ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑΚΗ ΗΘΙΚΗ
Υπάρχουσα νομοθεσία, πραγματικότητα και ηθικές υποχρεώσεις του χρήστη στο διαδίκτυο

Εργασία για το μάθημα:

Υπηρεσίες Προστιθέμενης Αξίας στο Διαδίκτυο

Των προπτυχιακών φοιτητών:

Κωνσταντίνος Γιαννακόπουλος (885)

Χρήστος Ζιγκόλης (897)

Απόστολος Κρητικός (914)

Γεώργιος Φιλίππου (1236)

Τμήμα Πληροφορικής

Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης,

Θεσσαλονίκη 2007

Περιεχόμενα

Ενότητα 1η

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Εισαγωγή

Ορισμός

Το ηλεκτρονικό έγκλημα είναι ένας όρος που χρησιμοποιείται για να περιγράψει την παράνομη δραστηριότητα στην οποία ηλεκτρονικοί υπολογιστές και δίκτυα αυτών χρησιμοποιούνται ως εργαλεία ή ακόμα πολλές φορές και ως στόχοι για την εκτέλεση αξιόποινων πράξεων.

Μορφές του ηλεκτρονικού εγκλήματος

Σύμφωνα με την συνθήκη της Βουδαπέστης που πραγματοποιήθηκε στις 23/11/2001 έγινε ταυτοποίηση των ηλεκτρονικών εγκλημάτων στις εξής 4 κύριες κατηγορίες.

1. Αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων (Παράνομη πρόσβαση, παράνομη υποκλοπή, επέμβαση σε δεδομένα)
   - DoS (Denial of Service)
   - Viruses
   - Password Cracking
   - Employee Theft
2. Αδικήματα που σχετίζονται με τους υπολογιστές (απάτη, πλαστογραφία)
   - Phising
   - Pharming
   - Credit Cards
3. Αδικήματα σχετικά με το περιεχόμενο
   - Παιδική πορνογραφία
4. Αδικήματα που σχετίζονται με τη καταπάτηση πνευματικής ιδιοκτησίας
   - Παράνομο downloading
5. Ευθύνες υποβοήθησης και κυρώσεις

Στην Ελλάδα, αλλά και παγκοσμίως, τα πιο συνηθισμένα ηλεκτρονικά εγκλήματα είναι τα ακόλουθα :

- Απάτες μέσω διαδικτύου
- Παιδική πορνογραφία
- Cracking και hacking
- Διακίνηση – Πειρατεία λογισμικού
- Απάτες με Πιστωτικές κάρτες
- Διακίνηση ναρκωτικών
- Έγκλημα στα chat rooms

Υπάρχουν πάρα πολλά παραδείγματα στις μέρες μας, και στην Ελλάδα και στο εξωτερικό, που κατηγοριοποιούνται σύμφωνα με τα παραπάνω, αλλά αρκετά από αυτά μένουν ατιμώρητα.

Ανάγκη κατάλληλης νομοθεσίας – Συνθήκη της Βουδαπέστης

Τα τελευταία χρόνια μαζί με την άνθιση της τεχνολογίας των υπολογιστών και κυρίως του διαδικτύου έχουν «επινοηθεί», κατά κάποιον τρόπο, και νέες μορφές εγκληματικότητας που χρήζουν ιδιαίτερης μεταχείρισης από πλευράς νόμου και ποινικών κυρώσεων. Υπεισέρχεται ο χαρακτηρισμός της ιδιαίτερης μεταχείρισης για το λόγο ότι αυτές οι εγκληματικές πράξεις απαιτούν εξειδίκευση και αυξημένη κατάρτιση από πλευράς του εγκληματία αλλά πιο πολύ του υπηρεσιακού οργάνου που χειρίζεται τις ανάλογες υποθέσεις.

Η ελληνική νομοθεσία έχει συντάξει νομοθετήματα σύμφωνα με τα οποία διαχειρίζεται τέτοια εγκλήματα. Εκτός από το εθνικό νομοθετικό πλαίσιο υπάρχουν και γενικές υποδείξεις που έχουν θεσπιστεί στο Συνέδριο της Βουδαπέστης, που έγινε στις 23 Νοεμβρίου 2001, από 26 χώρες της ευρωπαϊκής κοινότητας (μέσα στις οποίες και η Ελλάδα) και χώρες όπως η Αμερική και η Κίνα.
Σκοπός αυτού του άρθρου, όπως αναφέρθηκε παραπάνω, είναι να παρουσιάσει τις μορφές ηλεκτρονικού εγκλήματος και τις πτυχές της υπάρχουσας νομοθεσίας δίνοντας και ορισμένα ενδεικτικά παραδείγματα.
Ιδιαίτερη προσοχή δόθηκε στη σωστή ισορροπία μεταξύ των αναγκών της πάταξης των ηλεκτρονικών εγκλημάτων και του σεβασμού βασικών ανθρωπίνων δικαιωμάτων όπως αυτά προσδιορίστηκαν κυρίως μετά το Β’ Παγκόσμιο, το 1950 στο Ευρωπαϊκό Συνέδριο για τη προάσπιση των Ανθρωπίνων Δικαιωμάτων και των Βασικών Ελευθεριών όπως και σε άλλες διεθνείς συμφωνίες. Οι τελευταίες επαναβεβαιώνουν το δικαίωμα καθενός να έχει την άποψη του χωρίς παρεμπόδιση, όπως και την ελευθερία της έκφρασης, συμπεριλαμβανομένης της ελευθερίας αναζήτησης, λήψης και μετάδοσης πληροφοριών και ιδεών κάθε τύπου ανεξάρτητα από σύνορα. Πρέπει να γίνει σαφές το γεγονός ότι η Συνθήκη αυτή βασίστηκε σε συμφωνίες και νομοθεσίες μεταξύ των χωρών της Ευρώπης που προϋπήρχαν και έπρεπε να αναθεωρηθούν ούτως ώστε να κάνουν την εξιχνίαση ηλεκτρονικών εγκλημάτων πιο αποτελεσματική και να επιτρέψουν την συλλογή στοιχείων κατά τέτοιων εγκλημάτων σε ηλεκτρονική μορφή.

Κάθε χώρα πρέπει να δίνει στις αρμόδιες αρχές τη δυνατότητα :

- προστασίας συγκεκριμένων δεδομένων από την απώλεια ή παραποίηση.
- να ζητήσει την κατάθεση δεδομένων που υπάρχουν στον Η/Υ ενός πολίτη της χώρας όπως και πληροφορίες εγγεγραμμένων χρηστών από ISPs.
- κατάσχεσης υπολογιστικού συστήματος και έρευνας στα αποθηκευμένα δεδομένα αυτού.
- καταγραφή της κίνησης του δικτύου σε πραγματικό χρόνο.
- συλλογής ή εγγραφής με τεχνικά μέσα δεδομένων του δικτύου (υποκλοπή δεδομένων).

Επίσης, αποφασίστηκαν διατάγματα που προβλέπουν και προωθούν τη συνεργασία μεταξύ των χωρών. Αυτή η συνεργασία αποτελεί σημαντικό παράγοντα για την συνεχή βελτίωση των διατάξεων. Η επικοινωνία μεταξύ των αρμόδιων αρχών είναι αναγκαία για την εξιχνίαση διαδικτυακών εγκλημάτων.

Μέσα από αυτές τις προσεγγίσεις θα παρουσιαστούν αδυναμίες και ελλείψεις των νόμων, θα σχολιαστούν οι συνέπειες τέτοιων πράξεων και θα αναφερθεί το πλαίσιο της διαδικτυακής ηθικής μέσα στο οποίο πρέπει τυπικά να κινούνται οι χρήστες μέσα στο διαδίκτυο.

Κεφάλαιο 1ο

Μορφή 1η Αδικήματα σχετικά με την ακεραιότητα των δεδομένων

1. VIRUSES

1.1 Εισαγωγή – Ιστορική Αναδρομή

Μέχρι πριν από μερικά χρόνια οι viruses ήταν η βασικότερη απειλή των Ηλεκτρονικών Υπολογιστών. Οι viruses είναι προγράμματα τα οποία αναπαράγονται προσβάλλοντας άλλα αρχεία και εφαρμογές, προκαλώντας ζημιές στον υπολογιστή που προσβάλουν. Αργότερα εμφανίστηκαν τα worms, προγράμματα τα οποία δε χρειάζεται να προσβάλλουν άλλα προγράμματα για να πολλαπλασιαστούν, αφού έχουν τη δυνατότητα να αναπαράγονται μόνα τους, δημιουργώντας αντίγραφα του εαυτού τους με σκοπό να καταστρέψουν τα δίκτυα στα οποία διεισδύουν. Σε αυτά προστίθενται τα Trojans και τα backdoors Trojans. Τα Trojans φαινομενικά δεν προσβάλλουν τα προγράμματα, αλλά έχουν τη δυνατότητα να κλέβουν τα passwords και να capture keystrokes, επιτρέποντας την πρόσβαση τρίτων στον υπολογιστή.

Στις μέρες μας, λόγω της ευρύτερης χρήσης των υπολογιστών και του Internet, έχουν εμφανιστεί νέες απειλές, που είναι το ίδιο καταστροφικές, τα γνωστά malware. Ο όρος malware προέρχεται από τις λέξεις malicious software. Malware θεωρείται οποιοδήποτε πρόγραμμα, έγγραφο ή μήνυμα που μπορεί να προκαλέσει ζημιά στους υπολογιστές. Ζημιά θεωρείται τόσο η απώλεια δεδομένων από τον υπολογιστή όσο και η μείωση της απόδοσης του συστήματος. Εκτός από τα viruses, worms, Trojans and backdoor Trojans, malware θεωρούνται τα:

Dialer: Πρόγραμμα που πραγματοποιεί σύνδεση με έναν ειδικό αριθμό.

Joke: Ένα μη επιβλαβές πρόγραμμα που προσποιείται ότι πραγματοποιεί ζημιές στον υπολογιστή.

Security risk: Ένα νόμιμο εργαλείο που μπορεί να χρησιμοποιηθεί για malicious σκοπούς.

Hacking tool: Εργαλείο που επιτρέπει στους hackers να πραγματοποιούν ζημιές σε affected computers.

Vulnerability: Προγραμματιστικό λάθος σε μία εφαρμογή που μπορεί να χρησιμοποιηθεί για να προσπεράσει την ασφάλεια των υπολογιστών και για να ελέγξει κάποιος τρίτος τον υπολογιστή.

Spy program: Πρόγραμμα που συλλέγει στοιχεία σχετικά με τις συνήθειες και τα ενδιαφέροντα των χρηστών στο Internet και τα στέλνει σε διαφημιστικές εταιρίες.Hoax: E-mail που προειδοποιεί για viruses που δεν υπάρχουν.

Spam: The mass-mailing of unsolicited mail, which is generally commercial mail.

1.2 Virus, worms, trojans και backdoors

1.2.1 Viruses

Πρόγραμμα που μπορεί να εισέλθει σε έναν υπολογιστή με πολλούς τρόπους και μπορεί να προκαλέσει από απλές ενοχλήσεις μέχρι σοβαρές δυσλειτουργίες. Η είσοδος στον υπολογιστή μπορεί να γίνει από e-mail, Internet, μεταφορά δίσκων, κτλ.

Χαρακτηριστικά:

- Για να πολλαπλασιαστούν πρέπει να προσβάλλουν άλλα αρχεία και προγράμματα.
- Όταν τρέχουν μπορούν να προκαλέσουν από απλές ενοχλήσεις μέχρι και σοβαρές δυσλειτουργίες.

Η ονομασία τους οφείλεται στις ομοιότητες που έχουν με τους βιολογικούς ιούς. Ένας βιολογικός ιός για να αναπαραχθεί πρέπει να εισέλθει στο σώμα και να προσβάλει τα κύτταρα. Όπως ένας βιολογικός ιός ονομάζεται μικρο-οργανισμός, έτσι και ένας virus ονομάζεται micro-program.

1.2.2 Worms

Ένα worm είναι ένα πρόγραμμα παρόμοιο με ένα virus. Έχει τη δυνατότητα να πολλαπλασιάζεται μόνο του και να προκαλέσει αρνητικές επιπτώσεις στο σύστημα. Η βασική διαφορά τους από τους viruses είναι ότι δε χρειάζεται να προσβάλουν άλλα αρχεία για να αναπαραχθούν. Καθώς πολλαπλασιάζονται καταστρέφουν αρχεία. Μπορούν να πολλαπλασιάζονται με πάρα πολύ γρήγορους ρυθμούς και να επεκτείνονται στα δίκτυα προκαλώντας μέχρι και την κατάρρευση αυτών. Συνήθως στέλνονται με e-mail.

Κάποια γνωστά worms είναι: I Love You, Navidad, Pretty Park, Happy99 και ExploreZip.

1.2.3 Trojans

Τα trojans διαφέρουν τους viruses διότι δεν πολλαπλασιάζονται προσβάλλοντας άλλα αρχεία, αλλά και λειτουργούν διαφορετικά από τα worms αφού δεν πολλαπλασιάζονται.

Τα Trojans, όπως προδίδει και το όνομά τους, εμφανίζονται ως μη επιβλαβή προγράμματα που εισβάλλουν σε έναν υπολογιστή με οποιοδήποτε τρόπο. Όταν αυτά τα προγράμματα εκτελεστούν εγκαθιστούν στον υπολογιστή επιβλαβή

προγράμματα. Ένα trojan μπορεί να μην ενεργοποιήσει όλες του τις επιδράσεις από την αρχή, αλλά όταν ενεργοποιηθούν μπορούν να προκαλέσουν καταστροφή στο σύστημα. Έχουν τη δυνατότητα να διαγράφουν αρχεία, να καταστρέφουν πληροφορίες από τον σκληρό δίσκο, και να δημιουργούν σοβαρά κενά (backdoors) στο σύστημα ασφαλείας του υπολογιστή. Έτσι τα trojans αποκτούν πλήρη πρόσβαση στο σύστημα επιτρέποντας έναν τρίτο χρήστη να αντιγράψει, και να οικειοποιηθεί εμπιστευτικές πληροφορίες.

Κάποια γνωστά trojans είναι: Backdoor, Donald Dick, Crack2000, Extacis, KillCMOS and Netbus.

1.2.4 Backdoors

Πρόκειται για προγράμματα που προσβάλλουν τον υπολογιστή χωρίς να γίνονται αντιληπτά από τον χρήστη, καθώς θεωρούνται αρχικά μη επιβλαβή. Μόλις εκτελεστούν, δημιουργούν ένα κενό στο σύστημα ασφαλείας του υπολογιστή (backdoor) μέσω του οποίου μπορούν να αποκτήσουν τον έλεγχο του υπολογιστή που έχουν προσβάλλει. Αυτό επιτρέπει στον κακόβουλο χρήστη να κάνει ενέργειες ύστερα από συμβιβασμό με τον χρήστη, χωρίς ο χρήστης να είναι δυνατό να καταλάβει κάτι τέτοιο, ή να παρεμποδίσει την πραγματοποίηση λειτουργιών. Οι ενέργειες που ένας κακόβουλος χρήστης μπορεί να κάνει, μπορεί να αποβούν καταστροφικές για τον υπολογιστή που έχει προσβληθεί. Ένας κακόβουλος χρήστης μπορεί να διαγράψει αρχεία, να καταστρέψει όλες τις πληροφορίες που είναι αποθηκευμένες στον hard disk, να οικειοποιηθεί εμπιστευτικά στοιχεία και να τα στείλει σε κάποια άλλη διεύθυνση ή να ανοίξει τα communication ports του υπολογιστή, επιτρέποντας τον απομακρυσμένο έλεγχο του υπολογιστή.

Κάποια γνωστά backdoors είναι: Orifice2K.sfx, Bionet.318, Antilam και Subseven.213.

1.3 Η νέα γενιά των Malware

Η νέα γενιά των malware που έχει σαν σκοπό να αποκτήσει πρόσβαση στα προγράμματα του ανυποψίαστου χρήστη, να υποκλέψει προσωπικά δεδομένα και να πραγματοποιήσει συνδέσεις με τον υπολογιστή θύμα περιλαμβάνει:

1.3.1 Spyware

Είναι εφαρμογές που συγκεντρώνουν πληροφορίες σχετικές με τις προτιμήσεις του χρήστη, τα ενδιαφέροντά του και την όλη του δραστηριότητα κατά το browsing. Όλα τα στοιχεία που συλλέγονται στέλνονται στον δημιουργό του spyware ή σε τρίτους είτε άμεσα είτε αφού πρώτα αποθηκευτούν στον υπολογιστή του χρήστη. Τα spyware μπορούν να εγκατασταθούν στον υπολογιστή με πολλούς τρόπους. Ένας τρόπος είναι μέσω Trojan που τα εγκαθιστούν χωρίς την άδεια του χρήστη, άλλος τρόπος είναι μέσα από την επίσκεψη των web pages που έχουν συγκεκριμένα ActiveX controls ή κώδικα που εκμεταλλεύεται κάποια vulnerabilities των προγραμμάτων, άλλος τρόπος είναι μέσω shareware ή freeware applications που κατεβάζουμε από το Internet, κλπ.

Αυτά μπορούν να εγκατασταθούν με τη συγκατάθεση και επίγνωση του χρήστη ή και χωρίς.

1.3.2 Adware

Με τον όρο αυτό αναφερόμαστε στα προγράμματα που εμφανίζουν διαφημίσεις, Advertising Software. Αυτά τα προγράμματα εμφανίζουν διαφημίσεις με κάθε τρόπο pop-up windows, banners, αλλαγές στη home page του browser, κλπ. Τα διαφημιζόμενα προϊόντα συσχετίζονται με τους δημιουργούς των προγραμμάτων αυτών ή με τρίτους. Όπως και με τα spyware, η εγκατάσταση των προγραμμάτων αυτών μπορεί να γίνει είτε με τη συγκατάθεση και την επίγνωση του χρήστη ή και χωρίς.

1.3.3 Dialer

Πρόκειται για πρόγραμμα το οποίο έχει τη δυνατότητα να αποσυνδέει την τηλεφωνική σύνδεση στο Internet, χωρίς να γίνεται αυτό αντιληπτό από τον χρήστη και συνδέεται στο Internet μέσω ενός άλλου αριθμού που χρεώνει τον χρήστη πολύ υψηλότερο ποσοστό και προφανείς συνέπειες στο λογαριασμό τηλεφώνου του χρήστη.

