήστες του, πραγματοποιείται από ένα σύστημα CRM, μια συλλογή εργαλείων business intelligence, τα οποία αξιοποιούν διάφορα προσωπικά δεδομένα και δημιουργούν γνώση για το ίδιο το κανάλι, βασισμένη στα δεδομένα αυτά. Εδώ αξίζει να σημειώσουμε ότι τα εργαλεία για το CRM μπορούν να αποτελούν μέρος του CRM ή να είναι ανεξάρτητα, εάν το κανάλι έχει προμηθευτεί τέτοια εργαλεία και για άλλους σκοπούς.

Ενώ το CRM χρησιμοποιείται κάθε στιγμή, καθώς η επαφή του καναλιού με τους χρήστες του είναι διαρκής, είναι ένα στρατηγικό εργαλείο το οποίο αξιοποιείται από τους υπευθύνους για τόνωση της κοινωνικής συμπεριφοράς των χρηστών εντός αυτών των χώρων. Επίσης, από την ανάλυση των δεδομένων του CRM καθώς και άλλων στοιχείων που αφορούν στη γενικότερη συμπεριφορά των χρηστών, το κανάλι μπορεί να εντοπίσει χρήστες που είναι πιθανό να μειώσουν ή

και να τερματίσουν τη συχνότητα επίσκεψης τους, οπότε εκείνο έχει την ευχέρεια να προβεί, εάν το θελήσει, σε ανάλογες κινήσεις προς αυτούς.

2.3 *Η Παρουσία και η Χρήση του Διαδικτύου στην Ελλάδα*

Σύμφωνα με την έρευνα της *Nua -Internet Servers* το έτος του 2005, οι χρηστές του ιντερνέτ ανά την υφήλιο είναι κατανεμημένη ως εξής :

Εμφύλιος:……..605,60εκατ.

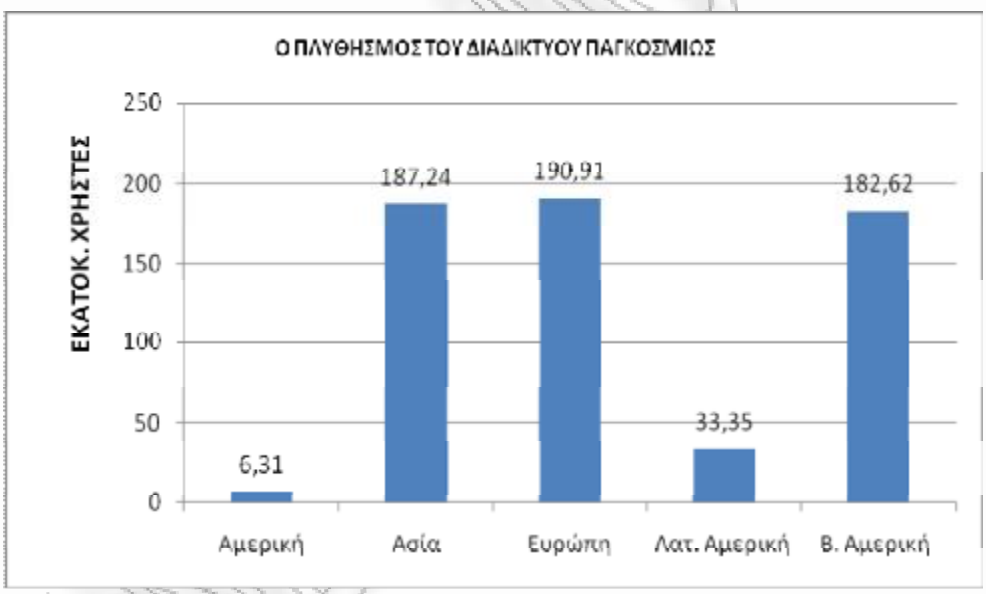
Αμερική:……6,31εκατ.

Ασία: ……187,24εκατ.

Ευρώπη:……190,91εκατ.

Λατ. Αμερική: ……33,35εκατ.

Β. Αμερική :……182,62εκατ.



Σχήμα .1 - Οι αριθμοί αντιστοιχούν σε εκατ. χρηστές.

Αποτελεί γεγονός πως ο συνολικός πληθυσμός της Ελλάδος ανέρχεται στα 11.338.624, ενώ ο αριθμός των χρηστών του διαδικτύου στην Ελλάδα κατά το 2007 ήταν περίπου 3.800.000.Το ποσοστό φθάνει το 33,5 % του συνολικού πληθυσμού. Το 2007 παρουσιάστηκαν ρυθμοί ανάπτυξης κατά 280% σε σχέση με το περασμένο έτος όσον αφορά την χρήση του διαδικτύου. Όμως το ποσοστό που καταλαμβάνει η χωρά στην Ε.Ε. για την χρήση ευρυζωνικών υπηρεσιών φτάνει το

1,5%, γεγονός που δείχνει ότι απαιτείται αρκετή προσπάθεια ακόμη για να υπάρξει μια ισορροπία μεταξύ Ελλάδας –Ε.Ε.[34]

Σύμφωνα με την έρευνα του παρατηρητήριου της κοινωνίας της πληροφορίας που παρουσιάζει η εφημερίδα «πρώτο θέμα», διαπιστώνεται ότι ο αριθμός των Ελλήνων χρηστών παρουσιάζει ελλείψεις στη χρήση του διαδικτύου και νέων προϊόντων τεχνολογίας και ιδιαίτερα όσον αφορά την προώθηση κοινωνικών υπηρεσιών πρόνοιας από δημόσιους οργανισμούς.

Σε ότι αφορά το επίπεδο εκπαίδευσης, καθολική σχεδόν χρήση Η/Υ και Διαδικτύου παρατηρείται στους κατόχους μεταπτυχιακών τίτλων σπουδών (91% και 87% αντίστοιχα), ενώ υψηλά ποσοστά σημειώνονται και για τους αποφοίτους τριτοβάθμιας εκπαίδευσης (78% και 68% αντίστοιχα). Όμως σε επίπεδο πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης η χώρα μας υστερεί κατά πολύ με ποσοστό 10% σε σχέση με τα παιδιά της Ευρώπης, που φτάνουν στο επίπεδο 36%. Όμως στα άτομα μέσης εκπαίδευσης τα ποσοστά απόκλισης είναι μικρότερα.

Βλέπουμε λοιπόν ότι η χρήση του διαδικτύου γίνεται από άτομα τα οποία το μορφωτικό τους επίπεδο είναι ιδιαίτερα υψηλό, κάτι το οποίο πιστοποιεί ότι η νέα τεχνολογία που έχει εισαχθεί για τα καλά στην καθημερινότητά μας, χρειάζεται κάποιες βάσεις παιδείας και τεχνολογικές γνώσεις καθώς και τεχνικές εξοικείωσης.

Επίσης η χρήση του διαδικτύου είναι ιδιαίτερα υψηλή από άτομα τα οποία ασχολούνται με την έρευνα, την εξέλιξη, και τις θετικές και τεχνολογικές επιστήμες γεγονός που είναι δύσκολο να εφαρμοστεί σε άτομα τα οποία δεν έχουν να κάνουν με το χώρο των προαναφερθέντων επιστήμων. Επομένως δεν μπορούν να αναπτύξουν μεθόδους και τρόπους σύγχρονης επικοινωνίας και διεκπεραίωσης συναλλαγών και συνεργασιών, άτομα που υστερούν στο χώρο των πιο πάνω επιστήμων, που δεν ήρθαν σε στοιχειώδη επαφή με την τεχνολογική κατάρτιση και την μαθησιακή γνώση των υπολογιστών.

Τα χαρακτηριστικά του Έλληνα χρήστη του διαδικτύου όπως δημοσιεύτηκε στην εφημερίδα «πρώτο θέμα» έχουν ως εξής. Πρόκειται για νέο ανδρικό πληθυσμό, με πολύ καλή μόρφωση, υψηλού εισοδήματος, με χώρο διαμονής σε αστικές πόλεις και κατέχοντας μεταπτυχιακούς τίτλους σπουδών, σύμφωνα με την έρευνα της κοινωνίας της πληροφορίας για το έτος του 2006. Όπως αναφέρει η εφημερίδα τα χαρακτηριστικά του Έλληνα χρήστη έχουν ως εξής. Το έτος 2006 οι άνδρες κάνουν χρήση ηλεκτρονικού υπολογιστή σε ποσοστό 45,1% και του διαδικτύου κατά 36% σε σύγκριση με τις γυναίκες που έχουν ποσοστό 32,8% και 24% αντιστοίχως[35].

[34] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[35] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

Οι πιο νέοι ηλικίας 16-24 δεν παρουσιάζουν μεγάλη απόκλιση από τους μεγαλύτερους και των δύο φύλων. Επικρατεί μια τάση αύξησης των χρηστών του διαδικτύου στις επαρχιακές πόλεις της χώρας μας με την Αττική να έχει τα ηνία (41,2%) ύστερα ακολουθεί το νότιο Αιγαίο (31,4%) και η κεντρική Μακεδονία (29,7%). Σε αγροτικές περιοχές από το 2005 καταγράφονται τάσεις ανάπτυξης διαδικτυακής χρήσης κατά 11 μονάδες[36].

Οι κυριότεροι λόγοι πλοήγησης στο διαδίκτυο για τους Έλληνες για το έτος του 2008, ήταν οι εξής :

E- Banking.…….13,2%

Εξυπηρέτηση και επικοινωνία με δημόσιες υπηρεσίες ……. 27,4%

Αναζήτηση δεδομένων για εκπαιδευτικούς σκοπούς ……33,3%

Εύρεση πληροφοριών για εξωτικούς προορισμούς……45,6%

Ανάγνωση διαδικτυακών περιοδικών τύπου ……49,4%

Αναζήτηση δεδομένων για εξόρυξη γνώσης ……58,3%

Ανταλλαγή εικόνων ,mp3,μηνυμάτων ……63,2%

Εύρεση δεδομένων για προϊόντα και υπηρεσίες……81,4%

Σχήμα 2 - Οι κυριότεροι λόγοι πλοήγησης στο διαδίκτυο για τους Έλληνες για το έτος του 2008.

Στη συνέχεια παρουσιάζονται αντίστοιχες έρευνες όσον αφορά τη χρήση του διαδικτύου στην επικοινωνία και την ψυχαγωγία. Όσον αφορά στην επικοινωνία είναι:

- *Αποστολή και λήψη ηλεκτρονικών μηνυμάτων 67,3%.*

[36] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

- *Ανταλλαγή γραπτών μηνυμάτων σε πραγματικό χρόνο, (π.χ. MSN instant messaging) 34,7%*
- *Διάβασμα ιστολογιών (weblogs, blogs) 25,6% .*
- *Πραγματοποίηση τηλεφωνημάτων μέσω διαδικτύου 21,6% .*

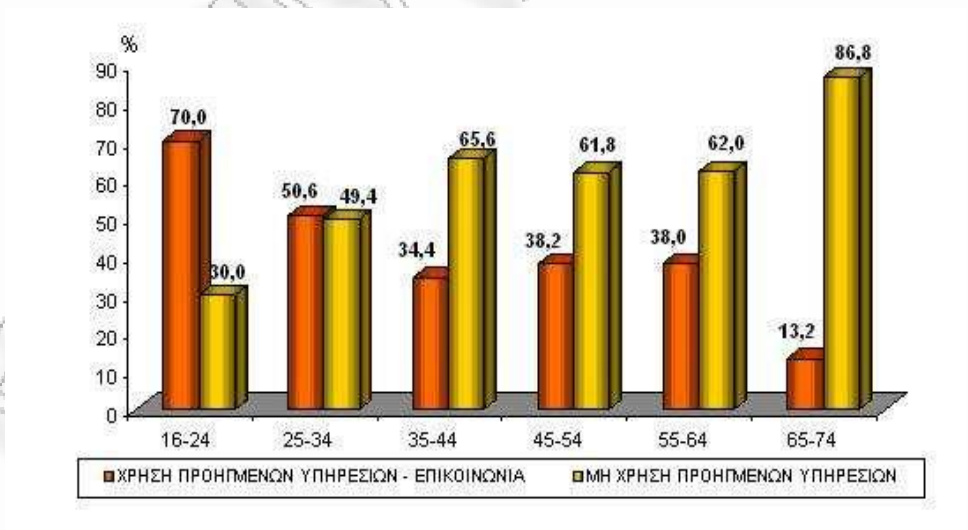
Όσον αφορά στην ψυχαγωγία είναι:

- *«Κατέβασμα» και ακρόαση μουσικής 46,4%.*
- *Ακρόαση web ραδιοφώνου / παρακολούθηση web τηλεόρασης 40,6%.*
- *«Κατέβασμα» και παρακολούθηση ταινιών 28,1% .*

Οι ηλικίες που χρησιμοποιούν το διαδίκτυο στον ελλαδικό χώρο, είναι οι εξής :

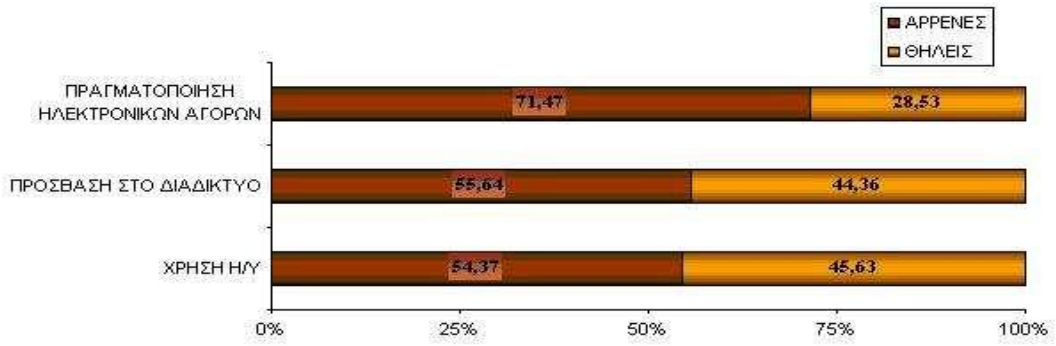
- *Για την ηλικιακή ομάδα 16–24 ετών, η λήψη και «διανομή» οπτικοακουστικού υλικού, δηλαδή, μουσικής, ταινιών και παιχνιδιών, αποτελεί τον κυριότερο λόγο πλοήγησης.*
- *Η ηλικιακή ομάδα 25 – 34 ετών, είναι η πλέον εμφανιζόμενη σε όλες σχεδόν τις δραστηριότητες.*
- *Για τις μεγαλύτερες ηλικίες 35–64 ετών, η αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες αποτελεί τον κυριότερο λόγο πλοήγησης.*

Το γράφημα δείχνει κατά ηλικιακή ομάδα, τη χρήση ή μη προηγμένων υπηρεσιών με σκοπό την επικοινωνία και την ψυχαγωγία:



Σχημα 3

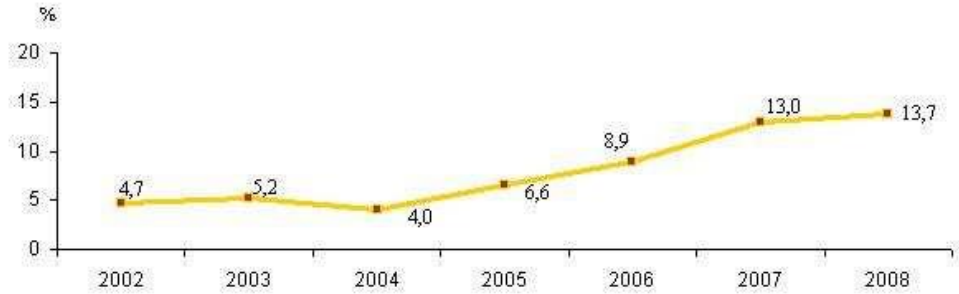
Επίσης, τα ποσοστά των ανδρών που έχουν πρόσβαση στο διαδίκτυο και πραγματοποιούν ηλεκτρονικές αγορές, είναι υψηλότερα από εκείνα των γυναικών, όπως παρουσιάζεται στο παρακάτω σχήμα:



Σχήμα 4

Οι αριθμοί της επισκεψιμότητας των πολιτών σε δημόσιους οργανισμούς για παροχή κοινωνικής πρόνοιας για το έτος του 2008 στην Ελλάδα, είναι οι εξής[37]. Οι χρήστες διαδικτύου κατά το πρώτο τρίμηνο του έτους 2008 οι οποίοι προέβησαν σε διαδικτυακές αγορές κατείχαν το ποσοστό του 13,7% οδηγώντας έτσι αύξηση κατά 5% σε σχέση με την περσινή χρονική περίοδο του 2007. Το γράφημα που επακολουθεί απεικονίζει αυτή την τάση :

ΠΟΣΟΣΤΑ e- ΕΠΙΣΚΕΠΤΩΝ ΓΙΑ ΤΟ ΕΤΟΣ 2008



Σύμφωνα με έρευνα από την Ευρωπαϊκή στατιστική υπηρεσία (EUROSTAT), προκύπτει ότι η χώρα μας κάνει περισσότερο χρήση του διαδικτύου από χώρες της Ε.Ε. όπως η Ρουμανία και Βουλγαρία που ανήκουν στην ευρωζώνη με ποσοστό 25% σε σχέση με το περσινό που ήταν 23%[38] .

Ο ελληνικός λαός βρίσκεται στην τελευταία θέση για το έτος 2007 με ποσοστό 7% των Ελλήνων να κάνουν χρήση του διαδικτύου ενώ στην αντίστοιχη χρονική περίοδο το ποσοστό στην

[37] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[38] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

ευρωζώνη κυμαίνονταν στο 42%. Το πρώτο τρίμηνο του 2006 το ποσοστό για την Ελλάδα έφτανε το 4% ενώ για τις χώρες ευρωζώνης του 30%. Για την χρήσης του διαδικτύου για εύρεση στοιχείων από τις μηχανές αναζήτησης (Google,Yahoo,κ.λπ.) ανέρχεται στο 36%, ενώ για τους Ευρωπαίους ανέρχεται στο ποσοστό του 57%[39].

Με ποσοστό 24% η Ευρώπη προηγείται. Επίσης το 6% των Ελλήνων χρηστών κάνει χρήση του διαδικτύου για την πραγματοποίηση τηλεφωνικών κλήσεων προς αυτές τις υπηρεσίες. Η έρευνα έδειξε ακόμη ότι το 5% των Ελλήνων δημιουργεί δικά του διαδικτυακά sites, έναντι του 10% των Ευρωπαίων[40]

Σύμφωνα με έρευνα της Eurostat, οι Έλληνες κατέχουν το 23% που μπορεί να χρησιμοποιήσει το διαδίκτυο ενώ το 4% έχει γρήγορη σύνδεση σε αυτό. Η χώρα μας έρχεται σχεδόν τελευταία στη χώρες ευρωζώνης στο θέμα του διαδίκτυο όμως άτομα από 16-24 ετών έχουν πρόσβαση στο διαδίκτυο μια φορά την εβδομάδα με ποσοστό 47%. Το 52% του Μ.Ο. των Ευρωπαίων έχουν πρόσβαση στο διαδίκτυο με πρώτη την Ολλανδία κατά 80% ακολουθεί η Δανία με 79%, ενώ στον αντίποδα βρίσκεται η χώρα μας με 23% με τη Σλοβακία με 27%[41].

Οι Ευρωπαίοι σε ποσοστό 32% έχουν γρήγορο Ιντερνέτ με πρώτη την Ολλανδία με 66% ενώ η χώρα μας φτάνει το 4%. Σε άτομα ηλικίας 25-54 ετών το ποσοστό των Ελλήνων που κάνουν χρήση του διαδικτύου φτάνει 27% και μεταξύ των 55-74 ετών το 4% ποσοστά από τα χειρότερα στην Ευρώπη. Το 2007 το ποσοστό των Ελλήνων που έκανε χρήση του διαδικτύου για κοινωνική πρόνοια, ανέρχεται στο 7% ενώ την αντίστοιχη χρόνια το ποσοστό της ευρωζώνης ανερχόταν στο 42%. Το πρώτο τρίμηνο του 2006 το ποσοστό για την Ελλάδα έφτανε το 4% ενώ για την τις χώρες της ευρωζώνης το 30%[42] .

Χρήση των μηχανών αναζήτησης για κοινωνική πρόνοια των Ελλήνων κάνει 36% ενώ οι Ευρωπαίοι χρησιμοποιούν τις μηχανές αναζήτησης σε ποσοστό 57% χρήση του email (ηλεκτρονικού ταχυδρομείου) στην Ελλάδα κάνει το 26% έναντι του 50% στην Ευρώπη. Επίσης το 12% των Ελλήνων χρηστών χρησιμοποιεί το διαδίκτυο για την εγκατάσταση προγραμμάτων και χρήση αυτών από τον υπολογιστή, κάτι που δεν ισχύει στην Ευρώπη κατέχει το 27%. Η χώρα μας υστερεί και στην διαδικτυακή συζήτηση με ποσοστό έναντι 11% έναντι των Ευρωπαίων που κατέχουν το 24%. Ακόμη το 6% του ελληνικού κοινού κάνει χρήση του διαδικτύου για την πραγματοποίηση

[39] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[40] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[41] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[42] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

τηλεφωνικών κλήσεων. Επίσης η έρευνα έδειξε ότι το 5% δημιουργούν ισόχωρους έναντι του 10%των Ευρωπαίων[43].

2.4 Το Μέλλον του Διαδικτύου

Το 2020 θα υπάρχουν μερικά δισεκατομμύρια συσκευές οι οποίες θα έχουν πρόσβαση στο πολύ φθηνό διαδίκτυο. Ο πρόεδρος του κέντρου τεχνολογικής πληροφορίας Louis Nudges, προβλέπει τη δημιουργία κινητού διαδικτύου που οποιοσδήποτε, θα έχει πρόσβαση με ταχύτητα 1 gigabyte όταν βρίσκεται μέσα στο δίκτυο[44].

Μέσο πρόσβασης στο διαδίκτυο, θα είναι και τα κινητά. Οι κυβερνητικές παρεμβάσεις θα είναι περιορισμένες καθώς οι επιχειρηματικές παρουσίες θα πηρεάζουν περισσότερο την διαλειτουργικότητα του δικτύου. Η ψηφιακή διαίρεση και οι καθεστωτικές ρυθμίσεις, δεν οδηγούν τόσο γρήγορα στην επιθυμητή διάσταση για το φανταστικό διαδίκτυο. Αποτελεί γεγονός πως η λειτουργικότητα θα εξαρτηθεί από την αντικατάσταση του ανταγωνισμού με την συνεργασία, ενώ ο Metcalf ο ιδρυτής της 3com και του Ethernet, δηλώνει ότι το διαδίκτυο θα ξεπεράσει της προσωπικές επικοινωνίες το 2020[45].

Τα εργαλεία ανάπτυξης εξυπηρετητών Παγκόσμιου Ιστού θα τείνουν όλο και περισσότερο στην παροχή δυνατοτήτων που θα ελκύουν τους χρήστες. Η διανομή του λογισμικού θα γίνεται όλο και περισσότερο μέσω του διαδικτύου με αποτέλεσμα να μειωθεί η χρησιμοποίηση CD-ROM και δισκετών και το video και audio streaming θα διαδοθεί ακόμα περισσότερο και η σύγκλιση της τηλεόρασης και υπολογιστή είναι πολύ κοντά. Θα αναπτυχθεί ιδιαίτερα η παροχή κοινωνικών υπηρεσιών και πρόνοιας και η στρατηγική χρέωσης των υπηρεσιών του διαδικτύου αναμένεται να αλλάξει και να προσαρμοστεί στο είδος δεδομένων που κάθε χρήστης διακινεί.

Οι μελλοντικές ιστοσελίδες του web θα αποτελούνται από περισσότερο κείμενο και περιορισμένο γραφιστικό κομμάτι. Η παρουσία πολλών εφέ θα είναι σημαντική. Αυτό γιατί ο χρήστης σε μια σελίδα θα ενδιαφέρεται για ειδήσεις που κυμαίνονται του 75% (της ιστοσελίδας), ενώ σε ένα έντυπο το 30% για πληροφορίες[46].

Η σχεδίαση μιας σελίδας για τον επισκέπτη που ψάχνει για εύρεση πληροφοριών είναι περιττή, θα τον κερδίσει μόνο ένας ιστότοπος που θα περιέχει πολλές πληροφορίες εύκολα και γρήγορα. Λιτότητα και κομψή σχεδίαση είναι το ζητούμενο για τους διαδικτυακούς χρήστες. Επίσης

---

[43] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[44] Κωνσταντίνου, Μ., (2000), Αρθρο "Διαφήμιση στο Ελληνικό ιντερνέτ - impressions ή χρονοχρέωση", Περιοδικό e-market.

[45] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

[46] Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών.

εύκολες στα ανοίγματα από τους browsers σελίδες και ελεύθερες εφαρμογές, θα είναι τα χαρακτηριστικά του διαδικτύου και των δημοσίων οργανισμών του μέλλοντος. Από την άλλη πλευρά σε άμεσα μέτρα πρέπει να προβεί η Ευρωπαϊκή Ένωσή ώστε να αποφευχθεί ο κίνδυνος για εξάντληση των διευθύνσεων IP.

Στο διαδίκτυο απομένουν μόνον 700 εκατομμύρια διευκρινίσεις ενώ ο μέχρι τώρα ο αριθμός τους φτάνει τα 4,6 δις. διευθύνσεις και ο αριθμός αυτός τείνει να μειωθεί έως το 2011. Με τη χρήση του πρωτοκόλλου IPV6 θα ξεπεραστεί το πρόβλημα καθώς θα δοθεί η δυνατότητα απεριόριστων συνδέσεων και δημόσιων οργανισμών.

Κεφάλαιο 3ο
Μεθοδολογία και Τρόπος Συλλογής Πηγών και Πληροφοριών Εκπόνησης Πτυχιακής Εργασίας

Σε αυτό το κεφάλαιο παρουσιάζονται οι τρόποι με τους οποίους ολοκληρώθηκε η συγκέντρωση των απαραίτητων στοιχείων για την συγγραφή αυτής της πτυχιακής εργασίας. Η συλλογή των στοιχείων ολοκληρώθηκε μέσω βιβλιογραφικής έρευνας και σχετικών πληροφοριών για την λειτουργία της διαδικτυακής μηχανής αναζήτησης Google των επιθέσεων που έχει δεχθεί μέσω διαφόρων κακόβουλων ενεργειών που έχουν σημειωθεί σε αυτά τα χρόνια λειτουργίας.

Από τις αντίστοιχες πηγές που αφορούν το συγκεκριμένο αντικείμενο μελέτης, εξάχθηκαν χρήσιμα συμπεράσματα σχετικά το πως λειτουργούν οι διαδικτυακές μηχανές αναζήτησης και ποια τα είδη κακόβουλων ενεργειών που μπορούν να δεχθούν στη λειτουργία τους.

Θα πρέπει να αναφερθεί πως η συλλογή πληροφοριών και δεδομένων αποτελούν τα κύρια στοιχεία μιας έρευνας και καταγραφής αυτής, σχετικά με την μελέτη ενός φαινομένου ή γεγονότος όπως και στην συγκεκριμένη περίπτωση[47]. Επιπλέον μπορούν να χαρακτηριστούν ως πρωτογενή στοιχεία για την έρευνα ενός θέματος, αφού παρέχουν σημαντικές πληροφορίες για αυτή αλλά και τις υποθέσεις που μπορούν να γίνουν. Οι πληροφορίες και τα δεδομένα σε αυτήν την συγκεκριμένη φάση μπορούν να τροφοδοτήσουν την σχεδιαστική διαδικασία του πλάνου θα παρουσιαστεί στην συγκεκριμένη έρευνα και πτυχιακή εργασία. Σε αυτό το πλάνο μπορούν να αναφέρονται ξεκάθαρα ο τρόπος με τον οποίο πραγματοποιήθηκε η συλλογή των πληροφοριών και πως τεκμηριώνονται μέσα στην μελέτη και εργασία.

Η έρευνα η οποία διεξήχθει στην συγκεκριμένη μελέτη, βοήθησε την φοιτήτρια στην κατανόηση του θέματος της πτυχιακής της εργασίας αλλά και στα καθημερινά γεγονότα που συνδέονται άμεσα με το θέμα που παραθέτει. Οι άνθρωποι διεξάγουν κάποια έρευνα για να συλλέξουν αποτελέσματα με ένα συστηματικό τρόπο, και επομένως να εμπλουτίσουν τις γνώσεις τους[48]. Κάθε ακαδημαϊκή έρευνα απαιτεί μια "*μεθοδολογία*" προκειμένου να αναλύσει τα αποτελέσματα.

[47] Saunders M., Lewis P. and Thornhill A., (2000), "Research Methods For Business Students", London: Prentice Hall.

[48] Saunders et all, (2005), "Specified ways for research and analysis of data", Prentice Hall.

Αυτή αποτελείται από τρόπους και μεθόδους παραγωγής και ανάλυσης δεδομένων έτσι ώστε οι διάφορες θεωρίες να δοκιμαστούν και να γίνουν αποδεκτές είτε να απορριφθούν. Επομένως η μεθοδολογία η οποία χαρακτηρίζεται ως πρωταρχική, σχετίζεται τόσο με την λεπτομερή έρευνα μέσω της οποίας συλλέγονται τα δεδομένα καθώς και με τις πιο γενικές φιλοσοφικές απόψεις. Ο τρόπος που σκεφτόμαστε σχετικά με την ανάπτυξη των γνώσεων μας, επηρεάζει σημαντικά τον τρόπο με τον οποίο διεξάγουμε την έρευνα[49].

3.1 *Συλλογή Δεδομένων*

Λόγω της βιβλιογραφικής και ερευνητικής φύσης της συγκεκριμένης εργασίας, ένα είδος μεθοδολογίας δευτερογενούς έρευνας χρησιμοποιείται για να οδηγήσει στα αποτελέσματα τα οποία επιθυμεί η φοιτήτρια. Ένας αριθμός μεθόδων εμπλέκεται, προκειμένου να την καταστήσει ικανή να επιτύχει μια μεγαλύτερη κατανόηση των πηγών που χρειάζεται για την ανάλυση των σκέψεων της σχετικά με το θέμα που ερευνά. Αυτό είναι αναγκαίο μέσα σε μια έρευνα και μελέτη, καθώς τα αποτελέσματα τα οποία συλλέγονται από μια συγκεκριμένη περιοχή μπορούν να είναι περισσότερο αποτελεσματικά από εκείνα που προέρχονται από κάπου αλλού. Κάθε μέθοδος συλλογής δεδομένων έχει τόσο πλεονεκτήματα όσο και μειονεκτήματα.

Ο συνδυασμός λοιπόν μεθόδων συλλογής πληροφοριών και δεδομένων, βοηθά σημαντικά στο να μειωθούν τα μειονεκτήματα που μπορούν να παρουσιαστούν στην έρευνα και τα οποία η συγγραφέας θέλει να ελαχιστοποιήσει. Βέβαια όπως θα αποδειχτεί και στην συνέχεια και όπως ήδη αναφέρθηκε παραπάνω, η έρευνα και μελέτη του συγκεκριμένου θέματος βασίζεται σε βιβλιογραφική έρευνα και συλλογής σχετικών στοιχείων για την λειτουργία της διαδικτυακής μηχανής αναζήτησης Google των επιθέσεων που έχει δεχθεί μέσω διαφόρων κακόβουλων ενεργειών που έχουν σημειωθεί σε αυτά τα χρόνια λειτουργίας.

3.2 *Δευτερεύων Δεδομένα*

Ως Δευτερεύων δεδομένα περιγράφονται εκείνα στα οποία οι πληροφορίες συλλέγονται και καταγράφονται από κάποιον άλλον νωρίτερα και για σκοπούς, οι οποίοι είναι διαφορετικοί από εκείνους του συγγραφέα[50]. Τα δευτερεύων δεδομένα παρέχουν την βάση για ένα καλό ιστορικό πληροφοριών, θέτοντας ικανή την συγγραφέα να καταλάβει το αντικείμενο εργασίας της καθώς και να παρέχουν σημαντικές πληροφορίες για στήριξη των θεωριών από την πρωταρχική έρευνα.

[49] Zikmund W.G., (2000), "Business Research Methods". London: Harcourt college publishers.

[50] Saunders M., Lewis P. and Thornhill A., 2000, "Research Methods For Business Students", London: Prentice Hall.

Είναι ευνόητο λοιπόν ότι μπορεί ευκολότερα κάποιος να βρει δευτερεύων δεδομένα για την έρευνα του, αφού αυτά έχουν γραφτεί προηγουμένως και έχουν εκδοθεί σε κάποια έντυπο τύπο ή στο διαδίκτυο. Τα περιοδικά και ο έντυπος τύπος είναι πρωταρχική φιλολογική πηγή για κάθε πληροφορία. Τα άρθρα σε αυτά είναι ικανοποιητικά προσβάσιμα και αναφέρονται σε ποικίλα θέματα της καθημερινότητας[51].

Επιπλέον τα βιβλία αλλά και τα άρθρα τα οποία χρησιμοποιήθηκαν σε αυτήν την συλλογή πληροφοριών και προτάσεων, παρείχαν πληροφορίες οι οποίες έδωσαν στην συγγραφέα την ευκαιρία να αναπτύξει αναλυτικά τις θέσεις της στην συγκεκριμένη έρευνα. Πάντα τα βιβλία αποτελούν μια αξιόπιστη μέθοδο συλλογής πληροφοριών, καθώς έχουν γραφτεί για ένα συγκεκριμένο σκοπό και παρέχουν συγκροτημένη σκέψη και ανάπτυξη αντικειμένου.

Το σημαντικότερο όμως πλεονέκτημα των δευτερογενών στοιχείων αφορά το μικρό κόστος και το σύντομο χρονικό διάστημα που απαιτείται για τη συλλογή τους. Αν οι πληροφορίες που απαιτούνται είναι διαθέσιμες με τη μορφή δευτερογενών στοιχείων, ο ερευνητής απλά χρειάζεται να προστρέξει στην πηγή τους, να τα εντοπίσει και να τα συγκεντρώσει. Αυτό συνήθως απαιτεί μικρό χρονικό διάστημα και μικρό κόστος.

Ακόμη και στην περίπτωση που υπάρχει κάποια χρέωση για τη χρήση τους, το κόστος είναι πολύ μικρότερο από αυτό που θα απαιτείτο για να συγκεντρώσει η εταιρεία τα στοιχεία αυτά. Πρέπει όμως να έχουμε υπόψη μας ότι όταν χρησιμοποιούνται δευτερογενή στοιχεία, είναι πολλές φορές αναγκαίο να γίνουν υποθέσεις και παραδοχές ώστε να καταστεί δυνατή η όσο αποτελεσματικότερη χρήση τους. Ο αποφασιστικός παράγοντας εδώ είναι η χρησιμοποίηση "λογικών" υποθέσεων και παραδοχών.

Μειονεκτήματα Δευτερογενών Δεδομένων

Παρά την σπουδαιότητα αλλά και την χρησιμότητα που παρουσιάζουν τα δευτερογενή δεδομένα στην διεκπεραίωση και συλλογή στοιχείων, εμφανίζουν τρία (3) σημαντικά προβλήματα :

- *Διαθεσιμότητα* : Για συγκεκριμένα προβλήματα είναι δυνατόν να μην υπάρχουν δευτερογενή δεδομένα
- *Ακρίβεια* : Ελλείψεις και μεθοδολογικές λεπτομέρειες που τις περισσότερες φορές δεν αναφέρονται καθόλου
- *Επάρκεια* : Μπορεί να υπάρχουν δευτερογενή δεδομένα τα οποία είναι διαθέσιμα και αρκετά ακριβή, αλλά να μην επαρκούν για να καλύψουν τις ανάγκες του συγγραφέα ή ερευνητή ενός θέματος

[51] Zikmund W.G., 2000, "Business Research Methods". London: Harcourt college publishers.

3.3 *Ανάλυση Δεδομένων*

Τα στοιχεία που συλλέγονται από την φοιτήτρια παράγουν ποιοτικά δεδομένα, τα οποία αναλύονται και επεξεργάζονται από το άτομο αυτό. Οι απαντήσεις που προσφέρονται σε αυτήν και σε συνδυασμό με τις πηγές που η ίδια έχει επιλέξει για να τεκμηριώσει την έρευνα της, θα την βοηθήσουν στην συνέχεια να εκτιμήσει σωστά τα γεγονότα και τις πηγές αυτές και να καταλήξει στα συμπεράσματα της.

Κεφάλαιο 4^{ο}

Η μηχανή Αναζήτησης της Google

Μηχανές αναζήτησης (search engines)

4.1 *Εισαγωγή στις μηχανές αναζήτησης*

Ένα από τα σημαντικότερα χαρακτηριστικά του διαδικτύου (Internet) είναι η ευκολία που παρέχει στην είσοδο οποιασδήποτε πληροφορίας, επιτρέποντας στους χρήστες του να εισάγουν στοιχεία για κάθε θέμα. Τα στοιχεία αυτά είναι συνήθως ελεύθερα διαθέσιμα σε όλους τους χρήστες, καθιστώντας έτσι το διαδίκτυο στο σύνολό του μία μοναδική πηγή πληροφόρησης και εύρεσης στοιχείων, που παρόμοια της δεν υπήρξε ποτέ μέχρι τώρα στην πορεία της ανθρωπότητας.

Η ραγδαία αύξηση της χρήσης του Παγκόσμιου Ιστού (World Wide Web), αλλά και των υπολοίπων υπηρεσιών του δικτύου, έδωσε στους χρήστες τη δυνατότητα να αποκτήσουν εύκολη πρόσβαση στην πληροφορία, αλλά παράλληλα και τη δυνατότητα παροχής στο δίκτυο όλων όσων αυτοί θεωρούν κατάλληλα. Ενώ όμως η πληθώρα πληροφοριών λογικά θα έπρεπε να είναι ευεργετική για τους χρήστες, οι οποίοι έχουν πλέον στη διάθεσή τους έναν τεράστιο όγκο στοιχείων, αυτή η ίδια πληθώρα προξενεί ένα σημαντικό πρόβλημα, που δεν είναι άλλο από το ότι οι χρήστες αδυνατούν τις περισσότερες φορές να εντοπίσουν τα σημεία εκείνα του δικτύου που περιέχουν τις πληροφορίες τις οποίες αυτοί χρειάζονται. Μολονότι όλο και κάποιον τρόπο μπορεί να σκεφτεί ένας χρήστης για να το επιτύχει, κανένας τρόπος δεν μπορεί να συγκριθεί σε πληρότητα, ταχύτητα και αποτελεσματικότητα με την χρήση των περίφημων μηχανών αναζήτησης (search engines) του Παγκόσμιου Ιστού.

Στο διαδίκτυο υπάρχουν αρκετές μηχανές αναζήτησης, οι οποίες τις περισσότερες φορές ξεκίνησαν από πειραματικά ερευνητικά προγράμματα (projects) και εξελίχθηκαν σε ολόκληρες εταιρείες, ενώ από πλευράς χρήσης εξυπηρετούν χιλιάδες χρήστες καθημερινά. Συνήθως, η παροχή των προσφερόμενων υπηρεσιών γίνεται δωρεάν, αν και ορισμένες μηχανές επιβάλλουν κάποιους περιορισμούς στη δωρεάν χρήση διαθέτοντας και πρόσβαση επί πληρωμή. Το τι είναι και πως ακριβώς λειτουργεί μία τέτοια μηχανή ακολουθεί παρακάτω.

Ορισμός της μηχανής αναζήτησης

Μια μηχανή αναζήτησης (search engine) θα μπορούσε να οριστεί ως το εργαλείο που επιτρέπει να εξερευνήσει κανείς τις βάσεις δεδομένων οι οποίες περιέχουν το κείμενο δεκάδων εκατομμυρίων ιστοσελίδων. Ένας άλλος ορισμός για τη μηχανή αναζήτησης είναι ότι είναι ένα πρόγραμμα. σχεδιασμένο ώστε να επιτρέπει τον εντοπισμό και την πρόσβαση σε αρχεία αποθηκευμένα σε έναν υπολογιστή, για παράδειγμα σε έναν κοινό διακομιστή (server) στο διαδίκτυο ή σε έναν άλλον, ανεξάρτητο και μεμονωμένο υπολογιστή.

Λειτουργίες της μηχανής αναζήτησης

Οι σημερινές μηχανές αναζήτησης δεν είναι κατασκευασμένες με τα ίδια μέτρα και σταθμά ούτε έχουν τις ίδιες ικανότητες. Εντούτοις, όλες ακολουθούν μερικά κοινά βήματα για την ανάκτηση της διαθέσιμης πληροφορίας μέσω διαδικτύου. Αυτά είναι τα παρακάτω:

Α) Οι μηχανές αναζήτησης “ψάχνουν” ιστοσελίδες διαθέσιμες στο διαδίκτυο και αποθηκεύουν πληροφορίες σχετικά με αυτές. Επιπλέον, χρησιμοποιούν προγράμματα, τα λεγόμενα “ρομπότ”, τα οποία είναι γνωστά και ως: “bots”, “robots”, “spiders”, “(web) crawlers”, “worms”, “intelligent agents”, “knowledge-bots”, “knowbots” ή “ants”. Τα ρομπότ “σερφάρουν” (surf) ή “έρπουν” (crawl) στο διαδίκτυο ακολουθώντας συνδέσμους (links) από μία ιστοσελίδα (webpage) στην επόμενη και συλλέγουν πληροφορίες, με βάση κάποια προκαθορισμένα κριτήρια (γνωστά ως αλγόριθμος), τις οποίες αποθηκεύουν στη βάση δεδομένων τους για ευρετηρίαση. Κάποιες φορές μια ιστοσελίδα αν και έχει εντοπιστεί από το ρομπότ μπορεί να μην έχει ευρετηριαστεί και δεν είναι διαθέσιμη για τους χρήστες μέχρι να συμβεί αυτό. Μια μηχανή αναζήτησης μπορεί να διαθέτει περισσότερα από ένα “ρομπότ”. Η λειτουργία αυτή πρέπει να επαναλαμβάνεται αδιάκοπα εξαιτίας της δυναμικής φύσης του διαδικτύου. Επομένως, το ρομπότ επιστρέφει στην ιστοσελίδα σε τακτά χρονικά διαστήματα (για παράδειγμα κάθε ένα ή δύο μήνες) προς αναζήτηση τυχόν αλλαγών. Όταν λοιπόν μια ιστοσελίδα αλλάζει, τότε η βάση της μηχανής ανανεώνεται με νέες πληροφορίες. Οι μηχανές αναζήτησης θα πρέπει να διαθέτουν ενημερωμένες βάσεις δεδομένων ώστε να παρουσιάσουν επίκαιρα αποτελέσματα και να είναι ανταγωνιστικές στην αντίστοιχη αγορά.