1.3.4 Cookies

Είναι μικρά text files τα οποία αποθηκεύονται στον browser του υπολογιστή του χρήστη. Οι πληροφορίες που περιέχουν μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς:

- Personalize web pages ανάλογα με τις προτιμήσεις του χρήστη.
- Συγκέντρωση στατιστικών σχετικών με τις web pages που έκανε browse ο χρήστης και πόση ώρα έμεινε σε αυτές.

Η χρήση τους δεν είναι κακόβουλη εκ των προτέρων, όμως όλα τα προσωπικά στοιχεία που δίνει ο χρήστης σε web pages (ακόμα και αριθμοί πιστωτικών καρτών) αποθηκεύονται σε cookies. Τα cookies που χρησιμοποιούνται στα user profiles μπορούν να χρησιμοποιηθούν είτε από διαφημιστές ή από τρίτους που μπορούν να χρησιμοποιήσουν αυτά τα προσωπικά στοιχεία καταπατώντας την προστασία των προσωπικών δεδομένων (privacy).

1.3.5 Spam

Είναι αυτόκλητα e-mail τα οποία όμως στέλνονται μαζικά και έχουν διαφημιστικό περιεχόμενο. Ο όρος προέρχεται από το spiced ham που είναι η πρώτη κονσερβοποιημένη στερεά τροφή που δε χρειαζόταν να διατηρείται στο ψυγείο. Ιστορικά, η πρώτη περίπτωση spam ήταν ένα γράμμα που έστειλε το 1978 η εταιρεία *Digital Equipment Corporation*. Η εταιρεία αυτή είχε στείλει μία διαφήμιση για τους DEC-20 υπολογιστές της σε όλους τους χρήστες του Arpanet (πρόγονος του Internet), στις δυτικές Η.Π.Α. Παρόλα αυτά, το όνομα spam καθιερώθηκε το 1994

όταν μία διαφήμιση εμφανίστηκε στο Usenet, από τους δικηγόρους Lawrence Cantera και Martha Siegel, οι οποίοι παρείχαν πληροφορίες για τις υπηρεσίες τους για τη συμπλήρωση αιτήσεων που χρειάζονταν για την έκδοση άδειας εργασίας στις Η.Π.Α. Η συγκεκριμένη διαφήμιση επιστράφηκε στα discussion groups με τη χρήση ενός script.

Χαρακτηριστικά αυτών των e-mail:

- Η διεύθυνση του αποστολέα είναι άγνωστη στον χρήστη και τις περισσότερες φορές είναι ψεύτικη, δηλαδή δεν υπάρχει καθόλου.
- Στο e-mail δεν μπορούμε να κάνουμε reply.
- Παρουσιάζεται ένα catchy θέμα στον χρήστη.
- Έχει διαφημιστικό περιεχόμενο.
- Τα περισσότερα είναι γραμμένα στα αγγλικά, διότι προέρχονται από τις Η.Π.Α. ή την Ασία.

Τα spam δε διαδίδονται μόνο μέσω e-mail. Ανάλογα με το μέσο με το οποίο διαδίδονται έχουν και αντίστοιχο όνομα. Έτσι έχουμε:

- Spam: Στέλνονται μέσω e-mail.
- Spim: Χρησιμοποιούν Instant Messaging applications (MSN Messenger, Yahoo Messenger κλπ)
- Split: Spam στην IP telephony. Η IP telephony χρησιμοποιεί το Internet για την πραγματοποίηση τηλεφωνικών κλήσεων.
- Spam SMS: spam που στέλνεται με τη μορφή SMS στα κινητά τηλέφωνα.

Τέλος, το spam είναι ένα φαινόμενο που αυξάνεται καθημερινά και αποτελεί ένα μεγάλο ποσοστό των e-mail που διακινούνται. Καθώς βελτιώνονται οι τεχνικές καταπολέμησης των spam και των spammers (αυτοί που στέλνουν τα spam), οι τελευταίοι τροποποιούν συνεχώς τις τεχνικές τους για να αποφύγουν τις μεθόδους πρόληψης και εξουδετέρωσης των χρηστών των υπολογιστών.

1.4 Vulnerability

Με τον όρο *vulnerability* εννοούμε ένα προγραμματιστικό λάθος σε μία εφαρμογή, το οποίο δημιουργεί κενά ασφαλείας στον υπολογιστή, όταν γίνει η εγκατάσταση της εφαρμογής αυτής, επιτρέποντας σε τρίτους να έχουν πρόσβαση σε αυτόν τον υπολογιστή. Όταν λέμε προγραμματιστικό λάθος, εννοούμε ότι κάποιες λειτουργίες αυτής της εφαρμογής μπορούν να την οδηγήσουν σε δυσλειτουργίες. Αυτό το bug μπορεί να χρησιμοποηθεί από έναν κακόβουλο χρήστη για να αποκτήσει πρόσβαση στον υπολογιστή χωρίς την άδεια του χρήστη δίνοντας του τη δυνατότητα να τρέχει εφαρμογές, να ανοίγει αρχεία, να διαγράφει δεδομένα ακόμα και να στείλει νέους viruses. Παρόλου που τα πιο συνηθισμένα vulnerabilities βρίσκονται στα operating systems, στους Internet browsers και στα mail programs, οποιοδήποτε πρόγραμμα μπορεί να έχει vulnerabilities: word processing applications, databases, sound file players, κλπ. Τα vulnerabilities δεν γίνονται αντιληπτά στον χρήστη από την αρχή και

δεν προκαλούν από μόνα τους κάποια δυσλειτουργία στον υπολογιστή, αλλά τον αφήνουν εκτεθειμένο σε viruses, worms και Trojans τα οποία μπορούν να έχουν καταστροφικές συνέπειες. Για την προστασία μας, θα πρέπει να ενημερωνόμαστε για τα vulnerabilities των προγραμμάτων που έχουμε εγκαταστήσει και να κάνουμε update με τα τελευταία security patches, τα οποία διατίθενται από τις εταιρίες αυτών των εφαρμογών και είναι διαθέσιμα στα websites τους.

Τέλος, μερικά γνωστά worms που εκμεταλλεύονται τα vulnerabilities των προγραμμάτων είναι: Blaster, Bugbear.B, Klez.I και Nachi.A.

1.5 Hoaxes and jokes

Πρόκειται για ομάδα μηνυμάτων που φαίνεται να ανήκουν στους viruses, στην πραγματικότητα όμως δεν είναι viruses.

Τα Hoaxes δεν είναι viruses, αλλά λανθασμένα μηνύματα που στέλνονται με email και προειδοποιούν τους χρήστες για viruses που δεν υπάρχουν. Η πρόθεσή και ο σκοπός αυτών των μηνυμάτων είναι, διαδίδοντας φήμες, να προκαλούν πανικό στους χρήστες στους οποίους στέλνονται. Οι “προειδοποιήσεις ” περιέχουν τεχνικούς όρους για να παραπλανήσουν τους χρήστες, ενώ κάποιες φορές αναφέρουν και το όνομα γνωστών πρακτορείων παρακολούθησης δημοσιευμάτων για να ξεγελάσουν τους χρήστες και να γίνουν πιστευτές οι αναφορές για viruses που αναφέρουν.

Τα Jokes είναι προγράμματα που σχεδιάζονται για να παραπλανήσουν τους χρήστες, αφού τους κάνουν να πιστεύουν ότι ο υπολογιστής τους έχει προσβληθεί από virus. Αυτά τα προγράμματα προσομοιώνουν τις καταστροφικές συνέπειες των viruses, όπως για παράδειγμα τη διαγραφή αρχείων από το δίσκο. Είναι περισσότερο ενοχλητικά παρά επιβλαβή, παρόλα αυτά, οι χρήστες για να προστατευτούν πρέπει να μην ανοίγουν τα συνημμένα αρχεία από τα ύποπτα email που δέχονται.

1.6 Η Δράση των viruses

Βασικοί στόχοι των viruses αποτελούν τα program files, δηλαδή τα αρχεία με επέκταση *com* και *exe*, όμως προσβάλλονται και άλλοι τύποι αρχείων όπως web pages (*html*), Word documents (*doc*), Excel spreadsheets (*xsl*), κλπ. Όταν ένα αρχείο προσβάλλεται από έναν virus, συμπεριφέρεται εντελώς διαφορετικά και οι συνέπειες στο σύστημα ποικίλλουν. Αν κάποιο αρχείο που έχει προσβληθεί από virus αποθηκευτεί σε έναν άλλο δίσκο, τότε ο virus μπορεί να προκαλέσει ζημιές και στα άλλα αρχεία που είναι αποθηκευμένα στον δίσκο αυτό.

1.6.1 ENTRY POINTS – SPREADING

Οι viruses μπορούν να εισβάλουν σε έναν υπολογιστή, μέσα από τα communication channels που χρησιμοποιεί για την ανταλλαγή πληροφοριών. Διακρίνονται τρεις κατηγορίες: Internet, Networks, Removable disks.

Το **Internet** αποτελεί το γρηγορότερο μέσο για τη διάδοση ενός virus. Αυτό ισχύει γιατί το Internet παρέχει πολλούς τρόπους μεταφοράς πληροφοριών: email, browsing web pages, μεταφορά αρχείων μέσω FTP, downloading programs, chat και newsgroups. Τρόποι διάδοσης στο Internet:

- *E-mail*: Αποτελεί τον πιο δημοφιλή τρόπο. Το 80% των viruses διαδίδονται μέσω email. Έχουν αναπτυχθεί μάλιστα και τεχνικές που επιτρέπουν στους viruses να διαδίδονται σε όλες τις επαφές του address book του υπολογιστή που προσβάλουν με αποτέλεσμα να προσβάλλονται και άλλοι υπολογιστές.
- *Internet browsing*: Κάποιες web pages περιέχουν Java Applets και ActiveX (προγράμματα που τις κάνουν δυναμικές), τα οποία όμως προσβάλλονται από viruses εύκολα. Οι viruses μπορούν να εισβάλλουν εύκολα στον υπολογιστή του χρήστη που επισκέπτεται αυτές τις σελίδες, ενώ κάποιοι άλλοι μεταφέρουν τους χρήστες σε σελίδες που έχουν προσβληθεί.
- *File Transfer (FTP)*: FTP σημαίνει File Transfer Protocol. Το πρωτόκολλο αυτό επιτρέπει την αποθήκευση δεδομένων (upload) και την αντιγραφή αρχείων (download) μεταξύ των υπολογιστών. Όταν ένα αρχείο κατεβαίνει από ένα FTP site αποθηκεύεται κατευθείαν στον υπολογιστή. Αρχεία από FTP sites μπορεί να περιέχουν viruses που κατεβαίνουν απευθείας στον υπολογιστή.
- *Newsgroups:* Η δυνατότητα που δίνεται στους χρήστες να κάνουν post messages τόσο σε online newsgroups όσο και στα chat (IRC, ICQ), αποτελούν μέσο διάδοσης των viruses, αφού τα messages αυτά μπορεί να περιέχουν viruses.

Τα **Networks** αποτελούνται από υπολογιστές που συνδέονται μεταξύ (μέσω cable, routers, κλπ). Κάθε υπολογιστής του δικτύου έχει πρόσβαση σε όλου τους υπολογιστές του δικτύου, βοηθώντας ομάδες ανθρώπων να δουλεύουν μαζί ανταλλάσσοντας πληροφορίες και χρησιμοποιώντας κοινόχρηστους πόρους. Αυτή η επικοινωνία μεταξύ των υπολογιστών βοηθάει στη διάδοση των viruses, αφού αν προσβληθεί ένας υπολογιστής, όλοι οι άλλοι υπολογιστές που συνδέονται με αυτόν μπορεί να προσβληθούν. Η αλυσιδωτή μεταφορά των viruses στους υπολογιστές του δικτύου μπορεί να το οδηγήσει σε παράλυση.

Removable disks είναι οι συσκευές αποθήκευσης δεδομένων (floppy disks, CD-ROMs, DVDs, κλπ). Αν ένα αρχείο που έχει προσβληθεί από έναν virus τον αποθηκεύσουμε σε μία τέτοια συσκευή, τότε θα προσβληθούν και τα άλλα αρχεία που είναι αποθηκευμένα σε αυτήν, αλλά και ο υπολογιστής στον οποίο διαβάσουμε το αρχείο αυτό.

1.7 Παραδείγματα

Loveletter.UNK **(Γνωστός ως I love you, Loveletter)**

Είναι ένα worm που διαδίδεται μέσω email ή μέσω αρχείων στο IRC. Εμφανίζεται ως ερωτικό μήνυμα και ξεκινά τη δράση του όταν ο χρήστης ανοίξει το συνημμένο αρχείο. Προσβάλλει τον υπολογιστή σον οποίο εκτελείται και έχει επιπλέον τη δυνατότητα να μεταδίδεται σε όλες τις επαφές του Address Book. Τροποποιεί το περιεχόμενο των αρχείων με επεκτάσεις: VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, JPG, JPEG, MP3 και MP2. Κλέβει από τον χρήστη προσωπικά δεδομένα και τα στέλνει στον author του.

Όταν ξεκινάει τη δράση του κατεβάζει το Trojan *Barok* από το Internet. Συλλέγει τα προσωπικά δεδομένα του χρήστη κάθε 48 δευτερόλεπτα. Αυτά τα δεδομένα είναι Windows passwords και name, password, telephone number, IP address και το DNS με το WINS του server που χρησιμοποιούνται για τη σύνδεση. Όλα αυτά τα δεδομένα τα στέλνει στο email: mailme@super.net.ph.

Το συγκεκριμένο worm αλλάζει τις επεκτάσεις VBS, VBE, JS, JSE, CSS, WSH, SCT και HTA σε VBS τροποποιώντας το περιεχόμενο των αρχείων και το μέγεθός τους. Επίσης μπορεί να προσβάλλει και αρχεία με επεκτάσεις: JPG, JPEG, MP3, MP2, COM, BAT, HTM, HTML.

Navidad.A **(Γνωστός ως Navidad, W32/Navidad.A-m, I-Worm.Navidad)**

Είναι ένα worm που μεταδίδεται μέσω email. Το worm αυτό ενεργοποιείται στους υπολογιστές που έχουν απαντήσει σε ένα email που τους στέλνεται. Το μήνυμα περιέχει ένα εκτελέσιμο αρχείο, το *NAVIDAD.EXE* που προσβάλει τον υπολογιστή. Πρόκειται για ένα επικίνδυνο worm το οποίο εμποδίζει εκτελέσιμα αρχεία να τρέξουν και εμφανίζει warnings και error messages όταν ο υπολογιστής ξεκινάει. Διαδίδεται πάρα πολύ γρήγορα, αφού στέλνει αντίγραφα του εαυτού του με τη μορφή email στις ηλεκτρονικές διευθύνσεις που περιέχονται στο Inbox του mail program, ως reply.

1.8 Επίσημα στοιχεία – GOOGLE

Google – The Ghost in the Browser

Η σκοτεινή πλευρά του Internet
Κακόβουλο κώδικα περιέχουν «μία στις δέκα ιστοσελίδες» στο Διαδίκτυο

Μία στις δέκα ιστοσελίδες που εξετάστηκαν σε βάθος από το Google βρέθηκαν να περιέχουν κακόβουλο κώδικα, ο οποίος μπορεί να βλάψει τον ηλεκτρονικό υπολογιστή του χρήστη.

Συγκεκριμένα, ερευνητές της εταιρείας υπέβαλλαν σε εις βάθος ανάλυση 4,5 εκατομμύρια ιστοσελίδες και διαπίστωσαν ότι 450.000 εξ αυτών μπορούσαν να εγκαταστήσουν κακόβουλο λογισμικό, εν αγνοία του χρήστη και, φυσικά, χωρίς τη συγκατάθεσή του (drive-by downloads).

Όπως σημειώνουν οι ερευνητές του Google στην εργασία τους με τίτλο *The Ghost in the Browser*, άλλες 700.000 ιστοσελίδες περιέχουν κώδικα ο οποίος θα μπορούσε ενδεχομένως να θέσει σε κίνδυνο τον υπολογιστή εκείνων που τις επισκέπτονται.

Η μέθοδος των λεγόμενων drive-by downloads τείνει να γίνει ολοένα και πιο συνηθισμένη για τη μόλυνση του υπολογιστή, την κλοπή ευαίσθητων δεδομένων ή ακόμα και την εξ αποστάσεως χειρισμό του μολυσμένου υπολογιστή.

Συνήθως οι δράστες χρησιμοποιούν τεχνάσματα για να προσελκύσουν το ενδιαφέρον του χρήστη (πορνογραφία, πρόσβαση σε υλικό προστατευμένο με πνευματικά δικαιώματα κ.ά.). Από εκεί και πέρα, χρησιμοποιούνται αδυναμίες των browsers για να εγκατασταθεί το κακόβουλο λογισμικό.

Οι ερευνητές σημειώνουν επίσης ότι οι δράστες συχνά εγκαθιστούν κακόβουλο υλικό σε «καθαρούς» δικτυακούς τόπους, χρησιμοποιώντας τα τμήματα εκείνα που δεν ελέγχονται από το διαχειριστή του site.

Τέτοια τμήματα μπορεί να είναι διαφημιστικά banner, ή μικρά προγράμματα (widgets) που απεικονίζουν ποικίλα πράγματα, επί παραδείγματι ένα ημερολόγιο ή ένα μετρητή επισκεψιμότητας.

Η σημαντική αύξηση του περιεχομένου στο Διαδίκτυο που δημιουργείται από τους ίδιους τους χρήστες (ιστολόγια, forum κ.λπ.) αυξάνει τους πιθανούς «φορείς» κακόβουλου λογισμικού, όταν π.χ. τρίτοι παραπέμπουν σε εικόνες ή άλλο υλικό, πιθανώς επιβλαβές.

Ακόμη διαπιστώθηκε ότι επιτήδειοι μπορούν να αποκτήσουν τον έλεγχο ολόκληρων servers, μολύνοντας όλες τις ιστοσελίδες που φιλοξενούν.

Όπως σημειώνει το BBC, η Google έχει ξεκινήσει ένα φιλόδοξο, όσο και δύσκολο, πρόγραμμα καταγραφής όλων των ιστοσελίδων του Διαδικτύου που μπορεί να είναι επιβλαβείς.

Αν και το Google διαθέτει ήδη μία λειτουργία προειδοποίησης των χρηστών, με σχετική ένδειξη στα αποτελέσματα αναζήτησης, οι ερευνητές παραδέχονται ότι «το να βρεις όλους τους φορείς ιών στο Internet προϋποθέτει σχεδόν πλήρη γνώση του Διαδικτύου στο σύνολό του».

2. Επιθέσεις Άρνησης Υπηρεσίας (DoS Attacks)

Στο κόσμο της ασφάλειας των υπολογιστών και των ηλεκτρονικών εγκλημάτων, μια επίθεση άρνησης υπηρεσίας (denial-of-service attack) είναι η προσπάθεια να καθιστούν οι πόροι ενός υπολογιστή απρόσιτοι στους προβλεπόμενους χρήστες τους.
Αν και οι τρόποι, οι στόχοι όπως και τα μέσα που χρησιμοποιούνται μπορούν να διαφέρουν, σε γενικές γραμμές τέτοιες επιθέσεις περιλαμβάνουν την πρόθεση ενός ή περισσότερων ανθρώπων να εμποδίσουν ένα Ιστοχώρο από το να λειτουργεί επαρκώς ή καθόλου, προσωρινά ή και επ' αόριστον.
Συνήθως οι δράστες τέτοιων επιθέσεων στοχεύουνε χώρους στο διαδίκτυο που φιλοξενούνται σε εξυπηρετητές που είναι γνωστοί για την αξιοπιστία τους και τα υψηλά κριτήρια ασφάλειας που πληρούν.

Μια συνηθισμένη μέθοδος επίθεσης περιλαμβάνει το «πλημμύρισμα» του εξυπηρετητή-στόχου με ένα καταιγισμό από εξωτερικές αιτήσεις ώστε να μη μπορεί να ανταπεξέλθει στις πραγματικές αιτήσεις που έρχονται από το διαδίκτυο ή να το κάνει τόσο αργά που να τον καθιστά στην ουσία ανενεργό. Σε γενικές γραμμές οι επιθέσεις άρνησής υπηρεσίας υλοποιούνται:

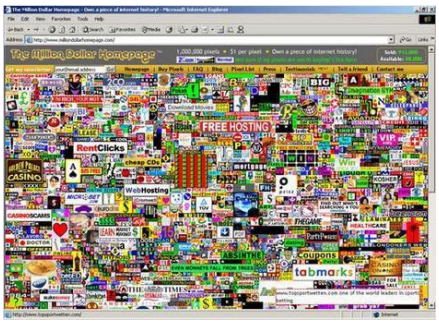
- αναγκάζοντας το μηχάνημα που έχει γίνει στόχος να κάνει επανεκκίνηση ή να καταναλώσει τους πόρους του στο βαθμό που να μη μπορεί να εξυπηρετήσει τη φυσιολογική κίνηση και/ή
- με τη διακοπή η παρεμπόδιση των μέσων επικοινωνίας μεταξύ του μηχανήματος-στόχου και των χρηστών που συνδέονται σε αυτόν ώστε να μη μπορούν να επικοινωνήσουν επαρκώς.

Χαρακτηριστικά τέτοιων επιθέσεων είναι :

- υπερβολικά αργή απόδοση του δικτύου,
- μη διαθέσιμοι ιστοχώροι ,
- αδυναμία πρόσβασης σε όλους τους ιστοχώρους του διαδικτύου,
- δραματική αύξηση στον αριθμό των spam μηνυμάτων.

Η άρνηση υπηρεσίας μπορεί να στοχεύει στη δυσλειτουργία ενός δικτύου ή ακόμα και ενός συγκεκριμένου ατόμου.
Οι επιθέσεις άρνησης υπηρεσίας καταπατούν τους νόμους περί της ορθής χρήσης του Internet και συχνά καθιστούν παραβίαση των νόμων συγκεκριμένων εθνών.

2.1 Παράδειγμα επίθεσης Άρνησης Υπηρεσίας
The Million Dollar Homepage



Ένα πρόσφατο παράδειγμα μιας τέτοιας επίθεσης ήταν η επίθεση που δέχτηκε η γνωστή ιστοσελίδα του Alex Tew, ενός Βρετανού φοιτητή που είχε την ιδέα να πουλάει pixels σε εταιρίες που θα ήθελαν να διαφημιστούν στην σελίδα του. Δυστυχώς η δημοσιότητα που κέρδισε, λόγο της ιδέας του, τράβηξε και κάποιους επίδοξους εγκληματίες.
Συγκεκριμένα τον Ιανουάριο του 2006 ο Tew έλαβε ένα e-mail με απαιτήσεις να πληρώσει $5000 αλλιώς θα δεχόταν επίθεση. Ο ίδιος αγνόησε το μήνυμα και στις 12 Ιανουαρίου ο server που φιλοξενούσε την ιστοσελίδα του δέχτηκε επίθεση και περαιτέρω μηνύματα που ζητούσαν αυτή τη φορά $50.000.
Αφού εξέτασε διάφορες προοπτικές χρησιμοποίησε μια υπηρεσία (DDoSprotection.com) η οποία να φιλτράρει τη κίνηση που δέχεται ο server του. Μία εβδομάδα μετά ο Tew έσπασε το όριο του $1 εκατομμυρίου πουλώντας και τα τελευταία του pixel σε μια εταιρία με διαιτητικά προϊόντα.

2.2 DNS Backbone DDoS Attacks

Οι DNS Backbone DDoS επιθέσεις είναι αρκετά και σημαντικά γεγονότα που έχουν να κάνουν με το Διαδίκτυο όπου οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας έχουν στόχο έναν ή περισσότερους από τους 13 κύριους DNS εξυπηρέτες του Internet. Τέτοιου είδους επιθέσεις ενέχουν τρομερούς κινδύνους εφόσον στοχεύουν κύριους DNS εξυπηρέτες των οποίων η δουλειά είναι να μεταφράζουν ονόματα διευθύνσεων κόμβων στα αντίστοιχα IPs τους.
Εφόσον οι εξυπηρέτες αυτοί παρέχουν υπηρεσίες ανεύρεσης κόμβων παγκοσμίως, τέτοιες επιθέσεις έχουν σαν στόχο την εξουδετέρωση του ίδιου του διαδικτύου και όχι απλά κάποιων ιστοχώρων.

Η πρώτη τέτοιου είδους επίθεση συνέβη στις 22 Οκτωβρίου του 2002 και κράτησε περίπου για μία ώρα. Από του 13 εξυπηρέτες οι 9 απενεργοποιήθηκαν αλλά οι υπόλοιποι 4 κατάφεραν να ανταπεξέλθουν.

Το γεγονός αυτό ήταν η πρώτη σημαντική προσπάθεια εξουδετέρωσης του Διαδικτύου. Η μεγαλύτερη βλάβη που είχε γίνει ποτέ πριν από την επίθεση αυτή ήταν η απενεργοποίηση 7 εξυπηρετών τον Ιούλιο του 1997 λόγω τεχνικών όμως προβλημάτων.

Μια δεύτερη επίθεση συνέβη στις 6 Φεβρουαρίου του 2007. Η επίθεση κράτησε για περίπου 5 ώρες. Αν και κανένας από του εξυπηρέτες δεν απενεργοποιήθηκε, οι δύο από αυτούς "υπέφεραν σημαντικά" ενώ άλλοι παρουσίαζαν τεράστια κίνηση. Το botnet που ήταν υπεύθυνο για την επίθεση βρέθηκε πως ξεκίνησε από τη Νότια Κορέα.
Στις 8 Φεβρουαρίου του 2007 ανακοινώθηκε από τη Network World ότι «Εάν οι ΗΠΑ βρεθούν στη μέση μιας τέτοιας μεγάλης κυβερνο-επίθεσης που θα έχει στόχο να υπονομεύσει τη κρίσιμη υποδομή πληροφοριών του έθνους, το Υπουργείο Άμυνας είναι προετοιμασμένο, με εντολή του Προέδρου, να εξαπολύσει μια κυβερνο-αντεπίθεση ή μέχρι και βομβαρδισμό του σημείου εκκίνησης της επίθεσης.» Η ανακοίνωση αυτή μάλλον οφείλετε στο γεγονός ότι ένας από τους DNS εξυπηρέτες είναι κάτω από τον έλεγχο του Υπουργείου Άμυνας των ΗΠΑ.

3. Password Cracking

Μια από τις τεχνικές που κάθε επίδοξος χάκερ αναπτύσσει στη προσπάθεια του να αποκτήσει πρόσβαση σε δίκτυα ή συγκεκριμένους υπολογιστές είναι αυτή που του επιτρέπει να μαντέψει ή να βρει κωδικούς των συστημάτων αυτών.
Αυτό που παραξενεύει τους περισσότερους ανθρώπους είναι το πώς ένας χάκερ αποκτά κωδικούς που του επιτρέπουν απεριόριστη πρόσβαση. Είναι αλήθεια πως υπάρχουν προγράμματα που ψάχνουν με αυτοματοποιημένο τρόπο για το σωστό κωδικό συστημάτων ή προγραμμάτων υπολογιστή. Αυτά χρησιμοποιούν κυρίως δύο τρόπους ανεύρεσης κωδικών. Ο ένας είναι με τη χρήση ενός ηλεκτρονικού λεξικού, ενός αρχείου ουσιαστικά που περιέχει έναν ικανό αριθμό λέξεων που χρησιμοποιεί το πρόγραμμα, αυτού του είδους η επίθεση ονομάζεται **dictionary attack**. Με τη χρήση αυτού του λεξικού το πρόγραμμα δοκιμάζει όλες τις λέξεις που υπάρχουνε σε αυτό και εάν ο κωδικός που αναζητείται είναι απλώς μια υπάρχουσα λέξη ή ένα όνομα, που λογικά υπάρχουν στο λεξικό, είναι θέμα δευτερολέπτων μέχρι αυτός να βρεθεί. Η δεύτερη προσέγγιση χρησιμοποιεί τη λογική της δοκιμής όλων των πιθανών συνδυασμών γραμμάτων και αριθμών μέχρι την εύρεση του σωστού κωδικού, κάτι που με τη βοήθεια των σύγχρονων υπολογιστών μπορεί να γίνει ακόμα πιο γρήγορα. Αυτή η προσέγγιση ονομάζεται **brute force attack** και μπορεί να έχει κάποια αποτελέσματα εάν ο κωδικός είναι μεν τυχαίος αλλά δεν είναι πολύ μεγάλος (Πίνακας 1).

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Πίνακας 1

Η πιο συνηθισμένη όμως τεχνική που χρησιμοποιείται από τους χάκερς είναι η κοινωνική μηχανική ή η προσπάθεια ανεύρεσης του σωστού κωδικού μετά από έρευνα των προσωπικών στοιχείων της ζωής του χρήστη που γνωρίζει και χρησιμοποιεί τον κωδικό. Μια επίσης πολύ κοινή τακτική των κοινωνικών μηχανικών είναι τα τηλεφωνήματα σε υπαλλήλους των εταιριών που έχουν στοχεύσει και η προσπάθεια εκμαίευσης κωδικών και ονομάτων χρηστών από αυτούς προσποιούμενοι πως είναι κάποιοι τεχνικοί του δικτύου ή κάποιο άτομο που χρειάζεται βοήθεια.

Όπως τονίζει ο γνωστός κοινωνικός μηχανικός Κέβιν Μίτνικ στο βιβλίο του «Η τέχνη της απάτης» ο πιο αδύναμος κρίκος στα ζητήματα ασφάλειας είναι ο ανθρώπινος παράγοντας. Όσο εξεζητημένα και προηγμένα να είναι τα συστήματα που προστατεύουν ένα δίκτυο ή έναν υπολογιστή, αυτά μπορούν να παρακαμφθούν από ένα ταλαντούχο κοινωνικό μηχανικό ο οποίος με διάφορες τεχνικές μπορεί να καταφέρει να αποσπάσει ονόματα και κωδικούς χρηστών ακόμα και από συνειδητοποιημένους υπαλλήλους εταιριών. Ο Μίτνικ ήταν από τους πρώτους και καλύτερους στο τομέα αυτό. Ο ίδιος χαρακτηριστικά αναφέρει πως στα 17 του ήταν ικανός να πείσει οποιονδήποτε υπάλληλο οποιασδήποτε τηλεφωνικής εταιρίας να κάνει κυριολεκτικά οτιδήποτε, είτε μέσω τηλεφώνου είτε πρόσωπο με πρόσωπο.

Μια άλλη συνηθισμένη τρύπα στην ασφάλεια δημιουργείται από τη χρήση κοινών και πολύ απλών κωδικών από τους υπαλλήλους εταιριών οι οποίοι πολλές φορές δεν αντιλαμβάνονται τη σημασία του να είναι αυτοί οι κωδικοί αρκετά δύσκολοι και κυρίως κρυφοί από όλους.

Η ερώτηση που γεννάται είναι: πώς ένας χάκερ μπορεί να βρει τα προσωπικά στοιχεία του ατόμου που έχει στοχεύσει; Η απάντηση είναι «πολύ απλά». Πρόσφατα μία ιστοσελίδα η Zabasearch.com προκάλεσε αρκετές διαμάχες και

συζητήσεις μεταξύ των ειδικών προσφέροντας δωρεάν κάτι για το οποίο μέχρι πρόσφατα έπρεπε να πληρώσεις. Χρησιμοποιώντας την ιστοσελίδα κανείς μπορεί να ψάξει για το όνομα οποιουδήποτε Αμερικανού πολίτη, τη διεύθυνση του, την ημερομηνία γέννησης, το τηλέφωνο του μαζί με συνδέσμους προς χάρτες της οικίας του, δορυφορικές φωτογραφίες μέχρι και μετεωρολογικές προβλέψεις για την περιοχή στην οποία αυτός διαμένει. Η ιστοσελίδα παρέχει και άλλες υπηρεσίες όπως πλήρη αναφορά του παρελθόντος ενός συγκεκριμένου ανθρώπου. Τέτοιες αναφορές πληρώνονται ($20) αλλά μπορούν να περιέχουν ολόκληρο το ιστορικό ενός ατόμου όπως διευθύνσεις διαμονής τα τελευταία 20 χρόνια, καταδίκες ή κατασχέσεις που του γίνανε λόγο χρεοκοπίας όπως και διευθύνσεις συγγενών. Αξίζει να πούμε πως την υπηρεσία την ξεκίνησε ένας ομογενής Έλληνας, ο Nick Matzorkis, που σκοπό είχε να δώσει τη δυνατότητα σε οποιονδήποτε να βρει πρόσωπα με τα οποία έχει χάσει επαφή και θα ήθελε να ξαναδεί. Ελπίζουμε τώρα να γίνεται και πιο ξεκάθαρη η επιλογή του ονόματος της ιστοσελίδας.
Υπάρχει μια πλήρης συζήτηση για τη νομιμότητα μιας τέτοιας υπηρεσίας στο FindLaw.com αλλά εν συντομία η αλήθεια είναι πως προς το παρόν η Zabasearch είναι νόμιμη γιατί χρησιμοποιεί κυβερνητικά και εμπορικά στοιχεία τα οποία είναι δημοσίως διαθέσιμα.

4. Employee Theft

Ο όρος αυτός χρησιμοποιείται για να περιγράψει την παράνομη υποκλοπή πληροφοριών και στοιχείων των επιχειρήσεων από τους υπαλλήλους των επιχειρήσεων αυτών. Οι υπάλληλοι αυτοί παρά τις συμβάσεις εργασίας και συμφωνίες εχεμύθειας που υπογράφουν με τις επιχειρήσεις στις οποίες εργάζονται, υποκλέπτουν ή διαγράφουν εμπιστευτικές και copyrighted πληροφορίες. Παρά τα συστήματα ασφαλείας των εταιριών, οι υπάλληλοι καταφέρνουν να χρησιμοποιήσουν αυτές τις πληροφορίες για προσωπικό τους όφελος, ακόμα και για να δώσουν στοιχεία στους ανταγωνιστές της επιχείρησης στην οποία εργάζονται.
Η ζημία που προκαλείται από αυτή τη μορφή κλοπής μπορεί να είναι πολύ μεγάλη αν λάβει κανένας υπόψη του ότι σήμερα είναι πιο εύκολη και γρήγορη η μετάδοση μεγάλου όγκου δεδομένων μέσω email, web pages, USB devices και DVD storage. Οι removable media devices είναι πλέον μικρότερες και έχουν μεγαλύτερη χωρητικότητα.

4.1 Η έκταση του προβλήματος

Το γραφείο Εθνικών Υποθέσεων στις Η.Π.Α. υπολογίζει ότι οι απώλειες από την κλοπή των δεδομένων κυμαίνονται ετησίως από $15 μέχρι $25 billion. Επίσης, υπολογίζεται ότι οι εργαζόμενοι κλέβουν από τους εργοδότες τους περισσότερα από $40 billion κάθε χρόνο. Το ποσό αυτό είναι 10 φορές μεγαλύτερο από το κοινό έγκλημα στις Η.Π.Α. ή αλλιώς το 1,5% της αξίας των εμπορικών συναλλαγών στον κόσμο, σε διάστημα ενός έτους. Ο καθηγητής Neil Snyder του University of Virginia εκτιμά ότι το 1/3 της ζημίας των μικρών επιχειρήσεων οφείλεται σε employee theft. Το ποσοστό της κλοπής των δεδομένων αυξάνεται κατά 15% κάθε χρόνο.

Σε σχετική έρευνα που έγινε σε περισσότερους από 9000 εργαζόμενους σε τρεις διαφορετικές βιομηχανίες αποδείχτηκε ότι το 34% των εργαζομένων παραδέχθηκαν ότι με κάποιον τρόπο έκλεψαν δεδομένα από τον εργοδότη τους. Τέλος, αξίζει να σημειωθεί ότι μία μελέτη του 1984 απέδειξε ότι οι υπάλληλοι της Canadian Bank έκλεψαν $382 million από τράπεζες, ποσό που είναι 9 φορές μεγαλύτερο από το ποσό που εκλάπη από ληστείες τραπεζών.

Η κλοπή δεδομένων από τις επιχειρήσεις συμβαίνει καθημερινά σε κάθε είδους επιχείρηση και με ποικίλους τρόπους. Υπολογίζεται ότι το 75% των δεδομένων που υποκλέπτονται δε γίνεται αντιληπτό. Οι οικονομικές δυσκολίες της εποχής μας, η έλλειψη αυξήσεων στους μισθούς και οι απειλές για περικοπές στους μισθούς και στις θέσεις εργασίας είναι οι λόγοι για τους οποίους οι εργαζόμενοι καταφεύγουν στην κλοπή των δεδομένων.