Β) Συλλέγουν, μέσω των ρομπότ, δεδομένα και τα αποθηκεύουν σε ευρετήρια (index) που βρίσκονται στη βάση δεδομένων της μηχανής αναζήτησης. Η πληροφορία που θα ευρετηριαστεί από τις ιστοσελίδες που εντοπίζονται εξαρτάται από το τι έχει καθοριστεί από κάθε μηχανή ως σημαντικό για το μηχανισμό λειτουργίας της (π.χ. URL, τίτλος, μέρος του πλήρους κειμένου). Από

τη στιγμή που η πληροφορία συμπεριλαμβάνεται στο ευρετήριο της μηχανής, τότε είναι και προσιτή στον χρήστη.

Γ) Επιτρέπουν στους χρήστες να ψάχνουν στη βάση δεδομένων τους μέσα από ένα περιβάλλον που παρέχει πολλαπλές δυνατότητες αναζήτησης. Η συγκεκριμένη λειτουργία έχει να κάνει με αυτό που αντιμετωπίζουν οι χρήστες μέσα από το περιβάλλον κάθε μηχανής αναζήτησης κατά τη διάρκεια υποβολής των ερωτημάτων τους σε αυτήν και κατά την ανάκτηση των σχετικών αποτελεσμάτων. Οι μηχανές αναζήτησης στην προσπάθειά τους να κερδίσουν ολοένα και περισσότερους χρήστες προσφέρουν γρήγορη αναζήτηση χωρίς να απαιτείται πρώτα μια επίσκεψη στη σελίδα τους. Αυτό το καταφέρνουν εν μέρει προσφέροντας μπάρες εργαλείων (toolbar), οι οποίες ενσωματώνονται στους δημοφιλείς, τουλάχιστον, πλοηγούς (Internet Explorer, Firefox).

Σύντομη ιστορική ανασκόπηση των μηχανών αναζήτησης

Από τα πρώτα βήματα του internet μέχρι το 1993 το FTP (File Transfer Protocol) ήταν ο πιο διαδεδομένος τρόπος ανταλλαγής αρχείων μεταξύ των χρηστών. Η 10^{η} Σεπτεμβρίου του 1990 έμελλε να είναι γνωστή ως η ημερομηνία εισαγωγής της έννοιας των μηχανών αναζήτησης στο Internet. Ο Peter Deutsch μαζί με τους Alan Emtage και Bill Heelan όλοι τους φοιτητές του πανεπιστημίου Mc Gill στον Καναδά ανήγγειλαν στο Usenet [Το USENET δημιουργήθηκε στα τέλη της δεκαετίας του 1970 (1979), ως ένα άτυπο μέσο διανομής ειδήσεων για το Λειτουργικό Σύστημα UNIX. Ήταν ειδικότερα κάτι σαν πίνακας ανακοινώσεων (bulletin board) μεταξύ δύο πανεπιστημίων στη Βόρεια Καλιφόρνια των Η.Π.Α.] τη λειτουργία του Archie, καλώντας τους χρήστες του δικτύου να το χρησιμοποιήσουν. Το Archie (συντομογραφία του Archiver, αρχειοθέτης) ήταν ένα σύστημα καταγραφής, σε καθημερινή βάση, των περισσοτέρων διακομιστών FTP που λειτουργούσαν, καθώς και των αρχείων που αυτοί περιλάμβαναν.

Το 1991 δημιουργήθηκε στο Πανεπιστήμιο της Μινεσότα από τους Mark Mc Cahill, Farhad Anklesaria, Paul Lindner, Dan Torrey, και Bob Alberti ένα νέο πρωτόκολλο, το Gopher (παραφθορά του “go for”, ήταν κάτι σαν το εμβρυακό στάδιο του Web), το οποίο χρησίμευε για την κατηγοριοποίηση και την παρουσίαση των εγγράφων ενός διακομιστή. Το 1992 στο Πανεπιστήμιο της Νεβάδα, αναπτύχθηκε από τους τους Steven Foster και Fred Barrie η Veronica (Very Easy Rodent-Oriented Net-wide Index to Computer Archives), μια μηχανή αναζήτησης που χρησιμοποιούσε το πρωτόκολλο Gopher. Σύντομα παρουσιάστηκε η η Jughead (Jonzy’s Universal Gopher Hierarchy Excavation and Display), μια άλλη μηχανή αναζήτησης που χρησιμοποιούσε και αυτή το Gopher.

Το 1994 ήταν η εποχή του WebCrawler, του πνευματικού παιδιού του Brian

Pinkerton, φοιτητή του Πανεπιστήμίου Ουάσινγκτον. Το WebCrawler ήταν η πρώτη μηχανή που κατέγραψε ολόκληρο το περιεχόμενο των σελίδων που επισκεπτόταν. Το 1995 έκανε την εμφάνισή του το Excite, δημιούργημα έξι φοιτητών του Πανεπιστημίου του Στάνφορντ, που βασίστηκε σε στατιστικές αναλύσεις σχετικές με τη συγγένεια των λέξεων.

Επόμενοι σταθμοί εξέλιξης αποτελούν οι μηχανές Lycos και AltaVista, με την πρώτη να καλύπτει τον εντυπωσιακά μεγάλο αριθμό σελίδων της εποχής (60 εκατ., 1996). Η AltaVista έμεινε γνωστή για τις αμείωτες επιδόσεις της, παρά τα εκατομμύρια των επισκεπτών που δεχόταν καθημερινά. Επιπρόσθετα το 1996, το MetaCrawler ήρθε να εισαγάγει την έννοια των μετα-μηχανών, δηλαδή, μηχανές σε ρόλο διαμεσολαβητή, οι οποίες μεταβιβάζουν τα ερωτήματα του χρήστη, σε πλήθος "πραγματικών" μηχανών αναζήτησης και επιστρέφουν τα συγκεντρωτικά αποτελέσματα. Το 1998, δύο φοιτητές του Στάνφορντ, οι οι Larry Page και Sergey Brin ανέτρεψαν τα δεδομένα και εφάρμοσαν ένα προηγμένο σύστημα αξιολόγησης των δικτυακών τόπων, τη μηχανή αναζήτησης Google.

4.2 *Η Μηχανή Αναζήτησης* **Google. Com**

"Η **Google** είναι μια από τις μεγαλύτερες εταιρίες δικτυακών υπηρεσιών. Η λειτουργία της ξεκίνησε τον Σεπτέμβριο του1998.Ο στόχος της είναι *να οργανώσει όλες τις πληροφορίες του κόσμου και να τις κάνει παγκόσμια διαθέσιμες*. Το Google ξεκίνησε σαν μια κολεγιακή εργασία από τον Λάρρυ Πέιτζ και τον Σεργκει Μπριν το 1996 για μια μηχανή αναζήτησης. Σήμερα η μηχανή αναζήτησης google είναι μια από τις δημοφιλέστερες, και οι φράσεις «*κάνω* ***google***», «*γκουγκλάρω*» και «*γκουγκλίζω*» είναι συνώνυμες με το «ψάχνω για πληροφορίες στο Διαδίκτυο.». Αντίστοιχα, στην αγγλική γλώσσα το ρήμα "***to google***" έχει αποκτήσει πλέον ταυτόσημη έννοια με το ρήμα «αναζητώ», και, πρόσφατα, το ίδιο ρήμα προστέθηκε στο αγγλικό λεξικό Merriam-Webster με όλα τα παράγωγά του (***to google*** > ***googling*** > ***googled***)."

Η ιστορία της Google είναι μία από αυτές τις λαμπρές ιστορίες που συνηθίζονται να γράφονται στα βιβλία και τα περιοδικά ως παραδείγματα προς μίμηση, ιδιαιτέρως από τους Managers των εταιρειών. Η Google ξεκινά την πορεία της το έτος 1999 με ιδρυτές δύο νεαρούς απόφοιτους του Πανεπιστημίου Stanford της Καλιφόρνια: τον Sergey Brin και τον Larry Page. Οι

δυο τους είχαν στα πλαίσια της διπλωματικής τους διατριβής αναπτύξει έναν αλγόριθμο αναζήτησης πληροφοριών στο διαδίκτυο που δεν είχε καμία σχέση με αυτούς που χρησιμοποιούνταν ήδη, π.χ. τους αλγόριθμους που εφάρμοζαν οι μηχανές αναζήτησης της Yahoo και της MSN[52].

Οι ηλεκτρονικές αυτές πύλες είχαν αρχικά οργανώσει τις πληροφορίες του διαδικτύου σε θεματικές ενότητες (π.χ. πολιτική, οικονομία, αθλητικά, εκπαίδευση κλπ.) στις οποίες ο χρήστης μπορούσε κατά βούληση να περιηγηθεί μέχρις ότου έβρισκε αυτό που τον ενδιέφερε. Αργότερα, ανέπτυξαν έναν αλγόριθμο αναζήτησης με βάση την λέξη-κλειδί που έδινε κάθε φορά ο χρήστης (π.χ Alta Vista). Το πρόβλημα ωστόσο ήταν ότι πολλές ιστοσελίδες επαναλάμβαναν επίτηδες πολύ συχνά αυτές τις λέξεις-κλειδιά στο περιεχόμενο τους με αποτέλεσμα ο χρήστης να κατευθύνεται τις περισσότερες φορές σε σελίδες άσχετες με το αρχικό αντικείμενο αναζήτησης του.

Ο αλγόριθμος "***PageRank***" που ανέπτυξαν ο Sergey Brin και ο Larry Page εφάρμοζε σε αντίθεση με όλα τα παραπάνω, ένα σύστημα αυτόματης αναζήτησης της λέξης-κλειδιού του χρήστη με βάση ένα σύστημα ψήφων (votes) που αξιολογούσε (α) την αξιοπιστία της ιστοσελίδας και (β) την σχετικότητα του περιεχομένου ως προς το αρχικό αντικείμενο αναζήτησης. Το 1999, με κεφάλαια που άντλησαν από venture capitalists, οι δύο νέοι έθεσαν σε εμπορική εφαρμογή τον αλγόριθμό τους, ιδρύοντας την Google. Η αποστολή της Google όπως την διατύπωσαν οι ιδρυτές της ήταν η οργάνωση των πληροφοριών του παγκόσμιου ιστού κατά τρόπο που να είναι χρήσιμος για τους ανθρώπους[53].

- **Googleplex**

Το Googleplex είναι η κεφαλή της Google, αφού όλες οι λειτουργίες της μηχανής αναζήτησης εμπνέονται και υλοποιούνται μέσα σ' αυτό το κτίριο.

Το όνομα έχει διπλό συμβολισμό:

1. αποτελεί λογοπαίγνιο της αγγλικής μονάδας μέτρησης ***googol***(10^{googol})
2. είναι συνθετικό των λέξεων ***Google*** και ***complex*** (=συγκρότημα), σε μια πιο γλωσσολογική ερμηνεία.

Το καινούργιο κτίριο που παραδόθηκε στην Google ειδικά διαμορφωμένο για τις ανάγκες της εταιρείας, είναι το δεύτερο μεγαλύτερο κτίριο της Νέας Υόρκης.Οι συνθήκες εργασίας χαρακτηρίζονται από τις καλύτερες που έχουν εφαρμοστεί σε εταιρείες, αφού η Google έχει προνοήσει για όλες τις ανάγκες των εργαζομένων, όπως είναι η ξεκούραση, τα τακτικά διαλείμματα

[52] Eisenmann T.R. and Herman K., (2006), "*Google Inc.*", Harvard Business review.

[53] www.google.com, 2010.

σε ειδικά διαμορφωμένους χώρους ή ακόμη και η ύπαρξη παιδότοπου για την φύλαξη των παιδιών των εργαζομένων.

- ***Υπηρεσίες της Google***
  - Google Search - Αναζήτηση
  - iGoogle - Προσωπική Σελίδα
  - Google Images - Αναζήτηση Εικόνων
  - Google Video - Αναζήτηση Βίντεο
  - Google Maps - Αναζήτηση Χαρτών
  - Google News - Αναζήτηση Ειδήσεων
  - Google Products Search - Αναζήτηση Προϊόντων προς πώληση
  - Google Blog Search - Αναζήτηση σε Blogs.
  - Google Book Search - Αναζήτηση Βιβλίων
  - Google Scholar - Αναζήτηση Μελετών
  - Special Search Αναζήτηση σε ειδικά θέματα
  - Search Features - Βρες βιβλία, ταινίες, μουσική και άλλα
  - Google Patents - Αναζήτηση Ευρεσιτεχνιών
  - Google Finance - Υπηρεσία πληροφόρησης οικονομικών νέων και ζωντανή μετάδοση του χρηματιστηρίου
  - Google Alerts - Υπηρεσία ειδοποιήσεων.
  - Google Toolbar - Πρόσθετο αναζήτησης στον browser
  - Google Desktop - Αναζήτηση στον υπολογιστή
  - Google Earth - Προβολή του πλανήτη από δορυφορικές εικόνες

Υπηρεσίες Επικοινωνίας

- Google Gmail - Υπηρεσία Ηλεκτρονικού Ταχυδρομείου
- Google Groups - Συζητήσεις διαφόρων θεμάτων
- Google Calendar - Ημερολόγιο
- Google Reader - Υπηρεσία εύκολης παρακολούθησης ιστοσελίδων
- Google Notebook - Σημειωματάριο
- Google Docs - Δημιουργος εγγράφων και υπολογιστικών φύλλων
- Blogger - Δωρεάν Δημιουργός Ιστολόγιου (blog)
- YouTube - Χώρος προβολής βίντεο
- Google Talk - Instant Messenger

- Google Sites - Google sites(δημιουργία ιστότοπου)
- Google Wave - Google Wave - Συνδυασμένη υπηρεσία επικοινωνίας και δικτύωσης

Υπηρεσίες Διαφημίσεων

- Google AdSense - Υπηρεσία παροχής διαφημίσεων σε ιδιοκτήτες ιστοσελίδων επί πληρωμή.

- **Η ΦΙΛΟΣΟΦΙΑ ΤΗΣ GOOGLE**

«Η τέλεια μηχανή αναζήτησης», όπως λέει ο Larry Page, συνιδρυτής της Google, «θα καταλάβαινε ακριβώς τι εννοείτε και θα σας έδινε ακριβώς αυτό που θέλετε». Όταν ξεκίνησε η Google, θα αποτελούσε ευχάριστη έκπληξη αν πληκτρολογούσατε ένα ερώτημα αναζήτησης και βρίσκατε αμέσως τη σωστή απάντηση. Η Google πέτυχε ακριβώς επειδή ήμασταν καλύτεροι και ταχύτεροι στην ανεύρεση της σωστής απάντησης σε σχέση με άλλες μηχανές αναζήτησης εκείνης της εποχής.

Όμως η τεχνολογία έχει προοδεύσει πολύ από τότε και το πρόσωπο του ιστού έχει αλλάξει. Αναγνωρίζοντας ότι η αναζήτηση είναι ένα πρόβλημα το οποίο δε θα λυθεί ποτέ, συνεχίζουμε να εξαντλούμε τα όρια της υπάρχουσας τεχνολογίας για να προσφέρουμε μια εύχρηστη υπηρεσία με ταχύτητα και ακρίβεια, στην οποία να έχει πρόσβαση οποιοσδήποτε αναζητά πληροφορίες, είτε βρίσκεται σε ένα γραφείο στη Βοστώνη ή σε ένα τηλέφωνο στην Μπανγκόκ. Χρησιμοποιήσαμε επίσης τα μαθήματα που πήραμε από την αναζήτηση για να αντιμετωπίσουμε ακόμα περισσότερες προκλήσεις.

Καθώς διατηρούμε το βλέμμα μας προς το μέλλον, αυτές οι βασικές αρχές καθοδηγούν τις πράξεις μας.

Δέκα πράγματα που διαπίστωσε η Google ότι είναι αλήθεια

1. **Εστιάστε στον χρήστη και όλα τα υπόλοιπα θα ακολουθήσουν μόνα τους.**

Από το ξεκίνημά μας, επικεντρωθήκαμε στην παροχή της καλύτερης δυνατής εμπειρίας για τους χρήστες. Είτε σχεδιάζουμε ένα νέο πρόγραμμα περιήγησης στο Internet ή μια νέα τροποποίηση της εμφάνισης της αρχικής σελίδας, φροντίζουμε πάντα να εξασφαλίζουμε ότι τελικά θα εξυπηρετήστε **εσείς** και όχι κάποιος δικός μας εσωτερικός στόχος ή ο απώτερος μας σκοπός. Η διεπαφή της αρχικής μας σελίδας είναι ξεκάθαρη και απλή και οι σελίδες φορτώνουν άμεσα. Η συμπερίληψη στα αποτελέσματα αναζήτησης δεν αποτέλεσε ποτέ εμπορεύσιμο είδος και η

διαφήμιση δεν σημειώνεται απλά με ξεκάθαρο τρόπο, αλλά προσφέρει σχετικό περιεχόμενο και δεν ενοχλεί. Και όταν δημιουργούμε νέα εργαλεία και εφαρμογές, πιστεύουμε ότι θα πρέπει να λειτουργούν τόσο καλά, ώστε να μη χρειάζεται να σκέφτεστε πως θα μπορούσαν να είχαν σχεδιαστεί διαφορετικά.

2. Είναι καλύτερο να κάνεις ένα πράγμα καλά, πάρα πολύ καλά.

Όντως αναζητάμε. Με μία από τις μεγαλύτερες ερευνητικές ομάδες παγκοσμίως να επικεντρώνεται αποκλειστικά στην επίλυση προβλημάτων αναζήτησης, γνωρίζουμε τι μπορούμε να κάνουμε καλά και πώς μπορούμε να το κάνουμε καλύτερα. Με συνεχείς επαναληπτικές διαδικασίες για δύσκολα προβλήματα, μπορέσαμε να επιλύσουμε περίπλοκα ζητήματα και να παρέχουμε συνεχείς βελτιώσεις για μια υπηρεσία που ήδη καθιστά την ανεύρεση πληροφοριών μια γρήγορη και ομαλή εμπειρία για εκατομμύρια ανθρώπους. Η αφοσίωσή μας στη βελτίωση της αναζήτησης μάς επέτρεψε επίσης να εφαρμόσουμε ό,τι έχουμε μάθει σε νέα προϊόντα, όπως το Gmail και οι Χάρτες Google. Η ελπίδα μας είναι να φέρουμε την ισχύ της αναζήτησης σε ανεξερεύνητες, έως τώρα, περιοχές και να βοηθήσουμε τους ανθρώπους να αποκτήσουν πρόσβαση και να χρησιμοποιούν ακόμα μεγαλύτερο μέρος των πληροφοριών που δε σταματούν να συσσωρεύονται στη ζωή τους.

3. Το γρήγορο είναι καλύτερο από το αργό.

Γνωρίζουμε ότι ο χρόνος σας είναι πολύτιμος, άρα όποτε αναζητάτε μια απάντηση στον ιστό την θέλετε αμέσως και σκοπός μας είναι να σας ικανοποιούμε. Μπορεί να είμαστε οι μόνοι άνθρωποι στον κόσμο που μπορούμε να πούμε ότι ο σκοπός μας είναι ο κόσμος να φεύγει από την αρχική μας σελίδα όσο το δυνατόν πιο γρήγορα. Αφαιρώντας περισσευούμενα δεδομένα από τις σελίδες μας και αυξάνοντας την αποτελεσματικότητα του περιβάλλοντος εμφάνισης των αποτελεσμάτων, η Google έχει σπάσει επανειλημμένα τα ίδια της τα ρεκόρ ταχύτητας, έτσι ώστε ο μέσος χρόνος απόκρισης για ένα αποτέλεσμα αναζήτησης να είναι ένα κλάσμα δευτερολέπτου. Έχουμε πάντοτε κατά νου την ταχύτητα με κάθε νέο προϊόν που κυκλοφορούμε, είτε είναι μια εφαρμογή για κινητά ή το Google Chrome, ένα πρόγραμμα περιήγησης το οποίο είναι σχεδιασμένο να είναι αρκετά γρήγορο για τον σύγχρονο ιστό. Και συνεχίζουμε να εργαζόμαστε για να τα κάνουμε όλα να λειτουργούν ακόμα ταχύτερα.

4. Η δημοκρατία στο Διαδίκτυο δουλεύει.

Η αναζήτηση Google λειτουργεί επειδή βασίζεται σε εκατομμύρια χρήστες που δημοσιεύουν συνδέσμους σε ιστοτόπους για να καθορίσει ποιοι άλλοι ιστότοποι προσφέρουν αξιόλογο περιεχόμενο. Εκτιμούμε τη σημασία κάθε ιστοσελίδας χρησιμοποιώντας πάνω από 200 σήματα και

μια πληθώρα τεχνικών, συμπεριλαμβανομένου του κατοχυρωμένου αλγόριθμού μας Κατάταξη σελίδας, ο οποίος αναλύει ποιοι ιστότοποι έχουν "ψηφιστεί" ως οι καλύτερες πηγές πληροφοριών από άλλες σελίδες του ιστού. Καθώς ο ιστός μεγαλώνει, η προσέγγιση αυτή βελτιώνεται μάλιστα, καθώς κάθε νέος ιστότοπος αποτελεί ένα ακόμα σημείο πληροφοριών και άλλη μια ψήφος που προσμετράται. Με την ίδια λογική, ασχολούμαστε ενεργά με την ανάπτυξη λογισμικού ανοικτού κώδικα, όπου η καινοτομία συντελείται μέσω της συλλογικής προσπάθειας πολλών προγραμματιστών.

5. Δεν είναι ανάγκη να βρίσκεστε στο γραφείο σας για να χρειαστείτε απαντήσεις.