Η κλοπή των δεδομένων μπορεί να έχει πολλές μορφές: από κλοπή και εμπορία αποθεμάτων του γραφείου και τη σπατάλη χρόνου ζητώντας άδειες χωρίς ουσιαστικό λόγο μέχρι την κλοπή και πώληση περιουσίας και εμπιστευτικού υλικού της επιχείρησης. Όταν ένας εργοδότης αντιλαμβάνεται την κλοπή δεδομένων από την επιχείρησή του και από κάποιον εργαζόμενο, αντιδρά συνήθως άμεσα και επιδιώκει την άμεση επίλυση του προβλήματος και την παραδειγματική τιμωρία του εργαζομένου.

Οι εργοδότες από την πλευρά τους, για να αποτρέψουν αυτό το φαινόμενο, ενισχύουν όσο το δυνατόν περισσότερο τους ελέγχους ακόμα και σε προσωπικό επίπεδο (σε κάθε υπάλληλο χωριστά) χωρίς να αποκλείονται οι «καλοπληρωμένοι» υπάλληλοι. Συνήθως οι εργοδότες προσπαθούν να αποκτήσουν αμεσότητα και καλές σχέσεις με τους υπαλλήλους τους, δίνοντάς τους bonus ή κάποια οικονομικά προνόμια, ανάλογα με την οικογενειακή τους κατάσταση (π.χ. ανάλογα με τον αν έχουν παιδιά).

Κεφάλαιο 2ο

Μορφή 2η Αδικήματα σχετικά με υπολογιστές

1. Credit Cards

Οι πιστωτικές κάρτες εκδίδονται από τις τράπεζες και σχεδόν στο σύνολο τους είναι ενταγμένες σε ένα από τα δίκτυα των παγκόσμιων οργανισμών πιστωτικών καρτών (Visa, MasterCard, American Express, κλπ). Στο εξωτερικό και ιδιαίτερα στις ΗΠΑ, πιστωτικές κάρτες εκδίδονται και από μεγάλες επιχειρήσεις και αλυσίδες καταστημάτων. Η πιστωτική κάρτα παρέχει στον κάτοχο τη δυνατότητα πραγματοποίησης αγορών/ ή και αναλήψεων μετρητών, με πίστωση, στην Ελλάδα ή/και το εξωτερικό.
Οι συναλλαγές του κατόχου χρεώνονται σε ένα ανοικτό λογαριασμό προκαθορισμένου ανώτατου ύψους (πιστωτικό όριο) και ο κάτοχος έχει την ευχέρεια τμηματικής ή ολοσχερής εφάπαξ εξόφλησης του χρεωστικού υπολοίπου. Στην πρώτη περίπτωση (τμηματική εξόφληση) ο κάτοχος επιβαρύνεται με τόκους επί του ανεξόφλητου υπολοίπου, ενώ στη δεύτερη το κόστος της κάρτας περιορίζεται στην συνδρομή και τυχόν άλλα έξοδα (αναλήψεις μετρητών , κλπ).
Οι πιστωτικές κάρτες διαφέρουν από τις χρεωστικές. Οι χρεωστικές κάρτες δεν παρέχουν στον κάτοχο πίστωση για τις αγορές, αλλά το ποσό της συναλλαγής μεταφέρεται αυτόματα από το λογαριασμό του κατόχου στο λογαριασμό του εμπόρου. Το πλεονέκτημα για τον κάτοχο είναι ότι με τη χρήση της χρεωστικής κάρτας ελέγχει το ύψος των αγορών του γιατί δε ξοδεύει χρήματα τα οποία δεν έχει. Αντίστοιχα το όφελος της τράπεζας είναι ότι παρακρατά από τον έμπορο ένα ποσοστό προμήθειας ως διαχειριστικό κόστος. Οι χρεωστικές κάρτες τείνουν να αντικαταστήσουν τη χρήση των μετρητών και των επιταγών (ιδιαίτερα για συναλλαγές μικρού ύψους), αλλά η επέκταση των έξυπνων καρτών (smart cards), εκτιμάται ότι θα περιορίσει τη χρήση τους.

1.1 Credit Card Fraud

Απάτη θεωρείται όταν ο κάτοχος της κάρτας δεν έχει γνώση των συναλλαγών που γίνονται με την κάρτα του ή όταν ο έμπορος “ξεγελιέται” και προσφέρει τις υπηρεσίες του πιστεύοντας ότι θα πληρωθεί από έναν λογαριασμό, αλλά μαθαίνει εκ των υστέρων ότι δεν πρόκειται να πληρωθεί. Τυπικά, ο απατεώνας χρεώνει την αγορά στην πιστωτική κάρτα ενός άλλου ατόμου. Στις μέρες μας, οι μισές απάτες που σχετίζονται με τις πιστωτικές κάρτες, κατευθύνονται online, που σημαίνει ότι οι απατεώνες κάνουν online αγορές με τα στοιχεία των πιστωτικών καρτών άλλων ατόμων.

Οι απάτες αυτές εμφανίζονται με τις εξής μορφές:

1.1.1 Κλοπή της κάρτας:

Όταν ο κάτοχος της κάρτας την χάνει ή του την κλέβουν. Ο κλέφτης είναι δυνατόν να κάνει αυθαίρετες αγορές με τη χρήση της κάρτας, μέχρι αυτήν να ακυρωθεί. Ο απατεώνας είναι πιθανό να πραγματοποιήσει αγορές πολλών χιλιάδων ευρώ, μέχρι ο νόμιμος κάτοχος της κάρτας ή η τράπεζα συνειδητοποιήσουν ότι η κάρτα είναι σε λάθος χέρια. Κάποια συστήματα πληρωμών είναι επιρρεπή και μπορεί να δεχτούν κλεμμένη πιστωτική κάρτα, αφού δεν απαιτείται η διακρίβωση της ταυτότητας του κατόχου της κάρτας. Παρόλα αυτά κάποια κέντρα παροχής υπηρεσιών, απαιτούν από τον χρήστη τον αριθμό ταχυδρομικού κώδικα και, στην περίπτωση που αυτός δεν ταυτίζεται με αυτόν που είναι καταχωρημένος στην κάρτα, η συναλλαγή αποτυγχάνει.

1.1.2 Οικειοποίηση λογαριασμού

Οι απατεώνες υποδύονται τους νόμιμους κατόχους των καρτών χρησιμοποιώντας κλεμμένα προσωπικά δεδομένα. Αυτοί οι απατεώνες έχουν τη δυνατότητα να αλλάζουν τα προσωπικά δεδομένα του νόμιμου κατόχου της πιστωτικής κάρτας (π.χ. διεύθυνση) με στοιχεία τα οποία ελέγχουν. Πρόσθετες κάρτες και αριθμοί PIN ζητούνται στις νέες διευθύνσεις, με τα νέα στοιχεία, και χρησιμοποιούνται από τους απατεώνες για να κάνουν αγορές. Κάποιες φορές ο απατεώνας προσπαθεί να προσθέσει τον εαυτό του ως συνδικαιούχο, έτσι ώστε να αποκτά πλήρη εξουσιοδότηση στον λογαριασμό, και να μπορεί να διαπράξει τις απάτες του ανενόχλητος.

1.1.3 Credit Card Mail Order

Χρησιμοποιώντας έναν κλεμμένο αριθμό πιστωτικής κάρτας, ή έναν computer generated αριθμό πιστωτικής κάρτας, ένας απατεώνας μπορεί να παραγγείλει προϊόντα. Αυτού του είδους η απάτη είναι γνωστή ως “Card Not Present” (CNP) και αναφέρεται σε συναλλαγές που γίνονται μέσω τηλεφώνου ή μέσω Internet, χωρίς να απαιτείται η παρουσία του κατόχου της πιστωτικής κάρτας στο σημείο πώλησης. Η VISA τονίζει ότι οι CNP έμποροι θα πρέπει να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν όλα τα απαραίτητα μέτρα για να προστατεύονται από αυτού του είδους τις απάτες και όλες τις απώλειες που αυτές είναι δυνατόν να τους προκαλέσουν. Αυτοί που κάνουν αυτές τις απάτες στοιχηματίζουν στο γεγονός ότι πολλά χαρακτηριστικά γνωρίσματα πρόληψης αυτής της απάτης δε λαμβάνονται. Το **3-D Secure™** είναι ένα πρωτόκολλο επικύρωσης που αναπτύσσεται από τη Visa και MasterCard για να προστατεύσει τις online πληρωμές καρτών, στο οποίο ο ιδιοκτήτης της κάρτας πρέπει να κάνει register στην εκδότρια τράπεζα.

1.1.4 Skimming

Είναι η κλοπή των πληροφοριών πιστωτικών καρτών από έναν ανέντιμο υπάλληλο ενός νόμιμου εμπόρου που με το χέρι αντιγράφει τους αριθμούς, ή που χρησιμοποιεί έναν μαγνητικό stripe reader σε μια pocket-sized ηλεκτρονική συσκευή. Συνηθισμένες περιπτώσεις skimming έχουν αναφερθεί σε εστιατόρια και bars όπου ο skimmer έχει στην κατοχή του την πιστωτική κάρτα του θύματος, χωρίς το θύμα να βλέπει τις κινήσεις του υπαλλήλου. Ο skimmer θα χρησιμοποιήσει ένα μικρό πληκτρολόγιο για να μεταγράψει διακριτικά τον 3ψήφιο ή 4ψήφιο **Card**

Security Code όποιος δεν βρίσκεται στο magnetic strip. Σε πολλές περιπτώσεις skimming έχει αναφερθεί ότι ο δράστης έχει τοποθετήσει μία συσκευή μετά την υποδοχή της κάρτας ενός Automated teller machine, το οποίο διαβάζει την μαγνητική ταινία (magnetic strip) καθώς ο χρήστης περνάει την κάρτα από το teller, χωρίς αυτό βέβαια να γίνεται αντιληπτό από τον χρήστη. Αυτές οι συσκευές έχουν συνήθως μία ενσωματωμένη κάμερα, που διαβάζει ταυτόχρονα το PIN του χρήστη. Για αποτραπεί αυτή η μορφή απάτης, οι κάρτες σε χώρες όπως η UK, εκδίδονται με ένα έξυπνο chip που πραγματοποιεί κωδικοποίηση δημοσίου κλειδιού. Το chip δεν μπορεί να αντιγραφεί, και προστατεύει τον αριθμό της πιστωτικής κάρτας, την ημερομηνία λήξης και το security code τα οποία μπορούν να αντιγραφούν. Ο δράστης αν έχει αυτά τα στοιχεία στην κατοχή του, μπορεί να χρησιμοποιήσει την κάρτα του θύματος σε CNP συναλλαγές.

1.1.5 Carding

Ο όρος αυτός χρησιμοποιείται από τους απατεώνες για τη διαδικασία που χρησιμοποιούν, για να ελέγξουν ότι τα κλεμμένα στοιχεία των πιστωτικών καρτών ισχύουν ακόμα. Ο δράστης θα παρουσιάσει το σύνολο των στοιχείων για κάθε πιστωτική κάρτα σε έναν ιστοχώρο, όπου θα έχει τη δυνατότητα να πραγματοποιήσει μία real time συναλλαγή, κάνοντας μια αγορά για ένα πολύ μικρό νομισματικό ποσό, ώστε να μη καταναλωθεί το πιστωτικό όριο της κάρτας, και να μην προκαλέσει την προσοχή κάποιου από τους ανθρώπους που ελέγχουν τη συναλλαγή. Συχνά χρησιμοποιείται η online δωρεά σε ένα site αντί για ηλεκτρονική αγορά, δεδομένου ότι δεν υπάρχει καμία ανάγκη να βρεθεί ένα προϊόν κατάλληλης τιμής για να προστεθεί στο καλάθι αγορών και να δοθούν λεπτομέρειες για την παράδοση του προϊόντος. Ο carder μπορεί να το κάνει αυτό με έναν web browser, ή μπορεί να γράψει ένα αυτοματοποιημένο λογισμικό στο interface του website's checkout ή στις billing forms. Παλαιότερα, οι carders χρησιμοποιούσαν προγράμματα γνωστά ως **generators** που παρήγαγαν αριθμούς πιστωτικών καρτών και στη συνέχεια τους δοκίμαζαν για να δουν ποιοι ήταν έγκυροι. Κάτι τέτοιο βέβαια δεν είναι δυνατό να γίνει σήμερα, επειδή τα credit card processing systems ζητάνε από τον χρήστη περισσότερα στοιχεία, όπως τη διεύθυνση, τον Card Security Code και την ημερομηνία λήξης της κάρτας. Στις μέρες μας, το carding μπορεί να χρησιμοποιηθεί μόνο για δεδομένα που αποκτούνται απευθείας από τα θύματα με τις μεθόδους Skimming και Phishing.

1.2 Πρόσφατες απάτες

Έξι άτομα χρέωσαν δύο πιστωτικές κάρτες αγνώστων μέχρι στιγμής, κατόχων με το χρηματικό ποσό των 4.800.000 ευρώ συνολικά με εικονικές συναλλαγές.

Πέντε Έλληνες και ένας Πακιστανός συνελήφθησαν από την Δίωξη Οικονομικών Εγκλημάτων της Ασφάλειας Αττικής για απάτη ιδιαίτερα μεγάλης αξίας σε βάρος τράπεζας. Συγκεκριμένα, ο ένας από τους συλληφθέντες είχε συστήσει ανώνυμη εταιρία με αντικείμενο την εμπορία ενδυμάτων και είχε ένα ίδιο κατάστημα στο κέντρο της Αθήνας, για αυτόν το λόγο είχε προμηθευτεί από την Τράπεζα μηχάνημα χρέωσης πιστωτικών καρτών. Προχθές το βράδυ ο ίδιος και οι συνεργοί του χρέωσαν δύο πιστωτικές κάρτες αγνώστων μέχρι στιγμής, κατόχων με το χρηματικό ποσό των 4.800.000 ευρώ συνολικά με εικονικές συναλλαγές, το οποίο κανονικά θα

έπρεπε να κατατεθεί από την τράπεζα στο λογαριασμό του εμπόρου. Η απάτη έγινε αντιληπτή όμως το επόμενο πρωί από την τράπεζα και ειδοποιήθηκε η Ασφάλεια η οποία εντόπισε τους δράστες και τους συνέλαβε. Οι συλληφθέντες οδηγήθηκαν στον εισαγγελέα ο οποίος τους παρέπεμψε σε τακτικό ανακριτή.

2. Phising – Νέα μορφή κυβερνο-εγκλήματος

2.1 Ορισμός

Ο όρος phising αναφέρεται σε εγκληματική δραστηριότητα στο χώρο του διαδικτύου. Είναι μια σχετικά καινούρια τεχνική που συνήθως αποσκοπεί στην υποκλοπή προσωπικών στοιχείων από ανυποψίαστους χρήστες.
Χρησιμοποιεί τεχνικές του social engineering, οι οποίες προσπαθούν να προσελκύσουν τον χρήστη με έξυπνους τρόπους και να του αποσπάσουν δεδομένα, όπως usernames, passwords, διευθύνσεις ηλεκτρονικού ταχυδρομείου, αριθμούς πιστωτικών καρτών κ.α.

Το phising διαδίδεται μέσα από emails και instant messages όπου προτρέπει τους χρήστες να επισκεφτούν ιστοσελίδες, οι οποίες είναι πλαστά αντίγραφα άλλων αξιόπιστων. Τα πιο ενδεικτικά παραδείγματα είναι το ebay και το paypal.
Οι χρήστες μπαίνοντας στις fake σελίδες δίνουν τους κωδικούς τους νομίζοντας ότι είναι η νόμιμη υπηρεσία.

Στο παρόν κεφάλαιο θα παρατεθούν μερικά γνωστά παραδείγματα phising που συνέβησαν στον κυβερνοχώρο τα τελευταία χρόνια.

2.2 Τεχνικές phising

2.2.1 Έξυπνη διαχείριση των links

Οι περισσότερες μορφές του phising χρησιμοποιούν μια ιδιόρρυθμη τεχνολογική απάτη που ενσωματώνει ορισμένους υπερσυνδέσμους σε emails οι οποίοι με τη σειρά τους οδηγούν σε sites-απάτες. Αυτά τα emails στέλνονται από συστήματα που χρησιμοποιούν το όνομα μιας γνωστής επιχείρησης ουσιαστικά για να «ψαρέψουν» χρήστες και με την προσθήκη ενός σοβαροφανούς κειμένου πετυχαίνουν τον στόχο τους.

Οι phisers αλλάζουν ελάχιστα τα URLs για να καταφέρουν το redirect που χρειάζεται. Για παράδειγμα μπορεί κάποιος να μην παρατηρήσει ότι το παρακάτω URL είναι λανθασμένο, **http://www.alpha.com.alphabank.com/** (πρόκειται για ενδεικτικό παράδειγμα) και να ακολουθήσει το link.
Μία άλλη έξυπνη τεχνική είναι η χρήση του συμβόλου @ στον υπερσύνδεσμο.
Για παράδειγμα η διεύθυνση
http://www.google.com@members.tripod.com/ μπορεί να αποπροσανατολίσει τον χρήστη που θα νομίζει ότι ακολουθεί σύνδεσμο του google.
Τέτοιες όμως προσπάθειες μπλοκάρονται από τους σύγχρονους browsers οι οποίοι προειδοποιούν τον χρήστη με μηνύματα και τον ρωτάνε αν θέλει να συνεχίσει την επίφοβη ενέργεια.

2.2.2 Πλαστογραφία ιστοσελίδων

Η απάτη δεν τελειώνει στα ύποπτα links. Όταν ένας χρήστης ακολουθήσει κάποιο από αυτά, θα βρεθεί μπροστά σε μια ιστοσελίδα που θα του είναι λίγο πολύ γνώριμη. Αυτό που γίνεται είναι ότι οι phisers έχουν κατασκευάσει ένα site ολόιδιο με το πραγματικό με τεράστιο ποσοστό ακρίβειας. Υπάρχουν ορισμένα προγράμματα που αυτοματοποιούν την κατασκευή ενός «ψεύτικου» site και είναι αρκετά διαδεδομένα ανάμεσα στους phisers. Ένα από αυτά είναι το Universal Man-in-the-middle Phishing Kit που προσφέρει στους phisers ένα απλό interface για την πιστή ανακατασκευή ενός site.