Ο κόσμος μας βρίσκεται όλο και περισσότερο εν κινήσει: όλοι θέλουν πρόσβαση σε πληροφορίες όπου και αν είναι, όποτε τις χρειάζονται. Εμείς πρωτοπορούμε με νέες τεχνολογίες και προσφέρουμε νέες λύσεις για κινητές υπηρεσίες οι οποίες βοηθούν ανθρώπους από όλο τον κόσμο να κάνουν αναρίθμητες εργασίες στο τηλέφωνό τους, από τον έλεγχο μηνυμάτων ηλεκτρονικού ταχυδρομείου και συμβάντων στο ημερολόγιο μέχρι την παρακολούθηση βίντεο και την πρόσβαση με αρκετούς διαφορετικούς τρόπους στην Αναζήτηση Google μέσω τηλεφώνου. Επιπλέον, ελπίζουμε να προωθήσουμε ακόμα περισσότερο την καινοτομία για τους απανταχού χρήστες κινητών με το Android, μια ελεύθερη πλατφόρμα ανοικτού κώδικα για κινητά. Το Android φέρνει τον ανοιχτό σχεδιασμό που διαμόρφωσε το Διαδίκτυο στον κόσμο των κινητών. Το Android δεν ωφελεί μόνο τους καταναλωτές, οι οποίοι έχουν περισσότερες επιλογές και νέες, πρωτότυπες εμπειρίες στο κινητό τους, αλλά ανοίγει ευκαιρίες αποκόμισης εσόδων για τις εταιρίες τηλεφωνίας, τους κατασκευαστές και τους προγραμματιστές.

6. Μπορείς να βγάλεις χρήματα χωρίς παρανομίες.

Η Google είναι μια επιχείρηση. Τα έσοδα που αποκομίζουμε προέρχονται από την προσφορά τεχνολογίας αναζήτησης σε εταιρείες και από τις πωλήσεις διαφημίσεων που εμφανίζονται στον ιστότοπό μας και σε άλλους ιστοτόπους στον ιστό. Εκατοντάδες χιλιάδες διαφημιστές παγκοσμίως χρησιμοποιούν το πρόγραμμα AdWords για να προωθήσουν τα προϊόντα τους εκατοντάδες χιλιάδες εκδότες εκμεταλλεύονται το πρόγραμμα AdSense για να προσφέρουν διαφημίσεις που είναι σχετικές με το περιεχόμενο των ιστοτόπων τους. Για να εξασφαλίσουμε την τελική εξυπηρέτηση όλων μας των χρηστών (είτε είναι διαφημιστές, είτε όχι), έχουμε ένα σύνολο αρχών, οι οποίες διέπουν τα διαφημιστικά προγράμματά μας και τις διαφημιστικές πρακτικές μας:

- Δεν επιτρέπουμε την εμφάνιση διαφημίσεων στις σελίδες αποτελεσμάτων εκτός και αν είναι σχετικές με το σημείο όπου εμφανίζονται. Και πιστεύουμε ακράδαντα ότι οι διαφημίσεις

μπορούν να παρέχουν χρήσιμες πληροφορίες αν, και μόνο αν, είναι σχετικές με ό,τι θέλετε να βρείτε - άρα είναι πιθανό ορισμένες αναζητήσεις να μην οδηγήσουν σε καμία διαφήμιση.

- Πιστεύουμε ότι η διαφήμιση μπορεί να είναι αποτελεσματική χωρίς να γίνεται υπερβολική. Δεν δεχόμαστε διαφημίσεις μέσω αναδυόμενων παραθύρων, τα οποία σας εμποδίζουν να δείτε το περιεχόμενο που ζητήσατε. Διαπιστώσαμε ότι οι διαφημίσεις κειμένου οι οποίες αφορούν το άτομο που τις διαβάζει, εξασφαλίζουν πολύ μεγαλύτερη αναλογία κλικ/εμφανίσεων από τις διαφημίσεις που εμφανίζονται τυχαία. Κάθε διαφημιστής, είτε μικρός, είτε μεγάλος, μπορεί να επωφεληθεί από αυτό το άκρως στοχοποιημένο μέσο.
- Η διαφήμιση στο Google φέρει πάντα την επισήμανση "Σύνδεσμοι διαφημιζομένων", έτσι ώστε να μην υπονομεύει την ακεραιότητα των αποτελεσμάτων αναζήτησης που προσφέρουμε. Δεν αλλοιώνουμε ποτέ τις κατατάξεις για να τοποθετούμε τους συνεργάτες μας πιο ψηλά στα αποτελέσματα αναζήτησης και κανένας δεν μπορεί να αγοράσει καλύτερη Κατάταξη σελίδας. Οι χρήστες μας εμπιστεύονται την αντικειμενικότητά μας και τα βραχυπρόθεσμα κέρδη δεν θα μπορούσαν ποτέ να δικαιολογήσουν την καταπάτηση της εμπιστοσύνης τους
-

7. Υπάρχουν πάντα άπειρες πληροφορίες εκεί έξω.

Αφού πλέον είχαμε καταφέρει την ευρετηριοποίηση περισσότερων σελίδων HTML στο Διαδίκτυο σε σχέση με οποιαδήποτε άλλη υπηρεσία αναζήτησης, οι μηχανικοί μας έστρεψαν την προσοχή τους σε πληροφορίες που δεν ήταν εύκολα και άμεσα διαθέσιμες. Ορισμένες φορές αρκούσε η ενσωμάτωση νέων βάσεων δεδομένων, όπως η προσθήκη αναζήτησης τηλεφωνικών αριθμών και διευθύνσεων, και επιχειρηματικών καταλόγων. Άλλες προσπάθειές μας χρειάστηκαν λίγο περισσότερη δημιουργικότητα, όπως την προσθήκη ικανότητας αναζήτησης σε αρχειοθετημένες ειδήσεις, ευρεσιτεχνίες, ακαδημαϊκές περιοδικές εκδόσεις, δισεκατομμύρια εικόνες και εκατομμύρια βιβλία. Και οι ερευνητές μας συνεχίζουν να εξετάζουν τρόπους για τη διάθεση όλων των πληροφοριών του κόσμου σε χρήστες που ψάχνουν για απαντήσεις.

8. Η ανάγκη για πληροφορίες υπερβαίνει κάθε σύνορο.

Η εταιρία μας ιδρύθηκε στην Καλιφόρνια, αλλά η αποστολή μας είναι να διευκολύνουμε την πρόσβαση στην πληροφορία για ολόκληρο τον κόσμο και σε κάθε γλώσσα. Για να το πετύχουμε αυτό, έχουμε γραφεία σε δεκάδες χώρες, διατηρούμε πάνω από 150 τομείς του Διαδικτύου και παραδίδουμε περισσότερα από τα μισά αποτελέσματά μας σε χρήστες που ζουν εκτός των Ηνωμένων Πολιτειών. Η διεπαφή αναζήτηση του Google προσφέρεται σε πάνω από 110 γλώσσες, προσφέρει στον κόσμο την δυνατότητα να περιορίζει τα αποτελέσματα σε περιεχόμενο το οποίο

είναι γραμμένο στη γλώσσα του και στοχεύει στην παροχή των υπόλοιπων εφαρμογών και προϊόντων σε όσο το δυνατόν περισσότερες γλώσσες. Χρησιμοποιώντας τα μεταφραστικά μας εργαλεία, οι χρήστες μπορούν να ανακαλύψουν περιεχόμενο που έχει γραφτεί στην άλλη άκρη του κόσμου, σε γλώσσες που δεν γνωρίζουν. Με τα εργαλεία αυτά και τη βοήθεια εθελοντών μεταφραστών, μπορέσαμε να βελτιώσουμε σε μεγάλο βαθμό και την ποικιλία και την ποιότητα των υπηρεσιών που μπορούμε να προσφέρουμε, ακόμα και στις πιο απόμακρες γωνιές της υφηλίου.

9. Μπορείς να είσαι σοβαρός και χωρίς κουστούμι.

Οι ιδρυτές μας έχτισαν την Google με την ιδέα ότι η δουλειά πρέπει να προσφέρει πρόκληση και ότι η πρόκληση πρέπει να είναι διασκέδαση. Πιστεύουμε ότι σπουδαία, δημιουργικά πράγματα είναι πιθανότερο να συμβούν όταν υπάρχει η κατάλληλη εταιρική κουλτούρα - και αυτό δεν περιορίζεται σε μεταμοντέρνες λάμπες και λαστιχένιες μπάλες. Δίνουμε έμφαση σε ομαδικά επιτεύγματα και υπερηφανευόμαστε για ατομικά κατορθώματα τα οποία συνεισφέρουν στη συνολική μας επιτυχία. Βασιζόμαστε πολύ στους υπαλλήλούς μας - δραστήρια, παθιασμένα άτομα με πείρα σε διάφορους τομείς και δημιουργική προσέγγιση στη δουλειά, στο παιχνίδι και στη ζωή. Η ατμόσφαιρά μας μπορεί να είναι άνετη, αλλά όταν προκύπτουν νέες ιδέες στην ουρά της καφετέριας, σε ένα ομαδικό μήτινγκ ή στο γυμναστήριο, ανταλλάσσονται, δοκιμάζονται και πραγματοποιούνται με ιλιγγιώδη ταχύτητα. Οι ιδέες αυτές μπορεί τελικά να αποτελέσουν την βάση ενός νέου έργου το οποίο προορίζεται για παγκόσμια χρήση.

10. Το εξαιρετικό δεν είναι αρκετό.

Θεωρούμε ότι το να είναι κανείς πολύ καλός σε κάτι αποτελεί μια αφετηρία, όχι τον τερματισμό. Θέτουμε στόχους για τους εαυτούς μας τους οποίους γνωρίζουμε ότι δεν μπορούμε να φθάσουμε ακόμα, επειδή γνωρίζουμε ότι στην προσπάθειά μας να τους επιτύχουμε θα προχωρήσουμε περισσότερο από όσο περιμέναμε. Χρησιμοποιούμε την καινοτομία και την επανάληψη, με σκοπό να πάρουμε κάτι που λειτουργεί καλά και να το βελτιώσουμε με απρόσμενους τρόπους. Για παράδειγμα, όταν ένας από τους μηχανικούς λογισμικού μας παρατήρησε ότι η αναζήτηση λειτουργούσε καλά για ορθογραφημένες λέξεις, αναρωτήθηκε πόσο καλά μπορούσε να αντιμετωπίσει τα ορθογραφικά λάθη. Αυτό τον οδήγησε να δημιουργήσει έναν εύχρηστο και πιο χρήσιμο ορθογραφικό έλεγχο.

4.3 *Η Εξαιρετική Στρατηγική Πορεία της Google Com*

Με την ίδρυση της εταιρίας Google το 1999, δημιουργείται μια νέα, δυναμική και πολλά υποσχόμενη αγορά μέσα στην ευρύτερη αγορά των εταιριών λογισμικού, πληροφορικής και διαδικτύου αυτή των μηχανών αναζήτησης. Με τον πρωτοποριακό αλγόριθμο "***PageRank***", η αναζήτηση πληροφοριών στο διαδίκτυο μπήκε σε μια νέα βάση και δημιούργησε σοβαρές προοπτικές εμπορικής εκμετάλλευσης αξιοποιώντας τα σημαντικά πλεονεκτήματα του νέου αυτού αλγορίθμου τα οποία και θα αναλυθούν στην συνέχεια.

Έτσι ενώ εταιρίες όπως η Yahoo! Και η MSN, οι οποίες διέθεταν ηλεκτρονικές πύλες στο διαδίκτυο (portals), παρείχαν μηχανές αναζήτησης μόνο ως μια επιπλέον εφαρμογή αυτών των πυλών, η Google τοποθετήθηκε στην αγορά προσφέροντας μία και μόνο υπηρεσία: αξιόπιστη αναζήτηση στο διαδίκτυο. Η Google δεν είχε έγχρωμη ιστοσελίδα γεμάτη διαφημίσεις και άλλες καταχωρήσεις, δεν είχε ηλεκτρονική πύλη στο διαδίκτυο ούτε πλήθος εφαρμογών και εργαλείων. Είχε μια απλή μόνο ιστοσελίδα που προσέφερε άμεση και αξιόπιστη αναζήτηση πληροφοριών στο διαδίκτυο[54].

Αν και αυτό σχολιάστηκε από πολλούς, στην πραγματικότητα η Google έδειχνε να έχει καταλάβει καλά τους κρίσιμους παράγοντες-κλειδιά για την επιτυχία στην συγκεκριμένη αγορά καθώς και για την σωστή λειτουργία του Operation Management σε αυτήν. Οι λόγοι αυτοί ήταν :

- *Ταχύτητα αναζήτησης πληροφοριών*
- *Εύρος αναζήτησης*
- *Αποτελεσματικότητα αναζήτησης (σχετικότητα λέξης-κλειδιού και αποτελέσματος)*
- *Φιλικότητα προς τον χρήστη*

Όσο και αν ακούγεται απίστευτο, μέσα σε μόλις ένα χρόνο από την έναρξη της λειτουργίας της η Google είδε τα έσοδα της να σκαρφαλώνουν από τα 0.2 στα 19.1 εκατ. Δολάρια. Η Google είχε πλέον αρχίσει να γράφει την δική της ιστορία και να αποτελεί απειλή για εταιρίες του μεγέθους της Yahoo!, Microsoft κλπ. Η επιτυχία της Google μπορεί να αποδοθεί στην αποτελεσματικότητα της στρατηγικής της η οποία θα αναλυθεί παρακάτω σε συνδυασμό με το εξωτερικό περιβάλλον της εταιρίας. Ως Operation Manager, θα πρέπει να λάβουμε υπ' όψιν το συγκεκριμένο παράδειγμα της εταιρείας Google Inc. και να αναλύσουμε τις θεωρίες πάνω στις οποίες στηρίχθηκε για να επιτύχει την συγκεκριμένη στρατηγική αλλά και την εξαιρετική πορεία της εντός του διαδικτύου[55].

Το Εξωτερικό Περιβάλλον : Ανάλυση PEST

[54] Eisenmann T.R. and Herman K., (2006), "*Google Inc.*", Harvard Business review.

[55] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.

Πολιτικό & Νομικό Περιβάλλον

Η Google έχει την έδρα της στην Καλιφόρνια, την μεγαλύτερη πολιτεία των ΗΠΑ. Οι Η.Π.Α χαρακτηρίζονται από πολιτική σταθερότητα και το πολιτικό τους σύστημα είναι αυτό της προεδρευόμενης κοινοβουλευτικής δημοκρατίας. Η νομοθετική εξουσία ανήκει στο Κογκρέσο (Congress) και η δικαστική ασκείται από το Ανώτατο Δικαστήριο των Η.Π.Α (Supreme Court) και τα επιμέρους δικαστήρια. Οι συνθήκες αυτές δημιουργούν ένα περιβάλλον ευνοϊκό στις επενδύσεις και στην επιχειρηματικότητα.

Οικονομικό Περιβάλλον

Η οικονομία των Η.Π.Α είναι μια ανεπτυγμένη καπιταλιστική οικονομία με χαμηλά επίπεδα πληθωρισμού και ανεργίας, υψηλό κατά κεφαλή ΑΕΠ, σημαντικές εξαγωγές πρώτων υλών και πετρελαίου καθώς και ανεπτυγμένο δευτερογενή και τριτογενή τομέα παραγωγής. Αν και τον τελευταίο χρόνο η οικονομία των ΗΠΑ έχει κλονιστεί από την κρίση των ενυπόθηκων δανείων υψηλού ρίσκου (subprime loans) και την κατακόρυφη πτώση του δολαρίου, εντούτοις, θα μπορούσε κανείς να πει ότι ευνοεί τις εγχώριες και ξένες επενδύσεις και την ανάπτυξη επιχειρηματικών πρωτοβουλιών.

Κοινωνικό Περιβάλλον

Οι Η.Π.Α αποτελούν ένα πολυ-πολιτισμικό και ανομοιογενές κοινωνικό περιβάλλον αποτελούμενο από Αφρο-Αμερικανούς, Ευρωπαίους, Κινέζους κλπ. Στις Η.Π.Α συνυπάρχουν πολλές κουλτούρες (κυρίαρχη αυτή του δυτικού πολιτισμού), θρησκείες και έθιμα-παραδόσεις. Επίσημη γλώσσα είναι η Αγγλική.

Τεχνολογικό Περιβάλλον

Οι Η.Π.Α διακρίνονται για το επίπεδο ανάπτυξης της τεχνολογίας τους σε όλους τους τομείς όπως ιατρική, βιομηχανία, τηλεπικοινωνίες κλπ. Επίσης υπάρχουν ανεπτυγμένες υποδομές τηλεπικοινωνιών (τηλεφωνία, διαδίκτυο κλπ.), μεταφορών (δρόμοι, αεροδρόμια, λιμάνια, σιδηρόδρομοι), υγείας (κλινικές, νοσοκομεία κλπ.) κοκ. Επίσης η εξοικείωση των πολιτών με το Internet είναι πολύ μεγάλη με ένα μεγάλο ποσοστό των συνολικών χρηστών να το χρησιμοποιούν καθημερινά για την εργασία, τις αγορές τους κλπ.

Το Ανταγωνιστικό Περιβάλλον: Ανάλυση Porter

Για την αξιολόγηση του ανταγωνιστικού περιβάλλοντος της εταιρίας θα χρησιμοποιήσουμε τη γνωστή ανάλυση Porter (Μήτρα 5 δυνάμεων του Porter).

Διαπραγματευτική ισχύς των πελατών

Οι παράγοντες εκείνοι που επηρεάζουν την διαπραγματευτική ισχύ των πελατών είναι σε γενικές γραμμές οι εξής :

- Το μέγεθος της πελατειακής βάσης

- Η αξία των αγορών συνολικά και ανά πελάτη

- Η ύπαρξη υποκατάστατων προϊόντων στην αγορά

- Ο βαθμός ελαστικότητας ζήτησης του προϊόντος ως προς την τιμή

- Το κόστος αλλαγής των πελατών (switching cost)

Στην περίπτωση της Google η διαπραγματευτική ισχύς των πελατών είναι θα έλεγε κανείς αρκετά περιορισμένη δεδομένου ότι :

- Ο αριθμός των χρηστών είναι τεράστιος ενώ ο αριθμός των «χορηγών» από τους οποίους η Google εισπράττει τα έσοδα της, είναι επίσης πολύ μεγάλος

- Υπάρχει τεράστια γεωγραφική διασπορά των πελατών

- Υποκατάστατο των μηχανών αναζήτησης ουσιαστικά δεν μπορεί να υπάρξει σήμερα. Παλιότερα υπήρχαν έντυποι κατάλογοι όλων των ιστοσελίδων του διαδικτύου αλλά πλέον αυτό είναι αντι-οικονομικό

- Η υπηρεσία της Google είναι δωρεάν για τον χρήστη και έχει ένα σχετικά μικρό κόστος για τον «χορηγό» (σύνδεσμος χορηγών)

Διαπραγματευτική ισχύς των προμηθευτών

Όσον αφορά την διαπραγματευτική ισχύ των προμηθευτών αυτή θα μπορούσε να πει κανείς ότι εξαρτάται από παράγοντες όπως[56]:

- *το μέγεθος της προμηθευτικής αλυσίδας*
- *την αξία αγορών ανά προμηθευτή*
- *το κόστος αλλαγής προμηθευτή (switching cost)*
- *την κάθετη ολοκλήρωση των προμηθευτών (προς την πλευρά της κατανάλωσης) κλπ.*

Στην περίπτωση της υπηρεσίας της Google δεν υπάρχει ουσιαστικά προμηθευτής αφού η εταιρία δεν μεταπωλεί κανένα προϊόν ή υπηρεσία. Αντίθετα αυτό που κάνει είναι να οργανώνει τις ήδη υπάρχουσες πληροφορίες στο διαδίκτυο και να τις κάνει χρήσιμες για όλο τον κόσμο.

Κίνδυνος από υποκατάστατα προϊόντα

Ο κίνδυνος από υποκατάστατα προϊόντα σχετίζεται αφενός με την ύπαρξη υποκατάστατων προϊόντων και υπηρεσιών, τον βαθμό αποτελεσματικότητας τους στην υποκατάσταση της σχετικής ανάγκης, την διαφορά ως προς την τιμή, το κόστος αλλαγής του πελάτη κλπ. Όπως αναφέρθηκε και παραπάνω σήμερα δεν υπάρχει κάποιο υποκάταστατο των μηχανών αναζήτησης στο διαδίκτυο. Είναι ο πιο οικονομικός, γρήγορος και αποτελεσματικός τρόπος αναζήτησης πληροφοριών στον παγκόσμιο ιστό.

[56] Eisenmann T.R. and Herman K., (2006), "*Google Inc.*", Harvard Business review.