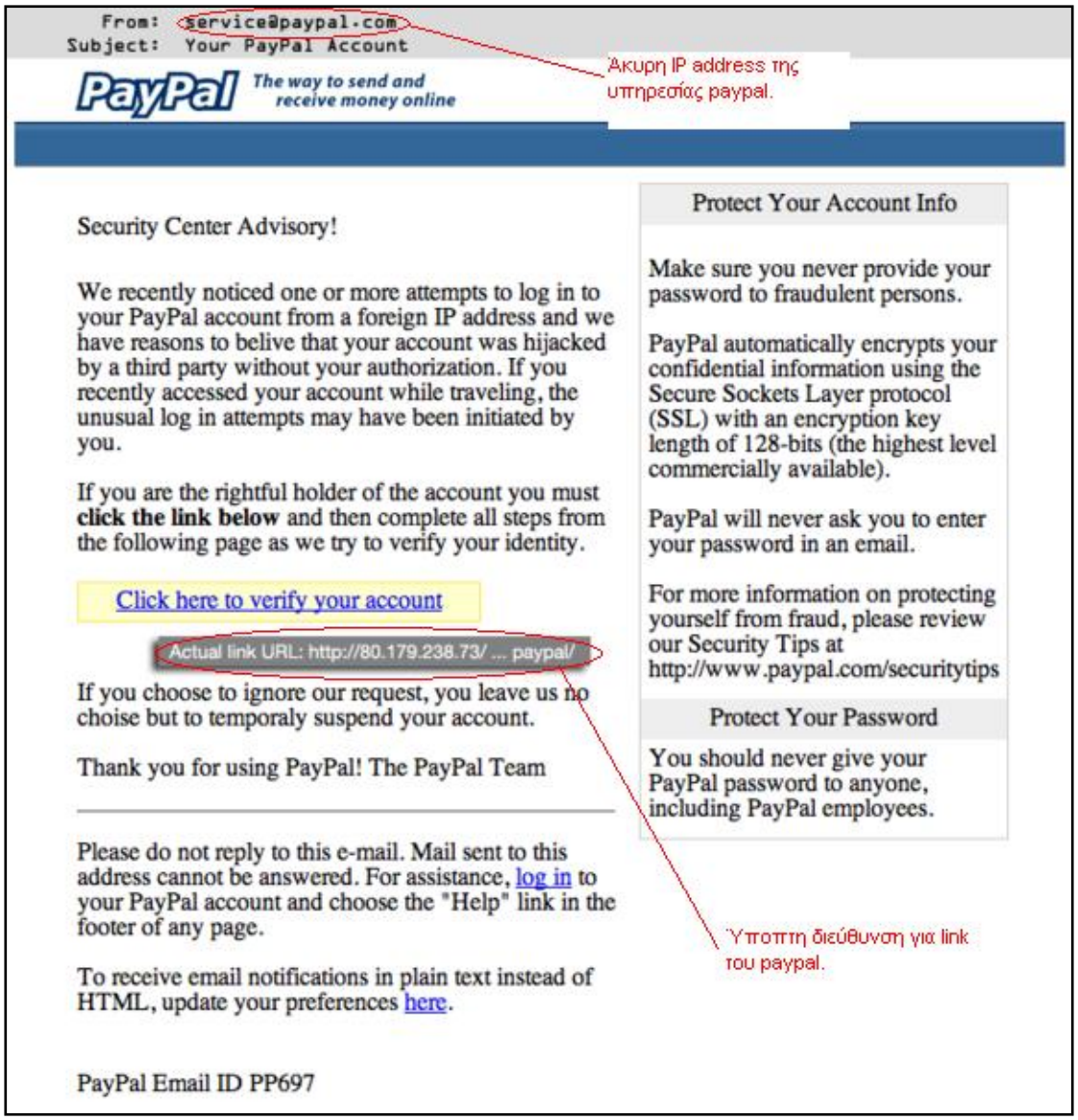
2.2.3 Phising μέσω τηλεφώνου

Εκτός από τα επικίνδυνα links, οι επίδοξοι phisers μέσα από τηλεφωνικές συνομιλίες με τον χρήστη στις οποίες ζητούνταν usernames και passwords έφταναν στον επιθυμητό στόχο. Η συνομιλία γίνονταν ανάμεσα στον χρήστη και σε ένα πληροφοριακό σύστημα το οποίο είχε by default ρυθμισμένα τα λόγια του ώστε να φαίνεται πιστικό.

2.3 Πραγματικά γεγονότα εγκληματικών δραστηριοτήτων phising

2.3.1 Παράδειγμα από Paypal phising

Η γνωστή, σε όλους μας που πράττουμε αγορές μέσα από το διαδίκτυο, υπηρεσία **paypal** έχει πέσει θύμα των phisers στο παρελθόν. Η μέθοδος που χρησιμοποιήθηκε είναι η τοποθέτηση ενός «ψεύτικου» link σε email(Εικόνα 1) και φυσικά η προσθήκη ενός κειμένου με επίσημο χαρακτήρα γραφής που έδινε την αίσθηση του αληθινού. Βέβαια υπήρχαν ύποπτες ενδείξεις που ήταν δύσκολο να της εντοπίσει ένας ανυποψίαστος χρήστης. Δείτε την Εικόνα 1 και θα καταλάβετε. Έχουν σημειωθεί πάνω της τα επίμαχα σημεία.



Εικόνα 1

2.3.2 Παράδειγμα από phising της SouthTrust τράπεζας

Σε αυτήν την περίπτωση οι phisers χρησιμοποίησαν μια εικόνα για να αποφύγουν τα φίλτρα που διατρέχουν το κείμενο για phising στοιχεία και με αυτόν τον τρόπο κατάφεραν και ξεγέλασαν αρκετούς πελάτες της τράπεζας SouthTrust. Δείτε την Εικόνα 2.

Εικόνα 2

2.3.3 Κακόβουλα emails δήθεν από την τράπεζα Πειραιώς

Πριν από λίγες μέρες το Κέντρο Υπηρεσίας Δικτύου του Α.Π.Θ. προειδοποίησε τους χρήστες του https://webmail.auth.gr ότι παρατηρήθηκαν ύποπτα μηνύματα δήθεν από την τράπεζα Πειραιώς που παραπέμπουν σε μεθόδους phising με επικίνδυνα links.
Το επίμαχο κείμενο είναι το εξής :

*"***Η Τράπεζα Πειραιώς συνεχώς αναπτύσσεται και προσφέρει νέες ευκαιρίες για τις επενδύσεις και τη χρηματοδότησή σας, νέες ευκολίες για την εξυπηρέτησή σας, μοναδικά προνόμια αποκλειστικά για εσάς.**
Θέλουμε να είμαστε δίπλα σας και να μαθαίνετε πριν από όλους τα νέα μας. Γι' αυτό, ξεκινάμε ένα νέο τρόπο επικοινωνίας με εσάς και θα σας ενημερώνουμε στο e-mail που μας έχετε ήδη δηλώσει.

Θα λαμβάνετε πληροφορίες για νέα προϊόντα και υπηρεσίες, για ειδικές προσφορές, για διαγωνισμούς, εκδηλώσεις και πολλά ακόμη!
Αν τυχόν δεν επιθυμείτε να σας ενημερώνουμε σε αυτό το e-mail, παρακαλούμε επιλέξτε "Τροποποίηση του e-mail σας" για να μας δώσετε κάποιο άλλο ή επιλέξτε "Διαγραφή από τη λίστα\" για να μη λαμβάνετε καμία ενημέρωση μέσω e-mail.

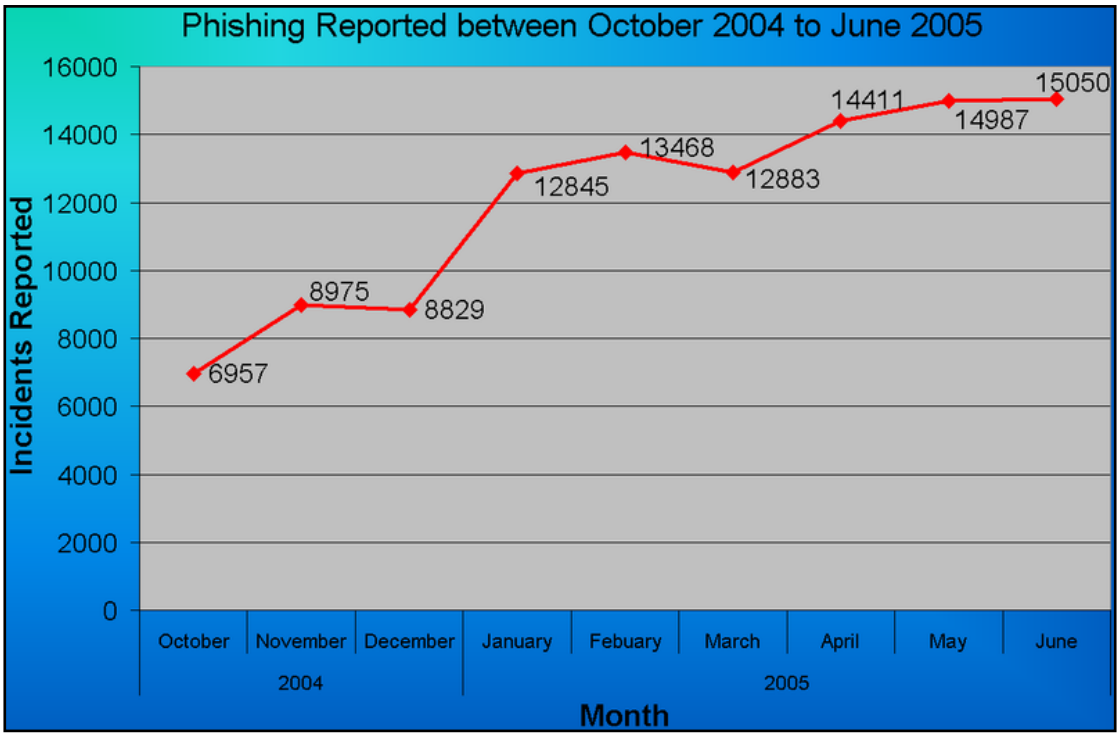
Σύντομα θα είμαστε κοντά σας με νέα και εκπλήξεις!

Τράπεζα Πειραιώς*"*

και είχε ως θέμα το : "**Piraeus Bank Newsletter**" και ως αποστολείς "**From: \"Piraeus Bank\" <news@piraeusbank.rjs0.com>**
Reply-To: \"Piraeus Bank\" news@piraeusbank.gr"

2.4 Ζημίες του phising

Στις Η.Π.Α. μέσα σε ένα χρόνο, Μάιος 2004 με Μάιο 2005, περίπου 1,2 εκατομμύρια χρήστες υπολογιστών έπεσαν θύμα του phising με τη ζημιά να κοστολογείται σε $929,000,000. Οι εταιρίες από μέρους τους είχαν ζημιές της τάξεως των $2,000,000,000 με αρκετούς από τους πελάτες τους να πέφτουν θύματα.
Στην Μεγάλη Βρετανία οι ζημιές από διαδικτυακές απάτες με στόχο τις τράπεζες, κυρίως του phising, φτάνουν τα 23,200,000 λίρες Αγγλίας το 2005 από 12,200,000 λίρες που ήταν το 2004.
Στην Εικόνα 3 παρατίθεται ένα σχεδιάγραμμα με την ανοδική πορεία του phising από τον Οκτώβριο του 2004 ως τον Ιούνιο του 2005.



Εικόνα 3

3. Pharming – Η εξέλιξη του phising

3.1 Ορισμός

Pharming χαρακτηρίζεται η επίθεση ενός hacker που στοχεύει στην ανακατεύθυνση των επισκεπτών μιας ιστοσελίδας σε μια άλλη ψεύτικη. Θυμίζει κατά πολύ τη μέθοδο phising αλλά τα τεχνικά κόλπα που χρησιμοποιούνται είναι αρκετά διαφορετικά.

Το pharming μπορεί να επιτευχθεί αλλάζοντας το hosts file στον υπολογιστή του θύματος. Το αρχείο αυτό είναι εγκατεστημένο στο σύστημα του Η/Υ και είναι υπεύθυνο για την αντιστοιχία των IP διευθύνσεων με τα URL των site.

Ένας ακόμη τρόπος επίθεσης είναι η εκμετάλλευση των τρωτών σημείων του λογισμικού ενός DNS server[2]. Ένας τέτοιος server είναι υπεύθυνος για να «μεταφράζει» τα ονόματα των διευθύνσεων του Internet σε IP addresses. Υπάρχουν όμως κενά ασφαλείας στο λογισμικό αυτών των servers και συνήθως είναι εκμεταλλεύσιμες από τους hackers.

Ο όρος pharming είναι κάτι ανάμεσα στο farming και στο phising(βλ. Κεφάλαιο Χ.ΧΧ). Τα τελευταία χρόνια άρχισαν να γίνονται οι πιο δημοφιλείς τρόποι για την κλοπή προσωπικών δεδομένων και το pharming ειδικά έχει ως στόχους κυρίως το ηλεκτρονικό εμπόριο(e-commerce) και τις ιστοσελίδες τραπεζών.
Βέβαια υπάρχουν αρκετές υλοποιήσεις αντι-pharming στα antivirus λογισμικά που καταφέρνουν σε ικανοποιητικό βαθμό να σταματήσουν αυτή τη μορφή ηλεκτρονικού εγκλήματος.

3.2 Οι τεχνικές λεπτομέρειες του pharming

Κάθε host στο Internet έχει μια IP διεύθυνση η οποία αναπαρίσταται από 4 αριθμούς χωρισμένους με τελείες(παρ. 155.207.250.99). Οι οντότητες στο Internet αναγνωρίζονται μεταξύ τους με τη βοήθεια τέτοιων αριθμών και κάθε πακέτο μεταφοράς δεδομένων συνοδεύεται από δύο IP διευθύνσεις, μία του αποστολέα και μία του παραλήπτη.

Σκεφτείτε τώρα πως ένας εγκληματίας θέλει να υποκλέψει προσωπικά δεδομένα από έναν λογαριασμό χρήστη. Αυτό που κάνει είναι να στήσει ένα «ψεύτικο» site που θα είναι πανομοιότυπο με αυτό της τράπεζας του χρήστη. Αυτή η μέθοδος θυμίζει το phising, αλλά το τελευταίο μπορεί εύκολα να αποφευχθεί αν ο χρήστης καταλάβει ότι η διεύθυνση είναι ύποπτη. Το **pharming** στηρίζεται στην ικανότητα του hacker να εισβάλει στον DNS server και να αλλάξει την σωστή IP διεύθυνση με την «ψεύτικη».
Να σημειωθεί ότι στις HTTPS σελίδες δεν υπάρχει πρόβλημα **pharming**.

3.3 Παραδείγματα pharming δραστηριοτήτων

- Τον Ιανουάριο του 2005, το domain name ενός μεγάλου παροχέα internet της Νέας Υόρκης, του Panix, δέχτηκε επίθεση από hackers που είχαν καταφέρει να ανακατευθύνουν τους επισκέπτες του site σε ένα άλλο παρόμοιο στην Αυστραλία.

- Το 2004 ένας έφηβος από τη Γερμανία κατάφερε να χακάρει το Domain Name του ebay.de.

- Τον Απρίλιο του 2005, ο Hushmail, ένας provider για emails, δέχθηκε επίθεση από έναν hacker που κατάφερε μέσα από συζητήσεις με έναν υπεύθυνο του DNS server να ανακατευθύνει τους χρήστες σε «ψεύτικο» site.

Κεφάλαιο 3ο

Μορφή 3η Αδικήματα σχετικά με το περιεχόμενο

1. Παιδική Πορνογραφία

Σύμφωνα με το άρθρο 9 της συνθήκης της Βουδαπέστης η παραγωγή, διακίνηση, εκπομπή, κατοχή ή πώληση υλικού παιδικής πορνογραφίας με τη χρήση υπολογιστών είναι παράνομη. Κάθε χώρα μέλος υποχρεούται να υιοθετήσει νόμους που να καθιστούν οποιαδήποτε από τις παραπάνω πράξεις εγκληματική. Σύμφωνα πάντα με τη Συνθήκη, σε κάποιες χώρες ενδέχεται το όριο ηλικίας όπου ένας άνθρωπός κρίνετε ως ενήλικος να είναι χαμηλότερο των 18 ετών αλλά σε κάθε περίπτωση δεν μπορεί το όριο αυτό να είναι κάτω των 16 ετών. Επίσης κάθε χώρα έχει το δικαίωμα να καθορίσει ποια από τα παραπάνω καθιστούν εγκληματική πράξη. Για παράδειγμα μια χώρα μπορεί να επιτρέπει σε ένα άτομο την κατοχή τέτοιου υλικού εφόσον είναι για καθαρά ιδιωτική χρήση.
Ο ορισμός πάντως της παιδικής πορνογραφίας διαφέρει από χώρα σε χώρα. Αξίζει να δώσουμε κάποια παραδείγματα τέτοιων διαφορών ώστε να γίνει πιο φανερή η πολυπλοκότητα του θέματος όπως και η δυσκολία ενός πλήρους και κοινού νομοθετικού πλαισίου.
Για παράδειγμα κάποιες χώρες απαγορεύουν την εμφάνιση ενός ανήλικου προσώπου σε σκηνές με σεξουαλικό περιεχόμενο ενώ κάποιες άλλες πάνε ακόμα πιο μακριά απαγορεύοντας κάθε απεικόνιση γυμνού παιδιού ασχέτως με το εάν αυτό παρουσιάζεται σε μια ερωτική σκηνή. Κάποιες άλλες χώρες θεωρούν εγκληματική κάθε τέτοια απεικόνιση ανεξάρτητα από το εάν ένα παιδί πήρε πρακτικά μέρος στη δημιουργία τους. Παραδείγματα τέτοιων απεικονίσεων μπορεί να είναι πίνακες, σχέδια ή ακόμα και εικόνες κατασκευασμένες με τη βοήθεια υπολογιστή. Σε άλλες χώρες η απαγόρευση δεν αφορά μόνο εικόνες παιδικής πορνογραφίας αλλά και γραπτό λόγο ο οποίος μπορεί να αναφέρεται σε ερωτικές σκηνές με ανηλίκους. Αν προσθέσουμε σε όλα αυτά τα διαφορετικά όρια που θέτει κάθε χώρα για την ηλικία ενός ανηλίκου όπως και το ότι αυτά τα όρια μπορεί να ποικίλουν ανάλογα με το περιεχόμενο στο οποίο εμφανίζονται (hardcore, soft-core πορνογραφία) γίνεται εύκολα κατανοητή η δυσκολία που ενέχει η δημιουργία ενός κοινώς αποδεκτού νομοθετικού πλαισίου.
Στο χώρο της τέχνης τα πράγματα γίνονται ακόμα πιο υποκειμενικά και χαρακτηριστικά, υπήρχαν περιπτώσεις όπου ταινίες ή φωτογράφοι κέρδιζαν βραβεία σε κάποιες χώρες ενώ σε κάποιες άλλες απαγορεύονταν λόγω του περιεχομένου τους που είχε να κάνει με κάποιου είδους καταγραφή της παιδικής σεξουαλικότητας.
Είναι ευνόητο πως το νομοθετικό πλαίσιο που προτάθηκε από το Συνέδριο της Βουδαπέστης αναγκάζεται να είναι αρκετά γενικό ώστε να καλύπτει τις περισσότερες περιπτώσεις παιδικής πορνογραφίας. Μετέπειτα, είναι ευθύνη της κάθε χώρας να δημιουργήσει πιο συγκεκριμένους και λεπτομερείς νόμους που να συμφωνούν και με τους δικούς της ηθικούς κανόνες.