Εμπόδια εισόδου στον κλάδο

Τα εμπόδια εισόδου στον συγκεκριμένο κλάδο σχετίζονται κυρίως με το υψηλό κόστος έρευνας και ανάπτυξης μιας τεχνολογίας ικανής να ανταγωνιτεί αποτελεσματικά τις ήδη υπάρχουσες καθώς και το κόστος προβολής μέσω του διαδικτύου της ίδιας της υπηρεσίας. Επομένως ο κίνδυνος εισόδου νέων ανταγωνιστών στον κλάδο θα πρέπει να εστιάσει κυρίως σε εταιρίες λογισμικού, πληροφορικής κλπ. μεγάλου μεγέθους και με παγκόσμια φήμη (π.χ. Norton κλπ.)[57]

Βαθμός ανταγωνισμού

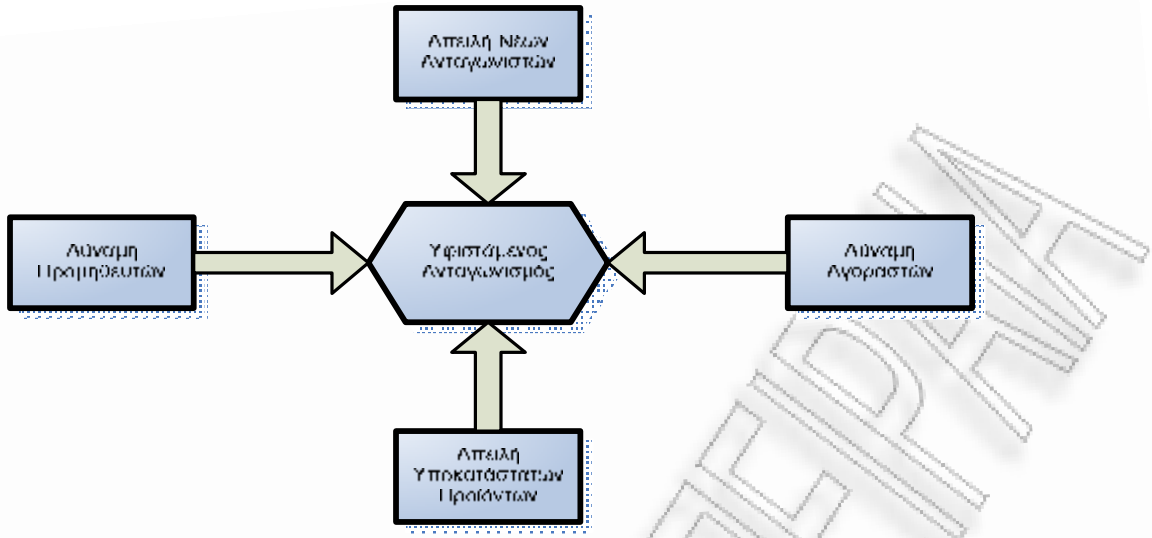
Ο βαθμός του ανταγωνισμού στην αγορά προσδιορίζεται σε γενικές γραμμές από παράγοντες όπως (Μπουραντάς και Παπαλεξανδρή, 1998) :

- *τον αριθμό των ανταγωνιστών*
- *το μέγεθος και τα ανταγωνιστικά τους πλεονεκτήματα*
- *τη μορφή και τα χαρακτηριστικά της αγοράς (π.χ. ολιγοπώλιο)*
- *τον ρυθμό ανάπτυξης της αγοράς*
- *τον βαθμό ασύμμετρης πληροφόρησης των ανταγωνιστών κλπ.*

Η αγορά των μηχανών αναζήτησης του διαδικτύου είναι ολιγοπώλιο και σε μεγάλο βαθμό ανταγωνιστική καθότι εκπροσωπείται από εταιρίες κολοσσούς όπως π.χ. την Yahoo!, την Microsoft κλπ. Ο ρυθμός ανάπτυξης της αγοράς είναι μεγάλος δεδομένης της συνεχής διόγκωσης του διαδικτύου και της συνεπαγόμενης μεγαλύτερης ανάγκης για αποτελεσματική αναζήτηση πληροφοριών. Επιπλέον, τα έσοδα πολλαπλασιάζονται με ανοδικούς ρυθμούς για τους παίκτες της συγκεκριμένης αγοράς αφού ολοένα και περισσότερες εταιρίες επιλέγουν την προβολή μέσω μηχανών αναζήτησης (π.χ. Google Adwords) ως μέσο διαφήμισης και προώθησης των πωλήσεων τους.

Σχήμα 5: Η μήτρα των 5 δυνάμεων του Porter

[57] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.



Πηγή: Μπουραντάς Δ., Παπαλεξανδρή Ν.(1998), Εισαγωγή στη Διοίκηση Επιχειρήσεων, εκδόσεις Μπένου, Αθήνα

Πως το Ανταγωνιστικό Πλεονέκτημα της Google Inc. την Βοήθησε στο Operation Management

Σε συσχετισμό με όλα όσα αναφέρθηκαν παραπάνω, στην παρούσα ενότητα αναλύεται ο τρόπος με τον οποίο η Google κατάφερε να γίνει ηγέτης στην αγορά των μηχανών αναζήτησης κερδίζοντας ανταγωνιστικό πλεονέκτημα. Η στρατηγικής της εταιρίας για την απόκτηση ανταγωνιστικού πλεονεκτήματος βασίστηκε στους ακόλουθους άξονες[58] :

Αποτελεσματική αναζήτηση φιλική προς τον χρήστη : η Google σε αντίθεση με τις υπόλοιπες μηχανές αναζήτησης είχε μια λευκή ιστοσελίδα απαλλαγμένη διαφημιστικών μηνυμάτων και άλλου περιεχομένου που αποπροσανατολίζουν τον χρήστη. Επίσης ο αλγόριθμος της Google (Pagerank) εξασφάλιζε ότι τα πιο σχετικά αποτελέσματα θα εμφανίζονταν κάθε φορά με βάση την λέξη-κλειδί που είχε εισάγει ο χρήστης. Τέλος η σελίδα αποτελεσμάτων δεν εμφάνιζε διαφημίσεις παρά μόνο μία λίστα «συνδέσμων χορηγών» στο δεξί τμήμα της σελίδας.

Έμφαση σε έναν τομέα : Η Google ξεκίνησε την πορεία της ως μια μηχανή αναζήτησης και τίποτα παραπάνω. Οι ιδρυτές της συνήθιζαν να λένε ότι: "σε εμάς αρέσει να κάνουμε μόνο ένα πράγμα καλά, πραγματικά καλά».

Ταχύτητα αναζήτησης : Χάρις στον πρωτοποριακό αλγόριθμό της η Google μπορούσε να επιστρέφει το αποτέλεσμα στον χρήστη με βάση την αντίστοιχη λέξη-κλειδί μέσα σε χρόνο ρεκόρ

[58] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.

Η δουλειά είναι το χόμπι μας : Αυτή είναι η κουλτούρα που περνάει η εταιρία σε όλους τους εργαζομένους της. Η δουλειά είναι το μέσο με το οποίο οι άνθρωποι της Google εκφράζουν την δημιουργικότητα τους.

Δημοκρατία στο διαδίκτυο : Η Google σέβεται το δικαίωμα των χρηστών για αντικειμενική πληροφόρηση και για αυτό φροντίζει να τους δίνει κάθε φορά τα πιο σχετικά αποτελέσματα με βάση την αναζήτηση τους

Τέλος ο πίνακας No. 1 δείχνει τον εκτιμώμενο αριθμό των πελατών του *Google wallet*, τον αριθμό των συνεργαζόμενων επιχειρήσεων, τον αριθμό και την αξία των συναλλαγών και τέλος το ύψος των εκτιμώμενων εσόδων από την υπηρεσία μέσα στην επόμενη τριετία (2009-2011).

Πίνακας No. 1: Εκτιμήσεις βασικών μεγεθών Google wallet

ΕΤΟΣ	***2009***	***2010***	***2011***
Αριθμός πελατών			
Αριθμός συνεργαζόμενων επιχειρήσεων	*2,000*	*5,000*	*9,000*
Αριθμός συναλλαγών μέσω Google Wallet	*5,000,000*	*7,000,000*	*9,000,000*
Αξία Συναλλαγών μέσω Google Wallet	*$25,000,000*	*$45,000,000*	*$65,000,000*
Εκτίμηση εσόδων	*$1,000,000*	*$2,100,000*	*$3,200,000*

ΚΕΦΑΛΑΙΟ 5^{ο}
ΟΙ ΕΠΙΘΕΣΕΙΣ ΠΟΥ ΕΧΕΙ ΔΕΧΤΕΙ ΤΟ ΔΙΑΔΙΚΤΥΑΚΟ ΚΑΝΑΛΙ ΤΗΣ Google Com».

Βασικό τμήμα του σχεδιασμού ενός συστήματος ασφαλείας για κάθε ηλεκτρονική υπηρεσία και ιστοσελίδα επιχείρησης που λειτουργεί στο διαδίκτυο, αποτελεί να εξακριβώσει τι επίπεδο ασφάλειας χρειάζεται και ποιές απειλές θα κληθεί να αντιμετωπίσει. Η επιλογή των μέτρων προστασίας γίνεται λαμβάνοντας υπόψη τι κόστος -οικονομικό, απόδοσης ή ενόχλησης λόγω της παρουσίας τους έχουν για την εταιρεία.

Το πρώτο λοιπόν, βήμα είναι να εντοπίστεί ο «εχθρός». Συνήθως οι άνθρωποι επικεντρώνονται στο είδος της επίθεσης ξεχνώντας ότι οι επιθέσεις είναι τα εργαλεία. Για παράδειγμα, ένας αποφασισμένος εισβολέας θα επιμείνει πολύ περισσότερο από ένα τυπικό εισβολέα. Έτσι, παρόλο που θα χρησιμοποιηθούν τα ίδια είδη επίθεσης, η επιμονή μπορεί να είναι αυτή που θα αποβεί καταλυτική για την επιτυχία ή μη της επίθεσης. Για το λόγο αυτό είναι σημαντικό να έχουμε προσδιορίσει:

- *Ποιοί είναι οι εχθροί μας.*
- *Ποιές είναι οι προθέσεις τους*
- *Ποιά είναι τα μέσα τους*

Συνοψίζοντας λοιπόν τα παραπάνω και αναφερόμενοι στις επιθέσεις που έχει δεχθεί το διαδικτυακό κανάλι –μηχανή αναζήτησης της Google.Com, οι εν δυνάμει εχθροί του πληροφοριακού συστήματος κατηγοριοποιούνται στις ακόλουθες ομάδες και οι οποίοι έχουν δράσει κατά της εταιρίας ως εξής[59] :

Hackers - Crackers

Είναι οι "αναρχικοί" του κυβερνοχώρου που έχουν εισβάλει στα πληροφοριακά συστήματα της Google.Com είτε για διασκέδαση, είτε για να καταστρέψουν, είτε για επίδειξη. Τους ελκύουν

[59] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.

όλοι οι απαγορευμένοι χώροι της Google.Com. Πολλές εταιρείες όπως η Google.Com συνηθίζουν να προσλαμβάνουν άτομα που εισέβαλαν στα συστήματά τους με τη λογική "*Καλύτερα να δουλεύουν για μας παρά εναντίον μας*". Άλλωστε αυτοί που παραβίασαν ένα σύστημα ασφαλείας της Google.Com ξέρουν καλύτερα από τον καθένα που μειονεκτεί και μπορούν να το βελτιώσουν.

Κλέφτες

Είναι όλοι αυτοί που εισβάλουν σε ένα σύστημα της Google.Com όλα αυτά τα χρόνια έχοντας ως στόχο την κλοπή δεδομένων που θα τους αποφέρει οικονομικά οφέλη είτε χρησιμοποιώντας τα, είτε πουλώντας τα σε ανταγωνίστριες επιχειρήσεις όπως η Yahoo!Com.

Ανταγωνιστές

Ένας ανταγωνιστής της Google.Com συνήθως, δεν εισβάλει για να κλέψει χρήματα, ούτε για να καταστρέψει αλλά για να αποκτήσει πληροφορίες της Google.Com που είναι σημαντικές προκειμένου να κυριαρχήσει στον "επιχειρηματικό πόλεμο".

Εσωτερικοί εχθροί

Δυσαρεστημένοι, αποξενωμένοι και άπληστοι υπάλληλοι της Google.Com που μπορούν να αποτελέσουν ένα ιδιαίτερα σοβαρό εκ των έσω κίνδυνο για τις βάσεις δεδομένων της συγκεκριμένης εταιρείας.

Ατυχήματα

Πολλές καταστροφές δεν είναι αποτέλεσμα πρόθεσης ούτε οργανωμένης επίθεσης, αλλά πρόκειται για ατυχήματα ή λάθη από αφέλεια στην επιχείρηση της Google.Com. Δεν είναι καθόλου ασυνήθιστο γεγονός εταιρείες να καταστρέφουν από μόνες τους τις βάσεις δεδομένων τους, ή να τις απελευθερώνουν στο internet κατά λάθος.

Έχοντας γνωρίσει τους πιθανούς εισβολείς του συστήματος, εν συνεχεία, περιγράφονται οι τρόποι που έχουν οι crackers για να αποκτούν παράνομη ή έστω παράτυπη πρόσβαση στα υπολογιστικά συστήματα της Google.Com, τα εργαλεία που χρησιμοποιούν για να κερδίζουν τον έλεγχο σε υπολογιστές, καθώς και τις διαθέσιμες τεχνικές στις οποίες καταφεύγουν για να προκαλούν ζημιές ή να «γονατίζουν» ένα σύστημα, ανεξαρτήτως της ισχύος του. Στο ξεχωριστό κείμενο στο τέλος της ενότητας περιέχετε ένα σύντομο γλωσσάρι με τεχνικούς όρους, η γνώση των οποίων βοηθά στην καλύτερη κατανόηση όσων ακολουθούν.

Εξάλλου, αν και επικρατεί η αντίληψη ότι οι crackers είναι άνθρωποι με υψηλό επίπεδο τεχνογνωσίας, καθώς και με άπειρα αποθέματα υπομονής και επιμονής, δυστυχώς διαπιστώνουμε ότι οι αρετές αυτές δεν είναι απαραίτητη προϋπόθεση για να μπορέσει κάποιος να μας προκαλέσει πονοκεφάλους ακόμα και ζημιές.

5.1 *Τύποι επιθέσεων της Google.Com*

Μία από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι crackers για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές στο site της Google.Com είναι οι επιθέσεις DoS (Denial of Service attacks). Το όνομα της τεχνικής (άρνηση εξυπηρέτησης) οφείλεται στο γεγονός ότι ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών (clients), εξαιτίας του τεράστιου πλήθους κίβδηλων αιτήσεων (bogus requests) που δέχεται από τον επιτιθέμενο.

Υπάρχουν διάφορα είδη επιθέσεων DoS, πολλά από τα οποία εκμεταλλεύονται εγγενείς αδυναμίες του ζεύγους πρωτοκόλλων TCP/IP. Για τα περισσότερα από αυτά είναι ήδη γνωστά τα αντίστοιχα μέτρα προστασίας της Google.Com. Συγκεκριμένα, οι διαχειριστές συστημάτων της Google.Com μπορούν να εγκαθιστούν patches σε λειτουργικά συστήματα και προγράμματα - διακομιστές, ώστε να αποτρέπουν επιθέσεις DoS ή να ελαχιστοποιούν τις συνέπειές τους. Όπως, όμως, συμβαίνει και με τους ιούς υπολογιστών, κατά καιρούς εφευρίσκονται νέα είδη ή παραλλαγές επιθέσεων DoS. Παραθέτουμε εν συντομία τέσσερις από τις διασημότερες παραλλαγές, σε αλφαβητική σειρά.

Ping of death

Αίτηση PING ή, αλλιώς, αίτηση ICMP, προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) του τελευταίου (πάνω από 64Kb). Τέτοια «παράτυπα» πακέτα μπορούν να «κρεμάσουν» υπολογιστές της Google.Com που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.

Smurf Attack

Έχει επιτευχθεί αποστέλλοντας αιτήσεις ICMP σε μια διεύθυνση εκπομπής (broadcast address) στο υπό επίθεση δίκτυο της Google.Com ή σε κάποιο άλλο, ενδιάμεσο. Η διεύθυνση επιστροφής (return address) των πακέτων ICMP της Google.Com πλαστογραφείται, ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου. Από τη στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου, λειτουργεί ενισχυτικά, δημιουργώντας από μία μόνο αίτηση ICMP δεκάδες ή και εκατοντάδες απαντήσεις, προκαλώντας με τον τρόπο αυτό πληροφοριακό «μποτιλιάρισμα».

Ας σημειωθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί το πολύ σε 255 μηχανήματα (ανήκουν όλα στο ίδιο υποδίκτυο), επομένως κατά τη διάρκεια μιας επίθεσης Smurf, από κάθε αίτηση PING μπορούν να παραχθούν μέχρι και 255 απαντήσεις. Καταλαβαίνουμε, λοιπόν, τον υπέρογκο αριθμό

των άχρηστων πακέτων που δημιουργούνται, όταν ο επιτιθέμενος στέλνει εκατοντάδες ή ακόμη και χιλιάδες πακέτα ICMP.

Syn flood attack

Πριν εγκαθιδρυθεί μια συνεδρία μεταξύ ενός πελάτη και ενός διακομιστή της Google.Com, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και ως «ακολουθία χειραψίας» (handshaking sequence). Εάν ο πελάτης αγνοήσει την τελευταία απάντηση SYN-ACK (SYNchronize ACKnowledge) του διακομιστή, ο τελευταίος επιμένει για ένα προκαθορισμένο χρονικό διάστημα. Ένας cracker μπορεί να εκμεταλλευτεί τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστή-θύμα της Google.Com ή ακόμα και για να τον «κρεμάσει». Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση (IP address) της Google.Com, κρύβοντας με τον τρόπο αυτό τα ίχνη του.

Tear Drop Attack

Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP της Google.Com. Όταν ένα τέτοιο πακέτο αποστέλλεται στο Internet, ενδέχεται να ταξιδεύει σε επιμέρους, μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου εκεί περιγράφεται η θέση του στο αρχικό πακέτο IP της Google.Com. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, ονόματι «Teardrop», το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο υπό συζήτηση πεδίο. Όταν ο υπολογιστής-στόχος προσπαθήσει να συναρμολογήσει τα «παραπλανητικά» αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει, εκτός και αν ο διαχειριστής συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch που διορθώνει το πρόβλημα.

Όταν σε μια επίθεση DoS της Google.Com συμμετέχουν περισσότερα του ενός μηχανήματα, έχουμε τις λεγόμενες κατανεμημένες επιθέσεις DoS (Distributed Denial of Service ή DDoS attacks). Στις επιθέσεις του είδους είναι δυνατόν να συμμετέχουν και προσωπικοί υπολογιστές ακόμα και το PC στο σπίτι μας χωρίς να το γνωρίζουν οι χρήστες τους. Ο επιτιθέμενος cracker κατορθώνει με κάποιον τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν εν αγνοία τους στην επίθεση.

Τη στιγμή που θα την εξαπολύσει, στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστής DDoS). Τότε, εκείνο ειδοποιεί μια συγκεκριμένη χρονική στιγμή καθέναν από τους υπόλοιπους υπολογιστές (πελάτες DDoS) και όλοι μαζί αρχίζουν να βάλλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να «πλημμυρίσει» και να μην μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών.

Ένας καλός τρόπος για να προστατεύουν οι υπεύθυνοι της Google.Com τους υπολογιστές τους, ώστε να μη χρησιμοποιούνται εν αγνοία μας, είναι να χρησιμοποιούμε κάποιο εταιρικό πρόγραμμα firewall. Αν και ένα μηχάνημα της Google.Com που έχει πέσει θύμα επίθεσης DoS ή DDoS μπορεί να επανέλθει σε ομαλή λειτουργία σχετικά εύκολα, υπάρχουν έμμεσες αρνητικές συνέπειες. Αναφερόμαστε σε οικονομικές ζημιές που οφείλονται στο χρόνο που ένας κεντρικός διακομιστής μένει εξουδετερωμένος, καθώς και στον τραυματισμό του κύρους της εταιρείας στην οποία ανήκει ο διακομιστής-θύμα.Είναι γνωστό, εξάλλου, ότι στην ιντερνετική εποχή ο ανταγωνισμός βρίσκεται μερικά «κλικ» μακρύτερα.

Απρόσκλητοι Ωτακουστές

Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων της Google.Com για να αναλύουν τη συμπεριφορά δικτύων και να εντοπίζουν (πιθανά) προβλήματα, είναι τα λεγόμενα «sniffer». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο.

Εάν το δίκτυο είναι βασισμένο στο TCP/IP της Google.Com, τότε επειδή το sniffer παρακολουθεί πακέτα IP, ονομάζεται και packet sniffer. Εξάλλου, σε ένα δίκτυο τοπολογίας αστέρα, όπως είναι πολλά τοπικά δίκτυα, τα πακέτα που φεύγουν από έναν κόμβο (μηχάνημα) εκπέμπονται προς όλους τους άλλους κόμβους του δικτύου. Ωστόσο, μόνο ο κόμβος για τον οποίο προορίζονται τα πακέτα θα τα χρησιμοποιήσει, οι άλλοι θα τα αγνοήσουν. Εάν, τώρα, ένα πρόγραμμα sniffer είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου σε «επιδιδόμενη» κατάσταση (promiscuous mode), τότε το μηχάνημα αυτό θα μπορεί να «βλέπει» όλα τα πακέτα που διακινούνται στο δίκτυο.

Οι διαχειριστές συστημάτων της Google.Com κάνουν χρήση των sniffer για να αναλύουν την κυκλοφορία των πακέτων σε ένα δίκτυο και να εντοπίζουν εστίες προβλημάτων. Επίσης, συχνά χρησιμοποιούν περισσότερα του ενός sniffer, στρατηγικά εγκατεστημένα σε διάφορους κόμβους του δικτύου, ώστε να εντοπίζουν εισβολές παρείσακτων.

Με άλλα λόγια, τα sniffer μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών (intrusion detection systems). Βλέπουμε, λοιπόν, ότι τα προγράμματα αυτά αποτελούν πολύτιμο εργαλείο για τους διαχειριστές συστημάτων. Ωστόσο, όπως ήδη θα έχει γίνει προφανές, τις υπηρεσίες τους μπορούν να εκμεταλλευτούν και οι crackers, αυτή τη φορά για όχι και τόσο θεάρεστους σκοπούς. Για παράδειγμα, ο cracker μπορεί να χρησιμοποιεί ένα sniffer για να υποκλέπτει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, διάφορα άλλα προσωπικά στοιχεία χρηστών, για να διαβάζει την ηλεκτρονική τους αλληλογραφία κ.λπ..

Ο προφανής τρόπος για να προστατευτεί ένα δίκτυο της Google.Com από την επιβλαβή χρήση των sniffer είναι να υπάρχει αυστηρή επίβλεψη στα προγράμματα που εγκαθιστούν οι

χρήστες στους υπολογιστές. Εάν ένας cracker δεν μπορεί να αποκτήσει φυσική πρόσβαση σε κάποιον υπολογιστή, τότε είναι απλώς ανίκανος να εγκαταστήσει ένα sniffer. Άλλος ένας τρόπος για την παρόπλιση των sniffer είναι η αποστολή δεδομένων σε κρυπτογραφημένη μορφή.

Το sniffer θα εξακολουθεί να συλλαμβάνει τα πακέτα, μόνο που τώρα δεν θα μπορεί να εξαγάγει κάποιο νόημα από τα περιεχόμενά τους. Βεβαίως, στην περίπτωση αυτή υπάρχει πάντοτε ο κίνδυνος της αποκρυπτογράφησης. Για το λόγο αυτό, προτείνεται η χρήση ισχυρής κρυπτογραφίας, με το ανάλογο κόστος σε υπολογιστική ισχύ. Το ζητούμενο, λοιπόν, είναι η χρυσή τομή ανάμεσα στη δύναμη των μεθόδων κρυπτογράφησης από τη μία, και στην ευκολία των χρηστών, από την άλλη.

Τέλος, υπάρχει μια ολόκληρη κατηγορία προγραμμάτων που μπορούν να εντοπίζουν ποιοι υπολογιστές σε ένα δίκτυο της Google.Com έχουν κάρτα δικτύου σε επιδιδόμενη κατάσταση. Έτσι, ο διαχειριστής συστήματος της Google.Com μπορεί να ελέγξει εάν κάποιος υπολογιστής τρέχει ένα sniffer, αν έχει δοθεί επίσημη άδεια για την εγκατάστασή του κ.λπ..

Αδιάκριτοι Διαβάτες

Μια άλλη τεχνική που χρησιμοποιούν διαχειριστές και crackers της Google.Com, καθένας για διαφορετικούς σκοπούς, είναι η σάρωση θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας της Google.Com. Από τη στιγμή που ο επίδοξος εισβολέας μάθει ποιες υπηρεσίες προσφέρει το μηχάνημα-στόχος, μπορεί στη συνέχεια να σχεδιάσει την επίθεσή του βασιζόμενος σε γνωστές αδυναμίες των περί ου ο λόγος υπηρεσιών. Επειδή μια διαδικασία port scanning αφήνει τα ίχνη της στα αρχεία καταγραφής (log files) του λειτουργικού συστήματος, ορισμένοι crackers χρησιμοποιούν ορισμένες «ύπουλες» παραλλαγές.

Μία από αυτές είναι η λεγόμενη «*ημι-ανοιχτή σάρωση SYN*» (half-open SYN scan). Κατά τη διάρκεια μιας τέτοιας σάρωσης, το πρόγραμμα συνδέεται στα port, αλλά τερματίζει καθεμία ακολουθία σύνδεσης, πριν αυτή ολοκληρωθεί. Από τη στιγμή, λοιπόν, που οι ακολουθίες σύνδεσης δεν ολοκληρώνονται, το λειτουργικό σύστημα στο μηχάνημα-στόχος συνήθως δεν τις καταγράφει, θεωρώντας ότι δεν συνέβησαν ποτέ. Ωστόσο, το πρόγραμμα που κάνει τη σάρωση μπορεί να καταλάβει εάν κάποιο port είναι «ανοιχτό», κρίνοντας από την απάντηση του λειτουργικού συστήματος. Υπάρχουν διάφορα εργαλεία για το μπλοκάρισμα των port scan. Αυτό που προτείνεται στους απλούς χρήστες είναι η χρήση κάποιου προσωπικού προγράμματος firewall της Google.Com.

Social Engineering

Ακούγεται ειρωνικό αλλά αποτελεί μια πραγματικότητα, το γεγονός ότι μία από τις πιο ύπουλες μεθόδους επίθεσης σε ένα σύστημα ασφαλείας δεν βασίζεται στην τεχνολογία αλλά στην ψυχολογία! Ως "***social engineering***" ορίζεται η "*τέχνη*" του να αποκτάς πρόσβαση σε ένα σύστημα, εξαπατώντας τους χρήστες και τους διαχειριστές του και αποσπώντας τους όλες εκείνες τις πληροφορίες που χρειάζονται.

Σε ένα πείραμα που έγινε της Google.Com, μια ομάδα από hackers ξεκίνησαν την προσπάθειά τους να διεισδύσουν σε ένα πληροφοριακό σύστημα της συγκεκριμένης εταιρείας. Μοναδικό τους όπλο είχαν τον τηλεφωνικό κατάλογο της εταιρείας. Τηλεφώνησαν στην εταιρεία της Google.Com, ζήτησαν να μιλήσουν με το γραμματεία του δικτύου και κατόρθωσαν μέσα σε εικοσιτέσσερις ώρες η ίδια η εταιρεία να τους δημιουργήσει λογαριασμό, να τους δώσει ID και κωδικό μέσω τηλεφώνου και μάλιστα να τους στείλει με courier μέσα στη νύχτα το απαιτούμενο, για την είσοδό τους στο δίκτυο, software.

Ιοί

Αναμφίβολα το Internet έδωσε μεγάλη ώθηση στην εξάπλωση των πάσης φύσεως ιών και μικροβίων. Στις μέρες της Amiga και των PC XT ο μόνος τρόπος για να «κολλήσει» κάποιος ένα ειδεχθές πρόγραμμα ήταν να χρησιμοποιήσει μολυσμένες δισκέτες, κυρίως με παιχνίδια. Τότε η μόλυνση με έναν ιό ήταν κάτι το συνηθισμένο μέχρι και γοητευτικό (το γνωστό μπαλάκι που έκανε βόλτες στην οθόνη).

Βέβαια, το αστείο τελείωνε με την οδυνηρή ανακάλυψη ότι οι δισκέτες ή ο σκληρός δίσκος ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του Internet στη ζωή μας, και συγκεκριμένα με το e-mail της Google.Com. Το ηλεκτρονικό ταχυδρομείο της Google.Com εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το email της Google.Com όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντάς τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται.

Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν τρέξετε τα εκτελέσιμα αρχεία/script που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου word, παραπλανώντας σας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Ας πάρουμε όμως τα πράγματα από την αρχή.

Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκρισή μας και να μολύνουν άλλα αρχεία. Είναι μικρά

κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές.

Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Internet. Υπάρχουν αρκετά ήδη ιών:

- *αυτοί που προσβάλλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) και είναι σχετικά σπάνιοι σήμερα,*
- *αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/File viruses),*
- *αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως, π.χ., του Word και του Excel (Macro viruses), και*
- *οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες. Υπάρχει και μία ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό e-mail κειμένου να μπορεί να κάνει τη ζημιά.*

Βέβαια, οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο οι ειδικοί μας προτρέπουν να αναβαθμίζουμε στη νεότερη έκδοση όλες τις εφαρμογές μας, ειδικά αυτές που σχετίζονται με το Internet. Με αυτό τον τρόπο μειώνονται αρκετά οι πιθανότητες μόλυνσης.

Δούρειοι Ίπποι

Δεν θα ήταν υπερβολή, εάν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών Internet της Google.Com, προέρχεται από τους δούρειους ίππους (Trojan horses). Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής «φωλιάζει» με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το Internet, το Trojan-διακομιστής, που τρέχει σιωπηρά στο υπόβαθρο (background), στέλνει ένα σήμα το οποίο λαμβάνει το Trojan-πελάτης (στο μηχάνημα του θύτη).

Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κράκερ αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλλει, αναλόγως του Trojan. Ο πρώτος μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού CD-ROM ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές

στο υλικό του υπολογιστή, όπως, π.χ., να του διαγράψει το BIOS ή να «χτυπήσει» τις κεφαλές του σκληρού δίσκου.

Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη.

Πώς όμως μπορεί να «μπει» ένα Trojan σε έναν υπολογιστή της Google.Com; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο e-mail ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι freeware ή shareware, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λπ. Υπάρχουν δύο τρόποι για να αποφεύγουμε τα Trojan. Ο πρώτος είναι να χρησιμοποιούμε ένα πρόγραμμα «Antivirus» ή «AntiTrojan».

Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν τα κατεβάζουμε ακόμα και στην περίπτωση που είναι ήδη εγκατεστημένα στο PC μας και να τα διαγράφουν. Ο άλλος τρόπος είναι να χρησιμοποιούμε ένα προσωπικό firewall. Κάθε φορά που ένα Trojan-διακομιστής θα προσπαθεί να «βγει» στο Internet, το firewall θα μας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία.

Μακροϊοί

Οι Μακροϊοί γράφονται σε γλώσσα μακροεντολών ενός επεξεργαστή κειμένου της Google.Com, λογιστικού φύλλου ή άλλων εφαρμογών και εισέρχονται σε οποιοδήποτε τύπο εγγράφου παράγουν οι εφαρμογές. Αυτό τα μολύνει απέναντι σε οποιοδήποτε λειτουργικό σύστημα κι αν εκτελείται η εφαρμογή.

Κουνέλια

Αυτά είναι προγράμματα, που όταν ξεκινήσουν, κάνουν πολλά αντίγραφα του εαυτού τους της Google.Com. Μπορούν να αντιγράψουν τον εαυτό τους στη μνήμη γεμίζοντας τη Ram και πιθανώς να καταρρεύσουν τον υπολογιστή. Σε αντίθεση με τους ιούς, τα κουνέλια δεν προσκολλούν τους εαυτούς τους σε υπάρχοντα αρχεία. Παρόλα αυτά, μπορεί να επιχειρήσουν να συγκαλύψουν τους εαυτούς τους υιοθετώντας ένα αθώο όνομα ή ενεργοποιώντας μια ιδιότητα της λίστας κρυφών αρχείων της Google.Com.

Σκουλήκια

Είναι παρόμοια με τα κουνέλια, αλλά είναι ικανά να μεταδοθούν από ένα μηχάνημα στο άλλο επί του δικτύου εκμεταλλευόμενα λογικά κενά σε πρωτόκολλα του διαδικτύου. Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, της Google.Com για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν

μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό.

Μάλιστα, το Melissa worm έχει αρχίσει ένα νέο γύρο καλυμμένο αυτήν τη φορά ως έγγραφο του Office για Mac. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα email σε όλη τη λίστα επαφών του Outlook.

Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail της Google.Com από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί τον ασκό του Αιόλου. Η μαζική αποστολή email, εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.

Δυστυχώς, όσα μέτρα προστασίας και αν λαμβάνουν οι υπεύθυνοι της Google.Com, πάντοτε τα προγράμματα που χρησιμοποιούν θα είναι ατελή, υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι αποφασισμένοι κράκερ. Πρόκειται για τα λεγόμενα «exploits», προγραμματιστικές αδυναμίες σε γνωστές και ευρέως χρησιμοποιούμενες εφαρμογές, τα οποία μπορούν να αξιοποιούν καταλλήλως οι crackers για να αποκτούν μη εξουσιοδοτημένη πρόσβαση ή έλεγχο σε συστήματα, να προκαλούν ζημιές σε υπολογιστές-στόχους κ. ο. κ. Συχνά, πάντως, οι υπεύθυνοι της Google.Com κυκλοφορούν αναβαθμίσεις ή διορθώσεις (bug fixes, patches) προγραμμάτων με γνωστά προβλήματα.

5.2 *Σχετικές αναφορές στο διαδίκτυο με τις επιθέσεις που έχει δεχτεί η μηχανή αναζήτησης google*

- ΠΗΓΗ:MEN 24-TEACH NEWS WEEKLY:GOOGLE Vs CHINA
  http://www.men24.gr/html/ent/288/ent.91288.asp

***Η Google** κατηγορεί την Κίνα για ενορχηστρωμένες επιθέσεις κατά της ίδιας και άλλων εταιρειών απειλώντας μάλιστα την απόσυρση της από τη Κινεζική αγορά.*

Η Google ανακοίνωσε την απόφαση της να διακόψει τη λογοκρισία στα αποτελέσματα των αναζητήσεων της υπηρεσίας Google.cn κάτι που προοιωνίζει σημαντικές εξελίξεις σε σχέση με την παρουσία της στην κινεζική αγορά. Η απόφαση έρχεται ένα περίπου μήνα μετά τη διαπίστωση μιας επίθεσης σε server της εταιρείας που είχε ως στόχο τους λογαριασμούς Gmail ακτιβιστών για τα ανθρώπινα δικαιώματα.

Σύμφωνα με τη Google, που έκανε λόγο για μια «ιδιαίτερα σύγχρονη και στοχευμένη ενέργεια», ενορχηστρωτής της επίθεσης είναι η κινεζική κυβέρνηση και για το λόγο αυτό θα ξεκινήσει συζητήσεις με τις αρχές της χώρας για τη συνέχιση της παρουσίας της εκεί.

Επιπλέον, η εταιρεία τόνισε ότι δεν είναι η μοναδική που δέχτηκε επίθεση, με τουλάχιστον 20 ακόμα εταιρείες που δραστηριοποιούνται στο χώρο του διαδικτύου, τα χρηματοοικονομικά, τη χημική βιομηχανία και αλλού να έχουν πέσει θύματα κλοπής πνευματικής περιουσίας.

Παράλληλα, έσπευσε να διαβεβαιώσει τις εταιρείες που χρησιμοποιούν Google App ότι τα δεδομένα τους δεν έχουν παραβιαστεί και ότι προέβη στη δημοσιοποίηση των ευρημάτων των ερευνών της για αποδείξει ότι είναι ιδιαίτερα ευαίσθητη σε θέματα διαφάνειας και εμπιστοσύνης.

Κρατική κατασκοπεία

Παρόμοιες επιθέσεις στο παρελθόν έχουν δεχτεί διάφοροι κυβερνητικοί οργανισμοί, εταιρείες και οι ένοπλες δυνάμεις των ΗΠΑ. Η επίθεση στη Google, σύμφωνα με στελέχη εταιρειών που δραστηριοποιούνται στον τομέα της πληροφορικής, είναι μέρος μιας κρατικά επιχορηγούμενης βιομηχανικής κατασκοπείας εκ μέρους της Κίνας. Οι περισσότερες εταιρείες, όμως, επιλέγουν να μην έρθουν σε ρήξη με την μεγαλύτερη οικονομική δύναμη του κόσμου.

Η περίπτωση της Google φαίνεται πως εξαιρείται από τον κανόνα. Αφενός είναι η πρώτη εταιρεία που λαμβάνει μέτρα και βγαίνει δημοσίως να διαμαρτυρηθεί αφετέρου στην υπόθεση παρενέβη και η υπουργός εξωτερικών των ΗΠΑ. Η Χίλαρι Κλίντον δήλωσε ότι «οι κατηγορίες της Google είναι ιδιαίτερα σοβαρές, εγείρουν σοβαρούς προβληματισμούς και θα ζητηθούν εξηγήσεις από την Κινεζική κυβέρνηση».

Μια τελείως διαφορετική άποψη εκφράζει το TechCrunch. Το γνωστό μπλογκ τεχνολογίας θεωρεί ότι πίσω από τις διαμαρτυρίες της Google βρίσκεται η αδυναμία της να συναγωνιστεί τη

Baidu που αναπτύσσει την πιο δημοφιλή μηχανή αναζήτησης στην Κίνα. Παρά τους συμβιβασμούς σε θέματα λογοκρισίας, το Google.cn δεν κατάφερε ποτέ να καλύψει τη διαφορά με το Baidu.com.

Η Baidu χειρίζεται το 60% των αναζητήσεων στην Κίνα και η Google έρχεται δεύτερη με 35% και τα κέρδη της Google στην κινεζική αγορά δεν είναι τόσα όσα να δικαιολογήσουν 700 υπαλλήλους, κυρίως καλοπληρωμένους μηχανικούς.

Τι μέλλει γενέσθαι

Αν η Google είναι αποφασισμένη να υλοποιήσει την απειλή της και να τερματίσει την τετράχρονη παρουσία της στην Κίνα, δίνοντας παράλληλα την ευκαιρία στη Baidu και τους αμερικάνους ανταγωνιστές της (Yahoo! και Microsoft) να γίνουν παγκόσμιες δυνάμεις είναι απόλυτα λογικό να το κάνει με τρόπο που θα αποφύγει να αποδεχτεί την ήττα της. Παράλληλα, έχει μια θαυμάσια ευκαιρία να βελτιώσει το προφίλ της στο δυτικό κόσμο. Η είσοδος του Google στην κινεζική αγορά το 2006 είχε συνοδευτεί με έντονα αρνητική δημοσιότητα εξαιτίας της απόφασης του να συμπλεύσει με τους περιορισμούς και τη λογοκρισία που ζήτησε το Πεκίνο. Για παράδειγμα, από τα αποτελέσματα των αναζητήσεων αποκλείονταν αναφορές στα γεγονότα του 1989 και την πλατεία Τιεν Αν Μεν ή τον εξόριστο Θιβετιανό ηγέτη Δαλάι Λάμα. Ένα χρόνο μετά, το 2007, αναγκάστηκε να παραδεχθεί δημόσια ότι η πολιτική της για την διατήρηση δεδομένων από αναζητήσεις είναι ασαφής. Δεν ήταν μια παραδοχή που έγινε εθελοντικά αλλά μετά από σχετικές πιέσεις της Ευρωπαϊκής Ένωσης. Την ίδια χρονιά, και μετά από έτη επικρίσεων, η Privacy International χαρακτήρισε τη Google εχθρική ως προς την προστασία των προσωπικών δεδομένων.

Επιλέγοντας στρατόπεδο

Το παράδοξο είναι ότι η στάση της Google βρίσκει σύμφωνους πολλούς αναλυτές της Silicon Valley και εταιρείες πληροφορικής. Η Yahoo! που επίσης διατηρεί μια μικρή παρουσία στην Κίνα της τάξης του 8% συντάχθηκε με τη Google καταδικάζοντας τις επιθέσεις. Αν και η Yahoo! China ανήκει από το 2005 στην εταιρεία Alibaba.com, η Yahoo! αποτελεί τον κύριο μέτοχο της τελευταίας.

Πολύ περισσότερο, όμως, βρίσκει σύμφωνους τους κατοίκους της χώρας. Πολλοί κινέζοι πολίτες να αφήσουν ευχαριστήρια μηνύματα και λουλούδια έξω

από τα γραφεία της στο Πεκίνο δηλώνοντας τη δυσαρέσκεια τους για την ολοένα και αυξανόμενη λογοκρισία. Πριν από τους Ολυμπιακούς του 2008, το Πεκίνο είχε καταργήσει τους ελέγχους και τις απαγορεύσεις σε ένα μεγάλο αριθμό ιστοσελίδων προκειμένου να προβάλει ένα πιο δημοκρατικό προφίλ. Μετά τους Ολυμπιακούς, οι απαγορεύσεις άρχισαν να αυξάνονται με εντατικούς ρυθμούς μέχρι να φτάσουν πρωτόγνωρα επίπεδα. Οι διαδηλώσεις στην Xinjiang τον περασμένο Ιούλιο είχαν ως αποτέλεσμα την καθολική απαγόρευση της πρόσβασης στο Ιντερνετ στην επαρχεία και το κλείσιμο των ξένων κοινωνικών δικτύων όπως το Twitter και το Facebook σε όλη τη χώρα.

"Thank you Google"

Η κυβέρνηση της Κίνας, από την άλλη πλευρά, έχει κάθε λόγο να φοβάται την αντίδραση της Google στη λογοκρισία. Πέρα από τα λουλούδια που δείχνουν ότι δεν ελέγχει όσο καλά θα ήθελε την κοινή γνώμη, πολλοί χρήστες προσπαθούν να βρουν τρόπο να παρακάμψουν τις απαγορεύσεις δημιουργώντας εικονικά ιδιωτικά δίκτυα και να αποκτήσουν πρόσβαση στις απαγορευμένες ιστοσελίδες. Αν και τα κινεζικά μέσα ενημέρωσης υποβάθμισαν την ιστορία, στα διάφορα forum εμφανίζονται δηλώσεις συμπάθειας υπέρ της Google που δεν αποκλείεται να πάρουν τη μορφή καταιγίδας.

Παράλληλα, δεν είναι καθόλου βέβαιο ότι η κινεζική κυβέρνηση αντέχει να ακολουθήσει σκληρή γραμμή. Πολλοί αναλυτές υποστηρίζουν ότι θα μπλοκάρει το Google.cn αν συνεχίσει η «ανταρσία» του Google για λόγους αρχής αλλά δεν μπορεί να προβεί στην απαγόρευση άλλων υπηρεσιών όπως τα Google Docs, το Gmail το hosting ιστοσελίδων σε σέρβερ εταιρείας. Στην περίπτωση αυτή θα δεχθεί ισχυρές διεθνείς πιέσεις και θα υποβαθμίσει το φιλελεύθερο προφίλ της. Αυτό που, όμως, είναι πιο σημαντικό για το Πεκίνο είναι πως η Google παραμένει ένας από τους ισχυρούς συνδέσμους των κινεζικών επιχειρήσεων με τη δύση και η κυβέρνηση είναι πρακτικά υποχρεωμένη να αναζητήσει συμβιβαστική λύση.