Η παιδική πορνογραφία έχει χαρακτηριστεί ως η Λερναία Ύδρα του Internet.
Χαρακτηριστικά παραθέτουμε κάποια στοιχεία που έχουν να κάνουν με τη παιδική πορνογραφία στο διαδίκτυο:

- 100.000 ιστοσελίδες
- 1 δισ. ευρώ ετήσιος τζίρος
- 20.000 νέες φωτογραφίες κάθε εβδομάδα
- 20 νέα παιδιά από 2 ως και 12 ετών εμφανίζονται κάθε μήνα

Σε πολλές χώρες τα εγκλήματα που σχετίζονται με τη παιδική πορνογραφία αντιμετωπίζονται ως εγκλήματα κατά της κοινωνίας και όχι σαν εγκλήματα κατά ενός ατόμου ή ιδιοκτησίας. Οι δύο κύριες κατηγορίες στις οποίες χωρίζονται αυτά τα εγκλήματα είναι πρώτον η παραγωγή πορνογραφικού υλικού και η εκμετάλλευση ανηλίκου που έχει συγκεκριμένα άτομα(παιδιά) ως θύματα και δεύτερον η κατοχή, διακίνηση ή πώληση τέτοιου πορνογραφικού υλικού και γενικά περιπτώσεις όπου δεν μπορεί να καθοριστεί ένα συγκεκριμένο άτομο ως θύμα.
Η πλέον εύκολη δυνατότητα πρόσβασης στο διαδίκτυο έχει φέρει ανησυχία σε πολλούς ειδικούς που ασχολούνται με το θέμα της παιδικής εκμετάλλευσης. Η ανησυχία τους εστιάζεται στη περίπτωση αύξησης τέτοιων εγκληματικών ενεργειών όπως και στην αλλαγή του προφίλ των παραγωγών και καταναλωτών παιδικής πορνογραφίας.
Οι ειδικοί είχαν από νωρίς καταλάβει την ανάγκη ύπαρξης και καταγραφής στατιστικών στοιχείων, σχετικά με τέτοιας φύσης εγκλήματα, τα οποία πρέπει να γίνονται αντικείμενα συστηματικής μελέτης. Με αυτόν τον τρόπο σε αρκετές ανεπτυγμένες χώρες έχει γίνει δυνατή η δημιουργία προφίλ και μεθόδων δράσης τέτοιων εγκληματιών. Επίσης η καταγραφή βοηθάει στη παρακολούθηση των τάσεων που υπάρχουν σε κάθε επίπεδο και είδος τέτοιων εγκλημάτων όπως και την αξιολόγηση της αποτελεσματικότητας. Σε κάθε περίπτωση πάντως, και ειδικά με τη έλευση των υπολογιστών, είναι σημαντικό οι αρχές να αποκτήσουν τα εργαλεία που θα τους δώσουν τη δυνατότητα να είναι πιο αποτελεσματικές. Πέρα από τη βοήθεια σε τεχνολογικό επίπεδο χρειάζεται και ανάλογη εκπαίδευση και κατανόηση που μαζί με τη χρήση στατιστικών και άλλων στοιχείων να δώσουν τη δυνατότητα να καταπολεμηθούν περισσότερα τέτοια εγκλήματα.
Οι επιτυχίες των διωκτικών αρχών, αν και πολλές, δεν είναι αρκετές για να περιορίσουν τη διακίνηση.
Αξίζει πάντως να σημειωθεί ότι το 2005 εκπρόσωποι του FBI σε ειδική τελετή που έγινε στη Ασφάλεια Αττικής βράβευσαν την Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος ως πρώτη ανάμεσα σε παρόμοιες υπηρεσίες 100 χωρών στην εξιχνίαση υποθέσεων παιδικής πορνογραφίας.
Κλασική περίπτωση παιδικής πορνογραφίας για τα Ελληνικά δεδομένα είναι η αναπαραγωγή σε ελληνικά sites φωτογραφιών παιδικής πορνογραφίας που έρχονται συνήθως από το εξωτερικό.

Κεφάλαιο 4ο

Μορφή 4η Αδικήματα σχετικά με τη καταπάτηση της πνευματικής ιδιοκτησίας

1. Παράνομο DOWNLOADING

1.1 Napster – Ο πρωτοπόρος

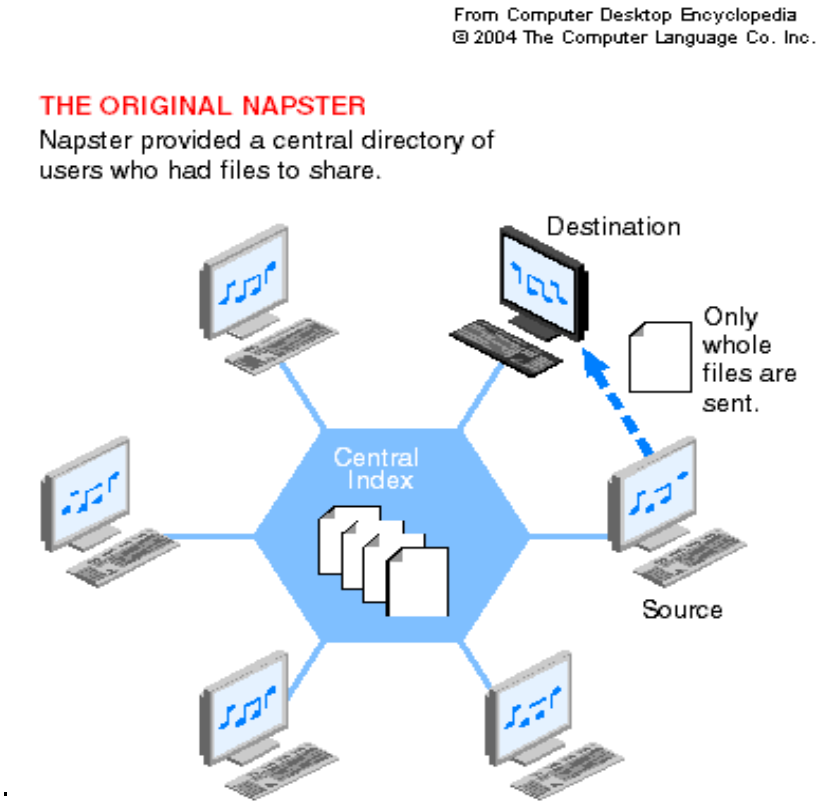
Το 1999 ξεκίνησε από τον Shawn Fanning μία προσπάθεια για την δημιουργία μιας υπηρεσίας διαμοιρασμού αρχείων στο Internet η οποία ονομάστηκε Napster.
Το Napster ήταν η πρώτη διάσημη υπηρεσία που χρησιμοποιούσε την τεχνολογία **peer-to-peer**[2], αλλά με μια διαφορετική φιλοσοφία.
Το peer-to-peer εξορισμού είναι μια υπηρεσία που στηρίζεται στην υπολογιστική ισχύ και στο εύρος του bandwidth των συμμετεχόντων στο δίκτυο. Το Napster στηρίζονταν σε αυτή τη λογική αλλά επιπλέον χρησιμοποιούσε κεντρικούς servers από τους οποίους περνούσαν τα αρχεία που διαμοιράζονταν και κρατούνταν πληροφορίες για τους συνδεδεμένους χρήστες στο δίκτυο(βλ. Εικόνα 1).

Η υπηρεσία με τον καιρό άρχισε να γίνεται αρκετά διάσημη και η καθημερινή συμμετοχή καινούριων χρηστών έκανε το Napster το πρώτο εργαλείο διαμοιρασμού αρχείων.

Όμως, πάνω στο δίκτυο του Napster διακινούνταν παράνομο υλικό, από μουσικά τραγούδια, ταινίες, φωτογραφίες ακόμη και προγράμματα. Αυτό κάποια στιγμή άρχισε να ενοχλεί τις εταιρίες παραγωγής και ξέσπασε ένας πόλεμος κατά του Napster που το κύριο χαρακτηριστικό του ήταν οι συνεχόμενες μηνύσεις και οι διεκδικήσεις πολλών εκατομμυρίων δολαρίων για παράνομη διακίνηση λογισμικού.

Στο επίκεντρο της υπόθεσης βρέθηκε η ίδια η υπηρεσία του Napster και πολλοί χρήστες του. Την αρχή των μηνύσεων την έκανε το συγκρότημα των Metallica οι οποίοι έδωσαν στις αρχές χιλιάδες usernames από χρήστες του Napster. Βέβαια, το τελειωτικό χτύπημα έγινε όταν κατάσχεσαν πολλούς από τους servers της υπηρεσίας στους οποίους υπήρχαν αποδεικτικά στοιχεία για καταδίκη των υπεύθυνων.

Το Napster μετά από 2 χρόνια σταμάτησε να λειτουργεί και αναγκάστηκε να πληρώσει συνολικά το ποσό των 36 εκατομμυρίων δολαρίων σε διάφορες εταιρίες.



Αρχιτεκτονική του Napster

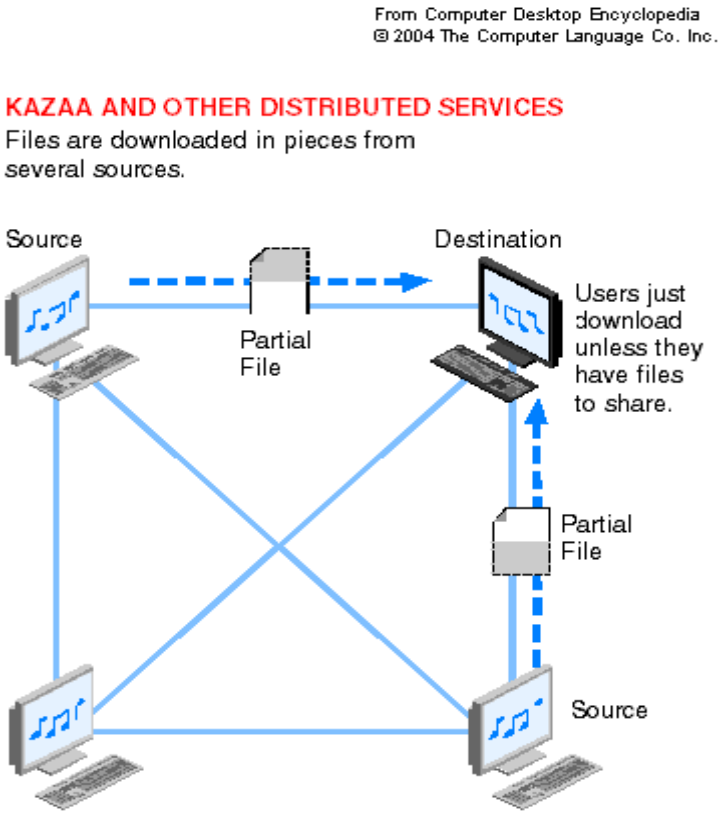
Εικόνα 1

1.2 Kazaa – Η εξέλιξη

Μετά την αποτυχία του Napster και την έκβαση που είχε, δημιουργήθηκε ένα κλήμα εκφοβισμού τους χρήστες του Internet για τη μελλοντική χρήση τέτοιων υπηρεσιών. Αλλά αυτό το συναίσθημα γρήγορα ξεπεράστηκε.

Η εταιρία Sharman Networks δημιούργησε ένα πρόγραμμα, το Kazaa που ερχόταν να ταράξει και πάλι τα νερά στο θέμα του peer-to-peer file sharing. Η λογική ήταν παρόμοια με αυτήν του Napster, αλλά υπήρχαν πολλές διαφορές στην αρχιτεκτονική(βλ. Εικόνα 2). Δεν υπήρχε η έννοια των κεντρικών servers και ο διαμοιρασμός των αρχείων γίνονταν από χρήστη σε χρήστη. Επίσης μια σημαντική διαφορά είναι ότι τα αρχεία τεμαχίζονταν σε τμήματα και κυκλοφορούσαν από τον έναν ηλεκτρονικό υπολογιστή στον άλλον. Ο κάθε χρήστης μπορούσε να κατεβάζει αρχεία στο υπολογιστή του αλλά δεν υποχρεούταν να μοιραστεί τα δικά του.

Το γεγονός ότι το Kazaa δεν διατηρούσε servers δικού του που να περιέχουν copyrighted υλικό, το έκανε αυτομάτως ανθεκτικό στις μηνύσεις που είχαν γίνει στο Napster. Η δικαιολογία ήταν λογική και σαφής : «Δεν είναι το Kazaa υπεύθυνο για τη παράνομη διακίνηση copyrighted υλικού, εφόσον δεν είναι αυτό που τα κατέχει και τα διακινεί.». Δεν ήταν εύκολο λοιπόν να σταματήσουν μια τέτοια υπηρεσία και πόσο μάλλον να αρχίσουν να διώκουν ποινικά τους εκατομμύρια χρήστες της υπηρεσίας.



Αρχιτεκτονική που χρησιμοποιεί το Kazaa

Εικόνα 2

Το Kazaa δεν ήταν το μόνο εγχείρημα μιας τέτοιας λογικής. Δεκάδες υπηρεσίες τέτοιου τύπου υπάρχουν αυτή τη στιγμή στο Internet και οι πιο γνωστές είναι :

- Gnutella
- LimeWire
- Morpheus
- eMule

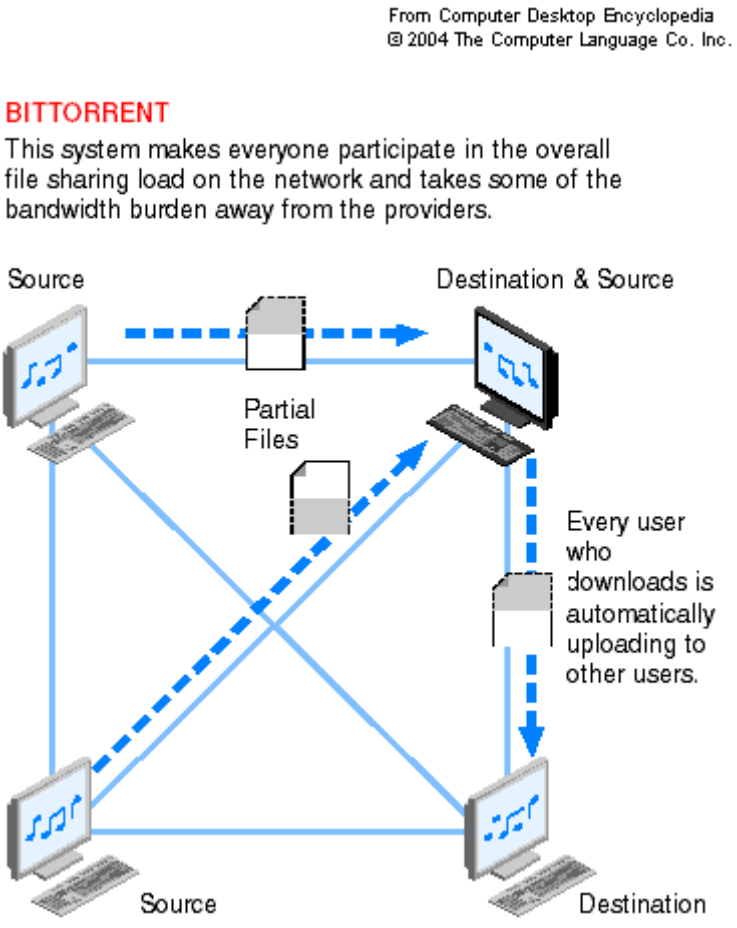
1.3 Torrents – Η σημερινή πραγματικότητα

Την επιτυχία των υπηρεσιών τύπου Kazaa δεν μπορούσαν εύκολα να την εμποδίσουν. Όμως, υπήρχε ένα μικρό πρόβλημα που προέκυπτε μέσα από την αρχιτεκτονική που χρησιμοποιούνταν.

Οι χρήστες επειδή δεν ήταν αναγκασμένοι να μοιράζονται τα δικά τους αρχεία δεν συνέβαλαν εξίσου στον διαμοιρασμό, αλλά μόνο επωφελούνταν από το υλικό των άλλων. Αυτό, δεν ήταν γενικό φαινόμενο και ουσιαστικό πρόβλημα ποτέ δεν υπήρχε. Όμως, έπρεπε κάπως να διασφαλιστεί η δίκαιη μοιρασιά και να μπορούσε ο κάθε χρήστης να «παίρνει» αν και μόνο αν «δίνει». Το κενό αυτό ήρθαν να το

καλύψουν τα torrents προγράμματα, τα οποία είναι ουσιαστικά κτισμένα πάνω στην λογική του διαμοιρασμού κομματιασμένων αρχείων από χρήστες σε άλλους χρήστες. Η μόνη διαφορά είναι ότι όσο κατεβάζεις ένα αρχείο συνεισφέρεις ταυτόχρονα στο διαμοιρασμού αυτού με άλλους χρήστες(βλ. Εικόνα 3). Στην ουσία κάνεις upload δεδομένα.
Βέβαια, υπήρχε και ένας άλλος λόγος που δημιουργήθηκαν τέτοια προγράμματα.
Η διακίνηση τεράστιου όγκου αρχείων δημιούργησε ένα κατανεμημένο σύστημα χρηστών που συμμετείχαν όλοι μαζί για ταχύτερη διακίνηση.

Την αρχή την έκανε το bitTorrent, αλλά ακολούθησαν και άλλα προγράμματα όπως το Azureus, το μTorrent, το Torrent Harvester κ.α.
Επίσης, υπάρχουν και sites που αποτελούν μηχανές αναζήτησης για torrent αρχεία. Χαρακτηριστικά παραδείγματα είναι το mininova, το isohunt κ.α.