ΠΗΓΗ:ΟΕΜ.GR:ΚΑΤΑΙΓΙΔΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ
http://oem.gr/main/index.php?option=com_content&view=article&id=278&Itemid=44

- Εν μέσω της σινο-αμερικανικής διένεξης για τις επιθέσεις σε ακτιβιστές χρήστες της Google, τουλάχιστον πέντε οργανώσεις για τα ανθρώπινα δικαιώματα στην Κίνα δέχονται τις τελευταίες ημέρες σαρωτικές επιθέσεις στους δικτυακούς τόπους τους.

Το **Chinese Human Rights Defenders**, ένα δίκτυο Κινέζων και ξένων ακτιβιστών, ανακοίνωσε ότι οι κυβερνοεπιθέσεις εναντίον του δικτυακού τόπου του ξεκίνησε το Σάββατο και συνεχίστηκε για περίπου 14 ώρες. Οι επιθέσεις ακολούθησαν την τακτική **DoS** (Denial of Service), δηλαδή υπερφόρτωσαν το σύστημα με αλλεπάλληλα αιτήματα σύνδεσης. «Οι επιθέσεις παρέλυσαν το δικτυακό τόπο του CHRD εξαντλώντας τους πόρους του διακομιστή» αναφέρει η ανακοίνωση που αναμεταδίδεται από το πρακτορείο AFP. Ο πάροχος διαδικτυακών υπηρεσιών της οργάνωσης έκανε λόγο για την «πλέον δριμεία» επίθεση που έχει δεχτεί μέχρι σήμερα. Όπως ανακοίνωσε το δίκτυο CHRD, οι άγνωστοι χάκερ έβαλαν επίσης στο στόχαστρο τους δικτυακούς τόπους Canyu, Rights and Livelihood Watch και New Century News, οι οποίοι προσφέρουν ενημέρωση για θέματα ανθρωπίνων δικαιωμάτων, καθώς και το Independent Chinese Pen, ένα σύλλογο συγγραφέων. Το δίκτυο CHRD ανέφερε ότι η προέλευση των επιθέσεων δεν έχει διευκρινιστεί, οι υποψίες όμως στρέφονται κατά της κινεζικής κυβέρνησης.

Το Πεκίνο επικρίνεται συχνά για την εκτεταμένη κρατική λογοκρισία στο Διαδίκτυο και έχει κατηγορηθεί επανειλημμένα για κυβερνοεπιθέσεις εναντίον ξένων κυβερνήσεων. Το τελευταίο επεισόδιο έρχεται λίγες εβδομάδες μετά την ανακοίνωση της Google ότι χάκερ από την Κίνα επιτέθηκαν σε χρήστες του Gmail που μάχονται για τα ανθρώπινα δικαιώματα, αλλά σε σε τουλάχιστον 20 ακόμα αμερικανικές υπηρεσίες. Η εταιρεία δήλωσε ότι δεν είναι πια διατεθειμένη να λογοκρίνει τα αποτελέσματα στη μηχανή Google.cn, ακόμα κι αν αυτό σημαίνει ότι πρέπει να αποχωρήσει από τη χώρα. Το Πεκίνο αρνήθηκε τις κατηγορίες, ωστόσο το Στέιτ Ντιπάρτμεντ απαιτεί εξηγήσεις.

ΠΗΓΗ: ΝΑΥΤΕΜΠΟΡΙΚΗ:ΜΕ ΑΠΟΧΩΡΗΣΗ ΑΠΟ ΤΗΝ ΚΙΝΑ ΑΠΕΙΛΕΙ Η GOOGLE,http://www.naftemporiki.gr/worldcup/story.asp?id=1764756

- Την αποχώρησή της από την αγορά της Κίνας εξετάζει σοβαρά η Google Inc., ιδιοκτήτρια της δημοφιλέστερης μηχανής αναζήτησης στο διαδίκτυο, μετά την επίθεση χάκερ στους λογαριασμούς e-mail δεκάδων χρηστών, που υπερασπίζονται τα ανθρώπινα δικαιώματα.

Σε ανακοίνωση που εξέδωσε αργά χθες ο αμερικανικός κολοσσός αναφέρει ότι πιθανόν να κλείσει το site και τα γραφεία του στην Κίνα, ενώ σημειώνει πως τουλάχιστον άλλες 20 εταιρείες από διάφορους κλάδους έχουν δεχτεί την επίθεση χάκερ. Εξαιτίας των επιθέσεων αυτών, σε συνδυασμό με τις απόπειρες λογοκρισίας στο διαδίκτυο, η εταιρεία αποφάσισε να σταματήσει να «φιλτράρει» τα αποτελέσματα στο site Google.cn, τονίζεται στην ανακοίνωση.

Μια πιθανή αποχώρηση της Google από τη χώρα θα στερήσει από την εταιρεία ετήσια έσοδα ύψους 600 εκατ. δολαρίων από τα 338 εκατ. χρηστών του διαδικτύου στην Κίνα και ενδεχομένως να βοηθήσει την εγχώρια Baidu Inc. να διευρύνει το προβάδισμά της στη μεγαλύτερη αγορά ίντερνετ στον κόσμο. Ο εκπρόσωπος του κινεζικού υπουργείου Βιομηχανίας και Τεχνολογίας Πληροφοριών αρνήθηκε να σχολιάσει το θέμα, υποστηρίζοντας πως δεν γνωρίζει πως έχει η κατάσταση, ενώ το θέμα δεν σχολίασε ούτε το υπουργείο Εξωτερικών.

Η ανακοίνωση της εταιρείας έρχεται σε μια περίοδο που οι σχέσεις ΗΠΑ – Κίνας είναι τεταμένες όσον αφορά την ελευθερία έκφρασης στο ίντερνετ, με την Αμερικανίδα υπουργό Εξωτερικών Χίλαρι Κλίντον να ετοιμάζεται να παρουσιάσει στρατηγική για ένα πιο ελεύθερο διαδίκτυο, το περιεχόμενο του οποίου δεν θα υπόκειται σε λογοκρισία. Οι μετοχές της Google υποχώρησαν κατά 6,68 δολάρια, ή 1,1%, στα 583,80 δολάρια στις μετασυνεδριακές συναλλαγές.

ΚΕΦΑΛΑΙΟ 6ο

Τρόποι Άμυνας για τις «Επιθέσεις» που Έχει Δεχτεί το Διαδικτυακό Κανάλι της Google.Com

Οι τρόποι άμυνας και πρόληψης που χρησιμοποιούνται συνήθως από την Google.Com για τις παραπάνω κατηγορίες «*πληροφοριακού πολέμου*», αναφέρονται στις παρακάτω εξής περιπτώσεις :

- *Πρόληψη*
- *Αποτροπή*
- *Ενδείξεις και προμηνύματα*
- *Ανακάλυψη*
- *Προετοιμασία για επείγοντα περιστατικά*
- *Απάντηση*

Οι συγκεκριμένες κατηγορίες είναι αλληλένδετες μεταξύ τους και ορισμένοι από τους μηχανισμούς χρησιμοποιούνται σε περισσότερες από μια κατηγορίες. Εξαίρεση αποτελεί η περίπτωση όπου εντοπίζονται τα περισσότερα έξοδα και τα οποία επιβάλλονται για την λήψη των κατάλληλων και απαιτούμενων μέτρων. Φυσικά δύναται να υπάρξουν περισσότερα έξοδα και τα οποία είναι λίγο δύσκολο να προσδιοριστούν αναλόγως.

Ο πρώτος τρόπος αντιμετώπισης των μεθόδων «*πληροφοριακού πολέμου*» της Google.Com, είναι εκείνος της *Πρόληψης*. Ο συγκεκριμένος τρόπος αποβλέπει στην αποφυγή μιας εκδήλωσης επίθεσης η οποία αιωρείται ουσιαστικά στον επιτιθέμενο μια πρόσβαση στην πηγή των πληροφοριών. Ο μηχανισμός που εμπλέκεται σε αυτόν τον τρόπο άμυνας, περιλαμβάνει την απόκρυψη σημαντικών πληροφοριών, τον έλεγχο εισόδου από τους χρήστες αλλά και την πιστοποίηση τους. Ουσιαστικά, η απόκρυψη των πηγών πληροφοριών στοχεύει στην κοινολόγηση των πληροφοριών σε μη εξουσιοδοτημένα πρόσωπα[60]. Οι σχετικοί αυτοί μηχανισμοί εσωκλείουν συστήματα ασφαλείας και διαχωρισμούς των πληροφοριών. Η πιστοποίηση που απατείται, έχει ως

[60] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.

στόχο την διαπίστωση της ταυτότητας των χρηστών μέσω της χρήσης κωδικών πρόσβασης και επαλήθευσης.

Ο δεύτερος τρόπος αντιμετώπισης της Google.Com, είναι εκείνος που αναφέρεται στην *Αποτροπή*. Η συγκεκριμένη μέθοδος στοχεύει στην τοποθέτηση αντιμετώπισης μιας μη ελκυστικής επίθεσης για ανάκτηση πηγών πληροφοριών της Google.Com. Στην κατηγορία αυτή εσωκλείονται οι νόμοι, οι ποινές που επέρχονται από αυτούς αλλά και οι αποζημιώσεις που μπορούν να προκύψουν. Ο έλεγχος ασφαλείας που μπορεί να λάβει χώρα σε αυτή την περίπτωση, διεξάγεται προληπτικά αφού ένας πιθανός επιτιθέμενος μπορεί να διαπιστώσει πως ενδεχομένως δεν χρειάζεται να εισχωρήσει σε κάποιο σύστημα και να κινδυνέψει για αυτό, αφού οι πληροφορίες που θα ανακτήσει ίσως να μην είναι αρκετα σημαντικές. Βέβαια, κάθε στοιχειώδης έλεγχος που θα διεξαχθεί, το μόνο που θα προσφέρει είναι βοήθεια και πρόληψη ενάντια στις μεθόδους «*πληροφοριακού πολέμου*».

Ο τρίτος τρόπος αντιμετώπισης τέτοιων φαινομένων της Google.Com, είναι οι *Ενδείξεις* και τα *Προμηνύματα*. Ο τρόπος αυτός λειτουργεί ως εργαλείο αναγνώρισης μιας επίθεσης από έναν απρόσμενο και ανεπιθύμητο παράγοντα. Μέσω αυτού του εργαλείου, μπορούν να παρθούν συγκεκριμένα μέτρα και νόμοι προκειμένου να αποτραπεί ή να καταστεί αδύνατη η επίθεση από αυτούς τους ανεπιθύμητους παράγοντες. Συνήθως οι κυβερνήσεις είναι αυτές που εφαρμόζουν τα μέτρα αυτά και ζητούν πληροφορίες από επιχειρήσεις και οργανισμούς που παρακολουθούν τέτοιου είδους επιθέσεις.

Ο τέταρτος τρόπος αντιμετώπισης, είναι εκείνος *Ανακάλυψης*. Η ανακάλυψη έχει και εκείνη σχεδόν τον ίδιο σκοπό με τις *Ενδείξεις και τα Προμηνύματα* και την στενή παρακολούθηση μιας επίθεσης μετά την έναρξη της. Τα εργαλεία που χρησιμοποιούνται σε αυτό τον τρόπο αντιμετώπισης, έχουν την ικανότητα να λειτουργούν μεθόδους, οι οποίες μπορούν να εντοπίζουν επιβλαβείς ή ψευδείς πληροφορίες και εν συνεχεία να επεξεργάζονται τις εισερχόμενες πληροφορίες. Οι μηχανισμοί αυτοί, περιλαμβάνουν επίσης κάποιες κρυφές κάμερες προστασίας αλλά και συστήματα ασφαλείας τα οποία χρησιμοποιούνται σε ηλεκτρονικούς υπολογιστές για τον εντοπισμό καταστρεπτικών ιών και βλαβερών ουσιών μέσα σε αυτούς.

Η πέμπτη κατηγορία αντιμετώπισης των μεθόδων «*πληροφοριακού πολέμου*» της Google.Com, είναι αυτή της Προετοιμασίας για επείγοντα περιστατικά. Ο τρόπος αυτός σχετίζεται άμεσα με την δυνατότητα ενός συστήματος για ανάκαμψη μετά την επίθεση που θα δεχθεί αλλά και την απάντηση του σε αυτό. Στην κατηγορία αυτή συγκαταλέγονται και η λήψη των αντιγράφων αλλά και η διόρθωση μιας βλάβης μετά από μια ισχυρή επίθεση. Με αυτόν τον τρόπο όμως δεν θεωρείται πιθανή η πρόβλεψη ή η πρόληψη κάθε επίθεσης. Ο αμυντικός «πληροφοριακός πόλεμος»

σχετίζεται άμεσα με την σωστή διαχείριση των κινδύνων αλλά όχι με την αποφυγή τους, σε οποιοδήποτε κόστος κάτι τέτοιο θα είναι αποδεκτό[61].

Σχεδιασμός Συστήματος Ασφαλείας της Google.Com

Ο σχεδιασμός του συστήματος βάσεως δεδομένων ασφαλείας της Google.Com οφείλει να αποτελεί τμήμα του αρχικού σχεδιασμού του συστήματος και όχι μια διαδικασία που θα εκτελείται μετά την εγκατάσταση του συστήματος. Οι λόγοι είναι απλοί: Αφενός είναι οικονομικότερο να σχεδιάζονται και να υλοποιούνται ταυτόχρονα το σύστημα και η ασφάλεια του και αφετέρου είναι λειτουργικότερο. Ο σχεδιασμός στηρίζεται σε πέντε βασικά βήματα :

- Βήμα 1: Δημιουργία πολιτικής ασφαλείας
- Βήμα 2: Προσθήκη των κατάλληλων μεθόδων προστασίας ανάλογα με το πληροφοριακό σύστημα που θα χρησιμοποιήσουμε
- Βήμα 3: Σχεδίαση του συστήματος προστασίας που θα καλύπτει το φυσικό, το δικτυακό περιβάλλον και το περιβάλλον του υπολογιστικού συστήματος.
- Βήμα 4: Ανάπτυξη διαδικασιών για την παρακολούθηση, τον έλεγχο, την συντήρηση και την αναβάθμιση του συστήματος ασφαλείας.
- Βήμα 5: Χρήση των συμπερασμάτων από την παρακολούθηση και τον έλεγχο του συστήματος με στόχο την βελτίωση τόσο του σχεδιασμού, όσο και της υλοποίησης και λειτουργίας του συστήματος.
-

Δημιουργία πολιτικής ασφαλείας της Google.Com

Στο πρώτο στάδιο πρέπει αρχικά να καθοριστεί η πολιτική ασφαλείας που θα ακολουθηθεί για το σύνολο του συστήματος της Google.Com. Αυτό περιλαμβάνει (υπολογιστές και δίκτυα), τα δεδομένα και τους ανθρώπους (διαχειριστές, προσωπικό συντήρησης, χρήστες, πελάτες). Η πολιτική ασφαλείας δημιουργείται μετά από ανάλυση και αξιολόγηση των αναγκών κάθε οργανισμού για τη διαθεσιμότητα, τους κινδύνους και τις δυνατότητες που πρέπει να διαθέτει το πληροφορικό του σύστημα. Απαρτίζεται από πλάνο που περιέχει τις διαδικασίες λειτουργίας και ελέγχου, τον απαραίτητο εξοπλισμό, αλλά και σενάρια, σχέδια και διαδικασίες αντιμετώπισης κρίσεων.

Σχεδιασμός Περιβάλλοντος της Google.Com

[61] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.

Το δεύτερο στάδιο περιλαμβάνει το σχεδιασμό του περιβάλλοντος που θα εγκατασταθεί η βάση δεδομένων της Google.Com. Με την έννοια περιβάλλον ορίζουμε όλα όσα υπάρχουν έξω από την εφαρμογή. Δηλαδή: οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα, καθώς και η φυσική τοποθεσία της εφαρμογής.

Σχεδιασμός Μηχανισμού Ασφαλείας της Google.Com

Το τρίτο στάδιο στο σχεδιασμό του συστήματος ασφαλείας της Google.Com αποτελεί η επιλογή των κατάλληλων μεθόδων προστασίας που θα χρησιμοποιηθούν. Γνωρίζοντας το γενικό σχεδιασμό της βάσης δεδομένων της Google.Com, την πολιτική ασφαλείας της εταιρείας, θα πρέπει ήδη να έχουμε καταλάβει ποιές είναι οι ανάγκες μας, τι προστασία θα χρειαστούμε και ποια τεχνολογία είναι η κατάλληλη.

Παρακολούθηση και έλεγχος

Για να είναι επιτυχής ο σχεδιασμός του συστήματος ασφαλείας της Google.Com είναι ιδιαίτερα σημαντικό να έχει ληφθεί υπόψη και να έχουν καθοριστεί οι διαδικασίες μέσα από τις οποίες θα παρακολουθείται καθημερινά η λειτουργία του και θα ελέγχεται σε τακτικά χρονικά διαστήματα η απόδοσή του. Έτσι θα γίνονται οι απαραίτητες βελτιώσεις, προσθήκες και αναβαθμίσεις.

Ανάλυση Επικινδυνότητας

Για την χάραξη της πολιτικής που ακολουθεί η Google.Com για την υλοποίηση της ασφάλειας της βάσης δεδομένων απαιτείται η ανάλυση επικινδυνότητας, όπου θα μελετηθούν οι εκθέσεις σε κίνδυνο (exposures) του συστήματος, προσδιορίζοντας τις ευπάθειες (vulnerabilities) και τις απειλές (threats) του με βάση τον υφιστάμενο έλεγχο (control). Τα αποτελέσματα μιας ανάλυσης επικινδυνότητας (risk analysis review) της υπολογιστικής και επικοινωνιακής υποδομής της εταιρείας θα προσδιορίσουν τις απαιτήσεις ασφαλείας της βάσης δεδομένων, καλύπτοντας τις παρακάτω συνιστώσες[62]:

- Φυσική ασφάλεια του συστήματος (physical security): Προστασία ολόκληρου του σχετικού εξοπλισμού από φυσικές καταστροφές.
- Ασφάλεια υπολογιστικού συστήματος (computer security): Προστασία των πληροφοριών της βάσης που διαχειρίζεται το λειτουργικό σύστημα (εφαρμογές, αρχεία δεδομένων, κ.ά.).

[62] Kelleher K., (2005), *"Who's afraid of Google?"*, Wired No.13.12, December.

- Ασφάλεια βάσεων δεδομένων (database security): Προστασία των περιεχομένων μιας βάσης δεδομένων.
- Ασφάλεια δικτύων επικοινωνιών (network security): Προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω τοπικών, τηλεφωνικών ή άλλων δικτύων (π.χ. Internet).
- Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές στην Προστασία Βάσης Δεδομένων

Οι ψηφιακές υπογραφές της Google.Com με σκοπό τη προστασία βάσης δεδομένων χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία διαθέτουν κάποιο μαθηματικό συσχετισμό μεταξύ τους. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί, να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο γεγονός ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής για τη προστασία βάσης δεδομένων της Google.Com εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού ή κατατεμαχισμού –“one way hash”. Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους. Η σύνοψη του μηνύματος είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί. Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

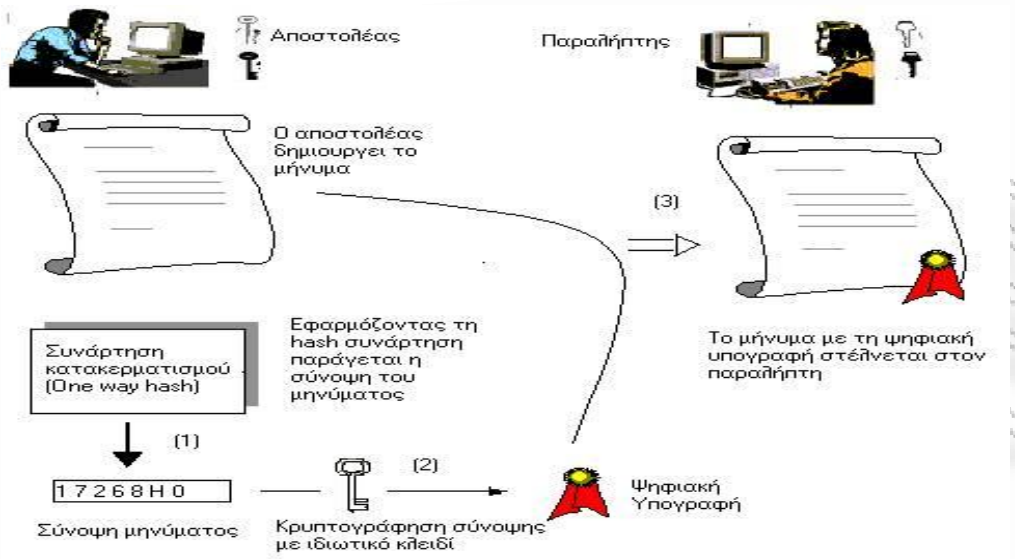
Η ηλεκτρονική υπογραφή για τη προστασία βάσης δεδομένων της Google.Com, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Η ψηφιακή υπογραφή και σε αντίθεση με την ιδιόχειρη υπογραφή είναι διαφορετική για κάθε μήνυμα. Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί -του αποστολέα, την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή

υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος. Μία ψηφιακή υπογραφή μπορεί να ‘πλαστογραφηθεί’ εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του.

Η χρήση της ηλεκτρονικής υπογραφής για τη προστασία βάσης δεδομένων της Google.Com περιλαμβάνει δύο διαδικασίες. Πρώτον την δημιουργία της υπογραφής και δεύτερον την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής για τη προστασία βάσης δεδομένων.

Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου και σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη.

Ο παραλήπτης δε, αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη), εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή). Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.



Οι παραπάνω διεργασίες γίνονται από το ανάλογο λογισμικό στον υπολογιστή του χρήστη της Google.Com.

Επαλήθευση ψηφιακής υπογραφής για τη προστασία βάσης δεδομένων

Προστασία Βάσης Δεδομένων με τη Χρήση Μεθόδου Firewall

Όταν λέμε τείχος προστασίας σε προσωπικούς υπολογιστές που εκτελούνται συναλλαγές βάσεων δεδομένων, εννοούμε ένα πρόγραμμα που ελέγχει την κυκλοφορία στη διασταύρωση του Η/Υ και του σχετικού διαδικτύου. Το τείχος προστασίας θα ελέγξει και θα αναφέρει ποια προγράμματα του Η/Υ θέλουν να επικοινωνήσουν με το ίντερνετ. Επίσης θα αναφέρει αν κάποιος / κάτι προσπαθεί να επικοινωνήσει με το κομπιούτερ που εκτελούνται οι τραπεζικές συναλλαγές. Βέβαια εκτός του ότι θα το αναφέρει, θα προσφέρει τη δυνατότητα να επιτρέψουν ή να απαγορεύσουν οι κάτοχοι και χρήστες την είσοδο ή έξοδο τραπεζικών πληροφοριών / προγραμμάτων από το κομπιούτερ τους. Ένα firewall αποτελείται από τρεις ομάδες συνιστωσών :

- *φίλτρα για μπλοκάρισμα και/ή παρακολούθηση μετάδοσης συγκεκριμένου είδους μηνυμάτων καθορισμένα από τον τύπο, τον προορισμό τους ή συνδυασμό και των δύο*
- *"gateways" για προώθηση των αποδεκτών μηνυμάτων από τη μια μεριά του firewall στην άλλη*
- *"application proxies" που εκτελούν έλεγχο ειδικής πρόσβασης σε εφαρμογές, παρακολούθηση και αναφορά.*

Γενικά υπάρχουν δύο είδη firewalls για τη προστασία βάσεων δεδομένων της Google.Com. Αυτά που λαμβάνουν αποφάσεις στο επίπεδο της μεταγωγής πακέτων (packet filters) και αυτά που ενεργούν στο επίπεδο των εφαρμογών (proxies). Φυσικά πολλά προϊόντα καλύπτουν και τις δύο κατηγορίες αλλά ο διαχωρισμός εξακολουθεί να υπάρχει μια και τα κριτήρια ασφάλειας είναι διαφορετικά για κάθε κατηγορία. Ένα packet filter ενεργεί σαν ένας συνηθισμένος δρομολογητής (router) με τη διαφορά ότι έχει άποψη για το αν ένα πακέτο δεδομένων πρέπει να περάσει από το ένα δίκτυο δεδομένων στο άλλο.

Για τους παραπάνω λόγους, η ασφάλεια ενός συστήματος βάσης δεδομένων και συναλλαγών της Google.Com αποτελεί πρωταρχική προϋπόθεση για την επιτυχή λειτουργία του, αφού τα δεδομένα που ανταλλάσσονται στις διάφορες επιχειρηματικές δραστηριότητες είναι ιδιαίτερα ευαίσθητα. Οι εφαρμογές και οι τεχνολογίες ηλεκτρονικού εμπορίου πρέπει να αντιμετωπίζουν με επιτυχία αυτά τα θέματα. Είναι σημαντικό να κατανοούνται οι κίνδυνοι αυτοί στα σημερινά περιβάλλοντα υπολογιστών. Η κατανόηση αυτή βοηθά τον διαχειριστή (manager) ασφαλείας μιας επιχείρησης ή τράπεζας στο να επιλέξει κατάλληλα και με ανάλογο κόστος- απόδοσης συστήματα που ελέγχουν και προστατεύουν τις πληροφορίες μιας τράπεζας. Οι βασικότερες μέθοδοι προστασίας τραπεζικών συστημάτων που εφαρμόζονται σήμερα στις ηλεκτρονικές συναλλαγές, αναφέρονται να είναι οι εξής:

- *Ασφάλεια βασισμένη στην εμπιστοσύνη*
- *Ασφάλεια μέσω απόκρυψης*
- *Σύστημα Password*

Η εγγυημένη ασφάλεια είναι απαραίτητη συνιστώσα των παραγόντων που θα επιτρέψουν την ευρεία διάδοση, χρήση και αποδοχή των βάσεων δεδομένων πάνω από «ανοικτά» συστήματα. Η δημιουργία ασφαλούς περιβάλλοντος ηλεκτρονικού εμπορίου και τραπεζικών συναλλαγών της Google.Com σημαίνει προστασία των δικτυακών πόρων και οντοτήτων από ενδεχόμενες απειλές και εγγύηση τουλάχιστον του ίδιου επιπέδου ασφαλείας με το συμβατικό εμπόριο και τρόπους πληρωμής για τα αγαθά ή τις υπηρεσίες. Μια πρακτική προσέγγιση του όρου μπορεί να αναφέρει πως ασφάλεια υπολογιστικού συστήματος βάσεων δεδομένων, υπάρχει όταν μπορούμε να βασιστούμε σε αυτό και στο λογισμικό που χρησιμοποιείται από τις συγκεκριμένες τράπεζες.

Μέσα σε αυτόν τον πλατύ ορισμό, υπάρχουν διαφορετικές μορφές ασφάλειας οι οποίες πρέπει να απασχολούν τόσο τους διαχειριστές όσο και τους απλούς χρήστες των δικτύων και των συστημάτων τους. Τα βασικά χαρακτηρίστηκα για να θεωρείται το σύστημα συναλλαγών της Google.Com ασφαλές είναι τα παρακάτω:

Εμπιστευσιμότητα (Confidentiality)

Είναι η διασφάλιση της πληροφορίας ή συναλλαγής βάσεων δεδομένων της Google.Com από οποιονδήποτε δεν έχει το δικαίωμα να την δει ή να κρατήσει αντίγραφό της. Αυτός ο τύπος ασφάλειας περιλαμβάνει τόσο την προστασία του συνόλου της πληροφορίας όσο και μέρους της, το οποίο από μόνο του μπορεί να δείχνει ότι δεν είναι κάτι το λανθασμένο αλλά μπορεί να οδηγήσει στην αποκάλυψη περαιτέρω σημαντικών πληροφοριών.

Ακεραιότητα δεδομένων (Data Integrity)

Θεωρείται η προστασία της πληροφορίας, συμπεριλαμβανομένων των προγραμμάτων, από το σβήσιμό της ή την με οποιονδήποτε τρόπο αλλοίωσή της χωρίς την άδεια του ιδιοκτήτη της. Η υπό προστασία πληροφορία περιλαμβάνει επίσης αντικείμενα όπως backup πληροφορίες και αρχεία βάσης δεδομένων.

Καταγραφή (Audit)

Ο διαχειριστής ενός δικτύου βάσης δεδομένων της Google.Com δεν πρέπει να ανησυχεί μόνο για τους χρήστες χωρίς άδεια πρόσβασης, αλλά και για εκείνους που αν και νόμιμοι κάνουν λάθη ή προκαλούν σκόπιμα κάποιο πρόβλημα. Σε τέτοιες περιπτώσεις πρέπει να καθορισθεί τι έχει συμβεί από ποιόν και τι επηρεάστηκε. Ο μόνος τρόπος να επιτευχθούν όλα τα παραπάνω είναι να γίνει χρήση κάποιων αρχείων καταγραφής της δραστηριότητας στο σύστημα και το οποίο να είναι ικανό να δώσει πληροφορίες για το ποιος προκάλεσε τι.

Διαθεσιμότητα (Availability)

Αφορά την προστασία των υπηρεσιών της Google.Com έτσι ώστε να μην υποβαθμιστεί η δυνατότητα παροχής τους. Εάν κάποια στιγμή ζητηθεί μια συγκεκριμένη υπηρεσία από νόμιμο χρήστη και δεν του δοθεί, αυτό ισοδυναμεί με την απώλεια της πληροφορίας που βρίσκεται στο σύστημα.

Συνέπεια (Consistency)

Η διασφάλιση ότι το σύστημα βάσης δεδομένων της Google.Com συμπεριφέρεται όπως αναμένεται από τους εξουσιοδοτημένους χρήστες του. Εάν το λογισμικό ή το υλικό μέρος του συστήματος της Google.Com αρχίσει να συμπεριφέρεται παράξενα, ειδικά μετά από κάποια αναβάθμιση ή μετατροπή τότε επίκειται καταστροφή. Τελικά η συνέπεια είναι η διασφάλιση της ορθότητας των δεδομένων και των προγραμμάτων που χρησιμοποιούνται.

Έλεγχος (Control)

Ο έλεγχος πρόσβασης στο σύστημα βάσης δεδομένων της Google.Com. Παράνομοι χρήστες και λογισμικό μπορεί να δημιουργήσουν μεγάλα προβλήματα αν δεν υπάρχει έλεγχος. Αν και όλες οι παραπάνω μορφές / υπηρεσίες ασφάλειας είναι εξίσου σημαντικές, διαφορετικοί τραπεζικοί οργανισμοί δίνουν διαφορετική προτεραιότητα στη καθεμία διότι αντιμετωπίζουν διαφορετικού είδους απειλές. Η ασφάλεια ενός τραπεζικού πληροφοριακού συστήματος συναλλαγών για παράδειγμα αποτελεί το κομβικό τεχνικό μέσο για την προστασία ενός συστήματος, τα δεδομένα που διαχειρίζεται ένα περιβάλλον, η τεχνική του διαχείριση και η διαθεσιμότητα του, καθώς αποτελούν τις τρεις παραμέτρους ενδιαφέροντος για τον καθορισμό αναγκαιότητας προστασίας του περιβάλλοντος αυτού και για την προτεραιότητα λήψης σχετικών μέτρων αν κάποιο επίπεδο προστασίας θεωρηθεί απαραίτητο.

Μιλώντας κάποιος για ασφάλεια στο εμπόριο και τις «απαιτήσεις» βάσης δεδομένων που είναι αναγκαίες σε κάθε σύστημα συναλλαγής, εννοείται συγχρόνως και κάθε είδος «πληροφοριακού πολέμου» το οποίο αναφέρεται στις επιθετικές και αμυντικές τραπεζικές επιχειρήσεις οι οποίες μπορούν να στρέφονται εναντίον των πηγών πληροφοριών και που χαρακτηρίζονται ως τύπου «νίκης-ήττας». Ένας από τους λόγους για τους οποίους διεξάγεται ο συγκεκριμένος «πόλεμος», είναι λόγω του γεγονότος ότι οι πηγές αυτές των τραπεζικών πληροφοριών παρουσιάζουν ιδιαίτερη σημασία για τους απλούς ανθρώπους και στελέχη των επιχειρήσεων στις μέρες μας.

Προστασία Βάσης Δεδομένων με τη Χρήση Passwords

Το Password Authentication Protocol (PAP) της Google.Com είναι ένα απλό πρωτόκολλο αυθεντικοποίησης που χρησιμοποιείται για την αυθεντικοποίηση ενός χρήστη σε κάποιο Διακομιστή Πρόσβασης Δικτύου (Network Access Server, NAS) που μπορεί να χρησιμοποιείται για παράδειγμα από παρόχους υπηρεσιών ίντερνετ για προστασία βάσης δεδομένων. Το PAP χρησιμοποιείται από το πρωτόκολλο PPP της Google.Com. Το PAP μεταδίδει μη κρυπτογραφημένους ASCII κωδικούς μέσω δικτύου και γι αυτό θεωρείται μη ασφαλές. Χρησιμοποιείται ως έσχατη λύση όταν ο απομακρυσμένος διακομιστής δεν υποστηρίζει πιο ισχυρό πρωτόκολλο αυθεντικοποίησης, όπως το CHAP ή το EAP. Ο πελάτης αποστέλλει όνομα χρήστη και κωδικό πρόσβασης Ο διακομιστής

αποστέλλει μήνυμα authentication-ack, εάν τα διαπιστευτήρια είναι αποδεκτά ή εναλλακτικά authentication-nak, εάν δεν είναι αποδεκτά (Adams, J., 1998).

Πακέτα PAP για Προστασία Βάσης Δεδομένων

Περιγραφή	***1 byte***	***1 byte***	***2 bytes***	***1 byte***	***Μεταβλητή***	***1 byte***	***Μεταβλητή***
Authentication-request	*Code = 1*	*ID*	*Length*	*Username length*	*Username*	*Password length*	*Password*
Authentication-ack	*Code = 2*	*ID*	*Length*	*Message length*	*Username*		
Authentication-nak	*Code = 3*	*ID*	*Length*	*Message length*	*Username*		

ΕΠΙΛΟΓΟΣ

Οι μεταφορείς πληροφοριών χαρακτηρίζονται ως συστήματα και αντικείμενα επικοινωνιών, τα οποία έχουν την ικανότητα να διακινούν ή να διαβιβάζουν πληροφορίες από ένα συγκεκριμένο μέρος σε κάποιο άλλο. Στα συστήματα αυτά συμπεριλαμβάνονται τα άτομα τα οποία μεταφέρουν τις πληροφορίες, τα διάφορα οχήματα και γενικά τα μέσα μεταφοράς καθώς και τα διάφορα μέσα μαζικής επικοινωνίας.

Ουσιαστικά κρυπτογραφία *(cryptography)* είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα τον οποίων η λύση είναι δύσκολο να βρεθεί. Κρυπτανάλυση *(cryptanalysis)* είναι η επίλυση αυτών των προβλημάτων και κρυπτολογία *(cryptology)* είναι ο συνδυασμός της κρυπτογραφίας και της κρυπτολογίας σε ένα ενιαίο επιστημονικό κλάδο. Το διαδίκτυο στην ευρύτερη σημασία του, αποτελείται από έναν σεβαστό αριθμό υπολογιστών που ενώνονται μεταξύ τους, δημιουργώντας ένα δίκτυο το οποίο στη συνέχεια συνδέεται με άλλα δίκτυα.

Η ιστορία της Google είναι μία από αυτές τις λαμπρές ιστορίες που συνηθίζονται να γράφονται στα βιβλία και τα περιοδικά ως παραδείγματα προς μίμηση, ιδιαιτέρως από τους Managers των εταιρειών. Η Google ξεκινά την πορεία της το έτος 1999 με ιδρυτές δύο νεαρούς απόφοιτους του Πανεπιστημίου Stanford της Καλιφόρνια: τον Sergey Brin και τον Larry Page. Οι δυο τους είχαν στα πλαίσια της διπλωματικής τους διατριβής αναπτύξει έναν αλγόριθμο αναζήτησης πληροφοριών στο διαδίκτυο που δεν είχε καμία σχέση με αυτούς που χρησιμοποιούνταν ήδη, π.χ. τους αλγόριθμους που εφάρμοζαν οι μηχανές αναζήτησης της Yahoo και της MSN.

Βασικό τμήμα του σχεδιασμού ενός συστήματος ασφαλείας για κάθε ηλεκτρονική υπηρεσία και ιστοσελίδα επιχείρησης που λειτουργεί στο διαδίκτυο, αποτελεί να εξακριβώσει τι επίπεδο ασφάλειας χρειάζεται και ποιές απειλές θα κληθεί να αντιμετωπίσει. Η επιλογή των μέτρων προστασίας γίνεται λαμβάνοντας υπόψη τι κόστος -οικονομικό, απόδοσης ή ενόχλησης λόγω της παρουσίας τους έχουν για την εταιρεία.

Ο γενικότερος τρόπος αντιμετώπισης των μεθόδων «πληροφοριακού πολέμου» της Google.Com, είναι εκείνος της Πρόληψης. Ο συγκεκριμένος τρόπος αποβλέπει στην αποφυγή μιας εκδήλωσης επίθεσης η οποία αιωρείται ουσιαστικά στον επιτιθέμενο μια πρόσβαση στην πηγή των πληροφοριών. Ο μηχανισμός που εμπλέκεται σε αυτόν τον τρόπο άμυνας, περιλαμβάνει την απόκρυψη σημαντικών πληροφοριών, τον έλεγχο εισόδου από τους χρήστες αλλά και την πιστοποίηση τους.

Ουσιαστικά, η απόκρυψη των πηγών πληροφοριών στοχεύει στην κοινολόγηση των πληροφοριών σε μη εξουσιοδοτημένα πρόσωπαΟ σχεδιασμός του συστήματος βάσεως δεδομένων ασφαλείας της Google.Com οφείλει να αποτελεί τμήμα του αρχικού σχεδιασμού του συστήματος και όχι μια διαδικασία που θα εκτελείται μετά την εγκατάσταση του συστήματος. Οι λόγοι είναι απλοί. Αφενός είναι οικονομικότερο να σχεδιάζονται και να υλοποιούνται ταυτόχρονα το σύστημα και η ασφάλεια του και αφετέρου είναι λειτουργικότερο

ΒΙΒΛΙΟΓΡΑΦΊΑ

- Adams, J., 1998, "*The next world war*", Simon and Schuster
- BloomBecker, B., 1990, "*Spectacular Computer Crimes*", Dow Jones – Irwin
- Branscomb, A. W., 1994, "*Who Owns Information*", Basic Books
- Cavoukian, A., Tapscott, D., 1997, "*Who Knows"*, McGraw-Hill
- Denning, D., E., 1982, "*Cryptography and Data Security*", Addison – Wesley

- Denning, P., J., 1990, "*Computers Under Attack : Intruders, Worms and Viruses*", ACM Press
- Diffie, W., Landau, S., 1998, "*Beyond Calculation*", The MIT Press
- Hager, N., 1996, "*Secret Power*", Craig Cotton Publishing, New Zealand, 1996
- Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books
- Kotler P., 2000, "*Research Methods*", Prentice Hall
- Libicki, G., M., 1995, "*What information is warfare?"*, National Defense University of USA
- Ludlow, P., 1996, "*High Noon on the Electric Frontier*", The MIT Press
- McCarthy, L., 1997, "*Intranet Security*", Prentice Hall
- Meinel, C., P., 1998, "*The Happy Hacker"*, American Eagle Publications
- Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall
- Rosenoer, J., 1997, "*CyberLaw"*, Springer – Verlag
- Timpton, H., F., Ruthberg, Z., G., 1993, "*Handbook of Information Security Management*", Auerbach
- Saunders et al, 2000, "*Business Research*", Routledge
- Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall
- Slade, P., 1994, "*Guide to Computer Viruses*", Springer – Verlag
- Schweizer, P., 1993, "*Friendly Spies*", The Atlantic Monthly Press
- Sterling, B., 1992, "*The Hacker Crackdown*", Bantam
- Taylor, A., 1999, "*The Hackers*", Routledge
- Wayner, P., 1996, "*Disappearing Cryptography*", Academic Press
- Eisenmann T., (2004), "*Betting on Google's future*", The Wall Street Journal, August 24, p.B2
- Eisenmann T.R. and Herman K., (2006), "*Google Inc.*", Harvard Business review
- Elgin B. and Hesseldahl A., (2005). "*Google's Grand Ambitions*", Business Week, September 5, p.35 [http://www.factiva .com, accessed 26/01/2007]
- Mahaney M. (2005), "*GOOG: Increased Conviction in Google, Citigroup Global Markets*"
- Kelleher K., (2005), "*Who's afraid of Google?"*, Wired No.13.12, December
- Μπουραντάς Δ., Παπαλεξανδρή Ν., (1998), "*Εισαγωγή στη Διοίκηση Επιχειρήσεων*", εκδόσεις Μπένου, Αθήνα
- Χολέβας Γ. (1995), "*Οργάνωση και Διοίκηση*", εκδόσεις Interbooks, Αθήνα
- Montana P., Charnow B., (1993), "*Μάνατζμεντ*", εκδόσεις Κλειδάριθμος

- Johansson J., (2006), “Global Marketing: foreign entry, local marketing & global management”, McGraw Hill International Edition
- Καζάζης Ν. (2000), “Αποτελεσματικό Μάρκετινγκ για κερδοφόρες πωλήσεις”, εκδόσεις Σταμούλης
- Κωνσταντίνου, Μ., (2000), Αρθρο “Διαφήμιση στο Ελληνικό ιντερνέτ - impressions ή χρονοχρέωση”, Περιοδικό e-market
- Jankowich, (2004), “Research Methods for studies and projects”, London: Macmillan Press Ltd.
- Saunders M., Lewis P. and Thornhill A., (2000), “Research Methods For Business Students”, London: Prentice Hall.
- Saunders et all, (2005), “Specified ways for research and analysis of data”, Prentice Hall
- Sekaran U., (1992), “Research Methods for Business, A Skill Building Approach”. New York: John Wiles and Sons Inc.
- Zikmund W.G., (2000), “Business Research Methods”. London: Harcourt college publishers.
- Eurostat, 2008, Στοιχεία Χρήσης Διαδικτυακών Υπηρεσιών

ΠΑΡΑΡΤΗΜΑ 1

Τα γραφεία της Google στην Ζυρίχη: ένας χώρος γεμάτος φαντασία και δημιουργικότητα

Privacy Eggs