Αρχιτεκτονική Torrent

Εικόνα 3

1.4 RapidShare

Το Rapidshare είναι ένα *one-click hosting* site που ξεκίνησε από την Γερμανία και έχει ως κύρια εισροή εσόδων τις συνδρομές από τους χρήστες.
Με τον όρο *one-click hosting* εννοούμε μια web υπηρεσία που επιτρέπει σε κάθε χρήστη να κάνει upload αρχεία μέχρι 100MB σε έναν ιδιωτικό server.
Στη συνέχεια το σύστημα επιστρέφει στον χρήστη ένα μοναδικό link
(παρ. hxxp://www.rapidshare.de/12345678/myfile.rar) και μέσω αυτού μπορεί κάθε χρήστης να κατεβάζει στον προσωπικό του υπολογιστή το αρχείο που θέλει.

Το όλο εγχείρημα πλαισιώνεται από κάποιους κανόνες που διαφέρουν για τα διάφορα είδη χρηστών. Υπάρχουν οι χρήστες που έχουν συνδρομή στην υπηρεσία και οι free χρήστες που δεν διαθέτουν account επί πληρωμής.

Οι free users έχουν το δικαίωμα να κατεβάζουν αρχεία συνολικού μεγέθους 100MB αλλά για τα επόμενα Bytes πρέπει να περιμένουν το ελάχιστο για 2 ώρες. Βέβαια, αυτός ο περιορισμός προσπερνιέται εύκολα με την αλλαγή της IP διεύθυνσης του χρήστη εφόσον το πρόγραμμα διαθέτει έλεγχο με βάση αυτήν.

Οι account users έχουν περισσότερα προνόμια όπως το απεριόριστο downloading αρχείων, την αποφυγή μποτιλιαρισμάτων στο δίκτυο και την επιλογή να διακόπτουν το κατέβασμα ενός αρχείου και την συνέχισή του αργότερα.

Όπως προαναφέραμε, το Rapidshare ξεκίνησε από την Γερμανία με domain name rapidshare.de. Γρήγορα όμως, και συγκεκριμένα τον Οκτώβριο του 2006 οι δίσκοι των servers του rapidshare.de γέμισαν με υλικό και ξεκίνησε μια προσπάθεια για την δημιουργία του rapidshare.com που σήμερα αποτελεί αναπόσπαστο κομμάτι της συνολικής επιχείρησης.

1.4.1 Η χαμένη «αγνότητα» του RapidShare

Το **Rapidshare** έφερε την επανάσταση στο χώρο του web hosting σε επίπεδο προσωπικών δεδομένων, αλλά η χρήση του ήταν ένα τεράστιο σκαλοπάτι για την καθημερινή διάπραξη εγκλημάτων στον τομέα της παράνομης διάδοσης copyright υλικού.
Υπάρχουν άπειρα παράνομα ανεβασμένα αρχεία από χρήστες της υπηρεσίας και η υπόθεση όσο πάει και καλύπτει όλες τις γωνιές του πλανήτη στις οποίες είναι διαδεδομένο το διαδίκτυο.
Εταιρίες παραγωγής ταινιών, μουσικής, προγραμμάτων και άλλων κλάδων προσπαθούν και πιέζουν κυβερνήσεις και αρμόδιους φορείς για να μπει ένα τέλος σε αυτού του είδους τις υπηρεσίες. Σύμφωνα με οικονομικές μελέτες τα λεφτά που χάνονται είναι της τάξεως των δισεκατομμυρίων ευρώ παγκοσμίως και υπάρχει μια άκαρπη, μέχρις στιγμής, κινητικότητα για την πάταξη τέτοιων εγκλημάτων και την απόδοση ευθυνών και κατηγοριών σε οποιονδήποτε υπεύθυνο.

Η προσπάθεια πάταξης συγκλίνει στην εύρεση των επίμαχων servers και στην καταστροφή των τελευταίων μετά από έλεγχο. Υπάρχουν συνέχεια αναφορές για κατεβάσματα διακομιστών που συντελούσαν στην υπηρεσία του Rapidshare, αλλά η συνολική προσπάθεια χαρακτηρίζεται ως αποτυχημένη, διότι η ανάπτυξη που υπάρχει σε τέτοιου είδους υπηρεσίες είναι ραγδαία και οι κοινότητες που τις υποστηρίζουν αποτελούνται από εκατομμύρια ανθρώπους.
Για του λόγου το αληθές, έχουν παρατηρηθεί servers του Rapidshare σε αρκετές χώρες του πλανήτη, ακόμα και σε μη-ανεπτυγμένες.
Είναι αρκετά δύσκολο να περιοριστεί αυτή η κατάσταση και, με τα τωρινά δεδομένα, ακατόρθωτο να σταματήσει τελείως.

1.5 YouTube

Το YouTube είναι το πιο δημοφιλές video sharing site αυτή τη στιγμή. Δημιουργήθηκε το 2005 από τρεις υπαλλήλους του PayPal με σκοπό να προσφέρει τη δυνατότητα στους χρήστες να ανεβάζουν στο internet videos τα οποία θα είναι διαθέσιμα προς παρακολούθηση από όλους.

Το YouTube χρησιμοποίησε την τεχνολογία του Adobe Flash για να προβάλει τα videos και από την πρώτη κιόλας στιγμή γνώρισε τεράστια επιτυχία η οποία οδήγησε στην αγορά της υπηρεσίας από την Google ένα χρόνο μετά έναντι του ποσού των 1,65€ δισεκατομμυρίων.

Όμως, οι υπεύθυνοι γύρω από αυτήν την υπηρεσία δεν έδωσαν την απαραίτητη προσοχή σε θέματα καταπάτησης πνευματικής ιδιοκτησίας και αρκέστηκαν στη συμπλήρωση κάποιων κανόνων χρήσης για αυτούς που απλά επισκέπτονται το site και για όσους ανεβάζουν videos στους servers της υπηρεσίας.

Οι κανόνες αυτοί απλώς προτρέπουν τους χρήστες κυρίως να μην ανεβάζουν videos που είναι copyrighted όπως video clips, σήριαλ κ.α. Συγκεκριμένα αναφέρει :

«***Copyright Notice: Do not upload copyrighted material for which you don't own the rights or have permission from the owner***.»

Παρά την παρουσία τέτοιων κανόνων, πολλοί χρήστες εκμεταλλεύονται την απουσία κατάλληλων αλγορίθμων που θα απαγορεύουν το ανέβασμα copyrighted υλικού και έχουν στείλει στους servers της υπηρεσίας χιλιάδες τέτοια videos. Βέβαια, πολλά από αυτά αποσύρονται κατόπιν αιτημάτων από εταιρίες που έχουν τα πνευματικά δικαιώματα ή ακόμα κατόπιν μηνύσεων κατά της υπηρεσίας(παρ. Viacom).

Η αλήθεια είναι ότι η υπηρεσία θα βρίσκετε πάντα αντιμέτωπη με τον νόμο εφόσον διαθέτει στους servers της copyrighted υλικό και το διαμοιράζει. Όμως, παρανομία διαπράττει και ο χρήστης που ανεβάζει το υλικό αυτό στο διαδίκτυο χωρίς τη συγκατάθεση του κατόχου των δικαιωμάτων και μάλιστα διατηρώντας την ανωνυμία του. Για αυτό, το YouTube περιόρισε λίγο τις δυνατότητες του

«ανώνυμου» χρήστη θέτοντας το όριο των 10 λεπτών στα uploaded videos. Αν ο χρήστης θέλει να ανεβάσει video πάνω από 10 λεπτά πρέπει να αποκτήσει περισσότερα δικαιώματα ως χρήστης δίνοντας τα πραγματικά του στοιχεία και όχι μόνο ένα email και ένα username.

Πάντως, η χρήση κατάλληλων αλγορίθμων θα αποτρέψει πολλές τέτοιες ενέργειες και θα προστατέψει την ίδια την υπηρεσία από μελλοντικές ποινικές επιθέσεις.

Ενότητα 2η

ΔΙΑΔΙΚΤΥΑΚΗ ΗΘΙΚΗ

Κεφάλαιο 1ο

Ηθική και ηλεκτρονικοί υπολογιστές

1.1 Εισαγωγή

Η εμφάνιση του World Wide Web το 1990 έπαιξε καταλυτικό ρόλο στην επέκταση του Διαδικτύου, το οποίο αναπτύσσεται ακόμα και σήμερα με πρωτοφανή ποσοστά. Η πρόσφατη αύξηση του Διαδικτύου έχει οδηγήσει όχι μόνο στη δημιουργία και εξέλιξη μιας τεράστιας βάσης γνώσης, αλλά και στην εμφάνιση πολλών προβλημάτων που αφορούν τη χρήση, τη διανομή και τη συντήρηση της γνώσης αυτής. Με την πάροδο του χρόνου καθίσταται σαφές ότι οι παραδοσιακοί κανόνες της συμπεριφοράς δεν ισχύουν πάντα στο Διαδίκτυο και έτσι, γίνεται προσπάθεια να αναπτυχθούν νέοι ηθικοί κώδικες.

Η *ηθική*[1] *(ethics)*, υπό την κλασσική έννοια, αναφέρεται στους κανόνες και τα πρότυπα που διέπουν τη συμπεριφορά ενός ατόμου απέναντι σε άλλα. Δεδομένου ότι η τεχνολογία και οι υπολογιστές γίνονται όλο και περισσότερο μέρος της καθημερινότητάς μας, πρέπει να καταλάβουμε ότι μαζί με τα πλεονεκτήματα που προσφέρουν εισάγουν ανάγκη για προβληματισμό σε κάποια ηθικά ζητήματα. Με άλλα λόγια, με την εμφάνιση του World Wide Web, εξελίσσεται και ο καθορισμός της ηθικής. Έτσι, ένας νέος τύπος ηθικής γνωστός ως *ηθική υπολογιστών*[2] *(computer ethics)* έχει προκύψει. Η ηθική υπολογιστών εξετάζει τα πρότυπα της συμπεριφοράς δεδομένου ότι αναφέρονται στους υπολογιστές.

Τι οδήγησε στην εμφάνιση της Ηθικής Υπολογιστών;

- Η ραγδαία εξάπλωση του WWW δημιούργησε διάφορα καινοφανή θέματα νομιμότητας.
- Η νομοθεσία έπεται κατά πολύ της εξέλιξης του διαδικτύου σε θέματα επικοινωνίας μεταξύ των χρηστών.
- Οι αρχές αδυνατούν να εφαρμόσουν τις κυρώσεις όπως και να εξαρθρώσουν εγκληματικές ενέργειες.
- Εμφανίστηκε η ανάγκη τεκμηρίωσης μιας διαδικτυακής ηθικής για να συμπληρώσει, προσωρινά τουλάχιστον, αυτό το νομοθετικό κενό.

[1] ***Ηθική (ethics):*** *(1) Ο κλάδος της φιλοσοφίας που μελετά τη συμπεριφορά των ανθρώπων και τις πράξεις τους. (2) Δογματική διδασκαλία που προσδιορίζει τι είναι καλό και τι είναι κακό. [Υδρία Cambridge Ήλιος, Λεξικό της Ελληνικής Γλώσσας]*

[2] *Με τον όρο **ηθική υπολογιστών (computer ethics)** αναφερόμαστε στη φύση και το κοινωνικό αντίκτυπο της τεχνολογίας των Η/Υ, καθώς και στη σχετική διατύπωση και εδραίωση πολιτικών (policies) για την ορθή χρήση τέτοιων τεχνολογιών. [The Research Center on Computing & Society at Southern Connecticut State University]*

Αν και υπάρχουν αρκετά ζητήματα που σχετίζονται με την ηθική των υπολογιστών και κατ' επέκταση του διαδικτύου, τρεις είναι οι βασικές κατηγορίες τέτοιων ζητημάτων που χρήζουν άμεσης διευθέτησης.

- Προστασία Πνευματικών Δικαιωμάτων (Copyright)
- Απόρρητο & Προσωπικά Δεδομένα (Privacy)
- Λογοκρισία (Censorship)

1.2 Προστασία πνευματικών δικαιωμάτων

1.2.1. Ορολογία – Εισαγωγικά στοιχεία

Με τον όρο *προστασία πνευματικών δικαιωμάτων* αναφερόμαστε στη μορφή προστασίας (όπως προβλέπεται από τη νομοθεσία) της πνευματικής ιδιοκτησίας[3] των αυθεντικών δημιουργών. Αυτός ο όρος έχει γίνει πιο κοινός κατά τη διάρκεια των τελευταίων ετών, ειδικά στα πλαίσια της ηθικής υπολογιστών. Αλλά σε τι ακριβώς αναφέρεται;

Προτού ερευνήσουμε την απάντηση σε αυτήν την ερώτηση, πρέπει πρώτα να συζητήσουμε την ύπαρξη της οργάνωσης παγκόσμιας πνευματικής ιδιοκτησίας (WIPO[4]). Αυτή η οργάνωση ιδρύθηκε το 1967 ως μια από τις ειδικευμένες αντιπροσωπείες των οργανώσεων Ηνωμένων Εθνών, και έχει παραμείνει από τότε αρμόδια για την προστασία της πνευματικής ιδιοκτησίας.

Σύμφωνα λοιπόν με το κείμενο της συνθήκης που καθιερώνει τη WIPO ως την αρμόδια οργάνωση για θέματα πνευματικής ιδιοκτησίας, δηλώνεται ότι η πνευματική ιδιοκτησία αναφέρεται γενικά στα δικαιώματα σχετικά (μεταξύ άλλων) με:

- Λογοτεχνικές, καλλιτεχνικές, και επιστημονικές εργασίες.
- Αποδόσεις καλλιτεχνών εκτελέσεων, φωνογραφημάτων, και ραδιοφωνικών μεταδόσεων.
- Εφευρέσεις σε όλους τους τομείς της ανθρώπινης προσπάθειας.
- Επιστημονικές ανακαλύψεις.

Ο σκοπός επομένως της WIPO είναι αφενός η προστασία της πνευματικής ιδιοκτησίας (με τη βοήθεια της συνεργασίας μεταξύ των εθνών - μελών του) και αφετέρου ο καθορισμός των νομικών και διοικητικών πτυχών για να επιτευχθεί ο παραπάνω σκοπός.

---

[3] ***Πνευματική ιδιοκτησία:*** *Από γενικής απόψεως αναφέρεται σε δημιουργίες της ανθρώπινης διάνοιας.*

[4] Ακρωνύμιο του ***World Intellectual Property Organization***

Η διεθνής Συνθήκη της Βέρνης για την προστασία των λογοτεχνικών και καλλιτεχνικών εργασιών το 1971 καθόρισε ότι οι εργασίες που προστατεύονται κάτω από πνευματικά δικαιώματα περιλαμβάνουν:

- Λογοτεχνικό και καλλιτεχνικό έργο[5]
- Δραματικό και δραματικο-μουσικό έργο
- Χορογραφικό έργο
- Φωτογραφικό έργο
- Έργο που αφορά τις εφαρμοσμένες τέχνες.

ΣΗΜΕΙΩΣΗ: Η προστασία πνευματικών δικαιωμάτων επεκτείνεται *στην έκφραση* και όχι *στις ιδέες, τις διαδικασίες,* ή *τις μεθόδους διαδικασιών* (όπως δηλώνεται στη Συνθήκη πνευματικών δικαιωμάτων WIPO του 1996).

1.2.2. Πνευματικά δικαιώματα & Ηλεκτρονικοί υπολογιστές

Όπως αναφέρθηκε παραπάνω ο συγγραφέας ενός λογοτεχνικού βιβλίου προστατεύεται από τον νόμο σε περίπτωση που, παραδείγματος χάριν, δημιουργηθούν παράνομα αντίγραφα του βιβλίου του ή μέρους αυτού χωρίς την άδειά του.

Συμβαίνει κάτι παρόμοιο με το λογισμικό που δημιουργείται για ηλεκτρονικούς υπολογιστές; Η απάντηση είναι ναι. Το λογισμικό, σύμφωνα με τη Συνθήκη πνευματικών δικαιωμάτων WIPO, προστατεύονται ακριβώς όπως τα λογοτεχνικά έργα προστατεύονται σύμφωνα με το άρθρο 2 της Συνθήκης της Βέρνης για την προστασία των καλλιτεχνικών και λογοτεχνικών έργων. Αυτό σημαίνει ότι τα προνόμια πνευματικών δικαιωμάτων που οι λογοτεχνικές και καλλιτεχνικές εργασίες απολαμβάνουν επεκτείνονται και στα προγράμματα υπολογιστών. Επομένως, μόνο ο ιδιοκτήτης των πνευματικών δικαιωμάτων απολαμβάνει το δικαίωμα να εγκρίνει την παραγωγή αντιγράφων του εν λόγω έργου.

Το ίδιο ισχύει για τα παιχνίδια υπολογιστών. Ο αμερικάνικος νόμος περί πνευματικών δικαιωμάτων δηλώνει ότι αν και η *ιδέα* για ένα παιχνίδι δεν προστατεύεται από πνευματική ιδιοκτησία, ο τρόπος της έκφρασης του συντάκτη (από καλλιτεχνικής, λογοτεχνικής ή μουσικής άποψης) είναι. Επομένως, είναι παράνομο να διανεμηθούν τα αντίγραφα των παιχνιδιών υπολογιστών χωρίς τη ρητή άδεια του ιδιοκτήτη.

Όσον αφορά τα έργα που δημοσιεύονται στο διαδίκτυο προστατεύονται και αυτά από πνευματικά δικαιώματα εφόσον ο δημιουργός θέλει να διεκδικήσει βέβαια πνευματική ιδιοκτησία. Όπως όμως και με τα παιχνίδια υπολογιστών η προστασία αυτή των πνευματικών δικαιωμάτων δεν περιλαμβάνει *τις ιδέες, τις διαδικασίες, τα συστήματα* ή *τις μεθόδους λειτουργίας*. Αυτό σημαίνει ότι το γεγονός ότι κάποιος

[5] Περιλαμβάνει κάθε δημιουργία του λογοτεχνικού, επιστημονικού και καλλιτεχνικού χώρου (ανεξαρτήτως του τρόπου έκφρασης).

δημοσίευσε ένα έργο στο διαδίκτυο δεν αποτρέπει κάποιον άλλο από το να αναπτύξει κάποιο άλλο έργο βασισμένο σε παρόμοιες αρχές ή ιδέες. Χαρακτηριστικό παράδειγμα, μετά την εμφάνιση των Web 2.0 υπηρεσιών στο διαδίκτυο, αποτέλεσαν τα video sharing / streaming sites. Η αρχή έγινε με το YouTube.com και ακολούθησε πλειάδα κλώνων.

1.2.3. Επίλογος

Είναι αλήθεια ότι σήμερα πολλά από τα ζητήματα ηθικής υπολογιστών και κατ' επέκταση του διαδικτύου έχουν να κάνουν με ζητήματα πνευματικής ιδιοκτησίας και δικαιωμάτων. Είναι σαφές ότι η αντιγραφή ορίζεται ως η χρήση της πνευματικής ιδιοκτησίας κάποιου άλλου και επομένως θεωρείται παράνομη.

Είναι καλό επομένως να γνωρίζουμε πότε η πνευματική ιδιοκτησία ενός έργου ανήκει σε εμάς και πότε σε κάποιον άλλο. Οι παρακάτω κανόνες (αν και γενικοί)επιλύουν, ως ένα βαθμό, αυτόν τον προβληματισμό:

- Εάν παραγάγατε την εργασία οι ίδιοι, κατόπιν είστε ο φυσικός συντάκτης και είστε κύριος των πνευματικών δικαιωμάτων οι ίδιοι.
- Εάν ως υπάλληλος δημιουργήσατε την εργασία στο πεδίο της απασχόλησης, ο εργοδότης σας είναι κύριος των πνευματικών δικαιωμάτων και θεωρείται στην πραγματικότητα συντάκτης.

Ο αμερικάνικος νόμος περί πνευματικών δικαιωμάτων παρέχει έναν πιο αναλυτικό κατάλογο κανόνων που σχετίζονται με την ιδιοκτησία των πνευματικών δικαιωμάτων. Μελετώντας τον προκύπτουν αρκετοί προβληματισμοί σχετικά με τα ζητήματα ιδιοκτησίας μερικοί από τους οποίους φαίνονται παρακάτω:

- Ποιος είναι ο φυσικός συντάκτης; Ποιος παρήγαγε την εργασία;
- Είναι η δημιουργία μια εργασία για τον υπάλληλό του/της;
- Είναι η δημιουργία μια εργασία για τον/την ως ειδικά ανατεθειμένη εργασία;
- Είναι το πρόσωπο κοινός συντάκτης της εργασίας;
- Το πρόσωπο έχει λάβει μια έγκυρη άδεια για να χρησιμοποιήσει η εργασία;
- Είναι τα δικαιώματα ότι το πρόσωπο έχει λάβει αναγνωρίσιμος και εκτελέσιμος βάσει του τρέχοντος νόμου;

Βλέπουμε λοιπόν ότι το να καθοριστούν αυστηρά οι κανόνες που διέπουν και προστατεύουν την πνευματική ιδιοκτησία είναι κάτι δύσκολο. Ακόμη και σήμερα τα δικαστήρια δεν έχουν καταφέρει να διευκρινίσουν πλήρως την σχέση μεταξύ των νόμων πνευματικών δικαιωμάτων και υπολογιστών. Ιδιαίτερα μετά την εμφάνιση και εξάπλωση του World Wide Web η παραπάνω διαδικασία έγινε ακόμη πιο ανέφικτη. Οι χρήστες του διαδικτύου θα πρέπει να περιμένουν αρκετά ακόμη μέχρι την ρητή σύνταξη νομοθεσίας για την προστασία της πνευματικής ιδιοκτησίας, οπότε μέχρι τότε, οι δημιουργεί μπορούν να ελπίζουν στην καλλιέργεια αισθήματος διαδικτυακής ηθικής από την κοινότητα των χρηστών του Διαδικτύου.

1.3 Απόρρητο & Προσωπικά Δεδομένα (Privacy)

1.3.1. Εισαγωγικά στοιχεία

Ακόμη και στην καθημερινή μας ζωή έχουμε το δικαίωμα από το νόμο να προστατεύουμε τα προσωπικά μας δεδομένα από υποκλοπή ή χρήση τους από τρίτους οι οποίοι δεν είναι εξουσιοδοτημένοι από εμάς. Επομένως έχουμε το δικαίωμα να απαιτούμε να μην υποκλέπτονται οι τηλεφωνικές μας επικοινωνίες, να μη γίνεται χρήση για διαφημιστικούς σκοπούς των προσωπικά στοιχείων που αφήνουμε για να κάνουμε μια αγορά ή όταν εγγραφόμαστε σε μια υπηρεσία κ.ο.κ.

Το Διαδίκτυο, που αποτελεί όπως λέγεται μικρογραφία του πραγματικού κόσμου, περιέχει παρόμοιους κινδύνους «ανήθικης» χρήσης των προσωπικών μας δεδομένων.

1.3.2. Cookies

Ένα cookie είναι ένα κομμάτι πληροφορίας όπου μια ιστοσελίδα συλλέγει από τους χρήστες που την επισκέπτονται. Η πληροφορία μπορεί να διαφέρει ανάλογα με το είδος της ιστοσελίδας (π.χ. ένα site διαφημίσεων συλλέγει συνήθως δημογραφικά στοιχεία όπως όνομα, φύλλο, ηλικία και όποια άλλη πληροφορία μπορεί να χρησιμοποιηθεί για διαφημιστικούς σκοπούς ενώ μια υπηρεσία ηλεκτρονικού ταχυδρομείου συλλέγει συνήθως αναγνωριστικά ή προσωπικά στοιχεία όπως όνομα, διεύθυνση κατοικίας, κλπ.). Οι πληροφορίες που κρατούν αυτά τα cookies αποστέλλονται στον server.

1.3.3. Πτυχές online απορρήτου

Η προστασία των προσωπικών μας δεδομένων όσο βρισκόμαστε online πρέπει να μελετηθεί σε δύο επίπεδα. Το πρώτο αφορά την προστασία μας ως άτομα από παρενόχληση ή και πολλές φορές απειλές από τρίτους που φέρονται να γνωρίζουν πώς να μας εντοπίσουν. Στην Αμερική υπήρχαν τέτοια κρούσματα εκβιασμού μέσω διαδικτύου εκφοβίζοντας κάποιους χρήστες για να επωφεληθούν. Σε ένα δεύτερο επίπεδο αφορά την προστασία των δεδομένων μας (αρχεία, λειτουργικό σύστημα, κλπ.). Επομένως σε αυτήν την δεύτερη περίπτωση δεν υπάρχει κίνδυνος σωματικής ή φυσικής με την γενικότερη έννοια βλάβης αλλά περισσότερο οικονομικής.

Αξίζει να σημειώσουμε σε αυτό το σημείο ότι υπάρχουν τρεις πολιτικές απορρήτου που ακολουθούνται από τους διαχειριστές υπηρεσιών διαδικτύου:

- Complete Privacy: Οι διαχειριστές συμφωνούν ότι δεν θα έχουν πρόσβαση σε κανενός είδους προσωπικό στοιχείο δηλαδή δεν θα κάποιο e-mail ή θα παρακολουθούν τις κινήσεις σου στο Διαδίκτυο. Αυτή η πολιτική συνήθως προσδίδει ένα μειονέκτημα στο έργο του διαχειριστή.

- Almost Complete Privacy: Οι διαχειριστές έχουν το δικαίωμα να ερευνήσουν στα email ή στις συνομιλίες (chat) κάποιου χρήστη αν υποπτευθούν παράνομη δραστηριότητα.
- No Privacy: Οι διαχειριστές έχουν το δικαίωμα να ερευνούν κάθε email που στέλνει ο χρήστης ανεξαρτήτου θέματος (άσχετα π.χ. με το αν το email φαίνεται να έχει επαγγελματικό ή εξαιρετικά προσωπικό χαρακτήρα).

1.3.4. Προστασία προσωπικών δεδομένων

Η προστασία των προσωπικών δεδομένων μας στο Διαδίκτυο επιτυγχάνεται συνήθως με τη χρήση αλγορίθμων κρυπτογράφησης. Έτσι έχει επικρατήσει οι διάφορες υπηρεσίες να χρησιμοποιούν τέτοιους αλγορίθμους οπότε λειτουργεί η ακόλουθη λογική: Ο αποστολέας στέλνει την πληροφορία η οποία κρυπτογραφείται πριν φύγει για τον παραλήπτη. Ο παραλήπτης λαμβάνει την πληροφορία αφού πρώτα αποκρυπτογραφηθεί και βλέπει το μήνυμα. Αν κάποιος υποκλέψει την πληροφορία στην πορεία είναι δύσκολο έως αδύνατο να δει την πληροφορία αν δεν κατέχει το κλειδί αποκρυπτογράφησης. Επανάσταση στους αλγορίθμους κρυπτογράφησης έφερε η εμφάνιση της RSA κρυπτογράφησης.

1.3.5. Οδηγίες για εξασφάλιση του απορρήτου

- Εκμεταλλευθείτε την ανωνυμία. Είναι καλύτερο να εμφανίζουμε ένα όνομα χρήστη που αποκρύπτει το φύλο και την ηλικία μας (π.χ. footballfan) παρά το αντίθετο.

- Συνηθίστε να χρησιμοποιείται διαφορετικές διευθύνσεις e-mail. Μπορείτε να χρησιμοποιείτε μία για επαγγελματικούς σκοπούς, μία για προσωπικό e-mail και ενδεχομένως μια τρίτη διεύθυνση για να την δηλώνεται σε sites που σας ζητούν κάποιο e-mail για επιβεβαίωση. Ακόμη ανάλογα με την χρήση για την οποία προορίζεται η εκάστοτε διεύθυνση θα πρέπει να διαφέρει και το ποσοστό αλήθειας των στοιχείων που τη συνοδεύουν.

- Είναι καλό να αποφεύγετε να συναντάτε κάποιον που έχετε γνωρίσει online προσωπικά ή αν πρόκειται να γίνει κάτι τέτοιο είναι καλό η συνάντηση να γίνει σε κάποιον δημόσιο χώρο και αφότου έχετε ενημερώσει οικογένεια ή φίλους. Είναι πολύ πιθανό το άτομο που θα συναντήστε να έχει δώσει ψευδή στοιχεία και να διαφέρει πολύ από αυτό που σας έχει δώσει να καταλάβετε ότι είναι.

- Διαβάστε την πολιτική απορρήτου ενός ιστοχώρου πριν στείλετε προσωπικά στοιχεία. Να θυμάστε ότι πολλοί ιστοχώροι πωλούν τις πληροφορίες αυτές σε διαφημιστικές υπηρεσίες.

1.4. Λογοκρισία (Censorship)

1.4.1. Εισαγωγικά στοιχεία

Πολλά από τα πράγματα που διατίθενται στο διαδίκτυο παγκοσμίως εμπίπτουν στην κατηγορία του ακατάλληλου ή άσεμνου υλικού. Έχει εκφρασθεί η άποψη ότι τέτοιου είδους υλικό θα πρέπει να λογοκρίνεται.

Η παρεμπόδιση ωστόσο ή η αλλοίωση προσωπικών απόψεων έρχεται σε αντίθεση με την ιδέα της ελευθερίας της έκφρασης και της διακίνησης ιδεών (όσον αφορά την Αμερική ελάχιστα πράγματα λογοκρίνονται λόγω άρθρου που περιλαμβάνεται στο σύνταγμα μετά την πρώτη τροποποίηση).

Είναι προφανές ότι οποιοσδήποτε νόμος και αν θεσπιστεί που να επιτρέπει νόμιμα λογοκρισία υλικού ή έργου που πρόκειται να δημοσιευθεί στο Διαδίκτυο θα πρέπει να μην αντιβαίνει με την ιδέα τις ελεύθερης διακίνησης ιδεών και επομένως για άλλη μια φορά ζητήματα λογοκρισίας πρέπει να εξετασθούν περισσότερο από την σκοπιά της διαδικτυακής ηθικής και όχι από αυτήν την νομοθεσίας.

1.4.2. Η λογοκρισία στο Διαδίκτυο

Οι περιπτώσεις λογοκρισίας στην ομιλία, το έντυπο υλικό και τη ραδιοφωνική αναμετάδοση έχουν εξεταστεί σε βάθος και πλέον είναι άριστα τεκμηριωμένα (π.χ. περίπτωση Larry Flynt). Λίγο πολύ τα ζητήματα λογοκρισίας που σχετίζονται με το διαδίκτυο είναι παρόμοια απλώς δεν έχει υπάρξει ουσιώδης κουβέντα και μέριμνα για αυτά. Οι προσπάθειες που γίνονται κατά καιρούς δεν αποδίδουν καρπούς γιατί είτε τα συμβούλια που αναλαμβάνουν να συζητήσουν τα συγκεκριμένα θέματα δεν είναι κατάλληλα καταρτισμένα, είτε γιατί στις συζητήσεις δεν λαμβάνονται υπόψη οι προτάσεις της ίδιας της διαδικτυακής κοινότητας.

Θα μπορούσαμε να πούμε ότι στο Διαδίκτυο μπορεί κανείς να βρει μια εκδοχή «του καλού, του κακού και του άσχημου», μπορεί δηλαδή κανείς να συναντήσει τόσο πληροφορίες ωφέλιμες όσο και προσβλητικές ή ακόμη επικίνδυνες. Η εξάπλωση του Διαδικτύου έχει οδηγήσει στην γρήγορη και εύκολη επικοινωνία των ανθρώπων ανεξαρτήτου τόπου διαμονής ή πρόσβαση σε ιατρικά δεδομένα και πληροφορίες αλλά παράλληλα κρύβει και αρκετούς κινδύνους (π.χ. οδηγίες για δημιουργία home made εκρηκτικών στις οποίες μπορεί να έχει πρόσβαση ένας ανήλικος).

Κατά καιρούς πολλές προσπάθειες έχουν γίνει για λογοκρισία ακατάλληλου ή άσεμνου περιεχομένου αλλά απέβησαν άκαρπες. Χαρακτηριστικές ήταν οι κινήσεις της American OnLine (AOL), δημοφιλούς φορέα παροχής υπηρεσιών Internet. Η συγκεκριμένη επιχείρηση προσπάθησε να ελέγξει το περιεχόμενο των συζητήσεων που εμφανίζονταν στα bulletin boards και forums της δημιουργώντας μια λίστα απαγορευμένων λέξεων οι οποίες όταν περιέχονταν σε κάποιο κείμενο ή σχόλιο το τελευταίο διαγράφονταν (δηλαδή λογοκρίνονταν). Όπως ήταν αναμενόμενο η συγκεκριμένη προσπάθεια ναυάγησε αφού διαγράφονταν και μηνύματα που δεν είχαν άσεμνο ή υβριστικό κείμενο. Χαρακτηριστικό παράδειγμα τα κείμενα που

δημοσιεύονταν σε ένα forum σχετικό με τον καρκίνο του μαστού διαγράφονταν αφού η λέξη «στήθος» περιλαμβάνονταν στην μαύρη λίστα.

Πέραν των προσπαθειών της AOL να κάνει κάτι για το άσεμνο υλικό που εμφανίζεται στο διαδίκτυο, το 1995 το Κογκρέσο ψήφισε το Communications Decency Act (CDA) που προσπαθούσε να επιβάλει ποινικές ρήτρες σε εκείνους που δημοσίευαν άσεμνες σελίδες στο διαδίκτυο. Αυτή η κίνηση έφερε πολλές αντιδράσεις κυρίως από τον οργανισμό Center for Democracy and Technology (CDT). Αργότερα εμφανίστηκε και το κίνημα Blue Ribbon Campaign[6] όπου οι σελίδες που συμμετείχαν ήταν σε μαύρο φόντο και είχαν σαν logo την γαλάζια κορδέλα.

1.4.3. Επίλογος

Παρόλες τις προσπάθειες για επιβολή λογοκρισίας μέσω της νομοθεσίας ή μέσω χειρισμών από τις ίδιες εταιρίες παροχής υπηρεσιών Internet, κανένα μέτρο δεν φάνηκε να λειτουργεί, για την ακρίβεια ούτε καν να μετριάζει το πρόβλημα. Αντίθετα έφερε στην επιφάνεια άλλου είδους δυσλειτουργίες ή και λογοκρισία υλικού που τελικά δεν θα έπρεπε να λογοκριθεί.

Οι πολέμιοι της CDA και βασικά το Center for Democracy and Technology πρότεινε, να μετατεθεί η ευθύνη για την λογοκρισία του ακατάλληλου για παιδιά υλικού στην ίδια την οικογένεια με προγράμματα ή υπηρεσίες που φιλτράρουν και απαγορεύουν την πρόσβαση σε site ακατάλληλου περιεχομένου σε παιδιά. Παράδειγμα τέτοιας υπηρεσίας αποτέλεσε το NetNanny.

[6] http://www.eff.org/br/

Βιβλιογραφία και Πηγές

PHISING - PHARMING

Phishing: Cutting the Identity Theft Line (By Rachael Lininger, Russell Dean Vines, Published 2005 Wiley Pub.)

The Pharming Guide – Understanding & Preventing DNS-related Attacks by Phishers (By Gunter Ollmann, NGS)

Internet Domain Names and Intellectual Property Rights (By United States Congress. House. Committee on the Judiciary. Subcommittee on Courts and Intellectual Property)

VIRUSES

http://www.pandasoftware.com/virus_info/about_virus/keys2.htm

http://www.sophos.com/pressoffice/imggallery/

http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/viruses.html

http://www.rbs2.com/cvirus.htm

http://www.globalscams.com/php/showScams.php?linkid=4&PHPSESSID=2f9fed

http://www.exportmichigan.com/itf_internet_fraud.htm

http://www.tulane.edu/~dmsander/Big_Virology/BVVirusList.html

EMPLOYEE THEFT

http://www.njlawblog.com/2004/10/articles/corporate-investigations-white-collar/employee-theft/

http://www.missouribusiness.net/docs/problem_employee_theft.asp

CREDIT CARDS

http://www.bestfrauds.com/

http://www.faughnan.com/ccfraud.html

http://www.scambusters.org/CreditCardFraud.html

http://home.insightbb.com/~rtrader977/fraud.html

http://www.itfacts.biz/index.php?id=P6441

INTERNET ETHICS

Ethics and the Internet (By Anton Vedder, Published 2001 Intersentia)

LAW

Internet and Online Law (By Kent D. StuckeyPublished 1996, Law Journal Press)

http://www.lawguru.com/ilawlib/ (The Internet Law Library)

http://www.lawnet.gr/

http://www.lancs.ac.uk/iss/rules/cmisuse.htm (LANCASTER UNIVERSITY)

DENIAL OF SERVICE

http://en.wikipedia.org/wiki/Denial_of_service

ΓΕΝΙΚΕΣ ΠΗΓΕΣ

http://www.ydt.gr/main/Article.jsp?ArticleID=83890 (ΥΠΟΥΡΓΕΙΟ ΔΗΜΟΣΙΑΣ ΤΑΞΗΣ)

http://www.e-crimecongress.org/ecrime2007/website.asp (E-CONGRESS)